

26

SPRING ISSUE

published by the
Joint Aircraft
Survivability
Program Office

AIRCRAFT SURVIVABILITY

CYBER SURVIVABILITY ANALYSIS



UAS Cyber Modeling:
Assessing Operational
Consequence Before and
During Drone Design

page 9

Simulated Digital Shrapnel:
Using Mission-Level
M&S to Quantify Cyber
Survivability in Full-
Spectrum Environments

page 15

Excellence in Survivability:
William "Data" Bryant

page 22

The Army Aviation Cyber
Incident Response Team:
What Do We Do After a
Cyber Attack?

page 25



Aircraft Survivability is published three times a year by the Joint Aircraft Survivability Program Office (JASPO), chartered by the U.S. Army Aviation & Missile Command, U.S. Air Force Life Cycle Management Center, and U.S. Navy Naval Air Systems Command.



JAS Program Office
701 S. Courthouse Road
Building 15, Suite 1G140
Arlington, VA 22204-2489
<http://jasp-online.org/>

Sponsor
Dennis Lindell

The views and opinions expressed in this journal are those of the authors and should not be construed as official positions of the U.S. Government or its agencies. Reader views and comments may be directed to JASPO.

On the cover:
ChatGPT-generated image

TABLE OF CONTENTS

4 FROM THE DIRECTOR'S DESK

by Dennis Lindell

5 NEWS NOTES

Compiled by Eric Edwards

7 JCAT CORNER

by CW3 Kyle Scharnhorst in collaboration with CW4 Franco Lopez and CW5 Cesar Urquiza

9 UAS CYBER MODELING: ASSESSING OPERATIONAL CONSEQUENCE BEFORE AND DURING DRONE DESIGN

by Charles Fisher and Arturo Revilla

Unmanned aircraft systems (UAS) have become a growing commodity on the battlefield. The recent conflicts in Ukraine and Gaza have particularly underscored their operational value and increased use in the planning, execution, and assessment of military operations and have demonstrated that these systems can significantly reduce costs and limit risk to personnel. Accordingly, the U.S. Department of War is taking actions to meet Administration-set "drone dominance" goals and has appropriated a budget estimated at \$1 billion. The Department is also pushing for more commercial solutions across the Services in an effort to speed up acquisitions and provide the Warfighter with much needed technologies that provide an upper hand in modern military engagements.

15 SIMULATED DIGITAL SHRAPNEL: USING MISSION-LEVEL M&S TO QUANTIFY CYBER SURVIVABILITY IN FULL-SPECTRUM ENVIRONMENTS

by William "Data" Bryant

Modern warfighting environments are increasingly complex and characterized by a convergence of kinetic and nonkinetic threats that challenge the survivability of aircraft and weapon systems across multiple domains. To help address this challenge, Congress mandated in the 2022 National Defense Authorization Act that the Department of Defense (DoD) expand survivability and lethality testing to include evaluation against a range of threats, including kinetic; cyber; electromagnetic spectrum (EMS); directed energy (DE); and chemical, biological, radiological, and nuclear (CBRN) effects. The Act also defined full-spectrum survivability as "a series of assessments of the effects of kinetic and nonkinetic threats on the communications, firepower, mobility, catastrophic survivability, and lethality of a covered system."

22 EXCELLENCE IN SURVIVABILITY: WILLIAM “DATA” BRYANT

by Eric Edwards

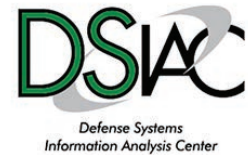
Fighter pilot, academic, aerospace engineer, military planner, strategy leader, risk analyst, methodology and model developer, author, speaker, and cyber survivability pioneer—the survivability community is fortunate to include each of these titles among its membership rolls. Rarely, however, do they all belong to the same person. But then there’s Dr. William Bryant. For more than 3 decades, Dr. Bryant—who is better known as “Data,” his former call-sign—has been supporting U.S. combat aviation mission effectiveness and weapon system survivability efforts with a unique toolset of operational experience, analytical acumen, innovative thinking, and collaborative information-sharing that has helped both planners and technologists better understand, prepare for, and excel in the ever-changing modern battlespace.

25 THE ARMY AVIATION CYBER INCIDENT RESPONSE TEAM: WHAT DO WE DO AFTER A CYBER ATTACK?

by Tom Barnett

Cyber attacks are threats that target the combat system’s infrastructure with impacts realized at the mission level. While today’s military aircraft were built to be safe, airworthy, reliable, and survivable, they were not designed with cyber threats in mind. Thus, over the past decade, the U.S. military has spent an inordinate amount of time and treasure attempting to address these cyber threats. Countless dollars have been poured into cybersecurity to achieve Authority to Operate, cyber testing to assess systems for weaknesses, and Defensive Cyber Operations to monitor and protect networks from bad actors. While these efforts have undoubtedly helped improve the cyber posture of legacy systems that were not designed to withstand cyber threats, they haven’t sufficiently answered the question, “What do we do after a cyber attack?” Accordingly, this article discusses the mission, development, and activities of the Army Aviation Cyber Incident Response Team (AA-CIRT), which was established to help address this question.

Mailing list additions, deletions, and changes may be directed to [jasp-online.org/stay-connected](mailto:contact@dsiac.org). Distribution of the *Aircraft Survivability* journal is supported by the Defense Systems Information Analysis Center (DSIAC).



DSIAC Headquarters
4695 Millennium Drive
Belcamp, MD 21017-1505
Phone: 443/360-4600
Fax: 410/272-6763
Email: contact@dsiac.org

Managing Editor
Eric Edwards
eric@survice.com

Art Director
Melissa Gestido

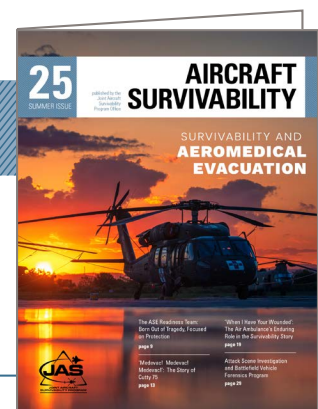
Mailing and Print Distribution
Mary Omiatek

Distribution Statement A:
Approved for public release;
distribution unlimited, per DoW
Office of Prepublication and Security
Review, Case No. 26-T-0618.

WANT MORE AIRCRAFT SURVIVABILITY?

Visit jasp-online.org/stay-connected to:

- ▶ Read/Download the Current Issue or Back Issues (PDF and HTML)
- ▶ Submit an Article Idea, News Note, Calendar Event, or Excellence in Survivability Candidate
- ▶ Join the Electronic and/or Hard-Copy Mailing List



FROM THE DIRECTOR'S DESK

by Dennis Lindell



Welcome to the spring 2026 issue of the *Aircraft Survivability* journal (ASJ). This year is a particularly special one for us, as it marks the 50th anniversary of the journal's first appearance. We'll be saying more about it in our summer issue, but it's remarkable to think that what began as a simple 4-page newsletter shared among a small, emerging community of survivability specialists in the summer of 1976 is now a 32-page, full-color technical journal distributed to the mail and email boxes of more than 40,000 technical professionals across the country.

It's also remarkable to consider how the discipline and community have changed over the last half century. There's probably been no bigger change than in the emergence of cyber as a threat type facing U.S. combat aviation. In fact, with today's heavy dependence on advanced computing and digital networks in all of our latest-generation air platforms—as well as our steady integration of artificial intelligence and autonomous capabilities in these systems—the risk of malicious computer code from adversaries is as real and dangerous to our aircraft, aviators, and missions as the most lethal of kinetic, electromagnetic, and other

threats. Thus, the focus of this spring issue is on some of the ways in which the community is using both traditional and novel tools and techniques to analyze, test, model, and improve the cyber survivability of our current and future aircraft.

To begin, Mr. Charles Fisher and Dr. Arturo Revilla highlight a 2024 study for the Army's Development Command Analysis Center regarding the use of several modeling and simulation (M&S) tools to assess different cyber-hardening approaches to unmanned aerial systems (UAS) and the overall impact on mission effectiveness. Importantly, these tools—the Cyber Operations Lethality and Effectiveness (COLE) application suite and the Full Spectrum Survivability Tool (FSST)—as well as others, are helping UAS designers and developers predict, analyze, and mitigate cyber threats even before these aircraft are fielded.

For our feature article, Dr. Bill "Data" Bryant of Modern Technology Solutions Inc. discusses the use of an analytical framework and mission-level M&S tools to better evaluate full-spectrum survivability, quantify the effect of different cyber threat drivers on mission success, and validate mitigation strategies. This approach, which is an extension of existing survivability analysis methodologies, promises to provide improved, mission-based quantitative analysis for both system and mission engineering efforts.

And speaking of Data Bryant, we're pleased to formally recognize him in this issue for his Excellence in Survivability. As his nickname aptly suggests, Data has been at the forefront of the community's venture into the previously uncharted skies of cyber survivability; and he brings to the task a rare and valuable combination of operational and leadership experience, academic achievement, and analytical skill that is helping the discipline successfully navigate this vital and challenging area.

In addition, Mr. Tom Barnett, the Cyber Engineering Lead for the Army's Capability Portfolio Executive Aviation for Engineering & Architecture, highlights the mission and activities of the Army Aviation Cyber Incident Response Team, as well as its coalition of Army and Joint partners. The team was established to help answer the important question—which is sometimes overlooked in cyber survivability efforts—of what to do *after* a cyber attack has occurred.

Finally, remember to check out our regular News Note, JCAT Corner, and Calendar of Events sections to stay connected with the latest news and events happening in and around the survivability community.

Thanks again for reading. [ASJ](#)

Sincerely,

A handwritten signature in black ink that reads "Dennis Lindell". The signature is written in a cursive, flowing style.

DR. HENNINGER NAMED NEW DOT&E DIRECTOR



In December, Dr. Amy Henniger was confirmed by the U.S. Senate to be the War Department's new Director, Operational Test and Evaluation (DOT&E). Previously, Dr. Henniger served as Senior Advisor for Advanced Computing in the Department of Homeland Security (DHS) S&T Technology Centers, providing leadership to programs and policy makers in artificial intelligence (AI), cybersecurity, data analytics, modeling and simulation (M&S), and quantum information science.

Dr. Henniger also has served in several technology leadership positions in the Defense and intelligence communities, including conducting digital engineering and standards work for the Office of the Under Secretary of Defense for Research and Engineering; serving as a Highly Qualified Expert (HQE) Army M&S Executive; advising the Army's Senior Analyst on studies supporting operational requirements analyses; serving as a Defense Intelligence Agency Senior Advisor and leading the development of the agency's Digital

Transformation Strategy; and serving as an HQE Senior Advisor for Software and Cybersecurity, assessing software and cybersecurity testing and evaluation on major Defense programs for DOT&E. In addition, she has more than 200 hours training with NSA Cyber Red Teams.

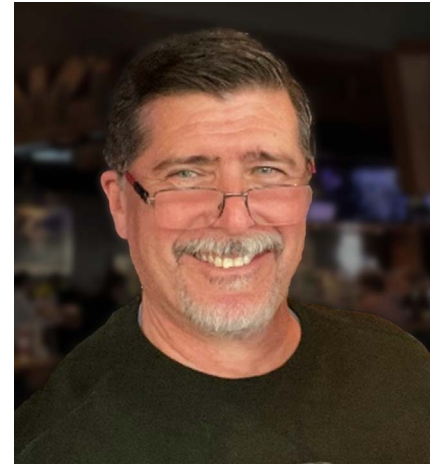
In the private sector, Dr. Henniger served at a federally funded research and development center, leading numerous strategic technology initiatives, including the development of a software assurance primer that has been recommended reading by the Cybersecurity Infrastructure Security Agency and the National Security Agency. She also founded a P&L center of Soar Technology, Inc., a tech startup focused on third-wave context-informed AI solutions, where she led research teams sponsored by the Defense Advanced Research Projects Agency and other Defense agencies. She also co-led the development of a distributed virtual training system used to train more than 1.5 million soldiers.

Dr. Henniger holds a Ph.D. in computer engineering, has taught undergraduate and graduate courses in computer science and AI, has authored more than 80 publications, and has been the recipient of numerous professional awards.

Congratulations, Dr. Henniger, on your new role at DOT&E!

ROBERT GIERARD RETIRES

In July 2025, longtime community leader Mr. Robert Gierard—or "RAG," as he's more commonly known—retired after more than 42 years of service in the



aviation defense technology, testing, development, analysis, and acquisition business. Many ASJ readers will recognize Mr. Gierard's name from his many articles (and award recognitions of other community members) on the National Defense Industrial Association's annual Aircraft Survivability Symposium, for which Mr. Gierard served as the longtime Chair of the Combat Survivability Division's Awards Committee. However, his own 4 decades of contributions to the survivability community are ones that certainly deserve recognition as well.

Earning a bachelor's and master's degree in electrical engineering from Carnegie-Mellon University and the Air Force Institute of Technology, respectively, Mr. Gierard began his aerospace career in 1981, taking a job as an electronic warfare test support engineer at the Air Force Electronic Warfare Center in San Antonio, TX. A few years later, he became the Special Test Program Manager and Chief of the Special Projects Branch for the Air Force Flight Test Center in Nevada, where he was responsible for the planning and execution of numerous important F-117 Nighthawk testing and analysis efforts

(including during Operation Desert Storm). Mr. Gierard then took his specialized knowledge and expertise to the B-2 System Program Office at Wright-Patterson, AFB, where he served from 1991 to 1994 as a Program Manager for the development and testing of several different aspects of the B-2 Spirit stealth aircraft.

In the fall of 1994, he moved to the Pentagon to serve as Chief of the Special Studies Division (“The Red Team”) in the Directorate of Special Programs for the Secretary of the Air Force (Acquisition). In this position, he served an Air Force subject-matter expert on the effectiveness of stealth aircraft, weapons, and technology in combat. And from 1999 to 2002, he was a senior low observables/counter-low observables analyst for the Central Intelligence Agency, supporting the Director of Central Intelligence’s Center for Weapons Intelligence, Non-Proliferation, and Arms Control.

In 2002, Mr. Gierard moved to the industry side of the community, serving as the Director of Operations Analysis for Lockheed Martin Aeronautics and its Advanced Development Programs (aka “Skunkworks”) and then (in 2013) for Raytheon’s Space and Airborne Systems in southern California. Finally, for the past 5 years, Mr. Gierard worked for Booz Allen Hamilton in Colorado Springs, CO, where he served as an independent contractor/strategy consultant and then a Lead Associate supporting NORAD’s J32 Domain Awareness Division.

