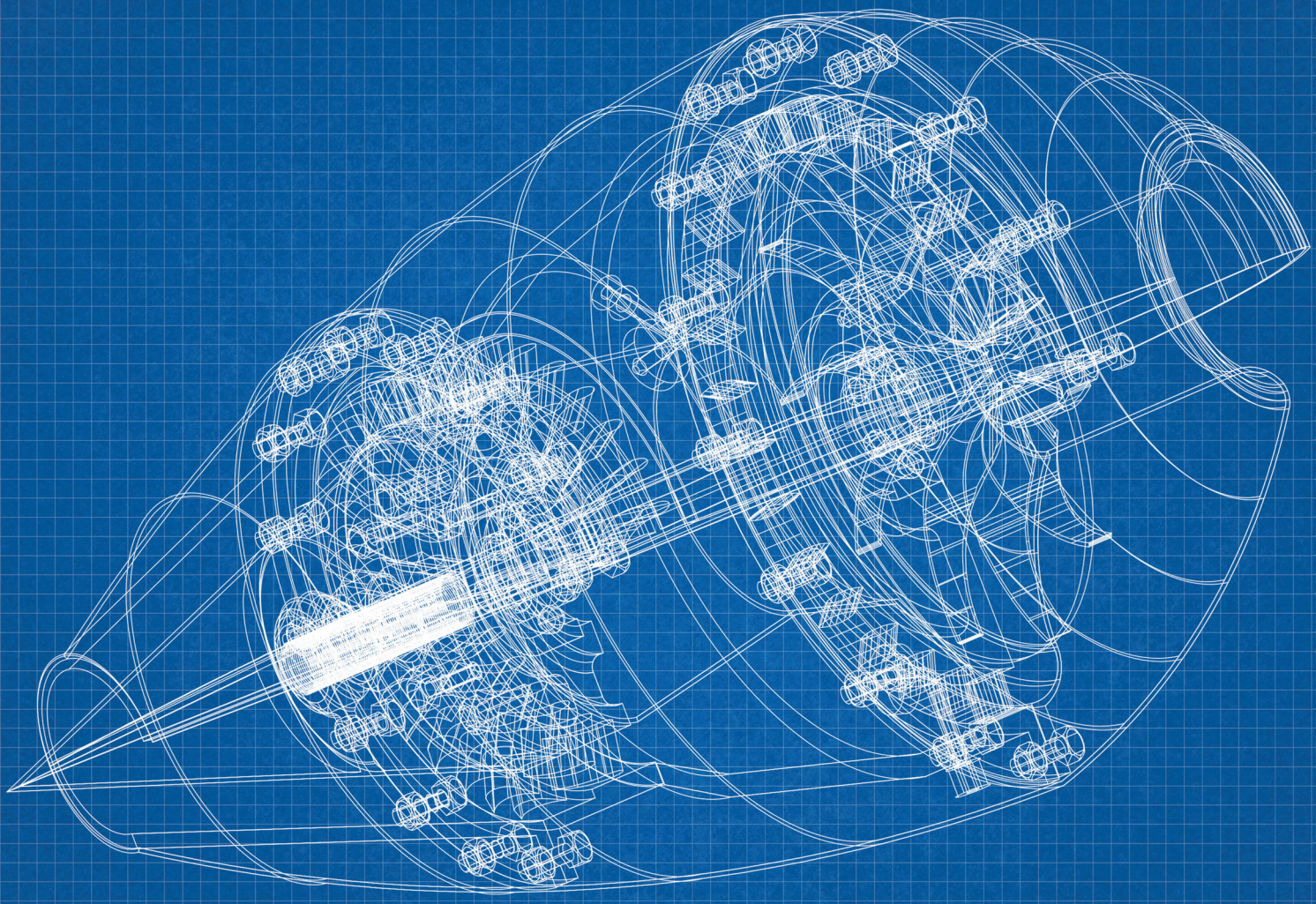
Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

THALES

MISSION RESILIENCE:
Adapting Defense Aerospace to Evolving Cybersecurity Challenges



Simon Handler, Trey Herr, Steve Luczynski, and Reed Porada

CYBER STATECRAFT
INITIATIVE

RESILIENCE

Scowcroft Center for Strategy and Security

*The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.*

Cyber Statecraft Initiative

*The **Cyber Statecraft Initiative** works at the nexus of geopolitics and cybersecurity to craft strategies to help shape the conduct of statecraft and to better inform and secure users of technology. This work extends through the competition of state and non-state actors, the security of the internet and computing systems, the safety of operational technology and physical systems, and the communities of cyberspace. The Initiative convenes a diverse network of passionate and knowledgeable contributors, bridging the gap among technical, policy, and user communities.*

Supported By

This report was produced as part of the Cyber Statecraft Initiative's work on resilience and aerospace cybersecurity with support from Thales. Thales is a global leader in new technologies for the aerospace, space, defense, security and transportation markets.

Intellectual Independence

The Atlantic Council and its staff, fellows, and directors generate their own ideas and programing, consistent with the Council's mission, their related body of work, and the independent records of the participating team members. The Council as an organization does not adopt or advocate positions on particular matters. The Council's publications always represent the views of the author(s) rather than those of the institution.

The Atlantic Council maintains strict intellectual independence for all of its projects and publications. Council staff, fellows, and directors and those who the Council engages to work on specific projects, are responsible for generating and communicating intellectual content resulting from Council projects. The Council requires all donors to agree to the Council maintaining independent control of the content and conclusions of any products resulting from sponsored projects. The Council also discloses sources of financial support in its annual reports to ensure transparency.

Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

CYBER STATECRAFT
INITIATIVE

MISSION RESILIENCE:
Adapting Defense Aerospace to Evolving Cybersecurity Challenges

Simon Handler, Trey Herr, Steve Luczynski, and Reed Porada

ISBN-13: 78-1-61977-174-1

Cover: Plane engine architect blueprint. Credit: iStockphoto/Jelena83

May 2021

Table of Contents

Executive Summary

Mission resilience, defined as the ability of a mission system to prevent, respond to, and/or adapt to disruption, is a critical attribute for defense aerospace systems. No software-intensive system, even in space, is immune to disruption. The consequences of abrupt and unexpected failure, whether caused by enemy action or error, could be widespread and meaningful. Defense organizations must prioritize the capacity to limit harm and gracefully overcome failures when they inevitably do occur in aerospace systems. These systems represent some of the United States' and its allies' most expensive and advanced capabilities, and as such, adversaries are keen to exploit their cybersecurity vulnerabilities for strategic gain. However, issues ranging from faulty acquisition practices to a failure-fearing organizational culture have plagued the US Department of Defense (DoD) and hindered its ability to develop and maintain resilient systems.

This report examines four practice areas for collaboration between the private sector and government across the defense aerospace community: fail open, segment systems, expand simulations and twinning, and speed your change. The practice areas introduced in this report each build off of a general principle of mission resilience outlined in the Atlantic Council and MIT Lincoln Laboratory's *How Do You Fix a Flying Computer?* report to present tailored recommendations, directly applicable to improving resilience for defense aerospace systems.[1] The operational environments in which aerospace systems operate present some inherently unique cybersecurity challenges for the defense community, but by adapting practices utilized by certain high-performing private sector firms, the DoD can adapt them to further its own pursuit of mission resilience.

