

VELOCITY

Insights for Federal Innovators

V1. 2023

BY **Booz Allen**

 USERNAME

 ******

☐ I consent to the use of my data

TRUST?



**Rebuilding Trusted
Relationships with
Emerging Technologies**



A NOTE TO READERS

The ideas and opinions contained herein are those offered by the individual authors. They are intended as considerations in the associated technical areas discussed. They do not necessarily represent the firm's views, but offer the breadth, depth and currency of Booz Allen's technical talent and that of our partners.

CONTENTS

DEPARTMENTS

05

Letter From
the CTO

Susan Penfield

62

The Final
Word

Horacio Rozanski



[Continue to Feature Stories >](#)

FEATURES

12

Workforce

**Achieving Engineering
Excellence in the Race
for Talent**

Strategies to Engage Top
Technical Talent

Haluk Saker

18

Startups

**Traversing the Valley
of Death**

A Q&A Discussion with
the Founding Visionaries
Behind Latent AI

Beau Oliver and Josh Strosnider

22

Society & Technology

**Trust: An Imperative
for Our Collective Future**

Rebuilding Trusted Relationships
Through Emerging Technology

*Sahil Sanghvi, Julie McPherson,
and Ryan T. Wright*

Page 18

“From a startup perspective, we’re building core technology capabilities to enable organizations to do many things. So, we have to be able to convey to the customers that, indeed, the technology can do what they want but is not limited to a specific use case.”

—**Sek Chai**, Chief Technology Officer of Latent AI

“Over the next 30 years we will see emergence of a highly distributed and edge-AI-enabled conflict threatening our national security. ... Nations that excel in AI, autonomy, quantum computing, brain-computer interfaces, and resilient self-organizing swarm systems, etc., will have distinct advantage.”

—Bilal Zuberi, General Partner at Lux Capital

54

Ventures

Invest, Activate, and Scale

Emerging Investment Models to Accelerate Mission Execution

Brian MacCarthy, James Gadea, and Helen Phillips

58

CIO Corner

Views From Our Modern Lakehouse

Inside Booz Allen’s Enterprise Data Platform

Brad Stone, Marisa Santisi, Matthew Langevin, Ramy Mansour, and Michael Tsyvine

MISSION SPOTLIGHTS

29

NATIONAL SECURITY
A New Paradigm for National Security Innovation?

Balancing New Technologies with Secure Collaboration
Munjeet Singh, Paul Chi, and Saurin Shah

34

DEFENSE
Achieving Decision Advantage by 2025

Components of the AI-Enabled Battlespace
Steve Escaravage and Matt Tarascio

38

CITIZEN SERVICES
Solving Global-Scale Challenges through a Data Ecosystem

Advancing Mission by Bridging Gaps between Physical and Digital Spaces
Frank DiGiammarino, Prachi Sukhatankar, Kathleen Featheringham, and Josh Strosnider

COLUMNS

COMPUTING TECHNOLOGY

The Quantum Cyber Threat 06

Preparing Today for the Forthcoming Post-Quantum Cryptographic Standards

JD Dulny, Jordan Kenyon, and Dylan Rudy

SOFTWARE DELIVERY

Enterprise DevSecOps in Action 09

From Code to Combat

Steven Terrana, Josh Boyd, Theresa Lynch, and Vincent Simpson

TECHNOLOGY DESIGN

Digital Twins for Modern Government 42

Widening the Aperture for Agility, Resilience, and Competitive Edge

Sandra Marshall, Trishna Lovley, Jennifer Jenkins, and Colin Corridon

CYBERSECURITY

Putting Zero Trust into Practice 46

Fitting the Pieces Together for Advanced Cyber Defense

Imran Umar, Michael Lundberg, and Matthew Snyder

EMERGING ISSUE

Metaverse and Web3: Hype vs. Reality 49

Collaboration, Experience, and Trust for the Next Wave of Technologies

Dan McConnell, Elliot Mandel, and Chris Hample



*The Helix, Booz Allen's Center for Innovation
(Washington, DC)*



At Booz Allen, I have a front-row seat to the discovery of mission capabilities and solutions. And today, as emerging technologies transform and enhance every area of government, it is a truly dynamic time to serve as chief technology officer.

Whether it's achieving decision advantage at the edge, optimizing intelligence for speed and impact, or modernizing services for the American public, new technologies are fueling far-reaching impacts, including some we can't yet predict. With the acceleration of so many advances, I believe we are at a critical juncture to explore, experiment, and reimagine how each mission will operate tomorrow and far into the future.

At this exciting moment, I'm pleased to share with you the first issue of **Velocity**, Booz Allen's annual publication to help leaders and practitioners in government and industry answer urgent questions and access fresh insights at the intersection of mission and technology. Those questions include: How can emerging technologies rebuild trust in digital society? What can we learn from current examples of mission transformation? What new capabilities are poised to impact the nation's most critical systems?

As historic opportunities come into focus, federal agencies in all sectors can benefit from the most powerful technologies they've deployed in generations—from digital twins (page 42) to quantum computing (page 6) and beyond. I invite you to explore the stories we've gathered of innovation unfolding in the federal sector. You'll find timely perspectives from Booz Allen experts together with voices from across the industry. In our cover article, my colleagues examine the erosion of trust in digital society and how emerging technologies can play a role in rebuilding it.

Today's waves of disruptive technology show no sign of slowing down, and your mission is at the center of the action. Together, we can spark new ideas about the future of government, learn from emerging trends and capabilities, and realize an ambitious vision for the future.

Thank you for taking this journey with us.

A handwritten signature in cursive script that reads "Susan L. Penfield".

Susan Penfield

*Chief Technology Officer
Booz Allen*

The Quantum Cyber Threat

NEW THREATS WARRANT NEW QUANTUM-READY DEFENSES

Dylan Rudy, Jordan Kenyon, and JD Dulny

By capitalizing on quantum mechanical properties, quantum computers process information in ways that fundamentally differ from today's "classical" computers. These novel computing techniques create exponential speedups for certain types of problems, including the math problems today's encryption algorithms use to protect data.

For this reason, quantum computers threaten to break the encryption that provides the essential foundation of modern cybersecurity. This ubiquitous threat will affect the Federal Government and every major commercial industry. Organizations need to begin preparing

today to transition to new cryptographic algorithms that provide security against both classical and quantum cyberattacks.

New Cryptographic Solutions

In 2016, the National Institute of Standards and Technology (NIST) opened a competition to identify classical solutions to this quantum threat. Known as Post-Quantum Cryptography (PQC), these solutions can be deployed with current computing resources. PQC algorithms demonstrate resistance to attacks using both classical and quantum computing hardware. In July 2022, NIST announced the first wave of algorithms selected as new quantum-resistant cryptographic

standards. In the same announcement, NIST detailed its plans for additional rounds of standardization.

The Federal Government has already taken action to begin the implementation of PQC from NIST, the National Security Agency, and the May 2022 executive mandate on "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems." The journey to post-quantum cybersecurity will be challenging, but organizations can begin making progress today by:

1 Inventorying their cryptographic algorithms; **2** Testing new cryptographic solutions; **3** Designing strategies for cryptographic agility

Lattices Securing the New CRYSTALS Algorithms

Figure 1A

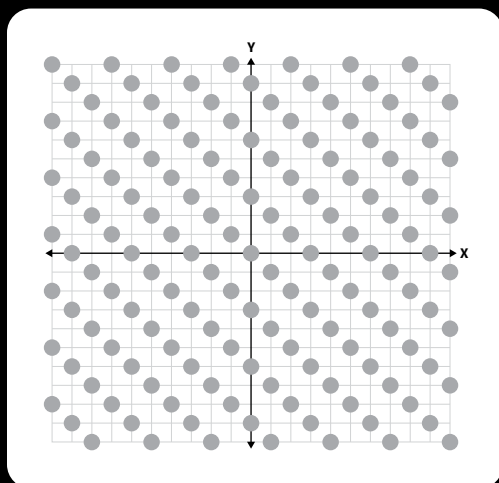


Figure 1B

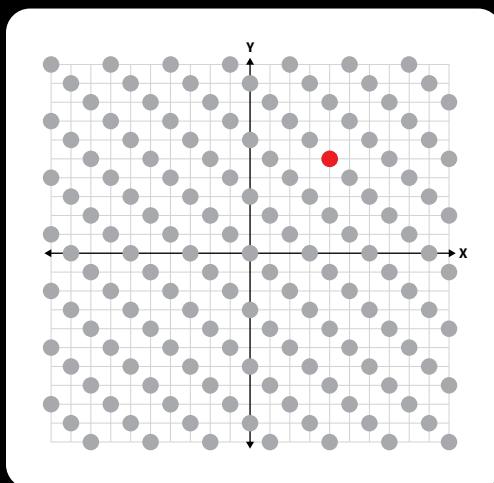
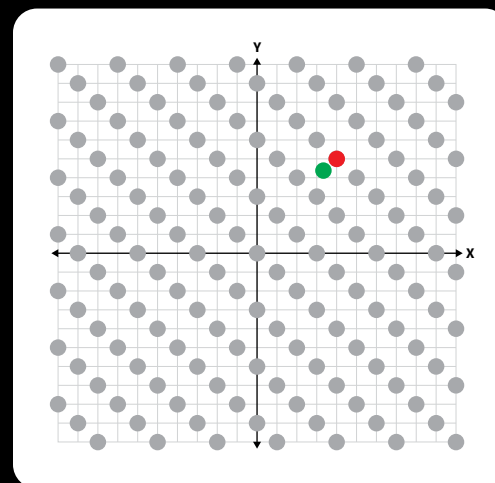


Figure 1C



Due to demonstrated resistance against attacks using quantum computers, many of the selected PQC algorithms use hard math problem in a lattice, described as a grid of points (Figure 1A). The server picks the secret point in red (Figure 1B), then publishes a public green point off the lattice (Figure 1C). Users encrypt their messages using the public green point and the server decrypts using the secret red point.

For an attacker to steal information, they would have to figure out the coordinates of the red point only knowing the lattice and the coordinates of the green point. The challenge becomes exponentially harder with the complexity of the lattices used in these PQC algorithms.

Figure 1

The journey to **post-quantum cybersecurity** will be challenging, but organizations can begin making progress today by inventorying their cryptographic algorithms; testing new cryptographic solutions; and designing strategies for cryptographic agility.

1 Inventorying Cryptographic Algorithms

Organizations must identify vulnerable cryptography within an enterprise before they can fully transition to quantum-resistant algorithms. Yet many lack an authoritative cryptographic inventory. The scope of this assessment is difficult to overstate. An organization can begin the process by identifying cryptographic algorithms used at authentication touchpoints and to secure data in transit and at rest. However, to efficiently guide PQC transitions, these inventories will need to do more than identify vulnerable cryptographic algorithms.

Truly robust inventories will assess cryptography lifecycles and policies governing them. They will allow organizations to understand their vulnerability to quantum cyberattacks and prioritize their highest-value assets and longest-lived data for early transition, and they will help mitigate risks of attacks focused on intercepting data today for later decryption with a cryptographically relevant quantum computer (CRQC).

2 Testing New Cryptographic Solutions

PQC algorithms will not be simple drop-in replacements for the vulnerable cryptography organizations currently deploy. Secure implementation requirements and performance tradeoffs require agencies to carefully test cryptographic solutions ahead of full-scale deployments. For example, PQC algorithms require much larger key sizes than today's cryptographic algorithms and may require upgraded hardware to accommodate the increased workload. Testing can inform decisions about procuring new equipment and implementing different PQC algorithms to secure different applications in the same enterprise.

The initial slate of quantum-resistant cryptographic standards selected by NIST include one key-establishment algorithm (CRYSTALS-KYBER) and three digital signature algorithms (CRYSTALS-Dilithium, FALCON, and SPHINCS+). These new algorithms make use of different hard mathematical problems than those used in today's public-key cryptography. Many of these algorithms rely on their problems being embedded in a mathematical structure known as a lattice to provide computational security against attackers using both classical and quantum computing hardware (see Figure 1).

Organizations can capitalize on the recent announcement by taking this opportunity to test these initial four algorithms within their own systems. As organizations develop cryptographic inventories and test the new algorithms in mission-critical use cases, it is important for them to define a methodology for future algorithm deployment and migration efforts. In the announcement, NIST highlighted its intent to continue vetting additional PQC algorithms based on different underlying mathematics to ensure computational diversity. Improving cryptographic agility will be instrumental in responding as NIST standardizes additional algorithms.