As far as plans for retirement go, Mr. Gierard says he is currently exploring how he can contribute to the Pike’s Peak Composite Squadron of the Civil Air Patrol, is digging all the holes his gardening wife requires, and is enjoying all the Colorado Front Range sunsets he can.

Congratulations, RAG, on your well-earned retirement, and thank you for your many years of service to the aircraft survivability community, the ASJ, and the U.S. Warfighter!

NEW AFRL RESEARCH ENVIRONMENTAL CHAMBER

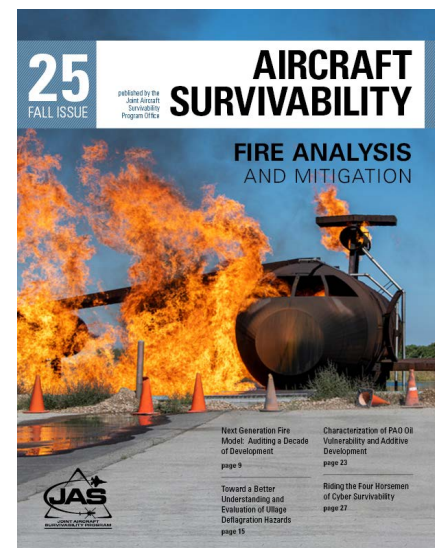
In May 2025, the Air Force Research Laboratory (AFRL) officially opened a new Research Environmental Center (REC) at Wright-Patterson Air Force Base, OH. The state-of-the-art chamber, which is part of AFRL’s Human Effectiveness Directorate, is being used to better test, understand, and improve the performance of both equipment and personnel operating in extreme environmental conditions. The REC can simulate a wide range of these conditions, including temperatures from -60 °F to 130 °F, humidity levels from 10% to 95%, up to 4 inches of rain per hour, and various dust-filled environments. The chamber’s stainless steel interior also has a removable chemical distribution chamber; access ports for wires, tubing, and cables; and an antechamber that serves as a buffer between the entrance and the main chamber (to prevent disruptions in the test environment). In addition, the REC’s

grated floor is rated up to 600 lb/ft² to accommodate heavy-equipment testing.

For more information, visit, <https://www.afrl.af.mil/News/Article-Display/Article/4207462/new-afrl-chamber-to-enhance-human-equipment-performance-in-extreme-environments>.

FALL 2025 ASJ ERRATUM

Note that in the printed version of the fall 2025 *Aircraft Survivability* journal (ASJ), the last name of one of the authors was inadvertently omitted on the authors’ byline on page 9. The byline should read “Adam Goss and Timothy Staley.” The ASJ apologizes for the oversight. **ASJ**



U.S. Air Force Photo by Richard Eldridge



U.S. Navy Photo

MODERNIZING JCAT: AGILE SURVIVABILITY FOR THE FUTURE FIGHT

The foundation of Joint Force air superiority is not defined solely by dominance but by resilience and adaptation. For decades, the Joint Combat Assessment Team (JCAT) has provided an essential feedback loop that allows the Joint Force to understand battlefield threats and improve the survivability of aircraft and the safety of their crews. As the character of warfare continues to evolve at an accelerating pace, so too must the methods used to preserve that resilience. Under the Joint Aircraft Survivability Program (JASP) Office, the Aviation Survivability Development and Tactics (ASDAT) Team is leading the modernization of JCAT capabilities to ensure relevance in tomorrow's Large-Scale Combat Operations (LSCO).

Recent global conflicts have provided critical insight into the future operational environment—one defined by pervasive unmanned aerial systems (UAS), contested communications, and persistent surveillance. Furthermore, the deliberate, hands-on forensic methodologies that proved effective

during the Global War on Terrorism (GWOT) are insufficient in a conflict where physical access to damaged aircraft may be denied and threat systems iterate on a weekly, not yearly, cycle. In response, JCAT modernization efforts are focused on increasing agility, accelerating capability integration, and expanding remote forensic analysis.

EVOLVING THE KIT FOR THE CONTESTED ENVIRONMENT

A primary line of effort is the evolution of the JCAT deployment kit. Legacy GWOT-focused loadouts are being replaced by lighter, more adaptable equipment optimized for operations in which emission control and signature reduction are paramount. The modernized kit prioritizes man-portability, low power consumption, and modularity, enabling small, forward-deployed teams to operate discreetly, even when disconnected from higher-echelon networks.

Central to this modernization is the integration of the Android Tactical Assault Kit (ATAK) into JCAT forensic collection methodology. ATAK enables assessment teams to digitally catalog

evidence, precisely geo-tag battle damage with imagery, and rapidly share initial findings through tactical networks. This capability improves both the speed and accuracy of assessments while reducing reliance on paper-based workflows and delayed reporting—which are critical advantages in LSCO conditions.

INTEGRATING UAS AND COUNTER-UAS LESSONS

The proliferation of UAS represents one of the most significant and persistent threats to Joint aircraft. Drawing direct lessons from the conflict in Ukraine, JCAT, enabled by ASDAT, has accelerated the evaluation and integration of commercial off-the-shelf (COTS) solutions to enhance aircraft survivability against this evolving threat.

This effort recognizes the dual nature of the UAS challenge. Near-peer adversaries continue to employ increasingly sophisticated UAS as part of integrated kill chains, while asymmetric actors leverage low-cost systems to threaten aviation operations across multiple theaters. By helping validate and integrate emerging counter-UAS technologies, JCAT provides critical data to inform tactics, techniques, and procedures and to support survivability improvements across the Joint Force.

OVERHEAD FORENSICS: THE J-FORCE FRAMEWORK

In an LSCO environment, the wreckage of a downed or damaged aircraft may be inaccessible, potentially located miles

inside denied territory. Addressing this challenge requires a fundamental shift from physical forensic access to remote assessment.

The JCAT Forensic Operations and Remote Collection Evaluation (J-FORCE) framework provides the structure for this shift. Through J-FORCE, JCAT leverages National Technical Means sensors and enablers at the Top Secret/Sensitive Compartmented Information level to support detailed battle damage assessments without physical access to the aircraft. These remote sensing capabilities provide commanders with timely, actionable intelligence to adapt operational plans, while also informing combat aviation survivability engineering, research and development (R&D), and test and evaluation (T&E) communities on newly observed threat systems and their methods of employment.

ACCELERATING THE ACQUISITION CYCLE

Even the most advanced survivability solution provides little value if it arrives too late to be relevant. Thus, JCAT, supported by ASDAT, is enabling a more responsive acquisition process by directly supporting the engineering, T&E, and acquisition communities responsible for aircraft survivability systems.

By providing high-fidelity forensic data and combat-relevant threat analysis, JCAT enables stakeholders to refine engineering designs, develop test events that reflect real-world threat conditions, and justify accelerated fielding timelines. This collaboration shortens the cycle from threat identification to the delivery of life-saving countermeasures to the Warfighter.

POSTURED FOR THE FUTURE FIGHT

The modernization of JCAT represents a comprehensive effort to reshape how the Joint Force approaches aircraft survivability. From enabling forensic assessment in austere Arctic environments to supporting operations across the vast distances of the Indo-Pacific Command theater, JCAT is being postured for global relevance in future conflicts.

Through agile equipment, rapid COTS integration, ATAK-enabled digital forensics, expanded remote assessment via J-FORCE, and acquisition support at the speed of relevance, ASDAT is helping to ensure that JCAT continues to deliver decisive survivability insights. In the future fight, success will favor forces that adapt fastest; and modernizing JCAT will ensure that the Joint Force retains that critical advantage. **ASJ**

ATTENTION ALL 'SPACE' TRAVELERS!



Have you checked out the JASP Space on DoDTechipedia? Here, you can find and share the latest information on what's been done, what's being planned, and who's conducting projects in the aircraft survivability and aerospace communities. Typical content includes:

- ▶ Information on current RDT&E projects, developments, and documents
- ▶ The latest in community M&S tools and technologies
- ▶ Announcements about upcoming training, meetings, and other community events
- ▶ Controlled information not available in public release formats.
- ▶ In addition, the site is expected to soon include sections for providing feedback on reports, answering surveys, and submitting queries. And remember it's all free and available to Government and contractor personnel with a DTIC account and proper access.

So let the space explorations begin! Visit:
<https://www.dodtechipedia.mil/dodwiki/display/JAS/JASP+Home>.

*For more information about the JASP Space, contact Mr. Darnell Marbury at t.d.marbury.ctr@us.navy.mil.
General user guidance is also available on DTIC's DoDTechipedia Team page at <https://www.dodtechipedia.mil/dodwiki/display/DAT/Welcome+to+DoDTechipedia>.*

UAS CYBER MODELING: ASSESSING OPERATIONAL CONSEQUENCE BEFORE AND DURING DRONE DESIGN

by Charles Fisher and Arturo Revilla



Unmanned aircraft systems (UAS) have become a growing commodity on the battlefield. The recent conflicts in Ukraine and Gaza have particularly underscored their operational value and increased use in the planning, execution, and assessment of military operations and have demonstrated that these systems can significantly reduce costs and limit risk to personnel. Accordingly, the U.S. Department of War is taking actions to meet Administration-set “drone dominance” goals and has appropriated a budget estimated at \$1 billion. The Department is also pushing for more commercial solutions across the Services in an effort to speed up acquisitions and provide the Warfighter with much needed technologies that provide an upper hand in modern military engagements.

The increased proliferation of commercially available drones also means, of course, an increased presence in the cyber domain, especially given the ever-increasing digital interconnectivity of systems to enable UAS warfare. The number of cyber vulnerabilities and corresponding available attack surfaces—as well as counter-UAS tools and technologies—has thus risen as well. As highlighted in a 2024 briefing by the U.S. Army’s National Ground Intelligence Center (NGIC), “UAS exploit tools are widely available, inexpensive, and require little sophistication and/or expertise” [1].

Academic research has reached similar conclusions. Peer-reviewed studies published in recent years document the increase in cyber attacks on commercial and military UAS. Many of these studies provide specific examples of attack types and insights into mitigation strategies that vendors and system owners could use to harden these technologies [2–4].

This article highlights a study performed in 2024 for the U.S. Army Transformation Decision Analysis Center to answer the question, “How can we use modeling and simulation (M&S) to examine hardening approaches to UAS that are still in the design phase of the acquisition life cycle using a mission-based impact analysis?” The M&S capabilities used for this study were developed under guidance by the Joint Aircraft Survivability Program (JASP) and the Director of Operational Test and Evaluation (DOT&E).

The primary M&S tool used for this analysis was the Cyber Operations Lethality and Effectiveness (COLE) suite of applications. As stated in the DOT&E Annual Report, COLE is “the

The increased proliferation of commercially available UAS also means, of course, an increased presence in the cyber domain, especially given the ever-increasing digital interconnectivity of systems to enable drone warfare.

Joint Munitions Effectiveness Manual capability for cyber vulnerability and resiliency assessments” [5]. This analysis also used the Full-Spectrum Survivability Tools (FSST), which were developed under DOT&E and highlighted in the spring 2025 issue of the *Aircraft Survivability* journal (ASJ) [6].

APPROACH

To examine potential cyber vulnerabilities that could be exploited in a UAS, we assumed the UAS to be composed of two major components: the unmanned air vehicle (UAV)—more commonly called the “drone”—and a ground segment composed of a control launch and/or command vehicle. Both elements can exist in multiple configurations. (Note that the examples used here are purely illustrative.)

The models drew on several sources, including an exemplar model-based systems engineering (MBSE) model; documentation developed for a 2022 symposium on cyber modeling tools; and the notional MQ-99 Berserker UAV, which is extensively discussed in the spring 2025 ASJ [7].

To narrow the analysis, researchers assumed a relatively constant ground-control vehicle, composed of a mission computer, databases, and communications systems. As shown in Figure 1, the ground-vehicle model included incoming communications, a controller area network bus, a launch system architecture, and a mission IT network separated from operational technology by a guard device. The mission system was composed of three workstations, a mission database, a mission computer, a cryptographic keystore, and a UAS antenna.

For the air vehicle, three progressively hardened designs were modeled (shown in Figures 2–4). The first represented a lightly modified commercial quadcopter with a MIL-STD-1553 data bus and a separate communications bus. The second added GPS, cryptographic devices, a maintenance interface, and a sensor payload, with encrypted primary bus communications. The third model represented a hardened military platform, incorporating segregated flight controls and mission payloads, an electro-optical and infrared subsystem, and synchronized encryption keys loaded from the ground vehicle.

ANALYSIS

System Under Test Characterization

Researchers did not model specific software, firmware, or operating systems because of the use of notal systems. Instead, they relied on two COLE frameworks: the dynamic state model and the connectivity model. The state model allows users to simulate changes to a system’s

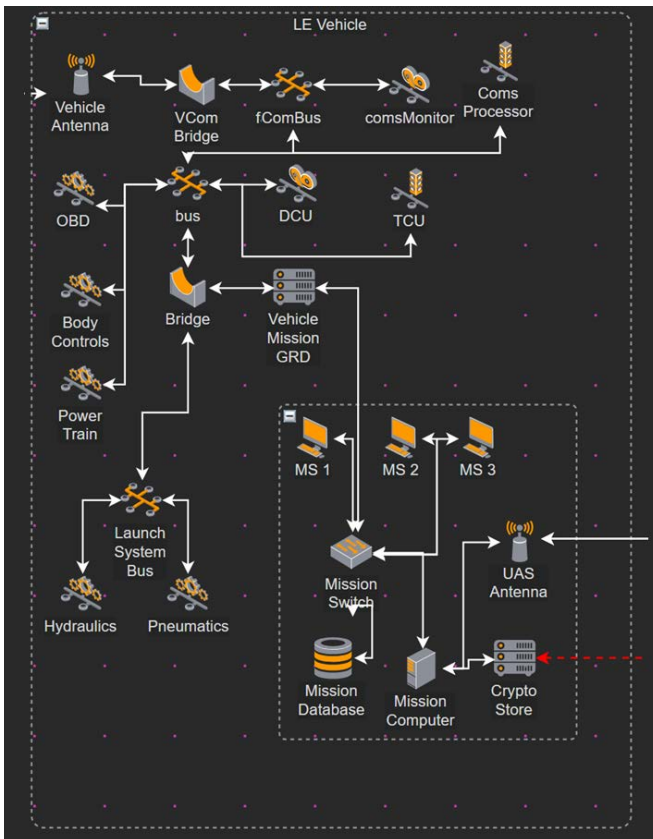


Figure 1. The COLE Network Model Developed for the Ground Control Vehicle.