1 Trey Herr, Reed Porada, Simon Handler, Orton Huang, Stewart Scott, Robert Lychev, and Jeremy Mineweaser, *How Do You Fix a Flying Computer? Seeking Resilience in Software-Intensive Mission Systems*, Atlantic Council, December 22, 2020, https://www.atlanticcouncil.org/in-depth-research-reports/report/how-do-you-fix-a-flying-computer-seeking-resilience-in-software-intensive-mission-systems/.

Introduction

Software is at the core of the critical mission systems that enable defense organizations to engage in modern warfighting. This code is the key to operational technologies like combat aircraft, complex sensor suites, autonomous systems, and space launch, leading to a convergence between the physical and digital worlds. The exploitation of software vulnerabilities can have consequences that transcend impact on data and equipment, posing risks to mission critical systems and—above all else—human life. Critical software flaws in aerospace systems kill people. The Federal Aviation Administration grounded Boeing's 737 Max for twenty months until it was satisfied that the company had fixed the aircraft's Maneuvering Characteristics Augmentation System,[2] deemed responsible for 364 deaths resulting from the 2018 crash of Lion Air Flight 610 and the 2019 crash of Ethiopian Airlines Flight 302.[3]

In the defense space, the United States and its allies face a rapidly changing threat landscape that includes adversaries that are particularly keen to exploit these vulnerabilities for strategic gain. For example, Chinese state-backed espionage operations have targeted and successfully compromised databases belonging to US and allied defense contractors to steal information about the development of the F-35 Lightning II.[4] Exfiltrated information on the jet has been leveraged by China's People's Liberation Army to develop its own stealth fighters, such as the J-20.[5] Adversaries have demonstrated a sustained interest in targeting military and defense industry networks,[6] and it is vital that mission system owners build resilience to maintain operational continuity through disruption.

Beyond implications of intellectual property theft, brittle systems, if left unaddressed, could be exploited by adversaries for operational and strategic gain. In 2019, the US Air Force and the Defense Digital Service contracted a group of ethical security researchers to search for vulnerabilities in the F-15 Eagle. The contractors successfully infiltrated the fighter jet's Trusted Aircraft Information Download Station, demonstrating that adversary hackers could hold the aircraft at risk.[7] Former Assistant Secretary of the Air Force for Acquisition, Technology and Logistics Dr. Will Roper asserted, "There are millions of lines of code that are in all of our aircraft and, if there's one of them that's flawed, then a country that can't build a fighter to shoot down that aircraft might take it out with just a few keystrokes."[8] The exercise is just one example of how the US Department of Defense (DoD) has struggled with the resilience of its mission systems in peacetime—a conflict would certainly exacerbate the problem. Adversary exploitation of such vulnerabilities in the event of a crisis or war in the Taiwan Strait, for example, could greatly reduce US combat power and have dire consequences for national security.

Mission systems are complex and require that sustained and serious attention be paid to their people, organizational processes, and technologies—three interdependent elements. Failure to account for each can result in brittleness and lead mission systems to fail under duress. While the phrase "continuous monitoring" is widely popular in the existing risk management canon, many of these, such as the Risk Management Framework[9] or the Joint Special Access Program Implementation Guide,[10] focus far more on initial system authorization and implementation of controls

2 Michael Laris, Lori Aratani, and Ian Duncan, "FAA Lifts Ban on Boeing 737 Max after Crashes in 2018 and 2019 Grounded the Jet," *Washington Post*, November 18, 2020, https://www.washingtonpost.com/local/trafficandcommuting/boeing-737-max-ungrounded/2020/11/18/c4d6c1a8-2902-11eb-8fa2-06e7cbb145c0_story.html.

3 Dominic Gates and Mike Baker, "The Inside Story of MCAS: How Boeing's 737 MAX System Gained Power and Lost Safeguards," *Seattle Times*, June 24, 2019, https://www.seattletimes.com/seattle-news/times-watchdog/the-inside-story-of-mcas-how-boeings-737-max-system-gained-power-and-lost-safeguards/.

4 Franz-Stefan Gady, "New Snowden Documents Reveal Chinese behind F-35 Hack," *The Diplomat*, January 27, 2015, https://thediplomat.com/2015/01/new-snowden-documents-reveal-chinese-behind-f-35-hack/.

5 Task and Purpose, "Hacked: How China Stole U.S. Technology for Its J-20 Stealth Fighter," *The National Interest*, The Center for the National Interest, July 10, 2019, https://nationalinterest.org/blog/buzz/hacked-how-china-stole-us-technology-its-j-20-stealth-fighter-66231.

6 Dustin Volz, "US Spy Agency Warns that Chinese Hackers Target Military, Defense Industry," *Wall Street Journal,* October 20, 2020, https://www.wsj.com/articles/u-s-spy-agency-warns-beijing-s-hackers-aiming-at-u-s-defense-industry-military-11603206459.

7 Joseph Marks, "The Cybersecurity 202: Hackers Just Found Serious Vulnerabilities in a U.S. Military Fighter Jet," *Washington Post*, August 14, 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/08/14/the-cybersecurity-202-hackers-just-found-serious-vulnerabilities-in-a-u-s-military-fighter-jet/5d53111988e0fa79e5481f68/.

8 Oriana Pawlyk, "Hackers Find Serious Vulnerabilities in an F-15 Fighter Jet System," Military.com, August 16, 2019, https://www.military.com/daily-news/2019/08/16/hackers-find-serious-vulnerabilities-f-15-fighter-jet-system.html.

9 "NIST Risk Management Framework," National Institute for Standards and Technology, November 30, 2016, https://csrc.nist.gov/projects/risk-management/about-rmf.

10 US Department of Defense, *Joint Special Access Program Implementation Guide (JSIG)*, April 11, 2016, https://www.dcsa.mil/portals/91/documents/ctp/nao/JSIG_2016April11_Final_(53Rev4).pdf.

rather than the evaluation of system health and security throughout the lifecycle. In areas such as defense aerospace, in which failure can result in catastrophic outcomes, brittleness is intolerable.

There are opportunities for the DoD to take lessons from certain high-performing private sector firms in developing and maintaining resilient mission systems and to better address some internal cultural brittleness. Indeed, defense aerospace systems do not stand alone in their low tolerance for failure—the energy (especially nuclear) sector is similar in this regard—but the defense aerospace arena provides a useful illustration of how defense organizations can adapt industry practices to achieve mission resilience. This report summarizes four areas of practice where private sector and defense communities could most readily collaborate to adapt innovative industry practice to the unique demands of the defense community to build, deploy, and maintain resilient aerospace systems.

Mission resilience is the ability of a mission system to prevent, respond to, and/or adapt to both anticipated and unanticipated disruptions, optimizing efficacy and long-term value. But building resilience in software-intensive systems requires more than honing the technology itself. It is especially the *people* of a system who enable and adapt the organizational processes and technologies and have the ability to implement resilient principles. In 2020, the Atlantic Council and MIT Lincoln Laboratory published a study of mission resilience, *How Do You Fix a Flying Computer? Seeking Resilience in Software-Intensive Mission Systems*, accounting for each of these system elements in providing four principles to guide defense organizations in the pursuit of mission resilience: embrace failure, manage trade-offs and complexity, always be learning, and improve your speed.[11] First, defense organizations must learn to embrace failure. Failures and disruptions are unavoidable, as there will always be threats for which no established plan exists. Defense organizations must come to grips with failure's inevitability in their software, so that they can better identify risks, maximize feedback, and avoid repeating mistakes.