3 Designing Strategies for Cryptographic Agility

Discussions of PQC often touch on the concept of cryptographic agility: the ability to rapidly find, monitor, update, and replace cryptographic algorithms without disrupting a larger system. Today's cybersecurity infrastructure was not built for cryptographic agility, but this era of new cryptographic standards and evolving threats requires a paradigm shift. Due to the evolving nature of quantum computing, this may not be the last time government and commercial entities will need to

update their cybersecurity postures to reflect changing cryptographic standards. While preparing to deploy forthcoming PQC standards, organizations should start developing cryptographic policies and protocols that allow them to rapidly respond to emerging threats.

Cybersecurity through Computationally Intractable Problems

Public-key cryptography protects data using two related “keys,” specific numbers that can be used to read otherwise obscured information. These cryptographic algorithms are used to establish secret keys, authenticate users, and encrypt data. The two keys consist of a publicly known value and a mathematically related private value.

To break public-key cryptography, an adversary would have to crack the computationally intractable problem underpinning it—like finding the two prime factors of a large number. Scientists have estimated that today's most sophisticated high-performance computing hardware would require more than a lifetime to complete this task. However, a cryptographically relevant quantum computer (CRQC) could solve these problems in hours using quantum algorithms that already exist. A CRQC is a fault-tolerant quantum computer with the sophistication required to break modern encryption algorithms. CRQCs don't exist yet, but it is just a matter of time as investments pour in from nations and corporations striving to secure computational advantage.

Hold Now, Decrypt Later Attack

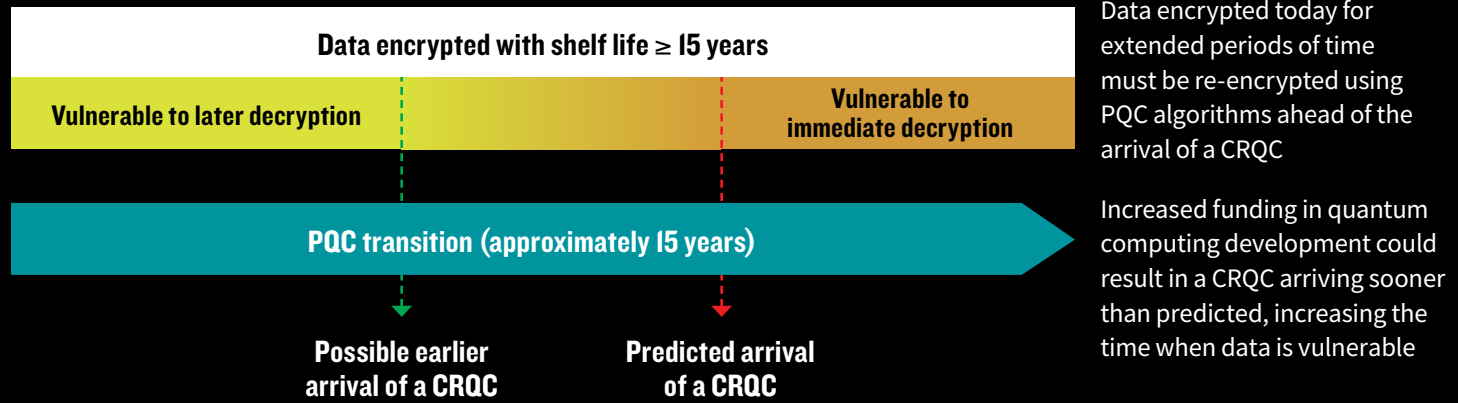


Figure 2: The Transition to PQC

The Transition to Post-Quantum Cryptographic Standards

The challenging timelines associated with the PQC transition underscore the importance of starting today. Figure 2 highlights the risk of waiting, given the uncertain arrival of a CRQC and extensive timeline to fully transition to PQC. NIST estimates that adopting PQC could take an organization approximately 15 years.

In September 2022, the National Security Agency announced its decision to deploy CRYSTALS-KYBER and CRYSTALS-Dilithium in an updated cryptosuite designed to protect National Security Systems (NSS). The goal is to ensure all NSS vendors retire currently deployed algorithms and

transition to using the new algorithms exclusively by 2035. To address the extensive risks CRQCs will pose to U.S. infrastructure and interests, organizations should start PQC transition planning and prototyping as soon as possible. Doing so will enable them to resecure high-value assets with the right PQC algorithms—and efficiently navigate critical tradeoffs in optimizing both security and performance.

Dylan Rudy, Ph.D. and **Jordan Kenyon, Ph.D.** are scientists at Booz Allen, and **JD Dulny, Ph.D.** leads the firm's quantum business.

SPEED READ

Quantum computers process information using novel computing techniques that threaten to break the encryption providing the essential foundation of modern cybersecurity.

The National Institute of Standards and Technology selected the first wave of algorithms that demonstrate resistance to attacks using both classical and quantum computing hardware.

Government and industry leaders can begin taking critical steps today to mitigate the risks quantum computers pose to their cybersecurity infrastructure by inventorying their cryptographic algorithms; testing new cryptographic solutions; and designing strategies for cryptographic agility.

Enterprise DevSecOps in Action

FROM CODE TO COMBAT

Theresa Lynch, Steven Terrana, Josh Boyd, and Vincent Simpson

Gone are the days when engineering teams started from zero. Whether we're talking IT, software development, or cybersecurity, commoditized toolkits and repeatable business processes eliminate the need to build from scratch every time—and can mitigate risk and technical complexity across the enterprise.

In *Accelerate: The Science of Lean Software and DevOps*, the authors Nicole Forsgren, Jez Humble, and Gene Kim found that high-performing development teams have “46 times more frequent code deployments, 440 times faster lead time from commit to deploy, 170 times faster mean time to recover from downtime, 5 times lower change failure rate (1/5 as likely for a change to fail).” The right set of standard, versatile, reusable tools and processes can empower high-performing teams to stand up development environments in literally hours rather than four to eight months, so they can start producing on day one.

Additionally, when developers are choosing from the same set of tools that are preconfigured for security and ready for integration, cyber teams are freed to spend less bandwidth on project-by-project configuration and enforcement and more time doing higher-pay-off work, such as maintaining zero trust access policies, monitoring activity across the network in real time, and investigating suspicious behavior when it occurs. Shared tools and technical governance can keep supply chain complexity from ballooning out of control, making it a far simpler proposition to continuously monitor and to verify that all vendors and service providers remain in a secure and trusted state.

To create this highly efficient foundation for continuous delivery across the life of a project or product, a templated DevSecOps pipeline plays a significant role. With near-immediate, quantifiable benefits to

software delivery speed and security, it opens the door for organizations to start incorporating standardization and technical governance at scale.

Enterprise DevSecOps Pipeline

Setting up a templated DevSecOps pipeline involves so many standard processes that it hardly makes sense to build a new one at the beginning of every project. By offering a preconfigured, preapproved pipeline—one that leaves sufficient room for tailoring where customization is necessary—organizations can reduce delivery times, freeing up more bandwidth for innovation where it matters most. This is especially impactful for complex enterprises that need access to continuous delivery with consistent security and a standard quality of deployment.



High-performing development teams have:

46 x
more frequent code deployments

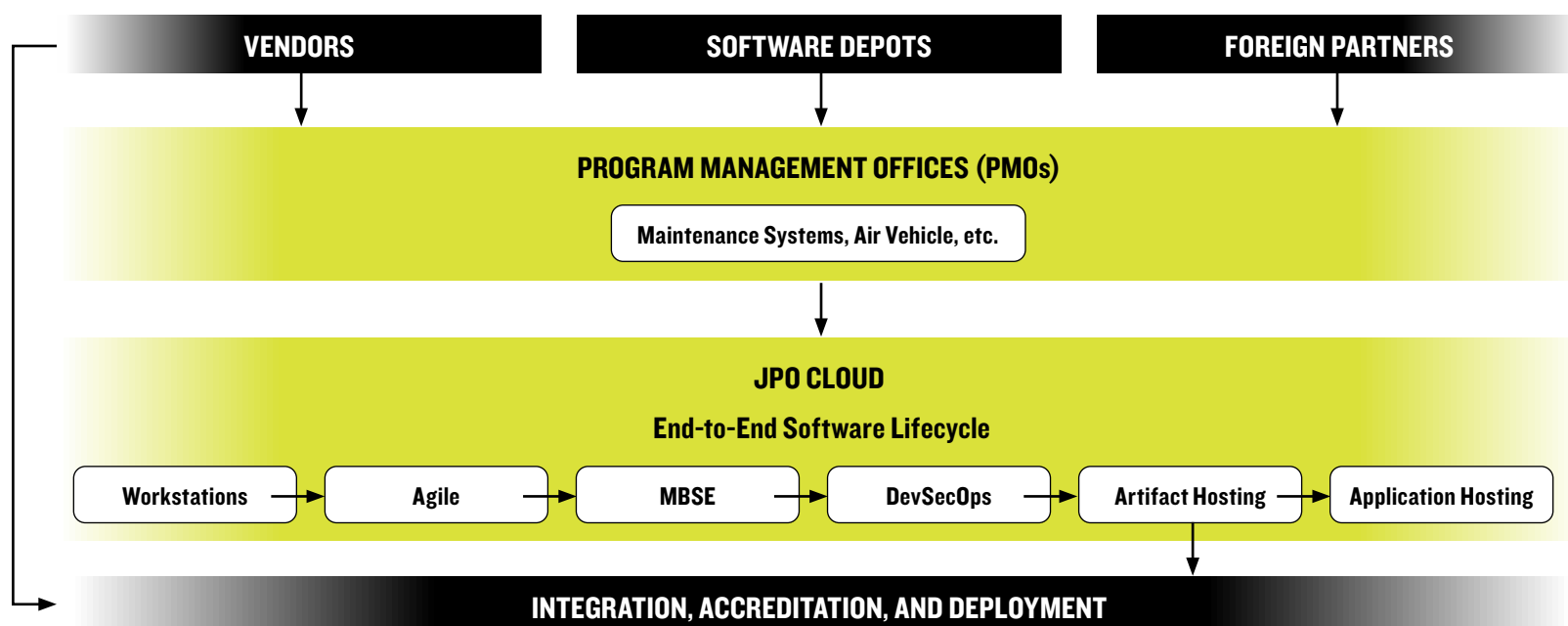
440 x
faster lead time from commit to deploy

170 x
faster mean time to recover from downtime

5 x
lower change failure rate

Source: *Accelerate: The Science of Lean Software and DevOps: Building and Scaling High Performing Technology Organizations*

Figure 1: End-to-end software development lifecycle



Let's look at an example of this in action.

F-35 Software Development at Scale

The F-35 is the world's most advanced multi-role fighter. It performs a variety of air superiority, strike, and other missions for the Air Force, Navy, and Marine Corps, as well as for militaries of select U.S. allies. The Defense Department plans to acquire more than 2,400 F-35s, while allies are expected to purchase hundreds more, according to the U.S. Government Accountability Office.

As expected, these complex aircraft present unique software development challenges. The F-35 is comprised of over 400 applications that span the entire spectrum of technology stacks, from hardware integrations to low-level firmware, graphical interfaces for the warfighter, and supporting mission systems. These applications are built using a myriad of programming languages (C/C++, Node, Java, Python, etc.) and jets are distributed around the world. F-35 leadership has been focused on strategic priorities for this global mission

and program that have included:

- **Lead Time to Development.** Decreasing the time it takes to develop new capabilities and upgrade systems at the speed of relevance.
- **Affordability.** Decreasing the cost per flight hour to maintain the aircraft (recently calculated at \$33,000).
- **Intellectual Property (IP) Rights.** Facilitating more open participation in software IP to introduce industry competition and drive down the costs of innovation.

As part of that journey, the F-35 Joint Program Office (JPO) sought a platform that would modernize the way its complex mission and business systems software is built, certified, and delivered to the field. Creating tool-agnostic, templated DevSecOps pipelines that can be reused by every team on the platform eliminates the need to build a dedicated pipeline from scratch for each new development project, saving weeks or even months with each project.

This government-owned platform will eventually support the software development efforts of 4,000 government software engineers, as well as many vendors and partner-country developers and hundreds of software applications. Historically, it was less common for the government to own the source code being developed for these applications as numerous Defense Industry Base (DIB) partners controlled the IP needed to modernize the F-35. With the new approach, these applications can be fully owned and controlled by the government, allowing for flexible and rapid innovation and delivery.

Today, the F-35 DevSecOps platform has four broad capabilities:

- 1) **A collaboration suite.** This supports agile processes, wikis, chats, and task management, enabling real-time collaboration among software engineers who often work remotely.