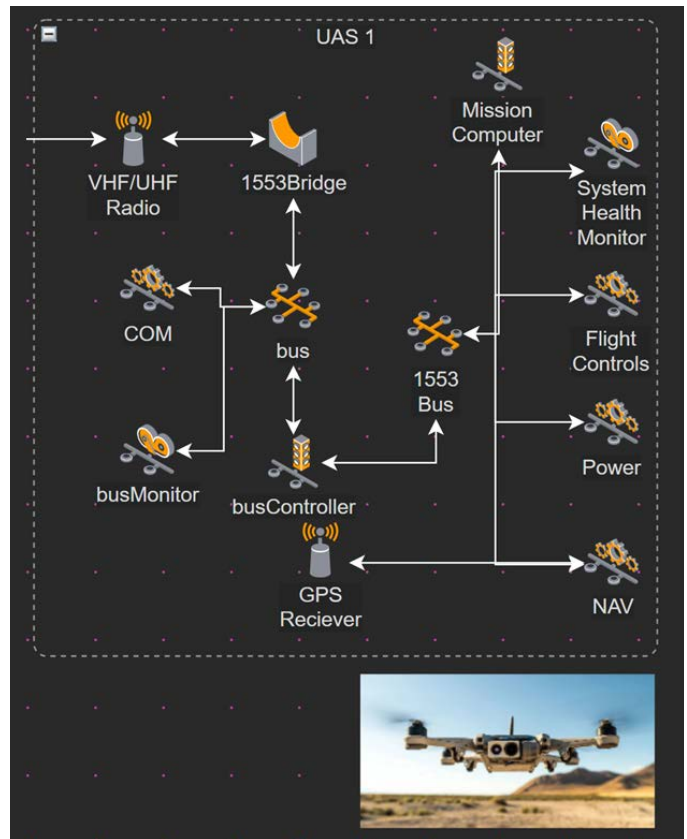


Figure 2. The COLE Model for the Small UAV, UAS 1.

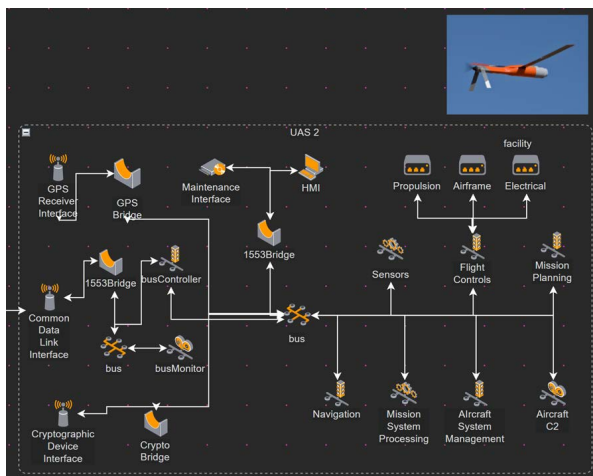


Figure 3. The COLE Model for the Medium UAV, UAS 2.

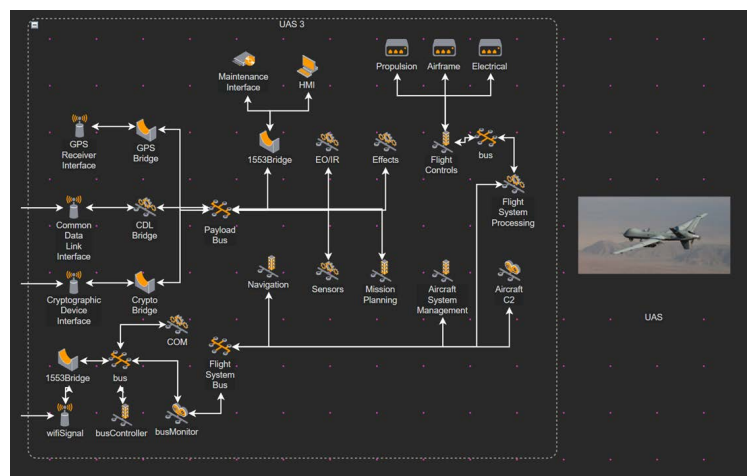


Figure 4. The COLE Model for the Large UAV, UAS 3.

condition—such as operational, degraded, or compromised—and observe cascading effects across the network. The connectivity model, informed by subject-matter expertise, evaluates how information flows between IT and operational technology components, accounting for firewall rules and architectural constraints. As shown in Figure 5, if a

user selects a node (depicted in yellow) and asks COLE to show accessible systems, the connectivity model examines the type of system the node is connected to, looks for firewall configurations that may be set, and shows the user which devices may be accessible from the selected node.

COLE's Risk Assessment application, developed with guidance from JASP, integrates these models with the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework. Users can simulate specific attack techniques, assign probabilities to each step, and calculate aggregate likelihoods across an attack path. The current

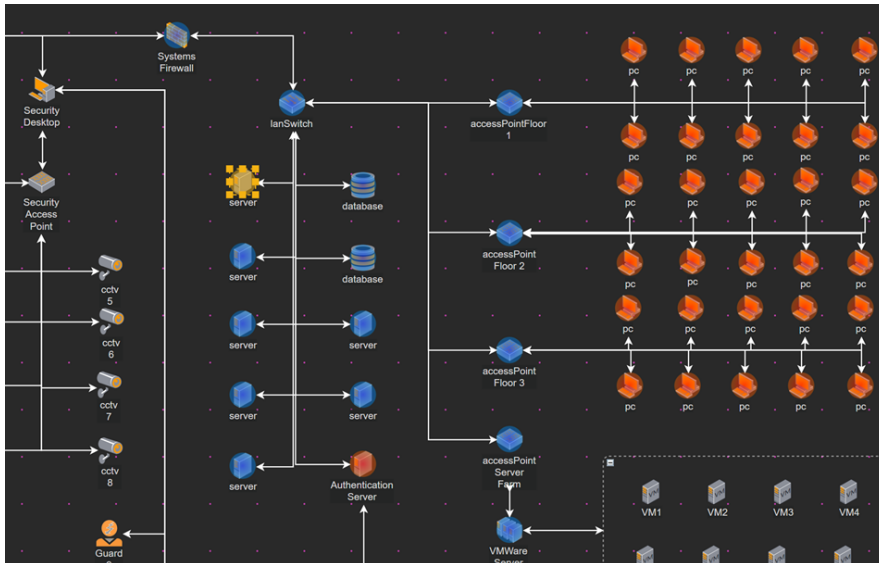


Figure 5. An Example of the COLE Connectivity Model in Use.

implementation assumes independent steps, though future versions will incorporate Bayesian conditional modeling.

Attack Scenarios

The study examined two attack scenarios. The first modeled a supply-chain interdiction attack targeting a communications remote terminal unit. The notional payload—activated by a radio-frequency signal—scans its bus, compromises a controller, and propagates until it reaches the flight controls, where it overwhelms the endpoint. Each step was assigned a 75% probability of success.

As expected, additional architectural barriers reduced overall success rates. The modeled likelihood of a successful attack fell from 41% in the simplest UAV design to 17% in the hardened configuration, illustrating how incremental design changes can significantly improve resilience. Table 1 shows the results of the modeled attacks.

Table 1. Results of Modeled UAV Attacks

UAV	Attack Steps	Likelihood Mean
UAV Small	3	41%
UAV Medium	4	31%
UAV Large	6	17%

Figures 6 and 7 show the modeled attack paths and the updated state and connectivity of the UAVs during and after the successful attacks. Nodes highlighted in blue indicate they are accessible from the various compromised locations, which are shown here with the hacker icon overlay.

Mission Impact

To assess operational consequences, the study integrated COLE outputs into the Joint Capability as a Service (JCaaS) architecture and the FSST toolset. A representative mission was constructed in the Advanced Framework for System, Integration and Modeling (AFSIM), simulating an integrated air-defense-system collection task involving two

expendable UAVs gathering radar and electronic support data.

In this scenario, the cyber attack targeted communications rather than flight controls. Each step of the attack was assigned a 50% likelihood of success, yielding an overall probability of 0.236. A time-based exposure model was used to represent the likelihood of activating the radio-frequency trigger (shown in Figure 8).

For this scenario, we focused the cyber attack on communications only. Therefore, the attack did not have to pivot to the flight controls and could just perform a denial-of-service on the communications device. We chose the large UAV as the target and lowered the likelihood of success to 50% for each step. This resulted in an overall likelihood of 0.236 with a corresponding 90% confidence interval, as selected in the Risk Assessment tool.

For the RF portion of the attack, we derived a simple time-based exposure model that calculated the probability that the payload was triggered (shown in Figure 9). This model assumes that if the UAV is exposed to the RF signal for some amount of time, the likelihood that the payload is triggered increases.

The results were passed to AFSIM and executed through Monte Carlo simulation (shown in Figure 9). Interestingly, as shown in Figure 10, in 20 runs the cyber attack affected mission outcomes twice, reducing detections compared with baseline scenarios.

SUMMARY

We believe this study was successful in showing how the COLE M&S tool

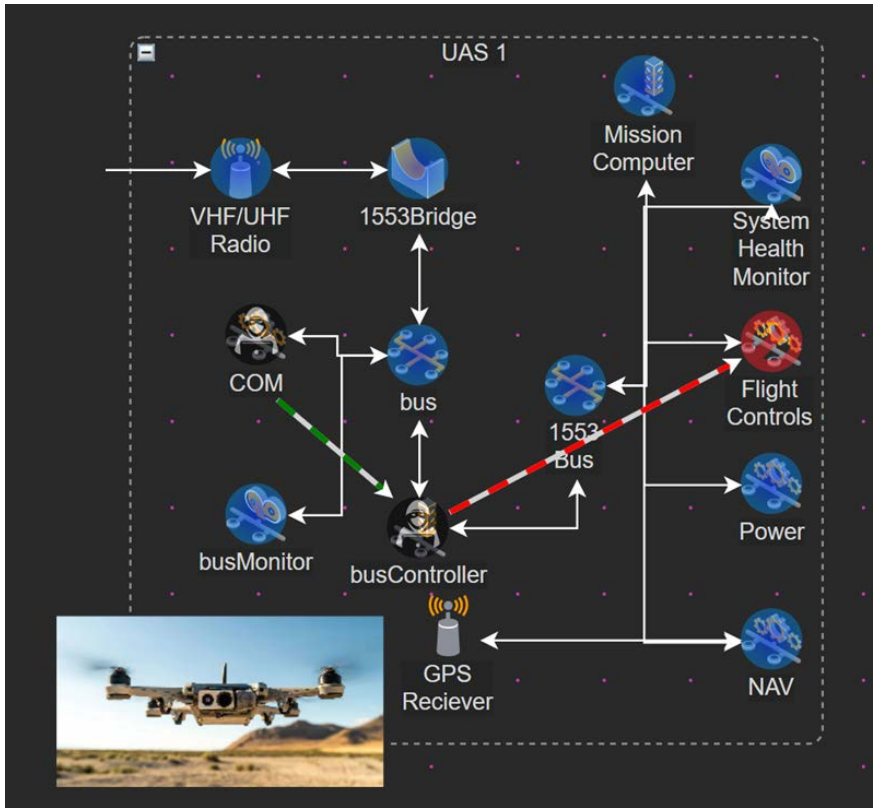


Figure 6. Attack Path for the Small UAV, UAS 1.

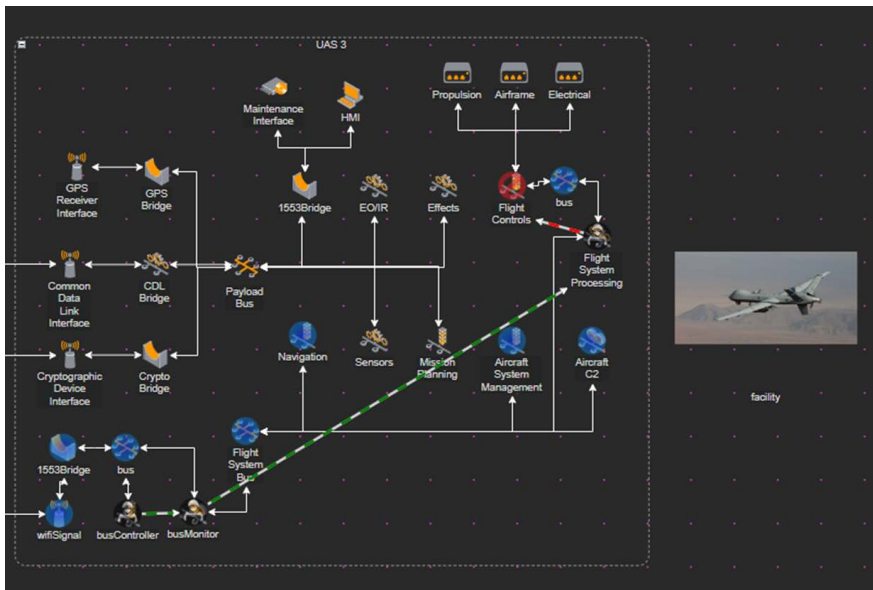


Figure 7. Attack Path for the Large UAV, UAS 3.

can be used before and during the design phase of an acquisition life cycle. Further, as designs and specific technologies are selected, we can model higher-fidelity attributes and examine specific attack paths and exploits that a cyber operator could

perform if they had access to the device. By integrating the COLE results into the JCaaS architecture, we were able to show mission impact of an RF-enabled cyber attack so mitigations and preventive measures could be taken during design and

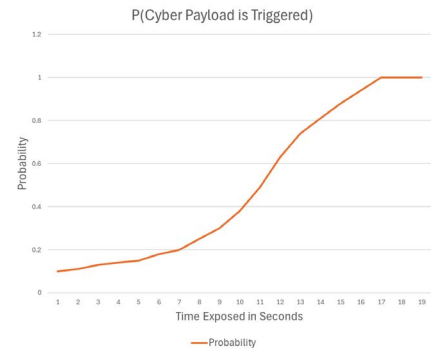


Figure 8. The Function Developed for the RF-Enabled Trigger on the Cyber Payload.

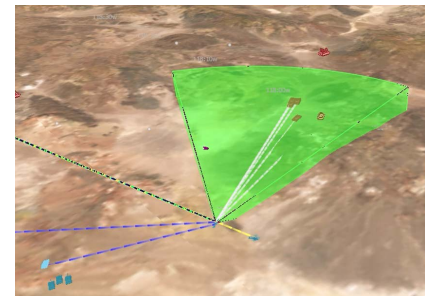


Figure 9. AFSIM Screenshot for the IADS Collection Mission.

deployment of the UAS to harden it against nonkinetic threats.