Defense organizations must also effectively manage trade-offs and complexity in their technology as well as organizational processes and choices in personnel. Managers must balance quality, scope, cost, and time—without trade-offs, each component will suffer. Third, defense organizations must always be learning. Resilient mission systems should be designed to prioritize a capacity to adapt to uncertain developments. By establishing and testing clear hypotheses, measuring with operational metrics, and observing outcomes, defense organizations can facilitate continuous learning and improvement. Fourth, defense organizations must also improve the speed of delivering and improving their software to build more resilient systems. By taking an analytical approach, the DoD can identify chokepoints that slow work-in-progress software and, critically, the process of updating it and patching its vulnerabilities. The more often mission systems can improve the speed and frequency with which they deploy secure software, the more resilient they will be. This report builds on these principles to examine four practice areas for collaboration between the private sector and government across the defense aerospace community.

11 Herr et al., *How Do You Fix a Flying Computer?*

What Sets Defense Aerospace Apart from Commercial Aerospace?

While defense aerospace systems face a different set of challenges than those of commercial industry, the DoD would benefit from learning from, and embracing, some of the practices of high-performing firms. Defense aerospace systems are hardly homogenous—a fighter jet utilizes software differently and faces different risks than a bomber or an on-orbit satellite—defense aerospace provides a useful framing for how to build resilience in systems with low tolerance for failure. Aerospace systems often operate in highly volatile environments, in which people, processes, and technologies are keys to resilience. Compromising quality under cost and schedule pressures and management issues, such as were deemed root causes behind the 2003 Space Shuttle Columbia disaster, can pose unacceptable risks to safety and security.[12] For defense aerospace systems facing ever-evolving threats, maintaining resilience is a matter of relentless adaptation.[13]

The DoD has some history of effectively developing and sustaining resilient aerospace systems. The Central Intelligence Agency and the Air Force's Project CORONA, which produced the United States' first reconnaissance satellites, served to model mission resilience in the different versions of the orbiting system it deployed from 1959 to 1972.[14] The program was created in response to an evolving environment and to address the deficiencies, arguably failure, of the Lockheed U-2 spy plane program in providing aerial photographic surveillance of the Soviet Union.[15] In 1960, the National Reconnaissance Office, a revolutionary organization for its time, was imagined to coordinate satellite reconnaissance activities.[16] Through its own failure, learning, and adaptation, Project CORONA innovated to provide the US government with critical strategic intelligence on the Soviet Union during the Cold War.[17]

Roughly fifty years later, however, the DoD is now falling short on ensuring sufficient resilience throughout its mission systems. A December 2020 report by the Government Accountability Office found DoD software development approaches and cybersecurity practices to have caused delays risking cost overruns in ten of fifteen DoD information technology programs selected for review.[18] According to the Defense Innovation Board's 2019 Software Acquisition and Practices Study, "the problem is not that we do not know what to do, but that we are simply not doing it."[19] This problem is particularly acute in the department's aerospace systems, as exemplified by the protracted, ongoing saga surrounding flaws in the F-35's Automated Logistics Information System, which was discarded then subsequently rebranded as the ostensibly new and improved Operational Data Integrated Network from precisely the same vendor.[20] Dr. Will Roper asserted that the Air Force's attack surface is broad and unevenly addressed, and that the organization "does a good job on the pointy edge of the spear that goes to war, but not as good of a job on all the things that enable it."[21] This lack of resilience in design, leading to years of delays and unpatched security

12 US National Aeronautics and Space Administration, Columbia Accident Investigation Board, *Columbia Accident Investigation Board*, vol. 1 (Washington, DC: Government Printing Office, 2003).

13 "Reframing the Cyber Crisis: Patterns in Adaptive Systems and Design for Continuous Adaptability," perf. Dr. David Woods, Department of Integrated Systems Engineering, College of Engineering, The Ohio State University, YouTube, January 22, 2021, https://www.youtube.com/watch?v=KzTv09fATeE.

14 "A Point in Time: The Corona Story," in *Reel America*, C-Span, September 7, 2014.

15 "U-2 Overflights and the Capture of Francis Gary Powers, 1960," US Department of State, n.d., https://history.state.gov/milestones/1953-1960/u2-incident.

16 Bruce Berkowitz with Michael Suk, *The National Reconnaissance Office at 50 Years: A Brief History*, Center for the Study of National Reconnaissance, National Reconnaissance Office, July 2018, Second Edition, https://www.nro.gov/Portals/65/documents/about/50thanniv/The%20NRO%20at%2050%20Years%20-%20A%20Brief%20History%20-%20Second%20Edition.pdf?ver=2019-03-06-141009-113&timestamp=1551900924364.

17 William J. Broad, "Spy Satellites' Early Role as 'Floodlight' Coming Clear," *New York Times*, September 12, 1995, https://www.nytimes.com/1995/09/12/science/spy-satellites-early-role-as-floodlight-coming-clear.html.

18 US Government Accountability Office, *Information Technology: DOD Software Development Approaches and Cybersecurity Practices May Impact Cost and Schedule*, 2020, https://www.gao.gov/assets/720/711529.pdf.

19 J. Michael McQuade et al., "Who Cares: Why Does Software Matter for DoD?" in *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage* (Washington, DC: Defense Innovation Board, May 3, 2019), https://media.defense.gov/2019/May/01/2002126693/-1/-1/0/SWAP%20MAIN%20REPORT.PDF.

20 Dan Grazier, "Uncorrected Design Flaws, Cyber-Vulnerabilities, and Unreliability Plague the F-35 Program," Project on Government Oversight, March 24, 2020, https://www.pogo.org/analysis/2020/03/uncorrected-design-flaws-cyber-vulnerabilities-and-unreliability-plague-the-f-35-program/; "F-35 Joint Strike Fighter: DOD Needs to Update Modernization Schedule and Improve Data on Software Development," US Government Accountability Office, March 18, 2021, https://www.gao.gov/products/gao-21-226.

21 Remarks by Dr. Will Roper, former assistant secretary of the Air Force for acquisition, technology and logistics, at an Atlantic Council Roundtable, "Aerospace Cybersecurity: Protecting the New Frontier," February 4, 2021, https://www.atlanticcouncil.org/commentary/article/protecting-the-new-frontier-seven-perspectives-on-aerospace-cybersecurity/.

flaws, has practical impacts.[22] In early 2021, Lt. Gen. Clinton Hinote, the Air Force's deputy chief of staff for strategy, integration and requirements, shared in an interview that, "We wouldn't even play the current version of the F-35. … It wouldn't be worth it. … Every fighter that rolls off the line today is a fighter that we wouldn't even bother putting into these scenarios."[23]

Mission resilience can neither be purchased up front nor tacked onto systems at the end of development. Fortunately, defense organizations could make significant strides on mission resilience in their aerospace systems by following the lead of some in the private sector and adapting certain commercial industry practices that have proven successful. Building a culture of resilience will entail incorporating changes into all stages of a system's lifecycle, tying together people, organizational processes, and technologies. This may also involve the federal government reasserting itself as the prime integrator in mission system development programs, giving it more direct control over design and organization choices and shortening the decision chain. This entails a willingness to assume greater program risk by defense civilian and uniformed leadership as much as a change in relationship with industry. Commercial industries, from pure software companies to healthcare firms to vehicle manufacturers, are embracing concepts of resilience engineering in their designs and operations. For internet-connected systems, concepts like Site Reliability Engineering, chaos engineering, DevOps (development and operations), and continuous integration/continuous deployment (CI/CD) methods are being leveraged by organizations to embrace failure and improve speed, both critical to improving overall system resilience.[24]

Private sector firms are not uniform in their rapidity, or enthusiasm, to embrace these methods; simply tying what any company does together with the defense community is not a recipe for success. Indeed, many of the concepts and examples discussed in this report are drawn from smaller firms and technology vendors, not the prototypical industrial base for the defense aerospace community. As efforts like the U-2 Federal Laboratory[25] and Kessel Run[26] have demonstrated, locking in reliance on these traditional defense vendors may well be holding back the potential for industry and defense aerospace collaboration. While the projects under development are not yet mission critical for live combat systems, and there are hurdles to reaching this kind of development, the prospects of these models are compelling. For the DoD, finding new partners and innovative methodologies for mission system development will be important, especially as software becomes increasingly critical to nearly every weapon system—to the point where software essentially *is* the weapon system.