By creating tool-agnostic, templated DevSecOps pipelines that can be reused by every team on the platform, it eliminates the need to build a dedicated pipeline from scratch for each new development project, **saving weeks or even months** with each project.

The foundational benefit of the F-35 DevSecOps platform is that it provides all stakeholders—including software depots, program management offices, vendors, and foreign partners—a **centralized, accredited environment** that supports the end-to-end F-35 software-development lifecycle.

2) An Engineering Suite. This provides tools and architectures that support model-based systems engineering and create a common environment for teams that design, architect, and gather requirements for new software. The engineering suite also accelerates requirements and validation processes.

3) A Software Suite. This gives developers a wide range of toolsets to create diverse portfolios of applications while enforcing security compliance controls and standards required for delivery.

4) Landing Zones For Software Products. This enables software teams to host their applications in the cloud in a way that complies with the Joint Program Office's governance and standards. The platform also serves as a cloud service provider for F-35 applications after they go into production.

The foundational benefit of the F-35 DevSecOps platform is that it provides all stakeholders—software depots, program management offices, vendors, and foreign partners—a centralized, accredited environment that supports the end-to-end F-35 software-development lifecycle (see Figure 1 on previous page). From local development environments and model-based systems engineering to DevSecOps and hosting, stakeholders from vendors to depots to foreign partners have shared services that accelerate software delivery and allow teams the autonomy to make their own decisions. For some teams, the autonomy to write the pipeline and own the infrastructure is worth it, particularly when there are unique requirements or they have already invested in work that is not easily refactored. Ultimately, the F-35 DevSecOps platform allows for the full spectrum of development, whether that is providing standardization for a fast path to capabilities or offering shared services for bespoke projects.

With a mesh of software factories, the team is also building and connecting shared spaces for collaboration; specific vendor enclaves for proprietary IP; and on-premises development, allowing components to flow between all the various factories. The platform's intrinsic flexibility and scalability will enable it to accommodate the hundreds of applications that will support the F-35, regardless of which programming languages and tools are needed to develop and maintain them. Moreover, the platform will save significant amounts of time that would otherwise be needed to build discrete pipelines for each application development team.

Balancing Competing Pressures

With increasing mission complexity and a backdrop of highly visible exploits and large-scale supply chain vulnerabilities, federal IT leaders are wrestling with often competing pressures: innovate quickly and at scale with rapidly advancing technology and mitigate risk in the face of an ever more relentless cyber threat. With no shortage

of national and global challenges on the horizon, standardization-focused tools and major programs, such as the F-35 Joint Program Office, demonstrate the ability to advance security and deliver rapid capabilities for today's mission.

It remains important to note that enterprise standardization must be balanced with strategic flexibility and customized for unique operations and technical environments. But technical governance and a well-equipped, standardized toolkit can give engineers the baselines they need to securely and efficiently accomplish their objectives while leaving plenty of room to innovate.

Theresa Lynch and Vincent Simpson
lead program management for the F-35 DevSecOps Platform.

Steven Terrana and Josh Boyd *advance Booz Allen's software factory capabilities, using programs like the F-35 as models to build standard patterns and common protocols for templated DevSecOps.*

SPEED READ

Commoditized toolkits and repeatable business processes eliminate the need to build from scratch every time and can mitigate risk and technical complexity across the enterprise.

Organizations that adopt a templated DevSecOps pipeline can save development teams thousands of hours, from setup to deployment. This is especially impactful for complex enterprises that need access to continuous delivery with consistent security and a standard quality of deployment.

The F-35 Joint Program Office created a DevSecOps platform to modernize the way its complex mission and business systems software is built, certified, and delivered to the field. It will eventually support the software development efforts of 4,000 government software engineers, as well as many vendors and partner-country developers and hundreds of software applications.





WORKFORCE

ACHIEVING ENGINEERING EXCELLENCE

in the Race for Talent

STRATEGIES TO ENGAGE TOP TECHNICAL TALENT

Haluk Saker

The war for technology talent is not new, but the competition is escalating. Non-technology and multi-industry companies are increasingly hiring from the same pool of skilled technologists as the largest technology companies and startups.

Within federal agencies, competing in this environment—and hiring and retaining top engineers and developers—impacts the success of the nation’s most critical mission systems. IT leaders within government need to navigate a unique set of factors compared to their industry counterparts, from hiring authorities to security clearances. The Government has launched several efforts to create new pathways for recruiting technical talent into mission programs. For example, the new U.S. Digital Corps is a two-year fellowship for entry-level technologists to work on specific projects, with the opportunity to convert to permanent positions.

As programs emerge to accelerate recruitment and meet critical demand, it is important to reexamine the end-to-end experience of engineers and technologists who design, build, and integrate mission-critical solutions as programs emerge to accelerate recruitment and meet critical demand. **Three important areas to address are prioritizing the right skills, engaging talent in new ways, and redefining roles for the future.**

While AI and data engineering capabilities are essential—and government must invest in them to stay ahead of near peers—they must be predicated on a **strong and modern technology foundation.**

Prioritizing the Right Skills

Across the Federal Government, agencies are investing in IT modernization to upgrade and secure critical digital infrastructures. With this, there is an immediate demand for skilled talent in areas such as cloud computing, programming, and software automation.

At the same time, there is an increased focus on recruiting experts in artificial intelligence (AI), machine learning (ML), and other emerging technologies. According to data from Emsi, job listings in the United States that included AI as a skill increased 91% in 2021, and those with ML increased 81% (source: economicmodelling.co.uk). While AI and data engineering capabilities are essential—and the Government must invest in them to stay ahead of near peers—they are predicated on a strong and modern technology foundation. It is imperative to continue focusing today’s recruiting and talent development on modern engineering and cloud-native development experience to enable a future technology workforce where AI expertise may become a dominant segment.

Here are three imperatives for technical hiring managers:

- **Don’t equate years of experience with skill:** The value of an engineer is indicated by the quality of their products—not by their years of experience. For example, a qualified candidate with two years of experience should be evaluated for target skill sets next to a candidate with 20 years of experience.
- **Don’t look for specific programming languages:** Federal government systems may take years to build and will often have a multiyear life span. Rather than looking for specific coding experience, interviewers need to evaluate candidates’ hands-on experience with modern technology stacks that they can apply throughout a system’s long life span.
- **Do evaluate more than programming skills:** Hiring managers should assess foundational skills, such as math, critical thinking, and problem solving. The best candidates demonstrate how to apply technology with purpose—considering performance, accessibility, resiliency, maintainability, interaction with the data store, and other factors that go beyond the ability to write code.

It is important to note that the technology workforce responsible for critical mission modernization—whether that’s upgrading a public-facing system or deploying new capabilities—should represent the layered and complex world we live in. New and different perspectives must address the nation’s greatest challenges, so inclusivity and diversity in the IT workforce are priorities across government.

“When the technologists who build the nation’s digital platforms reflect the public they serve, the systems they build are richer and more equitable and inclusive for all—factors that enhance user trust in government. HR leaders across government are integral to building the federal workforce of the future—where technical skills are evaluated along with a diversity in backgrounds and voices.”

Aimee George Leary, Booz Allen’s Global Talent Officer



A New Talent Model at Booz Allen

How Human Resources Is Innovating to Grow Technical Talent

To meet growing capacity, compounded by increasing demand for highly technical talent, Booz Allen determined it needed an additional 20,000 new hires over three years. To achieve this goal, the firm’s HR team built an integrated Technical Talent System that unified five traditionally separate components into one platform.

With the new framework, the firm began the journey by streamlining and standardizing job families for technical skills, using data and analytics to narrow more than 2,000 job families to 220—enabling the company to hire technical talent with greater consistency and scale.

More about this initiative and the five human capital components can be found in *Building an Innovative Model for Growing and Inspiring Tech Talent* by Aimee George Leary, talent strategy officer at Booz Allen, and Robin Erickson, vice president of Human Capital at The Conference Board (2022).





With the right contractual guardrails, engineers can expand their skillsets, continue to challenge themselves as they integrate new technologies, and more quickly see the impact of their work in production.

Engaging Talent in New Ways

Once technical talent is hired, organizations must keep them energized over time. Common levers such as compensation and career development paths help improve retention, but it is additionally important to consider the engineering experience and technology culture.

For example, many critical federal systems are built over multiple years. Technical talent may spend a large part of their career on a single system to scope, design, operationalize, and then maintain it. Phased design approaches can help keep talent engaged across multiyear projects and use modern development practices to:

- Segment the domain architecture into smaller services and applications, sequencing the launch of business processes
- Allow engineers to more rapidly test their work in a production environment, as microservices and applications
- Enhance the technology stack by allowing architects to harness the newest development technologies for different services over the course of a multiyear project

How agencies specify contracts will also impact the technology stack. There can be valid cases for technology lock-in when developing certain mission applications. However, where possible, contracts can be written in a flexible way, allowing technical architects to select the best capabilities for an evolving technology stack. With the right contractual guardrails and incentives, engineers can expand their skill sets, continue to challenge themselves as they integrate new technologies, and more quickly see the impact of their work in production.

Defining Roles for the Future

Standard engineering projects include a scope for roles such as Scrum Masters and solution architects. But delivering successful projects today requires an evaluation of new roles, both within government and for its technology partners. Specifically, senior roles in product management and engineering are key to accelerating large-scale delivery projects.

Product managers help track the vision and end state of an IT system and define an integrated roadmap for how to get there. With a deep understanding of strategy, planning, prioritization, and customer needs, product managers provide leadership and discipline to digital transformation, coordinating all aspects of development. They ensure the team delivers solutions that align with customers' needs and that meet expectations for user access and functionality.

By contrast, when siloed business- and feature-focused teams lead program delivery, projects suffer from communication gaps and lack of agility, the focus turns to outputs, not outcomes. As a result, requirements, development, and testing happen in isolation.

The **chief engineer** is also crucial to project success. The chief engineer oversees all individual technical leads and is accountable for the success of software delivery projects as well as the broader roadmap for IT implementations. The chief engineer makes final technology-related decisions for a cascade of stakeholders, including the chief software engineer, chief data engineer, and chief security engineer.



With a deep understanding of strategy, planning, prioritization, and customer needs, **product managers and analysts** provide leadership and discipline to digital transformation, coordinating all aspects of development.

Inside government agencies, the chief engineer is also critical in assessing contractor proposals and managing technical vendors. They are adept at determining whether the skills and qualifications within a proposal will likely translate into a better mission system—or if the requirements for a modern, resilient design need to be articulated with more precision to ensure success.

Ultimately, the challenges related to hiring and retaining top technical talent today are highly complex, and the solutions will be as well. But for the people working in and with government to implement successful technology programs, we can begin with prioritizing and evaluating candidates with in-demand technology skills, engaging and retaining them by employing a modern engineering environment, and reimagining the profile of technical leaders to coordinate delivery with an unyielding focus on the end state.

Haluk Saker is a senior vice president at Booz Allen overseeing large-scale software modernization. He is coauthor of the Enterprise DevOps Playbook.

SPEED READ

Prioritizing the right skills, engaging talent in new ways, and redefining roles for the future are the three important areas where progress can be made in the war for talent.

Using phased design processes and modern contracts will help keep talent engaged.

Delivering successful projects today requires an evaluation of new roles—specifically product manager and chief engineer—with an unyielding focus on the outcome for users.

Traversing the Valley of Death:

A DISCUSSION WITH FOUNDERS

On the perilous journey from prototype to successful application, new technologies must successfully navigate a risk-filled valley of death. It's there that many once-promising innovations are forever discarded. Numerous industry studies report that around nine out of ten technology startups eventually fail.

Startups focused on the government space may face this all-too-common fate when they lack access to government clients, an understanding of agencies' key problem sets, or direction from established partners to apply the right technology to the right problem at the right time. And the path to government adoption involves a complex acquisition process that is among the last, most daunting pieces of terrain to cross.

Reaching the Other Side, Unscathed

The federal government has an important, proactive role to play in cultivating a technology ecosystem where innovation is able to take root—and there are new approaches to consider around funding and contracting that are critical for creating the best environment for emerging technologies to thrive.

But in the process of helping innovative startups defy the odds and advance their innovations through and beyond the valley of death, it is valuable for government and industry leaders to understand the lived experiences of founders today.