Specifically addressing U.S. Army interests, this work was the first time to our knowledge that the effects of a cyber attack were shown in the context of a large-scale mission. As the Army further investigates the effects of cyber attacks on large-scale conflicts involving thousands of entities (simulated systems), it is imperative to augment the current kinetic-centric M&S tools with the inputs from the "cyber" (nonkinetic) engagement.

Additionally, as a proof of concept, this work shows it is possible to perform M&S on the individual systems and influence large-scale simulations. We thus envision a future in which the probabilities derived from tools such as COLE are used on large-scale simulations that provide input to decision makers on the size and scale

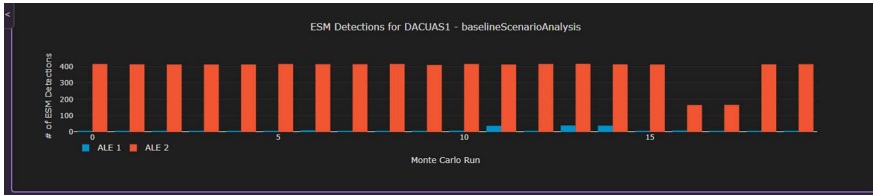


Figure 10. JCaaS Analysis Results Showing Mission Impact of the Cyber Attack Against a UAV.

of formations, as well as the proper deployment locations for these systems. In short, as far as we know, this is the first instance that a cyber model was used to observe impact on a mission due to the presence of a cyber threat on the environment. Future work will look at implementing this concept into large force-on-force simulations used by the Army for training and as part of analysis of alternatives studies (e.g., One Semi-Automated Force [OneSAF]). [ASJ](#)

ABOUT THE AUTHORS

Mr. Charles Fisher is currently the Director of the Cyber and Non-Kinetic Effects directorate at Applied

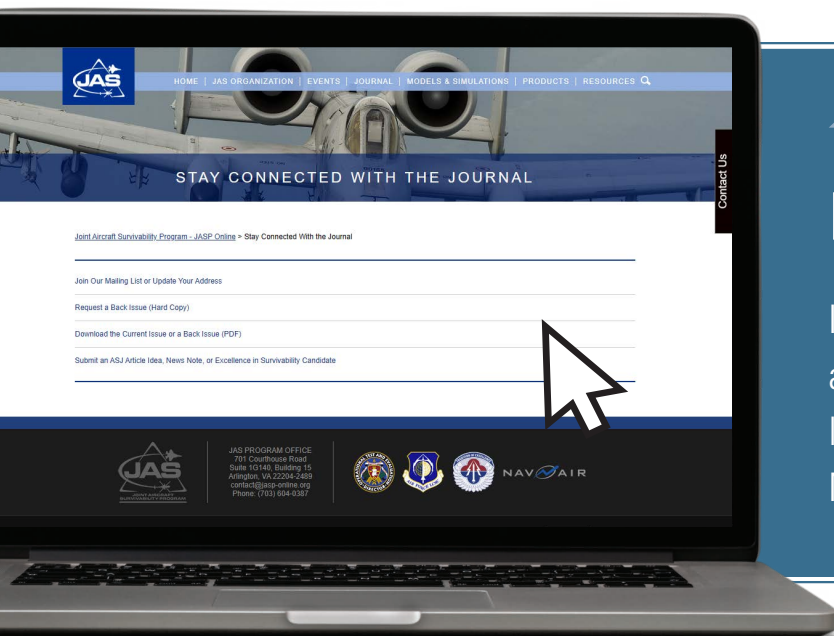
Research Associates, Inc. (ARA). He has more than 15 years of experience developing vulnerability and lethality models for the kinetic and nonkinetic weapons effects communities. Mr. Fisher holds a B.S. in mathematics from Fitchburg State University and an M.S. in applied mathematics from Worcester Polytechnic Institute.

Dr. Arturo Revilla is a Senior Cybersecurity Engineer at the Army's Transformation Decision Analysis Center (TDAC). He has more than 25 years of experience leading teams evaluating cybersecurity, assessing cyber-risk, and performing threat emulation on Army tactical and enterprise systems. Dr. Revilla holds a

Ph.D. in computer engineering and an M.S. and B.S. in electrical engineering from the University of Texas at El Paso.

References

- [1] Kendra et al. "Cyber Threats to DoD UAS Operations." Briefing, U.S. Army Intelligence and Security Command, National Ground Intelligence Center, February 2024.
- [2] Branco, Bruno, José Silvestre Serra Silva, and Miguel Correia. "Cyber Attacks on Commercial Drones: A Review." *IEEE Access*, vol. 13, 2025.
- [3] Oracevic, Alma, and Ahmad Salman. "Unmanned Aerial Vehicles in Peril: Investigating and Addressing Cyber Threats to UAVs." *IEEE Xplore*, 2024.
- [4] Yu, Aaron, Iuliia Kolotylo, Hashim Hashim, and Abdelrahman Eltokhy. "Electronic Warfare Cyberattacks, Countermeasures, and Modern Defensive Strategies of UAV Avionics: A Survey." *IEEE Access*, vol. 13, 2025.
- [5] Office of the Director, Operational Test & Evaluation. "FY 2024 Annual Report." <https://www.dote.osd.mil/annualreport/>, January 2025.
- [6] Fisher, Charles, Ashley Henderson, and John Crews. "Full-Spectrum Survivability Tools." *Aircraft Survivability* journal, spring 2025. Bryant, William. "Using M&S to Determine Cyber Survivability: Score Small and Let the Machines Do the Math." *Aircraft Survivability* journal, spring 2025.



HEARD ANY NEWS?

If you have a community-related event, announcement, or other news item you'd like to submit for consideration as a News Note, visit jasp-online.org/stay-connected.

SIMULATED DIGITAL SHRAPNEL: USING MISSION-LEVEL M&S TO QUANTIFY CYBER SURVIVABILITY IN FULL-SPECTRUM ENVIRONMENTS

William "Data" Bryant



Modern warfighting environments are increasingly complex and characterized by a convergence of kinetic and nonkinetic threats that challenge the survivability of aircraft and weapon systems across multiple domains. To help address this challenge, Congress mandated in the 2022 National Defense Authorization Act that the Department of Defense (DoD) expand survivability and lethality testing to include evaluation against a range of threats, including kinetic; cyber; electromagnetic spectrum (EMS); directed energy (DE); and chemical, biological, radiological, and nuclear (CBRN) effects. The Act also defined full-spectrum survivability as “a series of assessments of the effects of kinetic and nonkinetic threats on the communications, firepower, mobility, catastrophic survivability, and lethality of a covered system” [1].

Meeting this mandate requires the ability to integrate different threat models, data sources, and testing results into a coherent analytical framework. Most cyber survivability and cybersecurity analyses use methods such as qualitative analysis and control selection to manage risk, which do not easily integrate with the survivability analysis techniques used in more traditional threat domains, such as kinetic weapons. Cyber threats should instead be treated more like kinetic survivability threats, using an approach such as that of Aircraft Cyber Combat Survivability (ACCS) [2].

Once a similar analysis methodology is used for cyber, the different threat areas still need to be combined. Modeling and simulation (M&S) provides a practical means to achieve this integration [3]. M&S environments can be cost-effective, repeatable, and scalable and can serve as a potential integrator for full-spectrum survivability evaluation. For example, M&S can capture the interdependencies between threat areas, such as when a cyber attack disables a radar or electronic countermeasures system, thus rendering an aircraft more susceptible to subsequent kinetic engagements.

Mission-level simulations, such as the Advanced Framework for Simulation, Integration, and Modeling (AFSIM), provide a viable means to measure cyber survivability within a full-spectrum survivability environment, albeit one that must be validated using test and exercise data. This approach can provide mission-based quantitative analysis that can be used in both system and mission engineering to improve our expected mission performance, and the results can be validated using a combination of testing and exercises.

RISK MODEL

Effective measurement of cyber survivability requires a risk model that quantitatively links cyber threats to mission outcomes. The framework used in this article adopts the traditional definition of risk used in the DoD [4]:

$$\text{Risk} = \text{Impact} \times \text{Likelihood}$$

Risk then can be measured in terms of Expected Mission Loss (EML), which is calculated by multiplying impact and likelihood. Within the context of aircraft and weapon system survivability, impact in the preceding equation is the mission-level consequences of a successful cyber

attack, such as degraded mission effectiveness, loss of capability, or mission failure. In addition, likelihood represents the probability that an adversary successfully executes a cyber attack capable of producing those effects.

These two major components can then be broken down into four total components to yield the risk model that is referred to as four-factor (4F) (shown in Figure 1) [5].

Single system loss captures the percentage of mission capability that is lost if a cyber attack against a system is successful, while percent systems impacted is the percentage of systems that are expected to be affected by an attack. For example, an attack might affect only one system, half of the fielded systems, all the fielded systems, or any other percentage. Likelihood includes two terms: likelihood of attack launch and likelihood of attack success. Likelihood of attack launch represents the likelihood that an adversary will choose to launch a particular cyber attack. Likelihood of attack success is the probability that an adversary will achieve some mission impact given that the adversary chooses to launch a particular cyber attack. This parameter can be challenging to

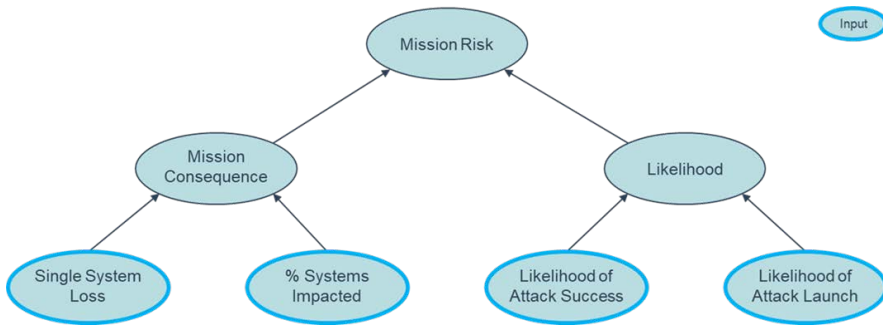


Figure 1. Four-Factor Risk Model.

determine, but we can use probabilistic attack trees to further decompose and analyze this probability.

PROBABILISTIC ATTACK TREES

Traditional cyber risk assessments often rely on ordinal scoring methods, producing values such as “low,” “medium,” or “high,” which lack transparency, repeatability, and quantitative rigor. Probabilistic attack trees provide a more structured and

defensible approach to quantifying the likelihood of a cyber attack’s success by representing the logical relationships between potential attack paths, system vulnerabilities, and adversary objectives. Each leaf in an attack tree represents a discrete event or precondition necessary for a cyber attack to succeed, while branches depict how those events combine to produce an overall probability of mission impact [6].

Probabilistic attack trees can be created using three primary sources of information: (1) historical or

design-based data, which provide empirically grounded probabilities for events such as insider threats or component failures; (2) simple linear models, which leverage human-informed statistical models to estimate attack success probabilities when direct data are unavailable; and (3) subject-matter expert (SME) assessments, which fill residual knowledge gaps using structured elicitation methods [6]. An example attack tree is shown in Figure 2.

Within the risk model framework, attack tree likelihood of attack success is multiplied by the other three 4F risk model terms to produce EML values. These parameters quantify the anticipated mission degradation due to cyber effects, allowing direct comparison with other threat domains, such as kinetic or EMS attacks. When validated through test and exercise data, these EML results provide a robust mechanism for linking cyber survivability metrics to mission risk.

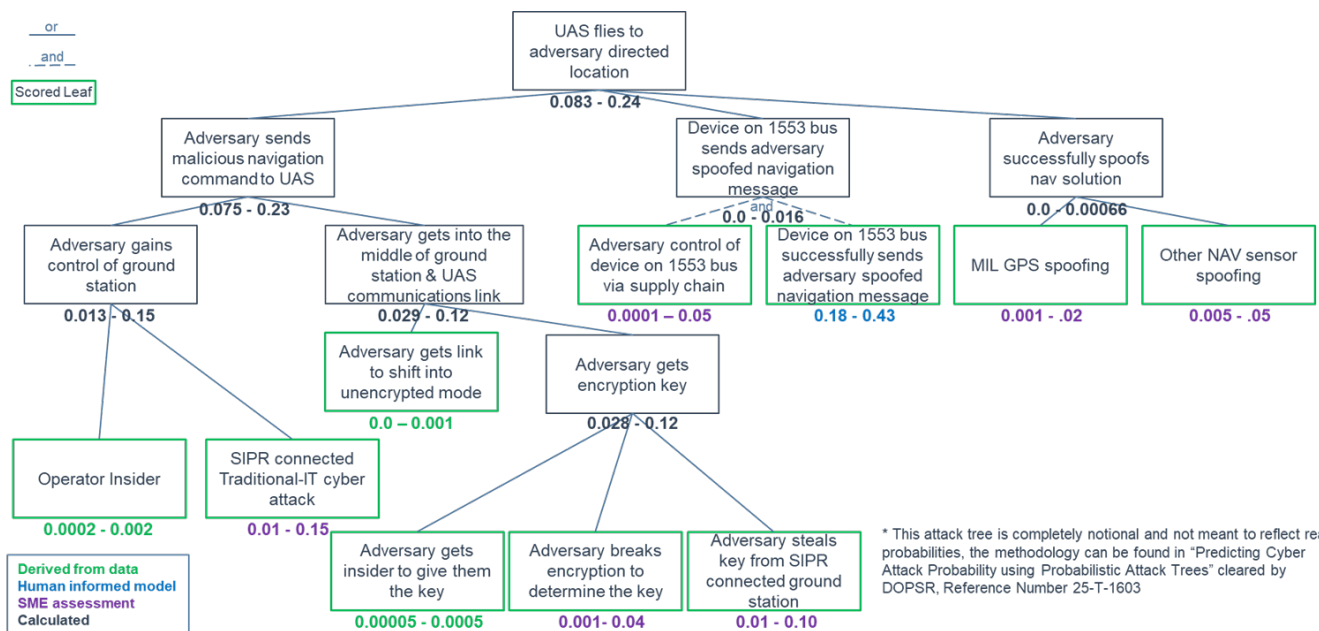


Figure 2. Example Notional Probabilistic Attack Tree.

MQ-99 Berserker Example

The MQ-99 Berserker is a completely notional unmanned aircraft system (UAS) created as a plausible early-concept vehicle for illustrating cyber survivability analysis and design tradeoffs. In the conceptual stage of design, the MQ-99 is a medium-sized, long-range autonomous UAS with an internal payload bay able to carry four GBU-39 small-diameter bombs (SDBs) or two AIM-120 advanced medium-range air-to-air missiles (AMRAAMs) [7]. The vehicle is launched from a transportable Electromagnetic Launch Runway System (ELRS) and supports mission updates from a ground station or airborne commander. In air-to-air loadouts, the Berserker acts as a force multiplier, loitering and receiving targeting direction from an airborne commander.