All will not be straightforward on the defense community side either. Adoption of these strategies in the defense aerospace community has been, and will continue to be, met with pushback and the attitude that "we are different." Defense aerospace creates and operates systems with high complexity (aircraft) and stakes (loss of life). An internet-based software company may have high complexity, such as a multinational distributed infrastructure, but often lacks the high stakes of loss of human life. The defense aerospace community can easily rationalize dismissing strategies to improve resilience when its systems are already operating near their limits and lives are at stake. Even commercial aerospace has stringent evaluation criteria and design standards. But what are the differences really, in terms of the operational environment, people, organizational processes, and technology that lead to this belief about aerospace systems?

Under combat conditions and more extreme mission parameters, the operational environment of defense aerospace systems is different in that it is less forgiving than that of many commercial industries, and the opportunities for operational lessons are smaller and fewer. Flying through air or space has constraints that do not exist in large distributed data centers, and the consequence of failure is different. Commercial companies can leverage advances in computing and communications without considering size and weight. Aircraft and spacecraft are limited by flight and orbital mechanics, where there are real constraints on size, weight, and power. While the software revolution has significantly changed that calculation for aircraft and spacecraft, the constraints of safety and security still demand different approaches to addressing disturbances in the environment. A surge in demand for a commercial company is solved by cloud load balancing and dynamic scaling, whereas demand for many defense aerospace

22 Joseph Trevithick and Tyler Rogoway, "F-35 Hit with Cluster Bomb of Damning Reports as Pentagon Eyes Full Rate Production," *The Drive*, June 12, 2019, https://www.thedrive.com/the-war-zone/28488/f-35-hit-with-cluster-bomb-of-damning-reports-as-dod-eyes-full-rate-production; Garrett Reim, "Lockheed Martin F-35 Deficiencies: Two Fewer in 2020, 871 Issues Remain," *Flight Global*, January 15, 2021, https://www.flightglobal.com/fixed-wing/lockheed-martin-f-35-deficiencies-two-fewer-in-2020-871-issues-remain/141969.article.

23 Valerie Insinna, "A US Air Force War Game Shows What the Service Needs to Hold Off—or Win against—China in 2030," *Defense News*, April 12, 2021, https://www.defensenews.com/training-sim/2021/04/12/a-us-air-force-war-game-shows-what-the-service-needs-to-hold-off-or-win-against-china-in-2030/.

24 Each of these practices is explored in more detail in Herr et al., *How Do You Fix a Flying Computer?*

25 Valerie Insinna, "The Tiny Tech Lab that Put AI on a Spyplane Has Another Secret Project," *Defense News*, February 11, 2021, https://www.defensenews.com/air/2021/02/11/the-tiny-tech-lab-that-put-ai-on-a-spyplane-has-another-secret-project/.

26 Jim Perkins and James Long, "Software Wins Modern Wars: What the Air Force Learned from Doing the Kessel Run," Modern War Institute, January 17, 2020, https://mwi.usma.edu/software-wins-modern-wars-air-force-learned-kessel-run/.

capabilities is constrained by production and logistics, be it hardcoded logic for the multimode radar system on a strike aircraft or the certification pipeline for a real-time operating system. The more extreme operational environments for some defense missions constrain the available solutions for the defense aerospace community, but do not preclude the application of some commercial strategies.

Another operational difference with the aerospace environment is the limited opportunity for defense organizations to learn. In the commercial world, there are various strategies to test out new capabilities in operations through A/B testing,[27] regional rollouts,[28] and chaos engineering.[29] In defense aerospace, due to typically low production rates, safety requirements, and risk aversion, these types of strategies do not translate. Commercial industries operate twenty-four hours a day, 365 days a year, and thus have many opportunities for feedback, operational surprise, and experimentation, which they have exploited to improve and reduce the risk of an unexpected "big bang"–style development. The defense aerospace community may not have the flexibility of the commercial operating tempo—some systems, like satellites, are always operating, while many others, like jets, fly relatively limited operational hours and rarely see full combat conditions—but still may be able to adjust and overcome these limitations on feedback and speed. The defense aerospace environment has a strong opportunity to leverage development and operational testing regimes to embrace these more regularized learning processes including through the various colored flag exercises.

The final area that presents challenges to defense aerospace beyond those faced by the private sector is technology. Commercial aviation organizations and their supply chains are able to leverage shared services for many of the capabilities being developed and delivered. Defense aerospace, by contrast, does not have the scale to drive technology innovation or cost reduction to the same degree, as it often relies on technology that requires large investment and slow cost recovery through low-rate production and flight certification. The private sector typically leverages the scale of production or the ability to share costs with others to lower the technology costs. Similarly, as a result of this cost, the private sector is more likely to pivot and leverage newer versions of technology, or totally new technology. Defense aerospace typically works with small iterations over longer periods of time.

Certain private industry firms have demonstrated a capacity to evolve more rapidly than the typical defense program. To remain competitive, defense organizations should work to embrace industry approaches that can be adapted to the unique requirements of defense operations. This is easier said than done but there are four practice areas that offer potential benefits and might translate the needs of the defense community and the innovative practices of some in the private sector most readily. Each of these four is associated with an aforementioned principle of mission resilience for defense organizations to adapt from the private sector: fail open (embrace failure), segment systems (manage trade-offs and complexity), expand simulations and twinning (always be learning), and speed your change (improve your speed).

1. Fail Open

Principle: Embrace Failure

There are some high-end, exquisite capabilities, such as stealth technology, that the DoD must keep hidden, because the sensitivities and investments in them are too great to expose to the external world. For everything else, the DoD would benefit from taking a hybrid approach to secrecy and openness in systems. The DoD has defaulted to classifying systems as a security strategy to the detriment of these very systems. Just because a system and, critically, its vulnerabilities remain classified does not mean they do not exist. Furthermore, the more that systems can be subjected to public scrutiny, the more they can be tested, fail, be honed, and be improved outside of highly choreographed evaluations. As commercial contractors take on a bigger role in the DoD's mission systems, attempting to keep systems secret may not necessarily be the most viable approach to development and security in every case. Part of the principle of embracing failure entails the practice of limiting secrecy.

When systems fail—as they inevitably do—it is critical that they fail open. Failing open, or operating to some extent under conditions of failure, is vital to avoid total failure. The department must move toward a more resilient approach that layers several levels of security, so that failure does not occur as soon as an adversary finds its way into a mission system. The DoD should take a blended approach to confidentiality through containerization and Kubernetes to prepare for loss of confidentiality, while allowing systems to fail open. A good example is the Airbus approach to defense system communications links. In short, the system's encryption and decryption devices are connected

27 "A/B Testing," *Optimizely*, n.d., https://www.optimizely.com/optimization-glossary/ab-testing/.