We recently spoke with the co-founders of one such startup, Latent AI, to get their first-hand perspectives on this journey. Latent AI was founded in 2018, and the company's tinyML technologies help organizations rapidly run complex algorithms in low-power environments. This major breakthrough in artificial intelligence (AI) engineering creates a new level of decision advantage possible for warfighters and analysts operating in demanding environments at the tactical edge. Here's what we learned from Jags Kandasamy (the company's chief executive officer) and Sek Chai (the company's chief technology officer) about what it takes to turn a smart idea into a powerful technology that goes on to transform real-world missions.

A Q&A WITH THE VISIONARIES BEHIND LATENT AI

Beau Oliver and Josh Strosnider



From left to right: **Jags Kandasamy**, Chief Executive Officer and **Sek Chai**, Chief Technology Officer at Latent AI

Q Let's start with the basics. In founding Latent AI, why did you decide to focus on AI at the edge?

A **SEK:** We knew organizations could achieve more with their AI systems and transition more efficiently to the edge. On the battlefield, where AI models are core to situational awareness, you're dealing with constraints on things like computing power and hardware, and you don't want a system to have to recharge or download data. There's a very similar kind of situation on the commercial side. Think about robotic and autonomous systems. We saw the dual-use applications of more agile AI technology, and we have gone about addressing the need for low latency and what we call adaptive AI.

Q Could you tell us about some of the challenges you encounter in navigating from initial development to providing your technology to the federal government?

A **JAGS:** We're a startup with limited resources, and we're trying to figure out—as a commercial company—how we fit in. We have to analyze what the government procurement processes are and what channels we can go after. How do we identify the points of contact within the different agencies and the challenges they're facing? And from a proposal perspective, do they really mean what they're saying, or is there a hidden question behind what they're asking for?

SEK: It's also hard when a customer asks for a very specific solution to solve a certain problem. From a startup perspective, we're building core technology capabilities to enable organizations to do many things. So, we have to be able to convey to the customers that, indeed, the technology can do what they want but is not limited to a specific use case. We're always learning as part of this journey on how to best position our technologies for new applications.





“It’s essential to have a sounding board and strategic partner throughout the process that provides hands-on counsel to help figure out the procurement process, how to prepare for procurements, and how to present things to government in a way that’s most useful for federal leaders.”

—Jags Kandasamy, CEO and co-founder of Latent AI

Q Speaking of what you’ve picked up along the way, what were some of the strategies you implemented to accelerate your journey across the valley of death?

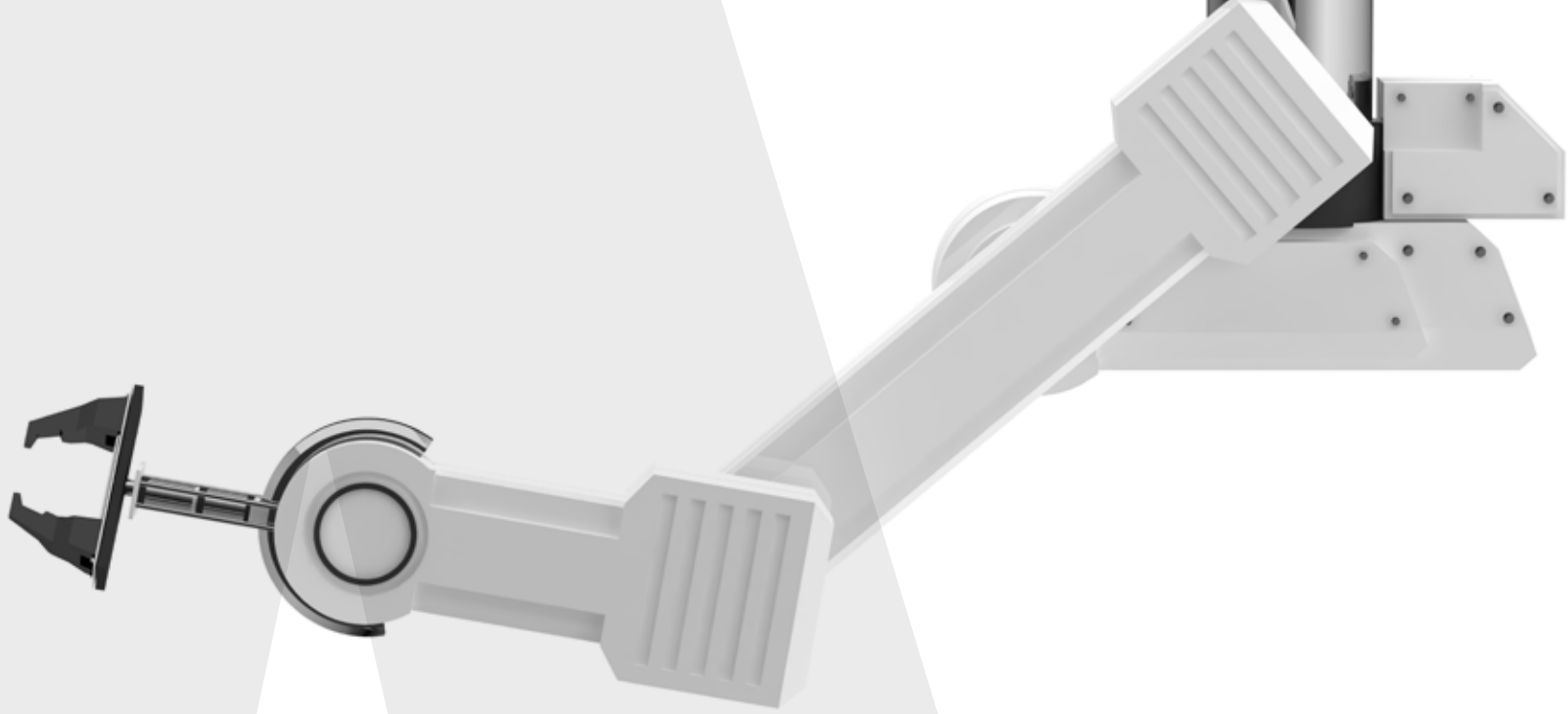
A **SEK:** One thing we’ve learned is to constantly and proactively look for feedback. Not only do we find partners and federal systems integrators helpful in navigating proposals and going out and talking to the Department of Defense, but we are engaging with their technical teams as well, including at Booz Allen. We know that our product needs to mature. It needs to meet requirements we may not initially know about. We put our products in front of those technical teams, so they’re using them and giving us feedback. And we’re taking that feedback, maturing the product, and incorporating new capabilities, so it’s never at a standstill. It evolves so that we can start solving mission-critical challenges.

JAGS: Another benefit of this feedback process is that as we build and deliver, we’re actually solving for both commercial and federal uses and battle-testing on both sides. The use cases may be different, and the feedback may be different, but all of that comes in to make the product more robust.

Q Let’s switch over to the client side for a moment. We know that federal IT leaders are inundated with investment decisions on a daily basis and all of the new capabilities that are emerging. And then you add in the acquisition process to manage on top of that. When thinking about clients, how does Latent AI continue building its understanding of customer needs to ultimately provide the most value to government?

A **JAGS:** We have a strong team—with multiple PhDs in the organization, people with expertise from the industry as well as the startup side, in terms of building excellent technology. But we needed to “get out of the building,” talk to customers, and figure out which direction we needed to go. It’s essential to have a sounding board and strategic partner throughout the process that provides hands-on counsel to help figure out the procurement process, how to prepare for procurements, and how to present things to government in a way that’s most useful for federal leaders.

Also, as a technology provider, we’re building a tool to be multipurpose, multiuse case, and multiuser friendly, and we may lose focus sometimes because we’re trying to broaden our approach. This is where our partnerships come in to help us think about specific features we can bring to bear and how we can technologically address some of the problems the customer is facing. This guidance has helped us focus while at the same time bringing us to a broader customer base.



Q Looking ahead, what are some of the mission use cases you're most excited about?

A JAGS: Our focus has been on computer-vision-related use cases, as new proposals come in and new horizons open up. We're looking at different data modalities we can solve for, like natural language processing, lidar and radar, electromagnetic data, and other things.

SEK: We're also engaged with Booz Allen teams in looking at the hybrid edge—not just the sensor edge itself, but the ability to put workloads around the network infrastructure, including 5G. We're talking about security as well, so that the deployed model has “watermark” capabilities to check where it came from, how it was trained, and if it's been tampered with.

Q We're excited to be a part of that journey. For other founders like you, we know how important it is to find the right mission use cases early on and have visibility into where real needs are and where their technology can realistically be adopted and applied. And government buyers can help accelerate access to emerging technologies by taking advantage of new acquisition authorities and continuing to provide constructive feedback to startup partners along the way.

To close, if you were talking to other founders navigating the government space, what are three things you would emphasize from your experience so far?

A JAGS: We would start by telling them to exercise as much patience as they can. We've learned a lot about patience through our strategic partners, as it takes a while for contract awards and adoption to happen. Once you win, it's for the long term and it's very strategic for you as a startup. Founders should also invest in education about the procurement process. What are all the vehicles the government uses to buy technology? And they should learn and share as much as possible, because you're going through all of this with the startup community. Always pay it forward.

Jags Kandasamy and Sek Chai co-founded Latent AI in 2018 as an early stage venture spinout of SRI International. The company has been recognized on CB Insight's AI 100 and was named the 2020 Startup of the Year by IoT World.

Beau Oliver and Josh Strosnider lead Booz Allen's partnership efforts as part of the CTO organization and help drive the firm's strategies to enable, differentiate, and expand federal access to emerging technologies. Booz Allen is a strategic investor and partner of Latent AI.

TRU

 USERNAME 

 *****

☐ I consent to the use of my data

TRUST?



ST*

An Imperative for Our Collective Future

HOW EMERGING APPROACHES AND TECHNOLOGIES CAN ESTABLISH
AND REBUILD TRUSTED RELATIONSHIPS AND EMPOWER USERS

Authors: Sahil Sanghvi, Julie McPherson, and Ryan T. Wright

Contributor: Adam McCormick

Our everyday interactions—with individuals, businesses, and government agencies—are underpinned by an implicit degree of trust. It guides and informs our behavior and our willingness to continue forward with fulfilling and mutually valuable relationships. For organizations, building and maintaining trusted relationships with their customers and partners has always been crucial to their long-term success.

Trust begins with understanding customer needs and meeting them. It requires the customer to be vulnerable and open with their needs and to believe that the organization will use that information to meet them. The greater the understanding of customer needs, the greater the value the organization can provide to the customer. In many cases, this trusted relationship can be an organization's competitive advantage. Similarly, government agencies require a degree of trust from citizens to deliver benefits and services in a meaningful manner. For long-term value, companies, agencies, and customers are best served when a high degree of trust is established and nurtured.

Over the past decade, trust has increasingly become a top priority for leaders. One indicator is the emergence of a new role in the C-suite: the chief trust officer—Salesforce established the position in 2016, Airbnb in 2019, and SAP in 2020. Although the chief trust officer's primary responsibilities vary among companies, at its core the role focuses on building customer confidence in the organization's handling and use of personal information. Historically, data privacy, security, and ethics have been viewed primarily through a legal and compliance lens—based on the nature of the organization's business, ensuring standards are met for PII (personally identifiable information), the Health Insurance Portability and Accountability Act (HIPAA), payment card industry (PCI) requirements, and other compliance becomes critical. But the advent of chief trust officers may signal a shift in focus moving forward to where leading companies view customers' trust as a competitive advantage. But what is driving this movement from compliance to strategic advantage?

For long-term value, companies, agencies, and customers are best served when a **foundation of trust** is established and nurtured. The erosion of trust is a problem worth solving now, and technology is a critical lever in the solution.



An Erosion of Trust

The number of data compromises in the U.S. reached all-time highs recently, leaving customers feeling concerned about how their personal data is secured. Customers are also increasingly wary of the ways in which companies use their data and how that data is shared with third parties and data brokers. These concerns have resulted in an erosion of trust and are exacerbated when customers feel that the value being provided isn't commensurate with the data being shared. This challenge of maintaining trust is not limited to interactions between customers and companies—it exists with government agencies as well and will be a challenge they will have to overcome.

The Impact on Society

Organizations that lack customer trust can lose revenue and brand reputation, and can even cease operating. The consequences for the Federal Government and the nation are more severe. Trust in the federal system is essential for it to achieve its basic mission and for democracy to flourish. The Government relies on constituent information to plan for the future, provide essential services to its citizens, understand and solve problems facing the nation, and identify and thwart threats to its security.