The conceptual architecture was built out in a model-based systems engineering tool and emphasizes cyber-physical interfaces: mission and flight computers, navigation, communications, propulsion and fuel-management controllers, and the ground control station. To illustrate defendable and resilient design, the concept includes a hardened cyber sentinel responsible for traffic monitoring, device resets, and transition of flight-critical systems into backup modes when malicious activity is detected.

To support quantitative risk analysis, a full set of probabilistic attack trees was constructed for the MQ-99. These attack trees map multiple attack pathways into explicit leaf events scored using historical data, simple linear models, and SME elicitation. There were more than 350 nodes in the full set of attack trees, and they

led to 21 distinct cyber attacks grouped into 8 risk groups.

MISSION-FOCUSED M&S

Scenario Modeled

The 21 cyber attacks were incorporated into a larger full-spectrum threat scenario, including a range of kinetic and nonkinetic threats. This scenario was unclassified and used purely notional threat parameters. The modeled scenario was a strike mission simulated in AFSIM in which two MQ-99 Berserkers penetrated contested airspace to engage six surface targets using SDBs. The unmanned strike package was tactically controlled by a manned fighter, with an E-3 Sentry providing battle management and sensor support. Precise threat placement was randomized for each trial to sample a wide range of threat geometries.

The defended environment included 2 medium-range surface-to-air missiles (SAMs), 1 short-range SAM, 2 high-power microwave (HPM) emitters, 1 high-energy laser (HEL), 1 GPS-jamming electronic warfare (EW) system, and the 21 discrete cyber-attack events targeting the MQ-99s.

The scenario was architected for high-volume Monte Carlo experimentation: individual threat elements or entire threat groups could be toggled on or off to isolate contributions to mission outcomes.

Each simulation run recorded the number of targets destroyed and number of Berserkers lost. This allowed easy aggregation into mission-performance statistics and conditional probabilities. The analysis conducted more than 1.2 million Monte Carlo runs to reduce error margins, producing statistically robust distributions of mission success and platform attrition to support sensitivity analysis, EML estimation, and risk attribution across specific threat domains.

Noncyber Results

While the focus of this article is on the cyber results, noncyber threat effects are presented in Figure 3 for comparison. The blue bars on the left capture the improvement in mission performance gained measured by the number of additional targets that were destroyed over the baseline case with all threats. For example, if the GPS jammer was removed from the scenario, almost 10% more targets were destroyed. This approach of

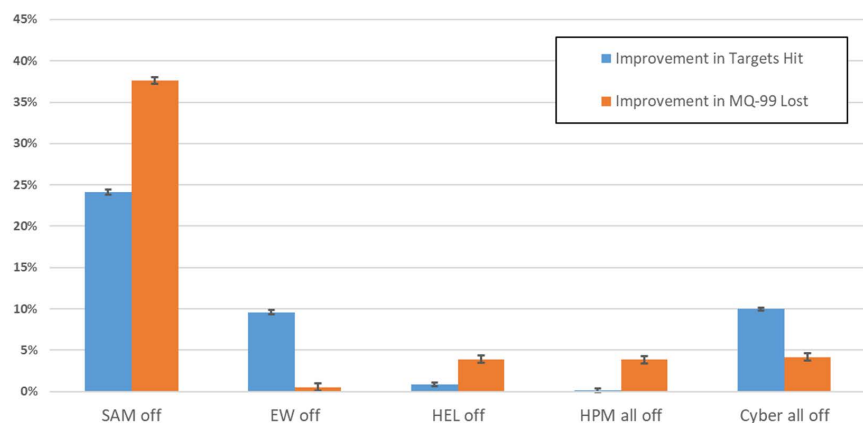


Figure 3. MQ-99 Threat Category Results.

deleting one threat at a time was important as it captured the contribution of the threat system in conjunction with all the other threats. The orange bars on the right capture the improvement in performance gained as measured by how many fewer MQ-99s were lost vs. the baseline case, and the black error bars present the 95% margin of error.

In this notional scenario, it can be seen at a glance that the SAMs are the most impactful threats, although all the threats have some effect. If the breakdown is done by individual threat system, further insights can be gained. For example, the medium-range SAMs are most lethal to the MQ-99, while the short-range SAM has the greatest impact on targets destroyed since it intercepts many SDBs on their way to targets.

Cyber Attack Modeling

For cyber attack modeling, likelihood inputs to AFSIM were specified as 90% confidence intervals, capturing uncertainty in each attack parameter, then converted into Gaussian mean

and standard deviation values for Monte Carlo execution. Three key probabilistic inputs were defined for each cyber pathway: (1) the likelihood of attack success as determined from attack tree-derived probabilities, (2) the likelihood of adversary employment of that attack type during the mission, and (3) the percentage of Berserker systems expected to be affected should the attack succeed. The values of these inputs can be determined via intelligence-based estimates, cyber test data, the results of exercises involving the subject threats and systems, or SME judgements. These parameters were applied at run-time to determine whether an attack occurred as well as which systems were impacted.

The resulting cyber effects were then scripted into AFSIM as degradations to specific system functions, ranging from minor sensor inaccuracies to complete loss of navigation, communication, or weapon-release capability. A representative sample is shown in Table 1, which summarizes how some of the cyber attack effects were implemented in the simulation.

These scripted mission-relevant degradations provided dynamic mapping of cyber effects to mission outcomes, linking probabilistic risk estimates to observable mission degradation within the AFSIM environment.

Cyber Survivability Results

The results from removing each of the 21 cyber attacks, one at a time, are detailed in Figure 4.

Note that the scale of the Y axis is highly expanded, and the top of the chart is only 2% EML. The black error bars represent the 95% margin of error, or the range within which the result would be expected to fall 95% of the time if the experiment was repeated numerous times. The large number of model iterations was largely required to shrink this error, since the probabilities associated with most of the cyber attacks were extremely small.

Several of the attacks, such as R1-0 and R3-1, predominantly affected the number of targets hit vs. MQ-99's lost,

Table 1. Example Cyber Attacks Simulated in AFSIM

Risk Group	Risk	How Simulated in AFSIM
R1: Adversary degrades UAS operations	R1-0: Adversary degrades UAS operations	If this risk occurred, we modeled it by degrading the affected MQ-99's navigation solution by introducing a random 0.5–15-m error in target location.
R2: Adversary flies UAS to adversary-selected location	R2-0: Adversary flies UAS to adversary-selected location	If this risk occurred, we modeled it by commanding the affected UAS to fly north out of the combat area and then crash into the ground.
R3: Adversary gains useful information from UAS	R3-1: Adversary gains mission planning and AV location data	If this risk occurred, we modeled it by adding additional tactical SAMs, assuming they brought them in as an additional resource since red was prepared for the attack.
	R3-3: Adversary gains technical and fleet health data	If this risk occurred, we increased the P_k of both types of SAM by 50% over the base value, assuming the technical data would improve detection and targeting capabilities.
R6: Adversary maliciously alters flight-critical AV component	R6-5: Adversary maliciously alters AV electrical system	If this risk occurred, we modeled it by flying the affected MQ-99 into the ground, simulating it had lost power, which is flight critical.
	R6-6: Adversary maliciously alters AV fuel management system	If this risk occurred, we modeled it by having the affected MQ-99 immediately return to base instead of prosecuting attacks at the beginning of the scenario since it was reporting emergency fuel.

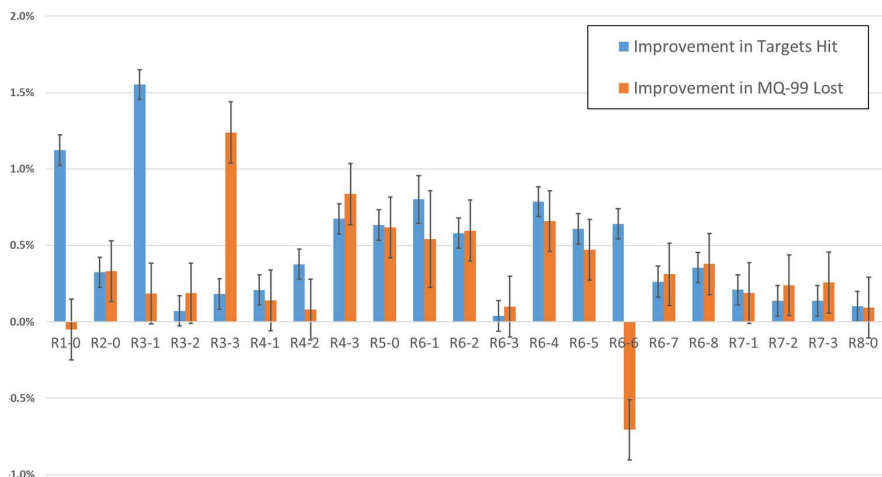


Figure 4. AFSIM 21 Cyber Attack Results.

which makes sense, as R1-0 affected targeting accuracy and R3-1 inserted additional short-range SAMs in the target area that were mostly targeting the incoming SDBs. R3-3 resulted in more MQ-99's being destroyed as the P_k 's of the medium-range SAMs were increased. R6-6 looks strange, as fewer targets were hit, but fewer MQ-99's were destroyed when this attack was removed. This actually makes sense, as R6-6 was a false fuel-low warning that caused affected MQ-99's to turn around and return to base before entering the target area. Once again, all of these attacks were purely notional and not intended to represent any real attacks, but they do illustrate how a wide range of attacks can be modeled.

ADDITIONAL CONSIDERATIONS

Verification and Validation

Similar results to those previously listed, on real systems, will only be useful if they approximate what is actually going to happen in a contested cyber and full-spectrum threat environment. DoD policy rightly requires that any M&S model go through appropriate verification and

validation, and these models should not be exempted.

However, cyber models are harder to compare to a baseline than physics-based models, which can be more easily verified with physical testing. In this case, cyber testing is a good starting point to ensure that the probabilities reflect the real difficulty of the modeled attacks. Single attacks can also be scaled up on cyber ranges where attackers and defenders interact. Finally, and most importantly, the entire approach can be validated by applying it against large-force exercises. The expected exercise vulnerability periods normally include some without simulated cyber attacks and some with them. The model's results should be congruent with what is seen in such testing and exercises, and the models should be updated as appropriate, while noting that even the large-force exercises have limitations in their ability to replicate real combat.

Using With System and Mission Engineering

The results of this type of analysis can also provide a quantitative foundation for supporting both systems

engineering and mission engineering trade studies. Within systems engineering, the ability to model and quantify cyber and full-spectrum effects enables designers to evaluate alternative design approaches and mitigation strategies early in the life cycle, when changes are least costly and most impactful. To illustrate, a range of MQ-99 radar cross section (RCS) reductions was compared against the mission gain of designing a new SDB carriage mechanism that enabled the carriage of six instead of four SDBs. Increasing the number of SDBs carried produced a greater mission gain, with 9.5% more targets hit and 5% fewer MQ-99 lost, than RCS reduction, with 1% more targets hit and 9% fewer MQ-99 lost. Simulating proposed design changes can help decision-makers optimize their available resources.

At the mission engineering level, the same simulation data can be extended to compare platform and capability options across different scenarios. Analysts can assess how combinations of manned and unmanned assets, alternative communication architectures, or new electronic protection measures influence aggregate mission success in contested environments. In this scenario, adding four air-launched decoys was simulated, along with increasing the accuracy of the SDBs or reducing the SDB's RCS. On the mission engineering side, adding the air launched decoys was the clear winner, as it resulted in 12.5% more targets hit and 18% fewer MQ-99 lost. All of these excursions, while purely notional, illustrate the types of tradeoff analysis that can be done linking technical design choices directly to operational performance.

CONCLUSIONS

Mission-level simulation tools such as AFSIM provide significant potential for improving the evaluation of full-spectrum survivability. By integrating cyber, kinetic, electromagnetic, and directed-energy threats into a unified digital environment, AFSIM enables analysts to explore how combinations of threat domains interact to affect mission outcomes. A key technique in this approach is the systematic isolation of individual threat contributions, removing one threat at a time while holding the others constant, to quantify the marginal impact of each threat on overall mission success. This technique provides a transparent and repeatable framework for identifying dominant threat drivers and validating mitigation strategies.

This study illustrates that cyber survivability can be meaningfully measured within such a framework, provided that cyber attack mechanisms likelihoods are quantified and their system-level consequences are well understood. Translating cyber effects into concrete events such as degraded targeting, communications loss, or false fuel indications allows cyber survivability to be analyzed alongside traditional threat types. Doing so transforms cyber

The results of this type of analysis can also provide a quantitative foundation for supporting both systems engineering and mission engineering trade studies.

vulnerabilities from abstract qualitatively measured risks into quantifiable mission-relevant risk, consistent with other established survivability analysis methodologies, which enables program managers to make better systems and mission engineering decisions.

However, the utility of M&S-based assessments does depend on verification and validation. The fidelity of modeled outcomes must be supported by empirical evidence derived from cyber testing, cyber ranges, and large-force live-fly exercises. Such events provide the operational data necessary to calibrate attack probabilities, effect magnitudes, and behavioral responses within the simulation environment. Establishing repeatable, data-driven correlations between simulated EML and observed test and exercise outcomes is therefore an essential next step.

Future work should focus on implementing this approach on real systems. The systems that are most appealing are those that already have robust M&S built, as adding the cyber effects to existing mission models should be relatively easy and inexpensive compared to starting a new M&S effort. Ultimately, validated mission-level simulation can evolve into a quantitative engine for survivability evaluation, providing the DoD with a consistent, scalable means to assess and enhance system resilience across all threat domains. [ASJ](#)

ABOUT THE AUTHOR

Dr. William “Data” Bryant is a cyberspace defense and risk leader who is a Technical Fellow for Modern

Technology Solutions, Incorporated (MTSI). His diverse background in operations, planning, and strategy includes more than 25 years of service in the Air Force, where he was a fighter pilot, planner, and strategist. Dr. Bryant helped create Task Force Cyber Secure, served as the Air Force Deputy Chief Information Security Office, and helped to develop Aircraft Cyber Combat Survivability with Dr. Robert Ball. He holds multiple degrees in aeronautical engineering, space systems, military strategy, and organizational management and has authored numerous works on various aspects of defending cyber physical systems and cyberspace superiority.