28 Ann Mar, "Rollout Strategy Explained," *Simplicable*, May 25, 2013, https://business.simplicable.com/business/new/what-is-a-rollout-strategy.

29 Fredric Paul, "Chaos Engineering Explained," *New Relic*, Blog, January 10, 2019, https://blog.newrelic.com/engineering/chaos-engineering-explained/.

via a communications link. In the event of an encryption failure on either end, the system enters a fail-open mode in which it alerts of a breach, but continues to operate without encrypting the messages.[30] This approach will not be possible for all systems and the discussion here is one of shifting design thresholds and assumptions, not a singular revolution for all national security systems.

For defense aerospace technologies, it is critical to differentiate between flight control systems and mission systems. There are certain systems on an aircraft, such as navigation or communications, maybe even weapons, that must operate in a fail-open state—the bare minimum flight control system to ensure safe flight conditions must remain operational and segmented from these other systems, as discussed in the next section. Defense organizations' prioritization of failing open should focus on mission systems.

Recommendation

Find the Chaos Monkey: Developed by Netflix, chaos engineering allows organizations to experiment on systems and find their failure points. While intentionally disrupting systems may be uncomfortable, the process is the essence of embracing failure and something that has paid off in spades for industry.[31] The practice could provide insights into how defense aerospace systems would perform through disruption and how they could be made more resilient. The DoD should implement chaos engineering as a core resilience practice in the testing and evaluation phase of defense aerospace systems to ensure that when systems fail, they fail open.[32]

2. Segment Systems

Principle: Manage Trade-Offs and Complexity

No mission system is a monolith. In addition to being comprised of people, processes, and technology, mission systems may well be a combination of discrete packages or programs. A combat aircraft's flight control software can be addressed independently of the software package that controls and interprets its synthetic aperture radar (SAR). The level of classification and development methodology used by the SAR software could be treated independently of the flight control system. Software packages can also be independently updated—witness the late September 2020 instance of a U-2 spy plane whose sensor package received a mid-air software update.[33] In this case, the sensor suite's software was managed independently of the aircraft's flight computer and was isolated from any safety-critical systems like fuel management or emergency recovery equipment, such that even if the update had failed, flight safety would not have been impacted.[34] The emphasis in design was on dissimilar systems working through an open and accessible interface model.[35]

This segmentation can be used to manage the on-ramp and adoption of CI/CD methodologies in mission systems, starting with more risk-tolerant or non-safety-critical systems first. There is good reason to be skeptical of the need for or utility of updating flight control software dozens of times a day and isolating those safety-critical and thus less fault-tolerant systems. A CI/CD pipeline can provide greater assurance of stability and less room for unexpected change, while still allowing for the benefits of agile development to be applied to other elements of the mission system.

Segmentation with a standardized system of communicating among segments can be a powerful tool to break down barriers to new vendors, more granular classification levels, and more easily distributed (or sequenced) development. The issuance of the famous Bezos API (application programming interface) Mandate was an example of this segmentation and communication logic. It required organizations across Amazon to maintain a standardized procedure for communication and resource provision among teams. This allowed teams across the company to interact with each other and pull data (rather than request it be pushed) in a universal and easily designed around manner.[36] This kind of standardization in outgoing communication and data formats helps address incompatible system designs.

30 Ray James et al., Communication Links, US Patent 10,887,054, filed November 16, 2016, and issued January 5, 2021.

31 Nick Heath, "AWS Outage: How Netflix Weathered the Storm by Preparing for the Worst," *TechRepublic*, September 21, 2015, https://www.techrepublic.com/article/aws-outage-how-netflix-weathered-the-storm-by-preparing-for-the-worst/.

32 See Embrace Failure recommendations in Herr et al., *How Do You Fix a Flying Computer?*

33 Valerie Insinna, "US Air Force Sends Software Updates to One of Its Oldest Aircraft Midair," *C4ISRNET*, October 19, 2020, https://www.c4isrnet.com/air/2020/10/09/the-air-force-updated-the-software-on-one-of-its-oldest-aircraft-while-it-was-in-the-air/; Frank Wolfe, "Development of Open Mission Systems Computer for U-2 Continues with Latest Kubernetes Demonstration," *Aviation Today*, December 15, 2020, https://www.aviationtoday.com/2020/12/15/development-open-mission-systems-computer-u-2-continues-latest-kubernetes-demonstration/.

34 The same US Air Force program just months later deployed a software package to automatically control a U-2's sensors mid-flight in conjunction with the pilot. Oriana Pawlyk, "Air Force U-2 Surveillance Plane Flies First Mission with AI Copilot," Military.com, December 16, 2020, https://www.military.com/daily-news/2020/12/16/air-force-u-2-surveillance-plane-flies-first-mission-ai-copilot.html.

35 "Open Architecture Management (OAM)," Virtual Distributed Library, US Air Force, n.d., https://www.vdl.afrl.af.mil/programs/oam/index.php.

36 Matthias Biehl, "The API Mandate—Install API Thinking at Your Company," API-University, n.d., https://api-university.com/blog/the-api-mandate/.

Approaching the software suite in a modern mission system, like a combat aircraft or an autonomous ground vehicle, as a network of modular elements can also provide greater flexibility to limit or remove functionality (constraining system complexity), isolate and harden high-value logic, and limit the scope of testing on integration of new functionality. Containerization is a popular modality of this modular approach in software design and deployment. Containers allow for a network of software functions and interdependent applications to be spun up and managed as a network, rather than a monolith. This kind of granular control also provides a means to isolate and harden specific high-value functions from the functionality of other systems, though containerization does not provide strong cryptographic or logical isolation. Segmentation for functionality or availability will not necessarily provide confidentiality guarantees and vice versa.

Much of the challenge of modern application security is based on the attack surface imposed by general purpose computing. In a classically low-key yet fundamentally important talk given in 2018, mathematical computer scientist Thomas Dullien articulated the risks posed by complex devices that were cheap and plentiful, but regularly being used and imperfectly constrained to imitate simple machines.[37] Modularizing software also minimizes the burden of testing new functionality by clarifying dependencies and reduces the risk of failure by isolating most changes from impacting safety-critical functions.

Segmentation will help manage the onboarding of agile methodologies into mission systems with safety-critical components, while also helping program managers address the complexity of their systems. Additionally, segmentation promotes better access control and least privilege, whereby users are given the bare minimum permissions necessary to accomplish their jobs. Complexity is a key contributor to unexpected failures and cascade effects that can quickly exceed a system's ability to operate under reduced functionality. Managing the complexity of a system—being able to adapt to evolving requirements while carrying a minimum backlog of legacy code and unused functions—is a key competency in secure and resilient development.

Recommendation

Segment to Secure: Those setting requirements for defense aerospace systems should embrace segmentation. Rather than leaving segmentation for mission or aircraft critical systems like flight controls, approach every piece of functionality as a module in development. Segmentation, together with standard common interfaces, would allow programs to decompose specific elements of software and hardware design along predictable lines—granting more granular classification, allowing the use of more specialized or less broadly equipped vendors, and releasing the whole of a program from dependence on the development schedule of one, less critical component. This decomposition of the supply chain would liberate program managers from having to join hardware and software development through the same prime vendor, and allow more rapid and flexible onboarding of more competitive vendors to sustain programs later in their lifecycles.