An erosion of trust in government impacts levels of engagement across every corner of society—from whether people are likely to vote in elections to whether they participate in policy debates, follow health guidelines, or respond to the U.S. Census. In fact, in 2020 the Census Bureau conducted a survey about participation and found that almost a quarter of respondents were “very concerned” or “extremely concerned” that their answers would be used against them. The confidence levels were notable enough for the bureau to establish a Trust & Safety Team that year, since poor participation could impact billions of dollars of federal funding to things like schools and clinics, as well as representation in Congress.

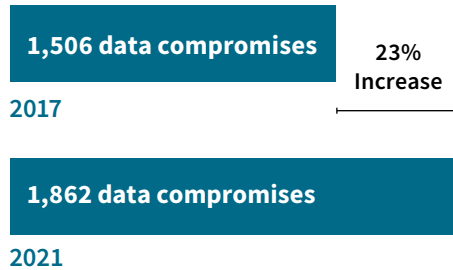
Given the fact that data privacy is a significant driver of distrust, it is not surprising that new policies and regulations are forcing government and industry to change how they collect, manage, and protect customer data. Since May 2018, U.S. companies that operate in the European Union must comply with the General Data and Protection Regulation (GDPR). Although the U.S. does not currently have a similar comprehensive data privacy regulation at the federal level, numerous bills are being developed and debated in Congress around privacy and data that will have an impact. At the state level, the 2020 California Consumer Privacy Act, which created privacy rights for the state's citizens, is changing industry privacy practices.

Ultimately, trust is the foundation that enables an organization to operate. It accelerates transactions and delivery of products and services with greater value. In the future, trusted companies will be the most successful and trusted government agencies will be better able to serve the public. In a data-driven world, access to information is crucial to performance, and the key to obtaining it is trust. Leading organizations are not waiting for regulation to take action. Eroding customer trust is a problem worth solving now, and technology is a critical lever in the solution.

EROSION OF TRUST IN SOCIETY

Record Data Compromises

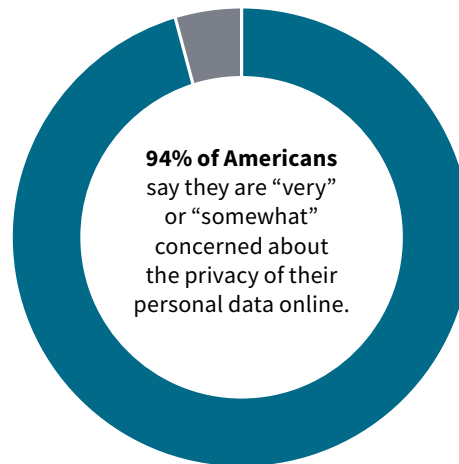
Data compromises reached an all-time high in 2021, impacting nearly 294 million people.



Sources from left to right: Identity Theft Resource Center; Knight Foundation; Pew Research Center

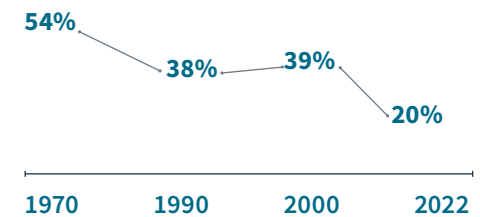
An Erosion of Trust

Most Americans are generally concerned about the privacy of their personal data online.



The Implications for Government

Trust in the federal system is essential for it to achieve its basic mission, but this erosion of trust is increasingly showing up in government.



The declining percentage of Americans that trust the government in Washington to do the right thing "just about always/most of the time" over the decades.

Dimensions of Trust in Technology

People often think of trust and technology in the context of data security and whether their data could be compromised via a hack or misuse. Security is one of trust's most complex features, but it encompasses much more than data breaches. Trust has roots in human psychology and has an emotional aspect as well. It is based on one's experiences and is predicated on the hope that an organization will provide a valuable, reliable product or service and has strong ethics and values. Let's explore the role of these three dimensions in designing and delivering customer-focused technology solutions.

1. Valuable: Does a product or service provide value to the customer that is commensurate with or, better yet, exceeds their perceived vulnerability and risk of sharing their data?

Giving away personal information—sometimes willingly, sometimes unknowingly—is part of everyday interactions. Yet every experience is a tradeoff: Is it worth it? This tradeoff exists along a continuum, as does the amount of information someone is willing to share. People are more inclined to exchange personal information with organizations if they receive desirable, high-quality products, services, information, or other benefits in return. At one extreme, a person signing up to receive a newsletter or breaking news alerts might feel the only information worth providing in exchange is their email address or cell phone number. At the other extreme, a U.S. citizen applying for a passport would understand the value in having to provide more comprehensive personal information.

Often, customers don't have transparency into how their information is shared, who it is shared with, or how it is used. The unregulated practices of data brokers in the U.S. exacerbates this. Data brokers obtain, aggregate, process, and sell information. This information is collected from several sources, and often users have no idea what personal information of theirs has been procured and aggregated by data brokers or who it has been sold to. This challenge looks likely to persist—several projections expect the industry to grow over the next few years. One proposed bill would begin to address that issue by prohibiting data brokers from selling and transferring certain sensitive data, including location and health information. But until data brokers are reined in, it should be the duty of organizations to reflect on their own data-sharing practices and vet any third-party organizations they work with to ensure customer data is shared and used in alignment with their agreements with customers.

Organizations should strive to deliver maximum value with the least amount of intrusion. Balancing this tradeoff is a continuous and ongoing effort and must be specific to the service or product being provided. Existing approaches, such as product management, human-centered design, and agile, iterative development, are more likely to result in the creation and delivery of value to customers. Early conversations and demonstration of value can enable organizations to build trust and momentum toward a long-term relationship.

DIMENSIONS OF TECHNOLOGY TRUST



VALUABLE



RELIABLE



ETHICAL

Our dimensions of technology trust provide a framework for organizations to build and deliver customer-focused solutions and services. These dimensions align with a long-standing academic understanding of trust in human psychology as explained by Mayer et al. in their article: “An Integrative Model of Organizational Trust,” *The Academy of Management Review* 1995. They outlined three factors that lead to trustworthiness: Ability, Benevolence, and Integrity.

Emerging Approaches: Synthetic data generation can be used to replace real customer information. Instead of using original customer information in analyses, synthetic data can be used as a realistic substitute to sensitive real-world data. For example, within a data set, people’s ages might be changed so long as the average age of the group stays the same. This technique is aimed at maintaining statistical utility. However, organizations will need to determine if the shift from real data to synthetic data results in a decline in value delivered to the customer. Synthetic data can also be used as a mechanism to shift away from sharing real data with third-party organizations if the insights derived from the synthetic data are actionable and useful for those third parties.

2. Reliable: Is the organization competent enough to deliver value to the customer and maintain their security and privacy?

A core component underpinning trust is the belief that companies and organizations providing services are competent and capable enough to do so in a manner that is consistent, reliable, safe, secure, and available when needed. Users need to feel that government and industry can protect their privacy, safeguard their information against breaches, and have the operational integrity and rigor to deliver the services they need. While achieving certainty in absolute terms with security, privacy, and resilience isn’t feasible, organizations should build on existing proven approaches as well as test emerging ones to move in this direction. Existing performance engineering and site reliability engineering approaches can help organizations commit to and ensure service performance at agreed-upon levels. As organizations increasingly leverage third-party software, proven approaches to secure their software supply chain will be critical as well.

Emerging Approaches: A growing number of commercial and government organizations are adopting a zero trust model—the underlying principle being “never trust, always verify.” This would represent a shift away from perimeter-based security models and

will likely deliver greater protection for user data and systems. The Federal Government, via a memorandum (M-22-09, issued January 2022), demonstrated its commitment to this approach by requiring agencies to achieve specific zero trust security goals by the end of fiscal year 2024.

Another emerging approach to consider is differential privacy. A method for balancing the need to collect, share, and report data with the obligation to protect it, differential privacy involves using an algorithm to inject “noise” into the data so that it is likely infeasible to identify whether any individual was in the original data set. For instance, the Census Bureau used differential privacy algorithms as part of its strategy to protect respondent information and confidentiality in demographic data that would be made available to the public.

While there is general consensus that a functional universal quantum computer is still in the distant future, the development of Shor’s algorithm and its application to break current-day encryption has put an emphasis on developing new cryptographic approaches—specifically, ones that would be computationally hard for a quantum computer to break. Post Quantum Cryptography (PQC) is an active area of research, and recently the National Institute of Standards and Technology (NIST) announced the selection of an initial set of four algorithms that could be “quantum-safe.” Organizations should monitor this space and, when appropriate, experiment and test these algorithms for the right applications.

3. Ethical: Does the organization maintain and practice ethical principles that align with customer values?

From a user perspective, an organization can provide valuable services and do so reliably; however, if the user doesn’t believe that the organization has the user’s best interests at heart and isn’t transparent about their intent, it is likely to cause distrust and hinder the relationship. This topic has come to the forefront



over the past several years as the intent and use of customer information has increasingly become opaque. With advances in machine learning and artificial intelligence (AI) capabilities, users are increasingly concerned about the use of their information and the lack of transparency in how decisions are made by algorithms. A recent article published by the Pew Research Center stated that, in their poll of 602 experts, about 68% said that ethical principles focused primarily on the public good will not be employed in most AI systems by 2030.

Emerging Approaches: The Department of Defense released a set of ethical principles for AI in February 2020 and followed up with their strategy and implementation pathway for Responsible AI in June 2022. Apart from defining principles and approaches to use these technologies ethically, driving transparency into how organizations make decisions and how customer data is used is critical to enabling confidence in the ethical behavior of the organization as well. Emerging approaches around Explainable AI (XAI) remain active areas of research—the Defense Advanced Research Project Agency (DARPA) is one such organization that has made this a priority. The XAI program aims to enable humans to understand, trust, and effectively manage AI capabilities. A step forward from transparency is to move toward control, where customers can control what data is collected, shared, and used. For example, in 2021 Apple launched a new feature that prompted users to provide input about whether they were comfortable with their actions being tracked by certain apps. This privacy feature provided a degree of control back to users. These approaches, which drive transparency, control, and validation of ethical and fair use of data, can enable trusted relationships with customers.

The Privacy Paradox

Designing and developing technology to build trust and mitigate erosion is complicated by a concept known as the Privacy Paradox. The Privacy Paradox is the difference between what a customer says is important to them and what that same person does in practice. Typically, customers, when surveyed, will state that privacy is extremely important to them and that they do not want organizations to use or share their data. In practice, however, these same customers expect highly tailored web experiences that are driven by their past behaviors. They also end up openly sharing personal information to a variety of less than trustworthy services when mechanisms such as gamification and nudging are employed. In sum, organizations are left with a paradox where customers ask for data protection and limited use, but also expect data-driven products and services that are completely tailored to them.

A conversation about trust and technology must address an emerging movement: Web3. Web3 is used as an umbrella term to capture a number of technologies such as digital assets, decentralized finance, blockchains, tokens, and decentralized autonomous organizations. Web3 is pitched as a shift away from the current state of the internet—one that is plagued with misinformation, privacy breaches, etc., and where data and control is concentrated with a few large companies. Web3 is still an evolving concept and has its own set of detractors. However, as this movement evolves, organizations and agencies must track it closely because it could have broad-reaching implications for building trust, delivering value, and demonstrating resilience and ethical behavior to customers.

Technology as a Trust Catalyst

The future, as envisioned by technologists, encompasses a blurring of the digital and physical worlds and a combination of robotics, autonomy, and AI elevating the role of humans by taking care of things that are best suited for automation. With this vision in mind, the challenge of trust becomes more important. On the positive front, most Americans—84%—do believe it is possible to improve the level of confidence Americans have in the Federal Government. And there's an opportunity to harness the momentum across government and industry as new and emerging approaches are incorporated into solutions to help break the cycle of distrust. Along with these approaches that can bolster value, reliability, and ethics, organizations must continuously assess customer expectations and needs to enhance trust in products, services, and interactions. Transparency about privacy and data-usage practices—by using clear, succinct language that does not require a law degree to understand—also inspires public trust in government and industry.

Just as technology played a role in public distrust of today's digital society, it has a bigger role in building it back up. The question is how we can harness the power of trusted solutions to enable a holistic response around reliability, ethics, and value—and importantly, ensure that individuals and communities can access the federal services and benefits they need with confidence.



Just as technology played a role in public distrust of today's digital society, it has a bigger role in building it back up.

Sahil Sanghvi is a distinguished technologist and head of strategy for Booz Allen's Technology Business. He has spent the past 15 years focusing on and advising senior executives on emerging technologies and their applications in government and industry.