References

- [1] 2022 National Defense Authorization Act, 118th Congress, §4172 (p. 2566) and §4173 (p. 2567).
- [2] Bryant, W. D., and R. Ball. “Developing the Fundamentals of Aircraft Cyber Combat Survivability.” Parts 1–4, *Aircraft Survivability*, spring 2020 (part 1), summer 2020 (part 2), fall 2020 (part 3), and spring 2021 (part 4).
- [3] Bryant, W., C. Fisher, D. Boseman, and J. Ivancik. “Digital Technology—A Universal Integrator—Enabling Full-Spectrum Survivability Evaluations.” *Naval Engineers Journal*, vol. 136, pp. 189–198, spring 2024.
- [4] Committee on National Security Systems. *Committee on National Security Systems (CNSS) Glossary*. CNSSI No. 4009, Washington, DC, p. 169, 2015.
- [5] Brown, A., W. Bryant, E. Moro, and M. Standard. “The Unified Risk Assessment and Measurement System (URAMS) Guidebook: Version 3.0.” Edited by W. Bryant, www.mtsi-va.com/weapon-systems-cybersecurity/, pp. 50–60, 2023.
- [6] Bryant, W. D. “Predicting Cyber Attack Probability Using Probabilistic Attack Trees.” *ITEA Journal of Test and Evaluation*, vol. 46, no. 4, December 2025.
- [7] Bryant, W. D. “The Unified Risk Assessment and Measurement System (URAMS) Guidebook: Version 2.0.” www.mtsi-va.com/weapon-systems-cybersecurity/, pp. 18–19, 2022.

EXCELLENCE IN SURVIVABILITY: WILLIAM “DATA” BRYANT

by Eric Edwards



Fighter pilot, academic, aerospace engineer, military planner, strategy leader, risk analyst, methodology, model developer, author, speaker, and cyber survivability pioneer—the survivability community is fortunate to include each of these titles among its membership rolls. Rarely, however, do they all belong to the same person. But then there's Dr. William Bryant. For more than 3 decades, Dr. Bryant—who is better known as “Data,” his former call-sign—has been supporting U.S. combat aviation mission effectiveness and weapon system survivability efforts with a unique toolset of operational experience, analytical acumen, innovative thinking, and collaborative information-sharing that has helped both planners and technologists better understand, prepare for, and excel in the ever-changing modern battlespace.

Most notably, in his current position as a Technical Fellow with Modern

Technology Solutions Inc. (MTSI), Data's been at the forefront of the survivability discipline's expansion into the uncharted skies of cyber warfare and full-spectrum system survivability. Thus, the Joint Aircraft Survivability Program Office (JASPO) is pleased to recognize Dr. Bryant for his ongoing Excellence in Survivability.

LAYING A STRONG FOUNDATION FOR SURVIVABILITY

Born in Escondido, CA, Data began his aviation career with more than 25 years of active-duty service in the U.S. Air Force. After he graduated from the U.S. Air Force Academy in 1993 with a degree in aeronautical engineering, his first “office” was the cockpit of an F-16 Viper. As a pilot, he gained invaluable first-hand experience with advanced combat aircraft technologies, tactics, and operations in the skies over Japan, South Korea, Iraq, and multiple U.S. Air Force bases. He would also add the title of flight instructor and evaluator, squadron commander, national-level operations planner and strategist, and senior cyber leader to his long list of operational assignments. Collectively, these assignments would lay a strong foundation for his eventual, holistic understanding of the battlespace, air operations, and the many threat types that challenge modern mission assurance.

Additionally, during his tenure at the Pentagon as the Deputy Director of the Air Force's Task Force Cyber Secure, Data led efforts to identify and close cyber vulnerabilities across operational technology (OT) and weapons systems. Recognizing the lack of centralized cyber defense for these critical assets, Data successfully advocated for and helped stand up the Air Force Chief Information Security Officer (CISO) office, which has become central to the Air Force's cyber strategy and implementation. Then, as the Air Force's Deputy CISO, Data also

Data has been at the forefront of the survivability discipline's expansion into the uncharted skies of cyber warfare and full-spectrum system survivability.

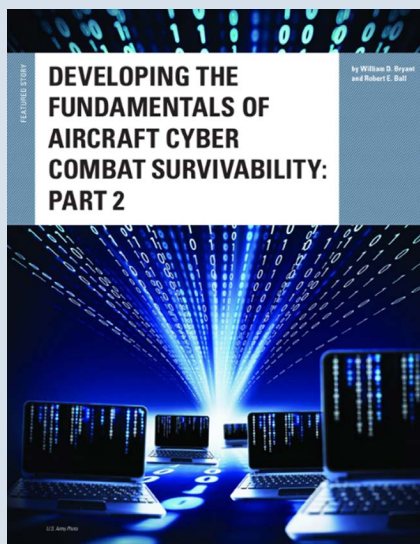


developed a strategic risk management framework tailored to cyber-physical systems, implemented new processes to enable secure agile development, and championed the integration of cyber-security into weapons system acquisition life cycles. Under his leadership, the Air Force deployed numerous new active defenses for OT systems, ultimately preventing multiple real-world cyber attacks that could've degraded mission readiness.

ESTABLISHING A NEW DISCIPLINE: CYBER COMBAT SURVIVABILITY

As his career progressed, Data also began to recognize a gap between traditional survivability models—focused largely on kinetic threats—and the emerging spectrum of nonkinetic threats, including software-driven threats that exploit vulnerabilities in networks, code, and digital infrastructure. Thus, he joined forces with aircraft survivability pioneer and long-time educator Dr. Robert Ball to co-develop the Aircraft Cyber Combat Survivability (ACCS) framework. The framework leverages the familiar, established Aircraft Combat Survivability (ACS) constructs of susceptibility, vulnerability, and recoverability but expands and adapts them to the cyber domain, offering a structured approach to assess and improve a system's ability to survive in a contested cyberspace environment. This groundbreaking work has been instrumental in helping to usher the survivability community into the full-spectrum survivability era.

Notably, Data has also worked to ensure that ACCS is not just a theoretical construct but can be used as a practical tool to inform design and testing decisions for current and future air



Data has worked to ensure that ACCS is not just a theoretical construct but can be used as a practical tool to inform design and testing decisions for current and future air platforms.

platforms. As detailed in the influential four-part series that Data and Dr. Ball authored for the *Aircraft Survivability* journal in 2020 and 2021, the ACCS's mapping of cyber risk to mission impact gives program managers and engineers actionable insights during the requirements generation, architecture selection, and verification planning processes. Accordingly, the framework continues to be widely discussed and adopted across the survivability engineering enterprise.

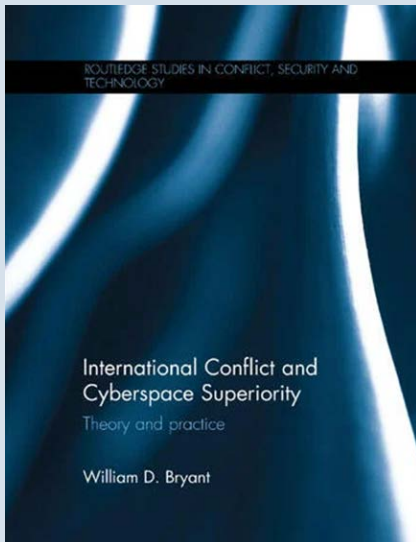
QUANTIFYING RISK AND INTEGRATING FULL-SPECTRUM ASSESSMENT

Another framework that Data envisioned and created was the Unified Risk

Assessment and Measurement System (URAMS). URAMS brings scientific rigor to the challenge of cyber risk assessment in complex cyber-physical systems using multiple analytical and risk measurement tools. It combines probabilistic modeling, model-based systems engineering, and scenario-based simulation to evaluate cyber risk at the mission level. Extending beyond just compliance checklists, the system enables program offices, testers, and acquisition decision-makers to understand not just whether a system meets security controls but how those controls affect mission effectiveness in the face of cyber threats. To do this, it incorporates probabilistic attack trees, mission-level simulation, and data-driven scoring to quantify risk exposure, giving stakeholders a defensible basis for engineering trade-offs and mitigation investments.

What makes Data's survivability- and cyber-related contributions especially remarkable is the extent of their scope and integration. Rather than siloing cyber survivability as a niche function, he has consistently argued—and demonstrated—that true survivability requires a full-spectrum view, considering not just physical destruction but also digital degradation, electromagnetic interference, supply chain attacks, and insider threats. To that end, he's been heavily involved in the development and maturation of full-spectrum survivability analysis, a unified approach that considers the interplay of current and emerging kinetic and nonkinetic threats across all domains. This unification helps ensure that no critical mission vulnerabilities are missed by traditional "stovepiped" security disciplines.

Data has also long emphasized that systems must be designed, tested, and



URAMS brings scientific rigor to the challenge of cyber risk assessment in complex cyber-physical systems using multiple analytical and risk measurement tools.

fielded with survivability in mind, not added later as an afterthought—an emphasis that, incidentally, mirrors that of the early pioneers of the survivability discipline itself. He has thus also worked closely with the Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E) and the Director of Operational Test and Evaluation (DOT&E) to develop numerous policies, roadmaps, and test and evaluation strategies that reflect this important view of survivability.

GAINING AND SHARING KNOWLEDGE

Not surprisingly, Data's record of academic accomplishments is just as long and impressive as that of his

professional ones. In addition to his previously mentioned bachelor's degree in engineering from the Air Force Academy, he was a distinguished graduate of the Squadron Officer School, he earned five master's degrees from five different schools (in the areas of military studies, organizational management, space systems, airpower art and science, and strategic studies), and he completed a doctorate in military strategy from the Air University's School of Advanced Air & Space Studies. In addition, he holds multiple professional certifications, including CISSP, C|EH, and Security+.

That said, Data has also recognized the importance of not only acquiring knowledge and expertise but also sharing that knowledge and expertise with others. He's thus been a prolific writer and speaker, authoring more than 20 peer-reviewed articles, conference papers, and book chapters, as well as serving as a frequent contributor in technical journals such as *Aircraft Survivability*, *ITEA Journal of Test and Evaluation*, *Strategic Studies Quarterly*, *Joint Forces Quarterly*, and the *Air & Space Power Journal*. Moreover, his book *International Conflict and Cyberspace Superiority* remains a ground-breaking text in the field of cyber superiority.

In addition, Data serves as a regular presenter at survivability conferences, as a guest lecturer at defense graduate schools, as a coach and mentor for acquisition professionals looking to better understand cyber risk and defense, and as a consultant to the Air Force Scientific Advisory Board.

Finally, though Data says he doesn't really have any "hobbies" outside of work—and it doesn't sound as if he has

time for any—he does enjoy spending time with his wife of 32+ years and their three children, especially hiking and exploring various national, state, and local parks.

Congratulations, Data, on this well-deserved award and thank you for your past and present contributions and leadership to the aircraft survivability community and the U.S. Warfighter!

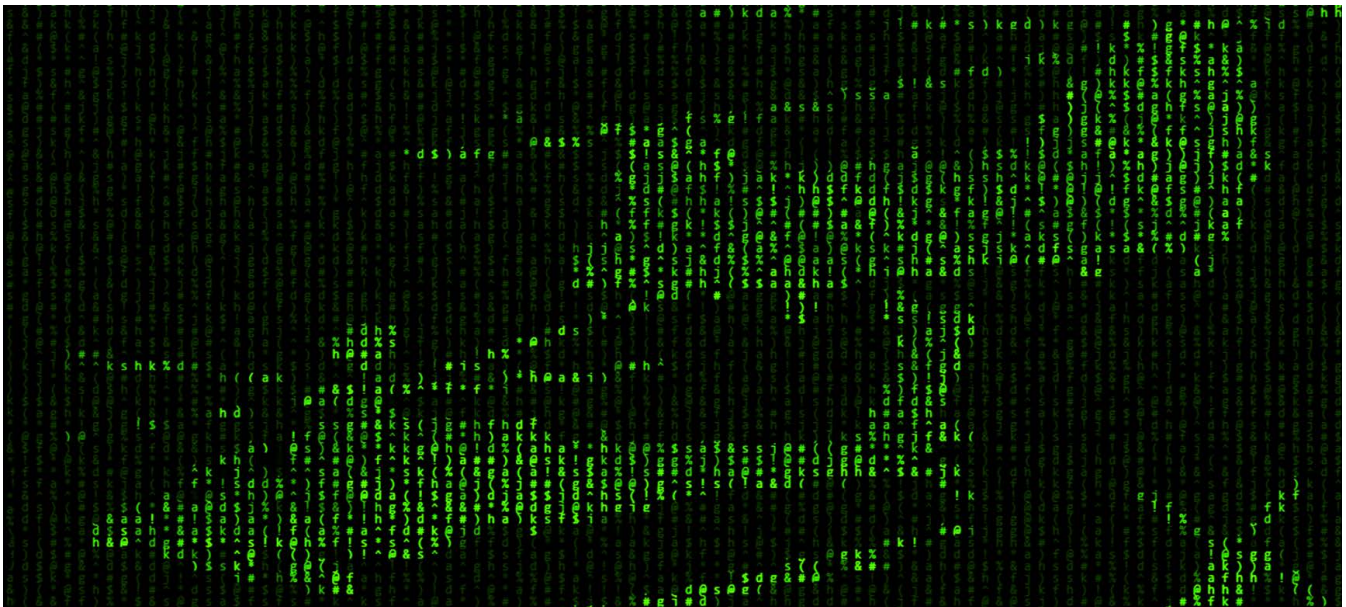
NOTE: ChatGPT was used to assist in the development of this article.

IN SEARCH OF EXCELLENCE

We're always on the lookout for deserving candidates to recognize for their Excellence in Survivability. If you have a colleague who has made important technical or leadership contributions in the field and you'd like to submit his/her name for consideration, please visit jasp-online.org/stay-connected.

THE ARMY AVIATION CYBER INCIDENT RESPONSE TEAM: WHAT DO WE DO AFTER A CYBER ATTACK?

by Tom Barnett



Cyber attacks are threats that target the combat system’s infrastructure with impacts realized at the mission level. While today’s military aircraft were built to be safe, airworthy, reliable, and survivable, they were not designed with cyber threats in mind. Thus, over the past decade, the U.S. military has spent an inordinate amount of time and treasure attempting to address these cyber threats. Countless dollars have been poured into cybersecurity to achieve Authority to Operate, cyber testing to assess systems for weaknesses, and Defensive Cyber Operations to monitor and protect networks from bad actors. While these efforts have undoubtedly helped improve the cyber posture of legacy systems that were not designed to withstand cyber threats, they haven’t sufficiently answered the question, “What do we do *after* a cyber attack?” Accordingly, this article discusses the mission, development, and activities of the Army Aviation Cyber Incident Response Team (AA-CIRT), which was established to help address this question.