3. Expand Simulations and Twinning

Principle: Always Be Learning

Mission resilience is predicated on understanding a system in detail. This requires precise knowledge of not just the organizational processes and people involved in its development and operation, but also the technology and how it responds to a range of operating conditions. Physical systems have a limit, and significant cost, associated with their use in the real world. This has led to the development of a variety of simulation methodologies to model technology's behavior and interaction with people in a manner that provides for better data collection and more fine-grained control alongside conventional forces and other training modes.[38]

A key practice to support this kind of simulation, known as twinning, is the construction of "digital twins"[39] for physical systems.[40] Twinning replicates the operating details of a physical system in a digital environment, modeled to

37 "Security, Moore's Law, and the Anomaly of Cheap Complexity—CyCon 2018," perf. Mr. Thomas Dullien, mathematical computer scientist, YouTube, June 20, 2018, https://www.youtube.com/watch?v=q98foLaAfX8.

38 Jennifer Mcardle and Caitlin Dohrman, "The Next SIMNET? Unlocking the Future of Military Readiness through Synthetic Environments," *War on the Rocks*, December 3, 2020, https://warontherocks.com/2020/12/the-next-simnet-unlocking-the-future-of-military-readiness-through-synthetic-environments/.

39 Aidan Fuller, Zhong Fan, Charles Day, and Chris Barlow, "Digital Twin: Enabling Technologies, Challenges and Open Research," *IEEE Access*, vol. 8, 2020, https://ieeexplore.ieee.org/abstract/document/9103025.

40 Slawomir Luscinski, "Digital Twinning for Smart Industry," *EAI*, Semantic Scholar, November 6, 2018, https://pdfs.semanticscholar.org/169d/9dafaae02ed07c99871e86d68aacd416f279.pdf.

varying levels of detail[41] from the representative to the obsessively minute depending on the need. Twinning can be used to simulate the behavior of a system in response to unusual operating conditions, project unexpected environmental interactions, simulate the impact of varying service conditions and system lifespans, and more. Twinning allows for low-cost testing and training on physical systems, helping develop procedures and address safety-critical failures in a low-consequence environment. For defense organizations to always be learning from these failures, be they simulated or otherwise, it is critical they capture as much information as possible on the causes of failure. Google's Site Reliability Engineering teams can serve as a helpful example of how to monitor, anticipate, and retrospectively analyze failure and its root causes.[42]

Twinning can help organizations[43] still developing a tolerance for failure and/or working with safety-critical systems simulate failure and learn more about their mission systems than might otherwise be possible. For example, some simulators built for the F-22 integrated stock aircraft components to improve the fidelity and performance of the simulated aircraft, instead of simply replicating their functionality in a simulated environment.[44] In civilian environments, twinning is used to support everything from simulating the failure rate[45] of mechanical components and factory planning[46] to enabling better anomaly detection[47] in human health. Twinning can also provide for more ready integration[48] of civilian and non-defense organization expertise alongside operational units and program offices, using the digital twin as the focal point rather than a deployed system. By simulating failures, twinning can avoid routine maintenance by more accurately predicting when repairs are necessary for mission systems. For navy ships, this means the ability to remain under way and avoid teardown maintenance for longer by utilizing known data. The same can apply to defense aerospace systems onboard ships, such as carrier-based aircraft like the F-18 E/F Super Hornets.[49]

One of twinning's shortfalls at the moment is its failure to regularly capture the entire system at play—people, process, and technology. This includes high-fidelity environmental impacts and system failures or degradation caused by ineptitude, the unintended consequences of sanctioned policies, or trouble in downstream dependencies. Twins must be purposefully subjected to the behavior of adversaries as well with all of the adaptive capacity they employ. There is a need to capture as much bureaucratic and sociological fidelity as possible given the impact that slow decision-making, poorly channelized information flow, or misaligned incentives can have on system performance and survival. Properly implemented, twinning offers near-term benefits to system owners through lower-cost information gathering and experimentation with "live virtual" technologies. Over the long term, the design and modeling of digital twins may provoke useful, if uncomfortable, questions about organizational structures and incentives, an equal if not greater benefit.

Recommendation

Measure at Machine Speed: Modeling is only as good as the quality of the model. Twinning, for all its value, fails to account for elements of a system beyond the technology itself. The first step the DoD could take to overcome this shortfall for aerospace systems is to measure everything—not just technology performance metrics. The adoption of requirements to measure everything, and the resulting volume and use of produced data, should feature in congressional requirements through the next several National Defense Authorization Acts to drive change in complement with DoD leadership. A holistic approach to twinning should also account for the people and processes of defense aerospace systems, measuring speed of software development–related processes, including deployment and feedback loops. These metrics should include values like failed deployments, availability, mean time to detect, mean time to deploy, change volume, and automated test

41 Rainer Stark, Carina Fresemann, and Kai Lindow, "Development and Operation of Digital Twins for Technical Systems and Services," CIRP Annals, May 1, 2019, https://www.sciencedirect.com/science/article/abs/pii/S0007850619300502.

42 Rob Ewaschuk, "Monitoring Distributed Systems," Google, 2017, https://sre.google/sre-book/monitoring-distributed-systems/.

43 Fei Tao and Qinglin Qi, "Make More Digital Twins," *Nature News*, September 25, 2019, https://www.nature.com/articles/d41586-019-02849-1?sf220071546=1.

44 Primary knowledge from one of the authors' direct experience working on the early portions of the F-22 test and acceptance program.

45 Birte Kier, "Getting There Faster with Digital Twins," *Engineered*, March 12, 2018, https://engineered.thyssenkrupp.com/en/getting-there-faster-with-digital-twins/.

46 Roland Rosen, Georgvon Wichert, George Lo, and Kurt D.Bettenhausen, "About the Importance of Autonomy and Digital Twins for the Future of Manufacturing," *IFAC-PapersOnLine*, vol. 48, no. 3 (August 31, 2015), https://www.sciencedirect.com/science/article/pii/S2405896315003808.

47 Benjamin Harris, "How 'Digital Twins' Are Harnessing IoT to Advance Precision Medicine," *Healthcare IT News*, February 10, 2020, https://www.healthcareitnews.com/news/how-digital-twins-are-harnessing-iot-advance-precision-medicine.

48 Maj. Wilson Camelo, "Tyndall AFB Takes F-22 Pilot Training to Next Level," US Air Force, July 30, 2014, https://www.af.mil/News/Article-Display/Article/486936/tyndall-afb-takes-f-22-pilot-training-to-next-level/.

49 Adam Stone, "What If the Military Relied on Digital Twins? What If the Military Relied on Digital Twins?" *C4ISRNET*, December 6, 2018, https://www.c4isrnet.com/it-networks/2018/12/07/what-if-the-military-relied-on-digital-twins-what-if-the-military-relied-on-digital-twins.

pass rates.[50] Considering these metrics can provide a full picture to program offices that would make twinning an aircraft or spacecraft a more meaningful practice.

4. Speed Your Change

Principle: Improve Your Speed

Defense aerospace and DoD acquisition have evolved over time to have people, processes, and technologies that change at the speed of what is perceived as the operational environment. Systems are designed for decades of use, with most of the focus on sustaining the components that face physical wear and tear. As such, the defense aerospace community has developed limited processes or technical approaches around increasing the rate of change of the software and internal capabilities of systems. These are typically mandated by external regulations, new customer needs, or availability of replacement components. Greater speed in the development, acquisition, and adaptation of defense aerospace technology is needed to leverage faster evolution of available capability and counter threats adopting and changing their technology.