Julie McPherson is an executive vice president and leader of Booz Allen's Digital and Solutions Business. She has spent the past 25 years advising senior executives across federal agencies and delivering mission-critical systems.

Ryan T. Wright is the C. Coleman McGehee Professor of Commerce and the senior associate dean of faculty and research in the McIntire School of Commerce at the University of Virginia. He has spent the past two decades examining the human psychology of privacy and cybersecurity.

SPEED READ

Customers are increasingly wary of the ways in which companies use their data and how that data is shared with third parties and data brokers. This has resulted in an erosion of trust.

Trust in the federal system is essential for it to achieve its basic mission and for democracy to flourish. The Government relies on constituent information to plan for the future, provide essential services to its citizens, understand and solve problems facing the nation, and identify and thwart threats to its security.

Organizations should provide a valuable, reliable product and have strong ethics and values. These three dimensions—valuable, reliable, ethical—are foundational to establishing and improving trust with customers and the American public.

Technology has played a role in eroding trust in today's digital society, but it has a critical role in building it back up. Organizations should evaluate and test emerging technologies and approaches to begin their journey in delivering trusted services.

A New Paradigm for National Security Innovation?

Navigating the Delicate Balance of Creating New Technologies Through Secure Collaboration

Munjeet Singh, Paul Chi, and Saurin Shah



The U.S. is facing an urgent crisis in the “great power competition” as other nations are accelerating advances in critical areas of tradecraft and emerging technologies. Unprecedented challenges and threats from strategic competitors are increasing pressure on the U.S. Intelligence Community (IC) to deliver actionable, timely information. An intersection of evolving adversarial threats, dynamic mission needs, rapidly advancing technologies, and a war for talent requires new approaches to prepare for future missions and conflicts.

The increasing urgency for the U.S. Government to adopt new capabilities for national security, such as artificial intelligence (AI), quantum computing, and next-generation networking, comes at a time when practically every major private sector industry outspends the Department of Defense (DoD) on innovation. But in this uniquely sensitive environment, with much at stake, there is a delicate balance between technology innovation and implementing strict security standards.

To access commercial innovation quickly and cost-effectively and to maintain a global edge, the IC can continue lowering the barriers for responsible innovation—ensuring compliance does not stand in the way of a national interest to stay ahead. Here, we explore where the paradigm is shifting to leverage established security frameworks, encourage new pathways for commercial investment, and scale technical talent through flexible working models.

Leverage Frameworks for Secure Collaboration

Security and mission assurance cannot be compromised for the sake of speeding up deployment for commercial technology. Since organizations do not have the ability to loosen critical controls, it is imperative to find other levers that make it easier for government to collaborate with industry. That includes establishing clear security minimums for alleviating pain points inherent to adopting and deploying commercial products in tightly secure environments.

The National Security Agency’s (NSA) Commercial Solutions for Classified (CSfC) is one exemplar mechanism ensuring classified data is protected as commercial innovation is embraced. Since the program’s inception, it has provided a framework and mechanism for the private sector to validate commercial products for use in classified systems that encrypt data at rest and in transit. The CSfC framework has supported the adoption of classified wireless and mobile devices and has been critical in helping the national security mission continue during the COVID-19 pandemic. CSfC created a clearly defined process for sourcing and integrating commercial products and has helped evolve long-held perspectives on the viability of using commercial technology to meet national security requirements.

Such constructs are allowing the Government to work differently with industry and leverage established standards to accelerate commercial product approval times. In addition to securing products in the federal space, continuous risk monitoring once a system has been authorized is an equally important area of focus for information assurance (IA) compliance.

In 2022, the DoD released a memo on the subject of Continuous Authorization to Operate (cATO). The memo states that cATO “represents a challenging but necessary enhancement of our cyber risk approach in order to accelerate innovation while outpacing expanding cybersecurity threats” and provides initial guidance for authorizing this increasingly important mechanism.

Platform One, a DevSecOps-managed service and capability, is an active model to watch. The U.S. Air Force created Platform One to accelerate the delivery of software to mission systems while reducing duplication of effort and time spent hardening new applications. The program established and adopted a cATO, allowing individual teams to experiment and rapidly release software while avoiding lengthy and unnecessary security sign-off gates. It ensures that proactive zero trust security is baked in from the first source code to the end user, and that security and compliance are continuous, automated, and comprehensive across the technology environment.

An intersection of evolving adversarial threats, dynamic mission needs, rapidly advancing technologies, and a war for talent requires new approaches to prepare for future missions and conflicts.

In addition to the cATO, Platform One also created a marketplace of certified, containerized instantiations of commercial solutions available across the community with the relevant security accreditation. Today, this marketplace—known as Iron Bank—offers 800-plus containers and counting. But the benefits extend to commercial partners, not just end users. Rather than requiring a partner to complete a typically arduous documentation process to ensure their software meets requirements, Iron Bank takes care of that end-to-end process. Vendors submit software, which Iron Bank then inspects, applies controls to, and containerizes for the marketplace. The result? Developers know that any software pulled from Iron Bank is safe and secure to use, and technology companies can seamlessly integrate new software for customer adoption without traditionally resource-intensive procedures. For startups or small enterprises, this could be their rare entry point into the federal marketplace.

Encourage New Pathways for Commercial Investment

The Federal Acquisition Regulation (FAR) has more than 2,000 pages of fine print to navigate, and paperwork can make or break contracting opportunities for technology providers—particularly for small organizations, startups, and commercial companies. With complex acquisition processes and stringent protocols for security and connectivity, commercial technology partners without deep experience or resources often struggle

to successfully integrate their technologies to advance national security systems (read more about the “Valley of Death” for startups on page 18).

“The battlefield for global power over the next 50 years is going to be in the universities, labs, and startups delivering new, innovative technology to the world,” said Chris Darby, the president and CEO of In-Q-Tel, in a powerful statement to Congress. “Investments in hard tech, including microelectronics, quantum computing, and biotechnology must be made, and, at the same time, we need to ensure that our significant national research investments have a path available for commercialization by American interests.” Darby emphasizes that China is building global technology leadership by fusing civil and military technology strategies to competitively invest in areas such as 5G communications and networks.

Venture capital for national security is a significant area of focus on the global stage, with the U.S. slowing down investments compared to near peers (further insights on venture capital trends are on page 54). Simultaneously, IC organizations can increasingly leverage alternative acquisition approaches so that a wider subset of partners can innovate based on objectives, rather than requirements, in small and scoped engagements.

“The battlefield for global power over the next 50 years is going to be in the universities, labs, and startups delivering new, innovative technology to the world.”

— **Chris Darby**, the President and CEO of In-Q-Tel, testimony to Congress (February 12, 2020)

For example, the Other Transaction Authority (OTA) contracting structure is gaining new traction across the Government. OTAs have been around since the 1950s and are giving federal leaders access to startups, accelerators, and commercial and nonprofit entities that may not have standing connections to national security missions. With their focus on targeted and well-defined prototypes, OTAs enable partners to demonstrate their technical value with proofs of concept before launching into production environments.

Consider the DoD’s “5G to Next G Program,” the Government’s major investment in 5G capabilities. Given the role of telecommunications technologies in the economy and networked warfare, the DoD has allocated over \$1.6 billion since fiscal year 2020 to create what is now the world’s largest investment in private 5G hardware, software, and services. By deploying agile, alternative contracting mechanisms—enabled

by small-scale OTAs—for example, \$10 million to \$20 million over 1 to 3 years—they are testing the utility of 5G across a broad range of clearly defined mission problems and use cases. By using this mechanism, the DoD has attracted a wide collection of leading traditional and nontraditional industry partners, networking providers, and startups to rapidly advance the military’s 5G capability (at one point during the first tranche of the program, more than 65 companies were involved).

As a result of the OTA, 5G concepts can be evaluated in a lab and partners can develop quickly without intensive security documentation and compliance. If a concept passes the early stages, it integrates into a higher-level lab that simulates the production systems to a greater degree of fidelity. This is where more stringent security testing kicks in, but by this time the partner has already proven value. The systematic ramp-up of complexity on the way from lab to theater allows for down-selecting of promising technologies through a sequence that encourages partners’ innovation (see Figure 1 on the following page).

Scale Technical Talent Through Flexible, Hybrid Operations

With a small pool of highly cleared talent—internal to the IC and within the workforce of technology partners—there are not enough cleared professionals to manage and deploy the innovations discussed so far in this article. This is an ongoing risk to national security. To scale intelligence capabilities, there is an increasing need to integrate new working models for today’s talent.

To this end, more organizations are integrating hybrid working models that allow professionals of varying clearance levels to work in a mix of secure compartmented information facilities (SCIFs) and unclassified spaces. New and flexible working models offer the IC advantages that include:

- **Increased productivity.** Engineering talent can be scaled by leveraging a “develop low side, deploy high side” approach.
- **Accelerated onboarding.** Organizations can immediately employ the skills of new talent waiting to be fully cleared, to tap into their talent in unclassified spaces and engage new recruits in rewarding mission work early on.
- **Broader regional access.** Select initiatives can be transitioned to geographically distributed SCIFs, opening access to innovation and talent across the country.

Successful pilots are enabling advances in areas like AI, zero-trust security, and specialized engineering. It’s a customized approach: Each organization evaluates what work is conducive to a hybrid working model across multiple classifications.

One intelligence agency put this into practice during the pandemic lockdown. By establishing modular, repeatable deployment on classified networks, remote and uncleared engineers could develop the code and then pass it to the classified team to securely migrate it onto classified networks. This alternative approach to collaboration increased productivity by almost 20%.

Phase 1

Scope Design concepts and/or trade studies

Duration Generally 6 months or less

Payment Terms Often payable milestones with fixed government obligation

Terms and Conditions Usually simple and flexible/little need to address difficult negotiation issues yet like intellectual property right as long as competition maintained

Awards Multiple

Phase 2

Scope Detailed design

Duration Generally longer duration (can be 12 months or more)

Payment Terms Milestone payments are often the most reasonable and specific approach should consider program, cost, and technical risks

Terms and Conditions If there's still ongoing competition, terms will be more detailed but many difficult negotiation issues may not be addressed/finalized

Awards Multiple

Phase 3

Scope Prototype build

Duration Will depend on the complexity and number of prototypes (often 12 months or more)

Payment Terms Milestone payments often still most reasonable and specific approach should consider program, cost, and technical risks

Terms and Conditions Terms and conditions must be fully negotiated before competition leverage is lost

Awards One

Phase 4

Scope Test and evaluation

Duration Usually based on negotiated test plan

Payment Terms Fixed price with incentives or reasonable approach to address risk

Terms and Conditions No additional terms generally needed

Awards One

Phase 5

Scope Fabrication of additional prototypes or production quantities

Duration Dependent on complexity and quantity

Payment Terms Firm fixed price, payable milestones

Terms and Conditions If any, additional terms might be necessary relating to production

Awards One

Phase 6

Scope

Lifecycle operations and support

Figure 1: Illustrative Structure of a Rolling Downselect
Source: DARPA Acquisition Innovation

Beyond implementing new operating models for talent, national security depends on the ability of the U.S. to accelerate AI adoption. Given the shortage of cleared talent, this requires a disruption in how organizations label the proliferation of information coming in from around the world through sensors and open-source data to train for machine learning (ML) models. Critical investments in technology that advances unsupervised ML methods can decrease the dependency on human-labeled data and enable a huge leap forward in tradecraft to remain ahead of adversaries.

Laying a Foundation for Future Missions

Given the escalating scope and complexity of the problems government leaders in the IC are being asked to solve, innovation must be scaled exponentially. Despite national leadership in mission-critical technologies, the ever-evolving technology race requires the ability to clear the way for emerging technology. Trusted frameworks for continuous innovation, investment, and acquisition models to accelerate critical technologies, along with talent models that can scale, will help continue to push boundaries and advance national interests through uncertain times ahead.

Munjeet Singh is a senior vice president and the leader of Booz Allen's Bright Labs incubator, an experimentation organization designed to develop, test, and incubate mission-centric solutions rooted in emerging technology.

Paul Chi is an executive vice president responsible for delivering technology solutions on behalf of clients across the IC. His expertise includes cyber, networking technologies, technical operations, advanced prototyping, and nontraditional approaches to difficult and ongoing mission challenges.

Saurin Shah is an AI leader in Booz Allen's national security business, delivering operational systems that modernize enterprise workflows and decision-making processes for the IC.



SPEED READ

To access commercial innovation quickly and cost-effectively and to maintain a global edge, the IC can continue lowering the barriers for responsible innovation.