FOCUS ON SURVIVABILITY

In the military aviation domain, as with all weapon systems, survivability is paramount. This is why the Joint Requirements Oversight Council mandated inclusion of the System Survivability Key Performance Parameter (SSKPP) into the requirements for all manned systems. While the survivability community has historically focused on kinetic threats, the ability to avoid or withstand nonkinetic threat types, such as cyber and electromagnetic spectrum, has also become increasingly recognized as an important consideration for full-spectrum survivability. This realization led the Joint Staff J6 to develop the Cyber Survivability Endorsement (CSE) to the SSKPP, which broadly aligns cyber survivability with the fundamental tenets of system survivability (as shown in Figure 1). The J6 office published this guidance in the Cyber Survivability Endorsement Implementation Guide (CSEIG) [1]. (For more background/details on the CSE, see Mr. Steve Pitcher’s article in the fall 2022 issue of Aircraft Survivability [2].)

Because cyber is assessed as part of the SSKPP, we have adopted the traditional pillars of **Prevent**, **Mitigate**, and **Recover** (as shown in the familiar “survivability onion” in Figure 2). The CSEIG also added a fourth pillar—**Adapt**—which is particularly relevant to cyber survivability. Currently, as a general rule for aircraft, prevention activities in the cyber domain happen *before* the mission, mitigation activities happen *during* the mission, and recovery and adaptation activities happen *after* the mission. Cybersecurity activities are primarily geared toward preventing cyber attacks. The pilot and crew can attempt to mitigate system-level effects during the mission, if possible.

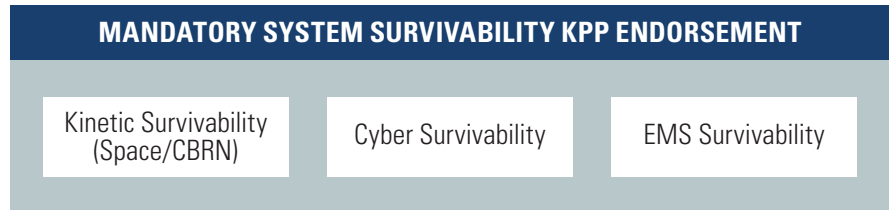


Figure 1. SSKPP Required Endorsements.

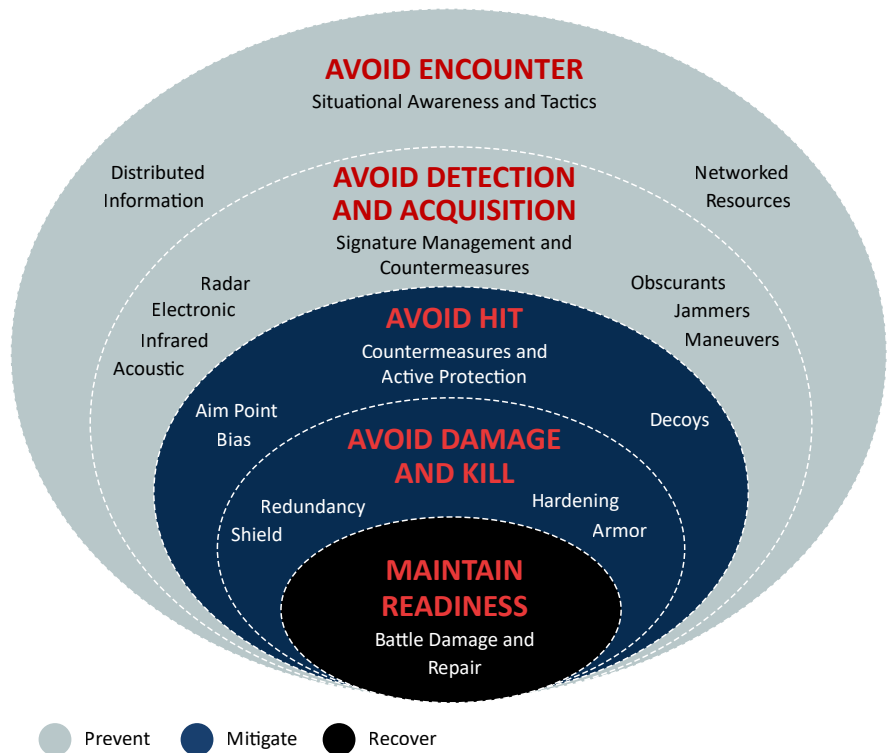


Figure 2. The Survivability Onion.

Recovery and adaptation tend to be executed at maintainer level to restore mission readiness.

THE NEED FOR CYBER INCIDENT RESPONSE

While aircraft structural/mechanical and safety-related status is routinely monitored and evaluated by maintenance teams to maintain readiness, damage due to hostile acts must be viewed through a different lens. This is where the Joint Combat Assessment Team (JCAT) contributes to aircraft survivability. When combat damage occurs, JCAT assesses this damage to determine the likely chain of events that

led to the damage. The team collects significant amounts of data and performs forensic analysis to establish threat parameters, damage to the platform and subsystems, and interactions with countermeasures, if any. The goal is to reconstruct the incident to determine how to adapt the fleet to the operational environment and threat capabilities going forward.

A similar approach is needed when the threat “weapon” is cyber. Cyber attacks can cause system failures or erratic behavior that may affect performance, mission effectiveness, and survivability. As such, we need a mechanism to perform the forensics to understand the event and provide a feedback loop to

the system owner in much the same way that JCAT does for other types of damage. And because cyber effects often resemble reliability failures, pilots, crew chiefs, and maintenance technicians need to consider cyber as a potential cause of failures or abnormal behavior. To meet this need for Army aircraft and related systems, the Capability Program Executive (CPE) Aviation established the AA-CIRT.

AA-CIRT REQUIREMENT

In 2019–2020, the Headquarters Department of the Army (HQDA) G-3/5/7 and the Assistant Secretary of the Army for Acquisition, Logistics, and Technology worked across the Army to establish the requirements and equities associated with responding to cyber attacks on weapon systems. This work resulted in HQDA Execution Order (EXORD) 251-20, titled Program Mission Assurance Weapon System (CYBER) Incident Response Plan [3], the purpose of which was to establish a standardized response and reporting process and to ensure all stakeholders understand and meet their responsibilities related to cyber incidents on weapon systems. In response to this HQDA EXORD, as well as language in the FY23 National Defense Authorization Act (NDAA)

Because cyber effects often resemble reliability failures, pilots, crew chiefs, and maintenance technicians need to consider cyber as a potential cause of failures or abnormal behavior.

Section 1559 [4], CPE Aviation initiated planning and coordination for AA-CIRT. Under this effort, a draft Concept of Operations (CONOPS) was developed to align CPE Aviation roles and responsibilities with stakeholders throughout the Army. The Joint Aircraft Survivability Program Office (JASPO) then expanded the scope with a requirement to synchronize this approach across the Services.

AA-CIRT VISION

The overall objective of AA-CIRT is to increase aircraft survivability through development of rapid response capabilities for suspected cyber attacks on aircraft and associated ground support equipment. The prospective end state is to field a mature cyber incident response and triage capability for aviation systems that leverages JCAT kinetic threat incident evaluations and provides coordination of platform and cyber subject-matter expertise to mitigate effects and recover operational readiness. As important as it is to respond to specific exploits, the feedback into the operational and acquisition communities is even more so. This is why, much like JCAT, AA-CIRT provides critical data and expertise to enable near- and long-term doctrine, organization, training, materiel, leadership and education, personnel, and facilities solutions.

DEVELOPMENT APPROACH

Rather than initiate a standalone process, AA-CIRT planners chose to closely integrate with existing JCAT, maintainer, and safety teams and processes; cyber assessment and testing capabilities within the CPE Aviation community; and Joint partners

in the Air Force and Navy to establish a comprehensive mechanism for responding to malicious cyber activity affecting aircraft operational technologies. Beginning with the Aviation Survivability Development and Tactics (ASDAT) team at Fort Rucker, AL—the Army’s instantiation of JCAT—the first priority was to align with, and adapt where necessary, the procedures laid out in the JCAT Pocket Guide [5]. This included update of the ASDAT Intelink site for incident reporting. Because the ASDAT team is a primary provider of course materials to the U.S. Army Aviation Center of Excellence (USAACE), AA-CIRT materials and aircraft cyber effects in general are being added into the “schoolhouse” curriculum for pilots and maintainers.

We also reached out to our Joint partners at the Naval Air (NAVAIR) Warfare Center Aircraft Division, at Patuxent River, MD, to collaborate with their Cyber Protection and Response Center and Aviation Cyber Forensics Lab. Our counterpart in the Air Force is the Cyber Resiliency Office for Weapon Systems (CROWS), at Wright-Patterson AFB, OH. Both organizations had received a similar requirement for aircraft cyber incident response and have capabilities and CONOPS at various levels of maturity. These collaborations proved to be extremely valuable.

Next, we surveyed weapon system and cyber expertise locally at Redstone Arsenal, AL. CPE Aviation provided leadership and resourcing from across the Office of the Chief Scientist, the Assistant CPE Engineering and Architecture, and the Office of the Chief Information Officer (OCIO). In addition, JASPO provided resourcing, direction, and coordination. The DEVCOM Aviation and Missile Center (AvMC) provided cyber engineering, aviation

data bus penetration testing expertise, and cyber threat analysis capabilities. The Redstone Test Center (RTC) supplied aircraft and cyber testing and instrumentation expertise, as well as world-class facilities (via the Aviation Flight Test Directorate), aircraft maintainers, and test pilots. In addition, the Aviation and Missile Command G2 office provided cyber intel analysts, and contractor partners across all these organizations were also instrumental to the work's success.

PROGRAM PHASES

CPE Aviation and JASPO also cochaired a monthly AA-CIRT Working Group to maintain an operational tempo and collaboration. Under the group's auspices, the effort was executed across the following three phases.

Phase 1: Planning, Tool Development, and Lab Testing

The first phase consisted of early planning and coordination among the various stakeholders, development of specialized tools to support forensic investigation, and testing in an aircraft system integration lab (SIL). Early efforts also included decomposing the Army EXORD, establishing roles and responsibilities among the stakeholders and team members, and drafting an initial AA-CIRT CONOPS, which included the basic team structure and external interactions, consistent with the Army EXORD. There were also early interactions with our NAVAIR and CROWS counterparts to benefit from their early lessons learned.

Recognizing the relatively unsecure nature of the MIL-STD-1553b data bus (pictured in Figure 3) and the lack of related data collection, the team leveraged its penetration testing and instrumentation expertise to develop several forensic tools for Army aircraft.

The first tool, developed by DEVCOM AvMC was a plug-in to its Common Bus Assessment Tool (ComBAT) (pictured in Figure 4). ComBAT has been used for aircraft cyber testing for years, but this effort added a device fingerprinting capability to help identify rogue terminals (leave-behind or otherwise compromised) masquerading as valid bus participants. Because each device has unique characteristics, such as waveform and response timing, the AvMC experts automated the capability to measure, capture, and distinguish



Figure 3. Typical MIL-STD-1553b Data Bus Traffic.

ComBAT has been used for aircraft cyber testing for years, but this effort added a device fingerprinting capability to help identify rogue terminals (leave-behind or otherwise compromised) masquerading as valid bus participants.

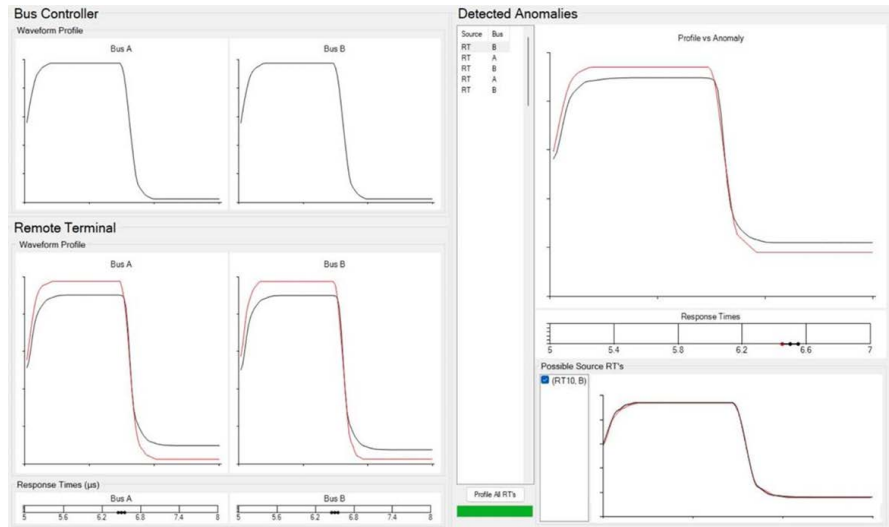


Figure 4. Plug-In Signal Captures.

these features for use in cyber incident response.

Next, because of the highly consistent nature of the MIL-STD-1553b data bus, the RTC team developed a message visualization tool—Greenlister—to allow an operator to quickly identify unexpected and invalid messages transmitted on a bus. As shown in Figure 5, the Greenlister tool augments the Cybersecurity Vulnerability Assessment Test Environment (CVATE), serving as a quick-look capability to analyze bus behavior to identify where deep-dive forensics may be needed.

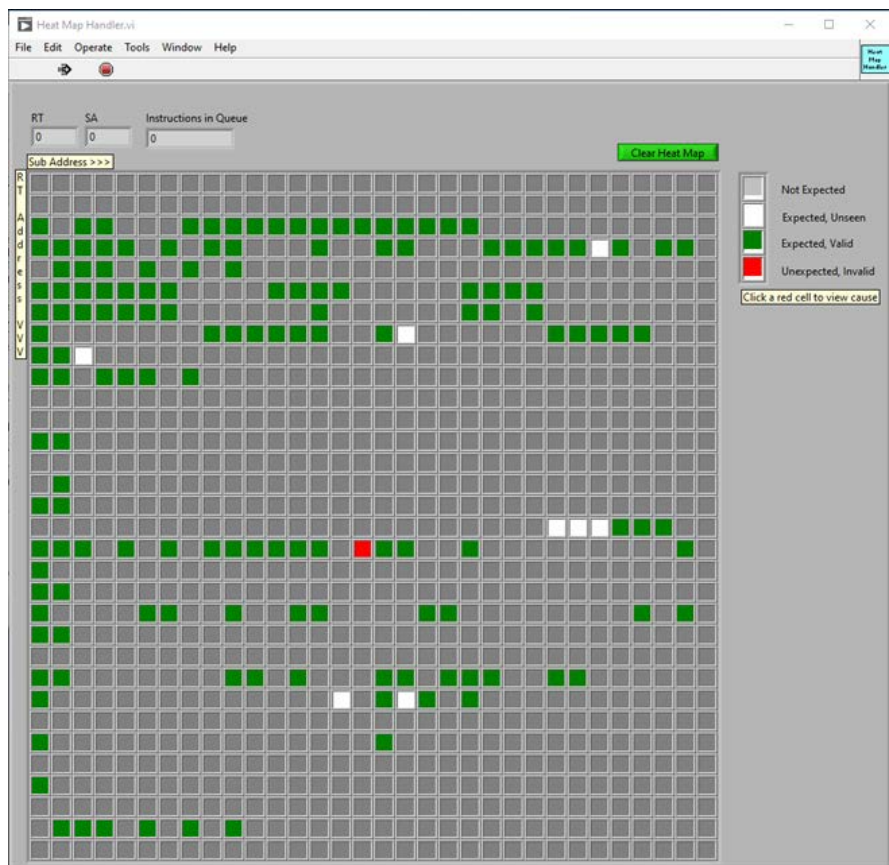


Figure 5. CVATE Greenlister Bus Traffic Display.