SpaceX has embraced an iterative design philosophy that involves quickly designing, building, testing, and launching prototype vehicles. Prototypes often fail, but that is part of the company's strategy of learning, fixing, and quickly moving on to the next prototype, while also planning for the appropriate budget to handle those failures if they occur. SpaceX's Starship program has experienced many launch failures and successive iterations, but it makes progress at a much faster pace than traditional government aerospace programs. For context, the National Aeronautics and Space Administration (NASA) has traditionally iterated at a much slower rate, opting instead to avoid risking failure before perfecting a rocket. In the aftermath of the Space Shuttle Challenger accident, NASA established the Independent Verification and Validation (IV&V) Program to ensure its software performs as expected for its critical missions.[51] However, while the mandated IV&V Program makes for highly reliable software, that software can be expensive, time consuming, and slow to integrate design changes. Government organizations like NASA have been hesitant to pursue the iterative design philosophy due to fear of failing publicly and the budgetary impacts of "wasting taxpayer dollars"—things self-funded companies like SpaceX can live with and not have to worry about, respectively.[52] Ironically, this attitude has started to shift as more rapid prototyping and iterative design appear to be at least partially responsible for the widening chasm between the cheaper (and fully operational) hardware developed by SpaceX and the more expensive, yet still in development, programs from established competitors like Boeing, Northrop Grumman, and Lockheed Martin.[53]

The commercial world realizes speed of change through the partitioning and automation of the system lifecycle, tighter and improved feedback loops, more but smaller changes, and acceptance of some failure. In industry, speed is a result of technological and process investments. The accumulation of small gains across various decisions has led to improvements in the sustainment of capability, and the ability to respond to changing customer demands and operational environments.

Breaking apart the technologies used in building and operating a mission system, referred to as decoupling the technology stack, enables industry to change out and evolve underlying infrastructure while running the same software base. If new processing becomes available, companies are able to leverage it once an Infrastructure as a Service (IaaS) provider offers it. Similarly, if there are new software infrastructure components available, the "mission" code can be isolated and the Platform as a Service (PaaS) can be updated without concern about the enterprise code. The private sector lacks the long, drawn-out acquisition process and competition for purchasing new hardware that plague the DoD.

Alternatively, the Amazon Web Services (AWS) ecosystem is a good example of separating platforms from applications. AWS is evolving and delivering new capability constantly, yet the applications running on top tend to keep running without significant change from the IaaS or PaaS

50 See Always Be Learning recommendations in Herr et al., *How Do You Fix a Flying Computer?*

51 "About NASA's IV&V Program," US National Aeronautics and Space Administration, March 9, 2015, https://www.nasa.gov/centers/ivv/about/index.html.

52 Eric Berger, "SpaceX Has Lost Its First Starship Prototype—Is This a Big Deal?" *Ars Technica*, November 21, 2019, https://arstechnica.com/science/2019/11/spacex-has-lost-its-first-starship-prototype-is-this-a-big-deal/.

53 Jeff Foust, "SpaceX Beat Gateway Cargo Contract Competitors on Price and Performance," *SpaceNews*, April 13, 2020, https://spacenews.com/spacex-beat-gateway-cargo-contract-competitors-on-price-and-performance/; Sissi Cao, "New Audit Reveals NASA Paid Boeing $2 Billion More than SpaceX for Same ISS Mission," *Observer*, November 15, 2019, https://observer.com/2019/11/nasa-audit-boeing-spacex-iss-ccp-mission-spacecraft-budget/; "NASA's Management of Crew Transportation to the International Space Station," US National Aeronautics and Space Administration, Office of Inspector General, November 14, 2019, https://oig.nasa.gov/docs/IG-20-005.pdf; Eric Berger, "Air Force Budget Reveals How Much SpaceX Undercuts Launch Prices," *Ars Technica*, June 15, 2017, https://arstechnica.com/science/2017/06/air-force-budget-reveals-how-much-spacex-undercuts-launch-prices/; Department of the Air Force, Air Force Financial Management and Comptroller, *Department of Defense Fiscal Year (FY) 2018 Budget Estimates*, May 2017, https://www.saffm.hq.af.mil/Portals/84/documents/Air%20Force%20Space%20Procurement%20FY18.pdf?ver=2017-.

users.[54] This allows the hardware and software to evolve at different rates and be managed with sometimes diverging development philosophies but maintain APIs and other abstractions, allowing access to these lower layers and enabling a diverse application ecosystem to grow. AWS can push out software updates on a quarterly or faster basis, and significant hardware updates yearly, similar to the approaches employed by Google and Microsoft.

The defense aerospace acquisition process can increase its speed by automating the system lifecycle. While the phases of typical DoD system development lifecycles are distinct and isolated, commercial best practices today have merged these phases into a continuous integration and delivery pipeline that allows for the design, development, and deployment of incremental changes that can go through testing and validation steps like a traditional process. Investment in automation is key to facilitating this and results in improved speed and feedback. Instead of creating manuals with numerous steps for operators to install, configure, and operate a system, this procedure can be automated and treated as code. Pipelines can be built around these steps to provide checks and feedback as soon as possible. A good example is the Checkov tool built to automatically validate new system deployments against organizational security policies.[55] This shift is part of a broader trend toward "infrastructure as code" whereby system design and deployments can be evaluated for security flaws and misconfigurations much like applications.[56] While shifting to these tools and concepts may initially slow certain aspects of the process, in the long term these automations allow for improved assessment of code quality, the ability to easily roll back changes, and the ability to push out fixes quickly.

Recognizing that a system is operating outside of tolerable parameters, and what may be causing that, is critical to being able to adapt and have resilience. The private sector can do that through automation, chaos engineering, and DevOps. Automation enables validation of configurations creating feedback and confidence of system state. Chaos engineering allows for discovery of system bounds before a system reaches them, and improves the developers', operators', and users' understanding of a system's performance. Finally, a DevOps culture creates shared responsibility and understanding in a system, and from a speed perspective provides the shortest feedback loop alerting system designers and developers to operational issues. In the defense aerospace world, these same concepts can be realized through similar automation, improved experimentation through digital twinning, and more exercises. Automation can improve the ability to configure, change, and restore system configurations.

Speed of change within defense aerospace systems can be realized through changes to the acquisition approach, system decoupling, automation, digital twinning, and exercises. Defense aerospace has done some of these activities in the past, but they need to be extended to continue to improve the speed of change of systems. Lt. Col. Richard Suter created Red Flag to help the Air Force "train as it fights" forty-five years ago.[57] The private sector mirrors that in chaos engineering and gameday exercises. The defense aerospace community can relearn this lesson from industry and expand what it means to "train as it fights" to increase its speed of change.

Recommendation

Formalize the Software Acquisition Pathway: Congress should use the fiscal year 2022 National Defense Authorization Act as a vehicle to formalize the DoD's software acquisition pathway interim policy, which, among other things, "simplifies the acquisition model to enable continuous integration and delivery of software capability on timelines relevant to the Warfighter/end user."[58] Congress can enhance the policy to further empower the DoD to enable micro contracts[59] within larger vehicles (e.g., pay for performance and delivery of working product every two- to four-week sprint).[60] The formalization of this policy will allow the DoD to translate some commercial practices that emphasize the importance of speed of change toward building and maintaining its defense aerospace systems.

54 For more on the the service models of cloud computing and some background on these technologies, see Simon Handler, Lily Liu, and Trey Herr, *Dude, Where's My Cloud? A Guide for Wonks and Users*, Atlantic Council, September 28, 2020, https://www.atlanticcouncil.org/ in-depth-research-reports/report/dude-wheres-my-cloud-a-guide-for-wonks-and-users.