This includes leveraging established security frameworks and encouraging new pathways for commercial investment through ventures, OTAs, and mechanisms that allow for cATO.

There are not enough cleared professionals to scale the capabilities required to keep pace with the mission, and the IC is reimagining working models to increase productivity and engagement across in-demand talent.

Achieving Decision Advantage by 2025

Components of the AI-Enabled Battlespace

Authors: Steve Escaravage and Matt Tarascio

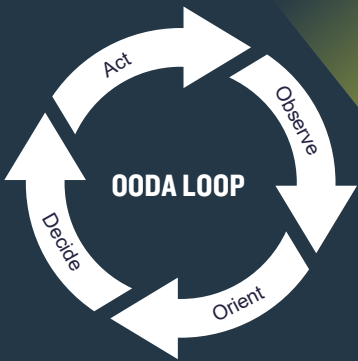
Contributor: Ki Lee

The very nature of warfare has changed. Until recently, the volume, readiness, and leadership of physical military assets—soldiers, weapons systems, sensors, and communication links—determined military power. Now, military power is increasingly derived from a new class of military assets: data, software, computing and networking infrastructure, artificial intelligence (AI), and autonomous systems. Supplementing, and in some cases replacing, their physical counterparts, a new age of digital warriors competes to scale, integrate, and continuously innovate these technologies and use them to create operational advantage—or “decision advantage”—on tomorrow’s digital battlefield.

Balancing the quickening pace of military engagement with a mounting deluge of real-time battlespace data, decision-makers must now consider increasingly complex decisions more quickly than ever before. During the Gulf War, minutes of deliberation

shifted the balance between deterrence and escalation across air, land, and sea. Today those minutes have become mere seconds—or less—for decision-makers to respond to cyber and hypersonic threats (see Figure 1). Already, Chinese and Russian military leaders have implemented doctrinal and operational shifts toward modern, decision-centric warfighting concepts, such as System Destruction Warfare and New Generation Warfare, that emphasize warfare in the information domain and decision-making at speed.

However, increasing the speed of decision-making alone is insufficient to achieve decision advantage. The complexity of current and future threat environments also demands that blue force commanders have greater and more diverse optionality while decreasing that of their adversaries. This “optionality advantage” enables more effective blue force decision-making while simultaneously imposing more complexity and constraints on our adversaries.



The pace of warfare is accelerating:

1 ns to 1 sec is equivalent of 1 sec to 32 years

DIMENSIONS	WWI	WWII
DECISION SPEED	Weeks	Days
NUMBER OF ASSETS	1–10	10–100
COMPLEXITY	Horses	Tanks

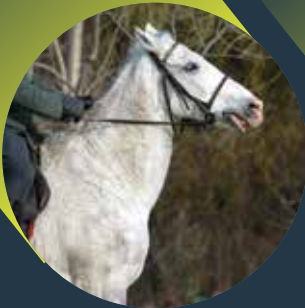


Figure 1: Conceptual evolution of warfare

The demands of optimizing decisions across an accelerating and expanding decision space while harnessing and exploiting vast amounts of all-domain data exceeds the threshold of human comprehension. Increasingly, decision-makers will rely on AI to bridge the gap by providing nuanced decision guidance and synthesis, while their adversaries do the same. Accordingly, a military force’s ability to rapidly act upon AI-driven recommendations will very likely determine military victory in the future.

What Enables Decision Advantage?

Decision advantage reflects the ability to close the OODA (Observe, Orient, Decide, Act) loop faster than an adversary. It can be broken down into a set of foundational components that form a rubric by which success on the future battlespace can be measured. These components are illustrated in Figure 2 and include the following:

Data Advantage: The operational availability of data describing friendly and adversarial forces, the operating environment, events, etc. Superior data enables greater situational awareness and preemptive action. More data is not necessarily better. Instead, relevancy, timeliness, accuracy, and granularity are paramount.

Algorithm Advantage: The accuracy, precision, speed, and robustness of heuristic and machine learning-based AI algorithms, also called AI models, used to inform warfighting activities. Comparable to the emergence of high-frequency trading in financial services, tomorrow’s warfighting operations will be guided by AI-powered algorithms, with and without humans in the loop. Faced with changing operational and threat environments, forces must be ready to rapidly adapt algorithms and implement them in real time. The side with the most powerful and efficient algorithms will lead the fight—they will be able to detect and classify adversary intent, calculate the best course of action through simulation, and select the optimal response before the adversary is able to do the same.

Integration Advantage: The ability to integrate new and improved technologies into existing warfighting systems and platforms in the least amount of time. Near-future operations centers will resemble Formula 1 pit crews, monitoring the performance of data pipelines and AI systems to understand what modifications will result in the greatest incremental advantage in the field. However, unlike F1 vehicles, future platforms will not need to enter a “pit” for mechanical adjustments; they will instead receive modifications as software updates in near-real-time over communication networks. Forces that can most quickly integrate, overhaul, and deploy new technologies into the fight will achieve short-term overmatch advantage against adversaries.

Interface Advantage: The degree of human-machine teaming through cognitive interfaces and robotics. The side best able to combine the strengths of humans and machines with the least friction will achieve decision and overmatch advantage on the battlefield. This is especially true for next-generation mission applications, where intuitive graphical user interfaces (GUIs), gesture-based controls, and mixed reality will be required to process highly dimensional, multi-domain data.

Infrastructure Advantage: The ability to access, use, and dynamically configure compute, networking, and storage technologies at fixed, deployed, and forward positions on the battlefield. Because data and algorithm advantages are dependent on underlying infrastructure to intake and process data feeds, innovations that enable efficient use of infrastructure will act as force multipliers.

Currently, the U.S. Department of Defense (DoD) portfolio of platforms and systems does not provide sufficient competitive advantage in these areas, requiring significant investment to modernize existing assets and develop new technologies to counter investments by strategic competitors.



VIETNAM WAR	GULF WAR	TODAY	TOMORROW
Hours	Minutes	Seconds	Nanoseconds
10–100	1,000+	1,000–10,000	10,000–100,000+
Air	Air, Land, Sea	Space, Swarms, Hypersonics	Cyber, Electronic Warfare, Directed Energy

“All-Domain Operations is “the biggest key to the future of the entire budget because if we figure that out, we’ll have a significant advantage over everybody in the world for a long time.”

— **Gen. John Hyten**, Former Vice Chairman of the Joint Chiefs



Figure 2:
Foundational components of decision advantage

How to Achieve Decision Advantage

Decision advantage is relative, temporal, and measured in terms of accuracy (i.e., correct decisions) and cycle time (i.e., time to decide). Decision-makers can rapidly close the OODA loop through cumulative advantage across a set of foundational components, as described above. Investment in the following key areas would address the gaps of current platforms and systems:

Enriched Data Sets: Empirical and synthetic data sets harvested and enriched through partnerships, events/exercises, and annotation services that inform military planning and course of action analysis on the battlefield.

Data Mesh: Distributed data ecosystem that supports diverse centralized to decentralized data architectures to enable human-to-machine and machine-to-machine processing.

Software Factories: Automated orchestration of modular services (e.g., software to AI) and the leveraging of DevSecOps/MLOps, to modernize mission and combat systems to enable the agility required of today's warfighters.

Edge Runtime Platform: Software-defined layer to include communications, data pipeline, inference engine, etc., to process data at the point of collection.

AI Models: Deployment-tuned models, from enterprise to edge, that address specific and evolving mission needs.

Counter AI Software Libraries: Software utilities to responsibly detect, deter, or utilize adversarial attack approaches on AI systems.

Mission Applications: Software applications with tailored interfaces for core warfighting functions, such as electromagnetic spectrum management and multi-domain battle management.

AI Human Machine Teaming Interfaces: Data visualization and human decision making interfaces to enable explainability and responsible calibration of AI models and systems.

Significant investment is required today to achieve the promise of AI-enabled decision advantage by 2025

AI-enabled decision advantage will not be realized by 2025 unless we reprioritize and focus our investments—starting today. This revolutionary battlespace capability is not something that will just appear or be available for purchase when needed. Significant investment in the right foundational components is necessary over time to build this capability through real-world applications. Further, time affords warfighters and leaders the opportunity act upon these machine-generated recommendations with trust (bias to action), efficiency, and thoroughness (precision)—essential components for decision advantage to take place at all. Investment over time will provide us the opportunity to define interfaces, educate and train our warfighters and senior leaders, develop TTPs (tactics, techniques, and procedures), and define interim and long-term effectiveness.

While growing complexity, optionality, and data availability will prove to be decision-makers' greatest assets on tomorrow's digital battlefield, they will also prove to be its newest challenges. The role of AI in guiding, synthesizing, and predicting wartime choices will only compound the existing need to innovate and invest in digital assets. To best capitalize on the benefits of warfare's new character, we must take immediate steps. Inaction today will yield paralysis tomorrow—and, with the forces and future of our country at stake, decision advantage must number among our highest priorities.

Steve Escaravage, executive vice president, leads Booz Allen's artificial intelligence business—helping clients with the operational integration of data science, machine learning, and AI solutions across all markets and sectors.

Matt Tarascio, senior vice president, leads efforts to accelerate integration of analytics, data science, and AI capabilities across defense missions, and guides strategy development to advance national defense.

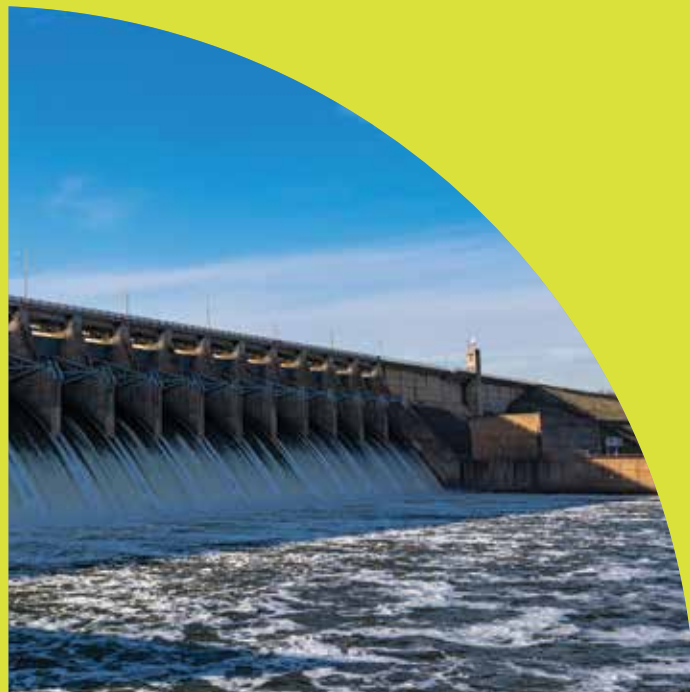
Ki Lee, senior vice president, drives technology application and adoption for Booz Allen's global defense business, with a focus on supporting mission needs and gaps.

SPEED READ

Today's defense leaders are afforded mere seconds—or less—to respond to cyber and hypersonic threats. The vast amounts of all-domain data exceed the threshold of human comprehension, and a military force's ability to rapidly act upon AI-driven recommendations will very likely determine military victory in the future.

Decision advantage is achieved by closing the OODA loop faster than adversaries and can be broken down into a set of foundational components that form a rubric to measure success on the future battlespace: data advantage, algorithm advantage, integration advantage, interface advantage, and infrastructure advantage.

AI-enabled decision advantage is only achievable if governments reprioritize and focus investments starting today. Significant investment in the right foundational components will allow entities to define interfaces, educate and train warfighters and senior leaders, develop TTPs, and define interim and long-term effectiveness.



MISSION SPOTLIGHT: CITIZEN SERVICES

Solving Global-Scale Challenges Through a Data Ecosystem

Advancing Mission by Bridging Gaps Between Physical and Digital Spaces

Frank DiGiammarino, Prachi Sukhatankar, Kathleen Featheringham, and Josh Strosnider

Global issues such as immigration and migration, climate change, humanitarian relief, and critical infrastructure transcend organizational silos. These matters of national criticality and security increasingly span global sectors and national interests. In turn, mission execution is taking on new speed, size, and urgency, which demands an evolution of mission intelligence from an *enterprise* to an *ecosystem* approach.