These tools and others were used during the first AA-CIRT Exercise in September 2023 at the CH-47F SIL in the CPE Aviation Enterprise Portfolio Integration and Conformance Center (formerly the Combat Aviation Brigade Architecture Integration Lab). This exercise allowed AA-CIRT stakeholders and technical experts to respond to a limited set of injected MIL-STD-1553b cyber effects alongside platform experts, pilots, crew, and ASDAT representatives. It also demonstrated the AA-CIRT tool set in a realistic system environment and served as the culmination of AA-CIRT Phase 1 activities.

The Phase 1 capabilities and accomplishments were demonstrated at the October 2023 Aviation Cyber Initiative (ACI) Cyber Rodeo at Redstone Arsenal, AL, to more than 160 attendees from across the U.S. Departments of War, Transportation (specifically the Federal Aviation Administration), and Homeland Security, as well as industry and

academia. In an attempt to raise awareness of cyber effects on military aircraft and to socialize the Phase 1 capabilities to the broader survivability and operational community, AA-CIRT was also presented at the 2024 Threat Weapons & Effects (TWE) Symposium at Eglin Air Force Base, FL.

Phase 2: CONOPS Development, Validation, and Live Testing

During the recently completed second phase, the AA-CIRT team formalized the CONOPS processes and interactions and coordinated closely with the ASDAT team at Fort Rucker and the U.S. Army Cyber Command (ARCYBER) at Fort Gordon, GA.

As shown in Figure 6, the AA-CIRT CONOPS was updated to include detailed incident resolution and reporting interactions, as well as an end-to-end process sequence among the stakeholders and participants. The focus of this CONOPS is exclusively on Aviation platforms, systems, and associated ground support equipment (i.e., “the aircraft and anything that plugs into the aircraft”). The AA-CIRT team coordinated the codified CONOPS processes, roles, and responsibilities with the ARCYBER Information Warfare Operations Center to maintain consistency with its Crisis Action Team Standard Operating Procedures. The JCAT Pocket Guide [5] was also updated to consider cyber as an option during initial event analysis.

The CONOPS established the Cyber Incident Coordination Cell (CICC) to be the “face of AA-CIRT” to the community and the clearinghouse for event management and internal and external reporting. The CICC is also responsible for coordination with system owners and program office(s) and all relevant stakeholders.

For instances where a cyber incident cannot be resolved by preliminary analysis and mitigations, the CONOPS established the Cyber Incident Response Team (Cyber IRT) to perform event triage and categorization, perform detailed

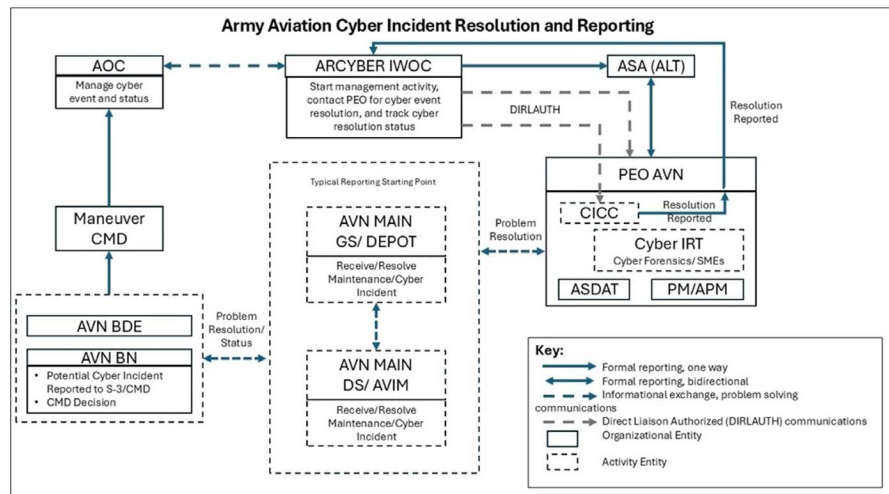


Figure 6. AA-CIRT Interaction Diagram.

forensics to determine root cause, recommend system and process modifications, and support the unit in returning the affected systems to operational status. To staff this team, penetration testers from the AvMC Cyber Threat Assessment Team (CTAT) were tapped due to their detailed knowledge of vulnerability assessments on Army aircraft. To successfully execute this mission, the Cyber IRT must maintain close coordination with ASDAT/JCAT, maintenance and safety teams, and program office subject-matter experts.

The CONOPS also includes multiple appendices with fillable forms for data collection and coordination, helpful lists, frequently asked questions, formats for response plans, and reporting throughout all phases of an incident.

Phase 2 culminated with an exercise on a live CH-47F aircraft in simulated flight at the Aviation System Test and Integration Lab at the Redstone Arsenal Airfield. The purpose of this event was to verify and refine the AA-CIRT CONOPS and to exercise the Cyber IRT on a multifaceted exploit that, while benign in impact, required multiple forensics steps and relied on skillsets

across cyber, engineering, hardware, and software domains. This event brought together all CICC stakeholders, Cyber IRT members, program office system engineers and cyber leads, maintenance teams and test pilots, and ASDAT representatives to collectively trace a potential cyber effect from initial pilot reporting, through unsuccessful maintenance attempts, and through multiple onboard and offboard devices and networks. The RTC team developed the novel exploit and built the entire test scenario to be as realistic as possible. The AvMC CTAT team successfully traced the problem “inside out” to find the specific attack surface, attack path, and root cause of the anomaly; removed the offensive software; and returned the affected systems to working order.

Phase 3: Program Documentation, Process Socialization Across the Joint Community, and Coordination With Service Cyber Commands

During the current third phase, the team refined the AA-CIRT CONOPS based on Exercise #2, particularly the appendices, and delivered the Army Aviation Cyber Incident Analysis and Reporting Methodology document to JASPO [6].

The next step for the AA-CIRT CONOPS will be publication through the formal CPE Aviation process.

To socialize the AA-CIRT processes, roles, and responsibilities within CPE Aviation, the team engaged the cyber leads across all aviation program offices to introduce the CONOPS and discuss program accomplishments and the path forward, including an update of all cyber incident response plans to align with AA-CIRT and Army policy. Once this activity is complete, it will supplement Risk Management Framework packages with technical details valuable to Cyber IRT. An example would be Cyber Attack Path Analysis diagrams, which serve as a “cyber roadmap” for our aircraft. There will also be follow-up sessions with the program office engineering teams, as they will be critical to resolving any cyber incident affecting their platforms and systems.

AA-CIRT will continue to maintain coordination and reporting mechanisms with ARCYBER, as well as our Navy and Air Force counterparts and their respective Service cyber commands. The team will also continue to work closely with JASPO and JCAT to develop and implement processes consistent with existing incident response tactics, techniques, and procedures (TTPs). Through the Army ASDAT team, we will provide input to USAACE curricula, including the Fundamentals of Aviation Combat Survivability Course.

In addition, per the age-old Army saying—“you fight the way you train”—we will plan future exercises as testing opportunities present themselves, with the goal of integrating cyber incident response exercises with

routine cyber developmental and operational testing (DT/OT), where feasible and approved.

Finally, it will continue to be important to establish feedback mechanisms with the acquisition, operational, and intelligence communities (incident details and recommendations for mitigations and/or requirements and training) to inform the community of threat TTPs and to ensure that our systems are strengthened and protected against future cyber attacks.

CONCLUSION

While the AA-CIRT mission seems straightforward, cyber incident response for aircraft systems is an area that, until recently, has been largely unaddressed. Only in the past 6–8 years have we begun to see policies requiring cyber incident response for weapon systems and recognized the need for the unique skillsets and collaborations necessary to respond when called. As discussed, the AA-CIRT effort has been a coalition of organizations across the Army Aviation and Joint communities to stand up a new capability to respond to cyber incidents impacting Army aircraft. Inspired by the experts within the JCAT and Safety Center communities—and their “all hands on deck” approach to aircraft incidents—the AA-CIRT team hopes to bring the same level of expertise and professionalism when the root cause of those incidents is cyber in nature. In the end, regardless of the type of threat weapon that caused the failure, the ultimate goal is to return the aircraft to an operational state and to improve survivability for future missions. **ASJ**

ABOUT THE AUTHOR

Mr. Tom Barnett is the Cyber Engineering Lead for the Assistant Capability Portfolio Executive Aviation for Engineering & Architecture, as well as a Cyber Technology Principal Investigator and subject-matter expert for the Combat Capabilities Development Command Aviation and Missile Center, where he established the Cyber Technology Area within the Missile Science and Technology portfolio. With approximately 40 years of systems engineering experience in cyber resiliency, system of systems hardware-in-the-loop and all-digital constructive simulations, radar and infrared sensors, integrated air and missile defense, and short-range air defense, Mr. Barnett also serves as the Technical Director for the Aviation Cyber Initiative (ACI) Cyber Rodeo series and is the Director of the annual ACI Cyber Rodeo-Redstone. He holds a bachelor’s degree in electrical engineering from Christian Brothers University.

References

- [1] Joint Staff/J6. *Cyber Survivability Endorsement Implementation Guide*. Version 3, Deputy Director for Information Warfare Requirements Division, July 2022.
- [2] Pitcher, Steve. “DoD Systems Need Cybersecurity and Cyber Resiliency to Achieve Cyber Survivability.” *Aircraft Survivability*, fall 2022.
- [3] Headquarters, Department of the Army. “Program Mission Assurance Weapon System (CYBER) Incident Response Plan.” HQDA Execution Order 251-20, 31 July 2020.
- [4] “James M. Inhofe National Defense Authorization Act for Fiscal Year 2023.” Section 1599, 2022.
- [5] Joint Combat Assessment Team. *JCAT Pocket Guide*. 1 January 2025.
- [6] U.S. Army Aviation Cyber Incident Response Team. “Army Aviation Cyber Incident Analysis and Reporting Methodology.” To be published.

CALENDAR OF EVENTS

MARCH

12th Joint Space Operations Summit

4–5 March in Oxon Hill, MD
<https://space.dsigroup.org/>

2026 IEEE Aerospace Conference

7–14 March in Big Sky, MT
<https://aiaa.org/events/2026-ieee-aerospace-conference/>

2026 Pacific Operational Science & Technology (POST) Conference

9–13 March in Honolulu, HI
<https://www.postconference.org/>

AIAA DEFENSE Forum 2026

17–20 March in Laurel, MD
<https://defense.aiaa.org/>

2026 Munitions Executive Summit

17–18 March in Parsippany, NJ
<https://www.ndia.org/events/2026/3/17/munitions-executive-summit>

APRIL

2026 MSS Active E-O Systems Symposium

6–10 April in Springfield, VA
<https://www.mssconferences.org/public/meetings/conferenceDetail.aspx?enc=6MzjytLmMAP3b02RW Ej7%2bQ%3d%3d>

High-Speed/Hypersonic Subarea of the Air Platforms Community of Interest Technical Roadmap Interchange Meeting 2026

15–16 April in Washington, DC
<https://dsiac.dtic.mil/events/high-speed-hypersonic-subarea-of-the-air-platforms-community-of-interest-technical-roadmap-interchange-meeting-2026/>

Simulation & Training Community Forum

22 April in Dayton, OH
<https://www.ntsaa.org/events/2026/4/22/stcf-2026>

MAY

NDIA Air Combat Survivability Division Multi-Systems Survivability Workshop

5–6 May at Wright-Patterson AFB, OH
<https://ndia.org/events>

Vertical Flight Society's FORUM 82

5–7 May in West Palm Beach, FL
<https://vtol.org/forum-and-events/annual-forum-and-technology-display/annual-forum-and-technology-display>

2026 Department of the Air Force Modeling & Simulation Summit

5–8 May in Colorado Springs, CO
<https://www.dafmss.org/>

JCAT Threat Weapons Effects Training

12–14 May at Eglin AFB, FL
<https://www.jasp-online.org/events/>

ASCEND 2026

19–21 May in Washington, DC
<https://www.ascend.events/>

JUNE

Aircraft Combat Survivability Short Course

2–4 June in Hartford, CT
<https://dsiac.dtic.mil/events/aircraft-combat-survivability-short-course-acssc-2026>

2026 International Powered Lift Conference

2–4 June in West Palm Beach, FL
<https://aiaa.org/events/2026-international-powered-lift-conference-iplc/>

Space Tech Expo

2–4 June in Anaheim, CA
<https://www.spacetecheexpo.com/anaheim>

AIAA AVIATION Forum 2026

8–12 June in San Diego, CA
<https://aiaa.org/aviation>

Training & Simulation Industry Symposium (TSIS) 2026

17–18 June in Orlando, FL
<https://www.ntsaa.org/events/2026/6/17/tsis-2026>

JASP Model Users Meeting

23–25 June at Offutt AFB, NE
<https://dsiac.dtic.mil/events/joint-aircraft-survivability-program-jasp-model-users-meeting-jmum-2026/>

JULY

Capitol Hill M&S Expo 2026

10 July in Washington, DC
<https://www.ntsaa.org/events/2026/7/10/capitol-hill-expo-2026>

ATTENTION: *Due to an increase in event postponements and cancellations associated with recent changes in DoW travel requirements, readers are encouraged to double-check with event sponsors and websites to confirm the status of an event before making final travel plans and reservations.*

The inclusion of an event in this calendar does not necessarily reflect the endorsement of that event or its sponsoring organization(s) by the Joint Aircraft Survivability Program Office.

To submit a relevant event for a future Calendar of Events or to update your mailing address, please visit jasp-online.org/stay-connected.