55 "Home," Checkov Bridgecrew, https://www.checkov.io.

56 Niamh Lynch, "Infrastructure as Code: Cycloid's Non-boring Guide for the Clueless," *Cycloid*, May 28, 2020, https://blog.cycloid.io/infrastructure-as-code-for-beginners.

57 Walter J. Boyne, "Red Flag," *AIR FORCE Magazine*, November 2000, https://www.airforcemag.com/PDF/MagazineArchive/Documents/2000/November 2000/1100redflag.pdf.

58 US Under Secretary of Defense, Department of Defense, "Software Acquisition Pathway Interim Policy and Procedures," Acquisition and Sustainment, Memorandum, January 3, 2020, https://www.acq.osd.mil/ae/assets/docs/USA002825-19%20Signed%20Memo%20(Software).pdf.

59 Recent policy changes to make the application of variously colored monies more flexibly applicable are welcome and covered but invite a broader conversation about where technology and software acquisitions are new versus sustaining or updates.

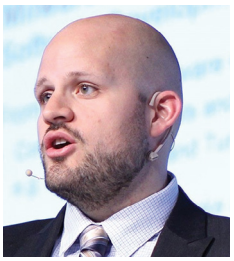
60 See Improve Your Speed recommendations in Herr et al., *How Do You Fix a Flying Computer?*

Conclusion

Defense aerospace systems comprise some of the most expensive and strategically significant mission systems utilized by the United States and its allies. Adversaries will continue to evolve their tactics and technological capabilities to challenge these systems, demanding that defense organizations similarly embrace constructive evolution and the principles of resilience. Defense organizations must embrace failure, manage trade-offs and complexity, always be learning, and improve their speed. While aerospace presents inherently distinct challenges from other spaces, defense organizations could look to the private sector and adapt commercial practices to implement the principles of resilience. The diverse challenges and opportunities in mission systems, ground components, and embedded software are worthy of more siloed discussion in future work. The low tolerance for defense aerospace systems to fail should not deter defense organizations' pursuit of their resilience, but rather underscore the dire need thereof.

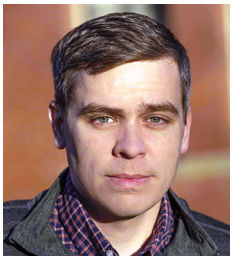
About the Authors

Simon P. Handler is an assistant director of the Atlantic Council's Cyber Statecraft Initiative, within the Scowcroft Center for Strategy and Security. In this role, he manages a wide range of projects at the nexus of geopolitics and international security with cyberspace. He leads the Initiative's work on various issue areas, including mission resilience and defense aerospace cybersecurity. Prior to joining the Atlantic Council, he served as a special assistant in the United States Senate, where he worked on foreign policy issues. During his time on the Hill, he was a congressional fellow with the Wilson Center's Congressional Cybersecurity Lab and Congressional Artificial Intelligence Lab, and completed the East-West Center's Congressional Staff Program on Asia. He holds a BA in International Relations & Global Studies, with a concentration in International Security, and Middle Eastern Languages & Cultures from the University of Texas at Austin.



Dr. Trey Herr is the director of the Cyber Statecraft Initiative under the Scowcroft Center for Strategy and Security at the Atlantic Council. His team works on cybersecurity and geopolitics including cloud computing, the security of the internet, supply chain policy, cyber effects on the battlefield, and growing a more capable cybersecurity policy workforce. Previously, he was a senior security strategist with Microsoft handling cloud computing and supply chain security policy as well as a fellow with the Belfer Cybersecurity Project at Harvard Kennedy School and a non-resident fellow with the Hoover Institution at Stanford University. He holds a PhD in Political Science and BS in Musical Theatre and Political Science.

Steve Luczynski is the board chairman for the Aerospace Village, a 501(c)(3) non-profit, whose volunteers strive to build relationships between government, industry, and the security researcher community to maintain secure air and space operations and preserve public trust in the aerospace sector. Additionally, he leads the COVID Task Force at the Cybersecurity and Infrastructure Security Agency, which he joined in 2020. In this role, he oversees the agency's support to national pandemic responses and efforts to provide cyber and physical security to the health and public health sector. Steve began his military career as an Air Force fighter pilot and served in his final assignment as the deputy director for cyber operations in the Office of the Under Secretary of Defense for Cyber Policy at the Pentagon. After retiring from the military in 2017, he was a chief information security officer in the private sector before joining CISA. Steve holds a bachelor's degree in Aerospace Engineering from Georgia Tech and a master's degree from the National War College.



Reed Porada is a security researcher and instructor at BCI focused on the socio-technical facets of system design and operations. His research has focused on helping get to the "so what" of both defensive and offensive cyber measures. To provide decision makers and teams with context for their work, Reed applies skills in systems thinking, communication, technology awareness, and hands on system assessments. At BCI, Reed focuses his research on understanding how attackers redefine system boundaries and use systems in unexpected ways. This work will help inform defensive approaches and develop better tools for reasoning about system security. Reed leads BCI training in cyber systems analysis, focusing on developing systems thinking skills of developers up to managers. Previously, Reed was a staff member at MIT Lincoln Laboratory for ten years. He was responsible for test and evaluation, test automation research, red-teaming of cyber systems, and blue system architectures in support of DoD and other government programs. Prior to joining Lincoln Laboratory, Reed was computer scientist at the Naval Research Laboratory focused on wireless communication systems. He holds an MS in software engineering from Carnegie Mellon University and a BS in Computer Science from University of Maryland, College Park.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*Richard W. Edelman
*C. Boyden Gray
*Alexander V. Mirtchev
*John J. Studzinski

TREASURER
*George Lund

DIRECTORS
Stéphane Abrial
Todd Achilles
*Peter Ackerman
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Colleen Bell
Stephen Biegun
*Rafic A. Bizri
*Linden P. Blue
Adam Boehler
Philip M. Breedlove
Myron Brilliant
*Esther Brimmer
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Teresa Carlson
James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
Beth Connaughty
*Helima Croft
Ralph D. Crosby, Jr.
*Ankit N. Desai
Dario Deste
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Thomas R. Eldridge
Mark T. Esper
*Alan H. Fleischmann
Jendayi E. Frazer
Courtney Geduldig
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Murathan Günal
Amir A. Handjani
Frank Haun
Michael V. Hayden
Amos Hochstein
*Karl V. Hopkins
Andrew Hove
Mary L. Howell
Ian Ihnatowycz
Wolfgang F. Ischinger
Deborah Lee James
Joia M. Johnson
*Maria Pica Karp
Andre Kelleners
Henry A. Kissinger
*C. Jeffrey Knittel
Franklin D. Kramer
Laura Lane
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Mian M. Mansha
Marco Margheri
Chris Marlin
William Marron
Gerardo Mato
Timothy McBride
Erin McGrain
John M. McHugh
H.R. McMaster
Eric D.K. Melby
*Judith A. Miller
Dariusz Mioduski
*Michael J. Morell
*Richard Morningstar
Dambisa F. Moyo
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Thomas R. Nides
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
W. DeVier Pierson
Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Robert Rangel
Thomas J. Ridge
Lawrence Di Rita
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Frances M. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Gine Wang-Reese
Ronald Weiser
Olin Wethington
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Ashton B. Carter
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Colin L. Powell
Condoleezza Rice
Horst Teltschik
John W. Warner
William H. Webster

*Executive Committee Members

List as of April 22, 2021

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor, Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org