Today, federal organizations are operating in a world where data is constantly changing, updating, and converging through new systems—from internet of things (IoT) sensors to physical and digital records. As civilian mission challenges and global crises increase in pace and scale, there is an exponential growth in the complexity and types of data that need to be analyzed to ensure readiness, situational awareness, and decision advantage. Meanwhile, immersive and data-rich capabilities from the gaming world are finding universal applications across all industries, including the government sector. Over time, success will be measured by how effectively organizations use all of their available data and create new value through extended reality, digital twins (page 42), the metaverse (page 49), and other emerging capabilities.

A parallel for this major data transformation in the civilian sector is the Joint All-Domain Command and Control (JADC2) strategy within the Department of Defense (DoD). JADC2 is a vast military IoT network—connecting sensors, weapon systems, data centers, and users to make data more accessible and interoperable. Its vision is to accelerate intelligence and decision making so defense organizations can address threats at the speed of relevance, which is a central focus for our nation's frontline defenses outside of the military, from homeland security to public health.

The next age of intelligence will be marked by the rapid collision of data from a global ecosystem and the delivery of immediate insights for trusted outcomes. Three fundamental shifts are necessary for civilian missions to harness large-scale data fusion, bring artificial intelligence (AI) to the enterprise, and bridge the gap between physical and digital experiences. Regardless of their mission area, federal leaders need to integrate AI across all elements of the IT infrastructure, apply data ethics and open standards for trusted decision making, and scale the data infrastructure from cloud to edge.

Integrate AI Across All Elements of the IT Infrastructure

The National Oceanic and Atmospheric Administration (NOAA) studies the dynamics behind global weather events so it can better predict and prepare for potentially catastrophic events. Later in the publication, our colleagues describe one mechanism that NOAA is building to do this: a digital twin of the earth (see page 42).

NOAA will bring together troves of observation data to create an authoritative source that can be trusted from a space and time perspective. The digital twin will be a comprehensive, visualized representation of massive global data, sourced daily from sensors, large satellite imagery, and environmental data from around the globe, underground, underwater, and in space. As data is collected and fused, it can then be visually explored in a spatial and temporal manner.

Ultimately, NOAA's investment will help democratize data that is leveraged for climate intelligence. This digital ecosystem, which allows for continuous data conditioning, assimilation, and fusion, will enable NOAA's stakeholders and decision makers to explore real-time climate data and understand dynamic environmental forces at work. In the future, the digital twin will be able to simulate and model future events. For example, modeling could be used to understand the potential for precipitation events in parts of the world where malaria spreads from standing water. More important, this information can be translated into preemptive actions rather than purely reactive measures. To make this possible, organizations like NOAA must take advantage of all the data that's available at the speed of relevance.

The next age of intelligence will be marked by the rapid collision of data from a global ecosystem and the delivery of immediate insights for trusted outcomes.

The quantity and diversity of this expanding world of data is challenging federal IT and mission leaders to think differently about ecosystem intelligence and push the boundaries of traditional engineering. Traditional analysis techniques have focused on leveraging the power of data through enterprise- and agency-level solutions—siloed from other entities. Today, however, data formats need to be fluid and available for use in any format, from the cloud to the edge, and even in fully disconnected environments. Likewise, legacy infrastructures typically apply analytics and models at the application layer, riding on top of the IT infrastructure. However, AI should be leveraged across all elements of the IT infrastructure to harness the power of DataOps and data fusion at the scale of the mission.

Apply Data Ethics and Open Standards for Trusted Decision Making

When addressing issues such as public health or migration, the downstream impacts of late, imprecise, or inaccessible intelligence are matters of national and individual security, and they underscore the criticality of trust, openness, and the responsible use of data.

In the mission environments this article references, a data misstep or error can significantly impact communities around the world. If AI engineering is incorrectly associated with model pipelines, analysts may see data from an inaccurate space and time perspective. Organizations must apply intentional care and methods to understand the performance of models, the potential drift of the parameters governing the outputs, and the provenance of the data used to train the models. Leaders, analysts, data scientists, AI professionals, and operators must be able to trust that the information they are receiving is ethical and appropriate to inform actions in the real world.

To create trusted mission intelligence that can truly scale, the digital ecosystem must:

- **Integrate AI across the board.** To be effective, AI needs to be integrated across the data lifecycle, from cleanup to output.
- **Ensure that data is ready for AI modeling.** Organizations need the infrastructure in place to ensure the data is in the right form to inject into models.
- **Identify critical gaps in the modeling.** If a model is introduced to the system without testing and validation of performance standards, it will disrupt other models.
- **Deliver insights at the speed of relevance.** Getting data for AI modeling is one thing; getting it fast enough to impact real-world events is what matters to the mission.
- **Create data access for the right people.** Data and tools need to be democratized across stakeholders to enable trusted decision making.

Today, there are many instances in which data is locked behind proprietary systems, which hinders the ability to fully leverage critical information. As part of a data transformation, the democratization of information from disparate siloed systems

is a fundamental principle to be embraced and mandated.

This democratization of data increases the equitable access to information and situational awareness for decision makers and stakeholders around the world.

Ultimately, organizations require a modern and flexible architecture with open standards that can update and shift with ease as new data and capabilities are integrated over time. For instance, the DoD originally designed Advana, an enterprise data platform, to process and analyze “boardroom data,” as the former department’s chief data officer, Dave Spirk, described it. But the platform is now part of JADC2 testing to connect battlefield data and provide more comprehensive mission insights. It is a compelling example of how use cases can be enhanced to meet dynamic priorities within a flexible infrastructure.

This approach also represents a broader trend in the public sector space. Gartner® predicts that, by 2024, more than 25% of government requests for proposals (RFPs) for “mission-critical IT systems” will require solutions architecture and variable licensing that support a composable design approach.

For mission areas where a profound data collision enables operators and analysts to prepare for large-scale events in the future, this open architecture is essential for continuous AI integration and data fusion, and for an embrace of AIOps (AI for IT operations). To support scalable engineering practices for model and data pipelines, open standards are key to accelerating the integration of capabilities in a trusted and reliable manner—and to prepare mission leaders and communities for multisector, long-term, and cascading disruptions, such as those that are observed during extreme weather events or public health emergencies.

Scale the Data Infrastructure from Cloud to Edge

To serve and protect communities around the world, critical missions increasingly require the integration and modeling of data from operations and the field.

Consider the multitude of systems and sensors involved in immigration and migration. For example, data is collected globally, often in parallel, through people- and cargo-screening technologies (e.g., X-Ray, video), aerial footage taken in daylight and at night, and security and body cameras. Countries also have access to a breadth of documentation and records, such as immigration forms, passport data, manifests, and flight data. To turn all of this data into intelligence—and take near-immediate action—operators need the ability to rapidly fuse different types of physical and digital data.

U.S. Customs and Border Protection (CBP), the nation’s largest federal law enforcement agency, lives this complex reality. CBP is responsible for the security of national borders in a rapidly changing operating environment, beyond the walls of a traditional IT enterprise. Today, the agency’s solutions must extend far beyond the enterprise and require processing capabilities at the point of data collection.

Gartner® predicts that, by 2024, more than 25% of government requests for proposals (RFPs) for “mission-critical IT systems” will require solutions architecture and variable licensing that support a composable design approach.

Source: Gartner Top Technology Trends in Government for 2022

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Success is no longer about an individual agency or even a single nation solving a problem, but rather a coalition to create a trusted, comprehensive data ecosystem.

Large-scale data fusion, assimilation, and AI are now central to CBP's mission. This past year, the agency helped establish the Border 5/Migration 5 (B5M5) partnership between Australia, Canada, New Zealand, the UK, and the U.S. to enhance and scale data-sharing capabilities. The partnership is collectively investing in technologies that include augmented and virtual reality, blockchain, and biometrics.

Partnerships like B5M5 are necessary to address larger issues and patterns at a global scale—no matter the mission focus. Success is no longer about an individual agency or even a single nation solving a problem, but rather a coalition to create a trusted, comprehensive data ecosystem.

Envisioning a Data Evolution

In civil societies, large-scale data fusion and AI have the power to improve safety, resilience, and security. Organizations need the ability to process and decipher information from around the world and from a proliferation of sensors, physical and digital experiences, and intersecting mission areas.

Research has shown that natural disasters displace populations and lead to migration over time. Political turmoil, civil unrest, and environmental changes can also lead to increases in events like immigration and human trafficking. Used together, field and operational data can connect the dots between major humanitarian issues to inform in-the-moment decision making, global policymaking, and readiness for the next crisis.

The missions highlighted in this article demonstrate how the Government is harnessing an ecosystem of intelligence for critical decision making. As data is freed from locked platforms for more flexible and accessible insights, agencies can take on greater challenges, including those outside their traditional organizational structures. Through increased collaboration, data can more readily deliver reliable insights to wherever the mission is—from the IT enterprise to the operators at the front lines.

Frank DiGiammarino leads technology exploration and strategy for Booz Allen's chief technology office, focusing on expanding emerging businesses and building new partnerships with the firm's technology and innovation ecosystem.

Prachi Sukhatankar is a vice president in Booz Allen's civil sector with a focus on climate, infrastructure, and matters of domestic resilience. She has over 20 years of experience leading the strategy, engineering, and delivery of digital transformation in both private and public sector organizations.

Kathleen Featheringham is a principal in Booz Allen's BrightLabs incubator, with an expertise in building capabilities for data transformation and AI across the Federal Government.

Josh Strosnider leads Booz Allen's partnership efforts as part of the CTO organization and helps drive the firm's strategies to enable, differentiate, and expand federal access to emerging technologies.

SPEED READ

To serve and protect communities around the world, federal agencies need to harness large-scale data fusion, bring AI to the entire enterprise, and bridge the gap between digital and physical experiences.

Civilian issues, such as immigration and climate change, span global sectors and national interests and defy traditional organizational silos. Success on these issues is no longer about an individual agency or even a single nation solving a problem, but rather a coalition to create a trusted, comprehensive data ecosystem.

There is exponential growth in the complexity and types of data that have to be analyzed to ensure readiness, situational awareness, and decision advantage for civilian missions. An ecosystem approach to mission intelligence is needed to address matters of national criticality and security at the speed, size, and urgency that exist today.

Organizations require a flexible architecture and open standards to support critical decision making at the scale of the mission and to shift with ease as new data and capabilities become available.

Digital Twins for Modern Government

WIDENING THE APERTURE FOR AGILITY, RESILIENCE, AND COMPETITIVE EDGE

Authors: Sandra Marshall, Trishna Lovley, Jennifer Jenkins, and Colin Corridon

Contributors: Ramesh Soni, Jen Congdon, and Kathleen Featheringham

In 2022, Tyndall Air Force Base showcased a digital “Installation of the Future” as part of its rebuild process. In this extended reality space, leaders run simulations, spot project vulnerabilities, and make advanced operating decisions. It is one of the newest models to show how digital twins are enabling federal agencies to strategically test innovative approaches and solutions (and prepare for emergencies) without ever reaching the limits of the actual world.

With estimated market growth from \$5.1 billion in 2020 to \$115 billion by 2035, digital twins are fast becoming a cornerstone in the design, manufacture, and operations of everything from the products we use to the buildings and cities where we work and live. As digital twin technologies quickly grow more capable, federal agencies, from defense to critical infrastructure, are increasingly positioned to leverage advanced insights from previously untapped data for improved mission outcomes. Components of a successful adoption include understanding the architecture, integrating a system of systems, overcoming challenges of scale, and translating data into meaningful, intuitive visualizations.

Digital twins are technically realistic replications of objects, processes, or systems. They are directly connected (twinned) to their physical counterparts through continuously updated data and information feeds across their lifecycle, used to solve complex challenges.

Understanding the Architecture

Imagine hundreds of millions of disparate data streams that are connected to create unbroken threads of insight. Together these digital threads can solve large, complex, and dynamic problems on the ground, in the earth’s atmosphere, and even in outer space. It sounds like the future, but this type of innovation is already taking hold through digital twin capabilities. For example, the U.S. Space Force is acquiring digital twin technology to have a real-time picture of risks and the state of space, including space debris, weather, and communications.

Dave Rhodes, senior vice president for digital twins at real-time 3D platform provider Unity, points to the increasing sophistication of these platforms, which enable organizations to create simulated experiences through immersive capabilities. “Advanced digital twin environments allow users to visualize 3D assets and real-time data in large synthetic environments that mimic the real world with unprecedented accuracy,” he says.

As more organizations embrace large-scale, networked digital twins—and as they integrate more users and more disparate data for complex mission areas—technical leaders need to consider and navigate a host of investment decisions. These range from ensuring that the technology meets user needs and expectations to connecting vast amounts of data in a meaningful way and integrating digital models across a product lifecycle.

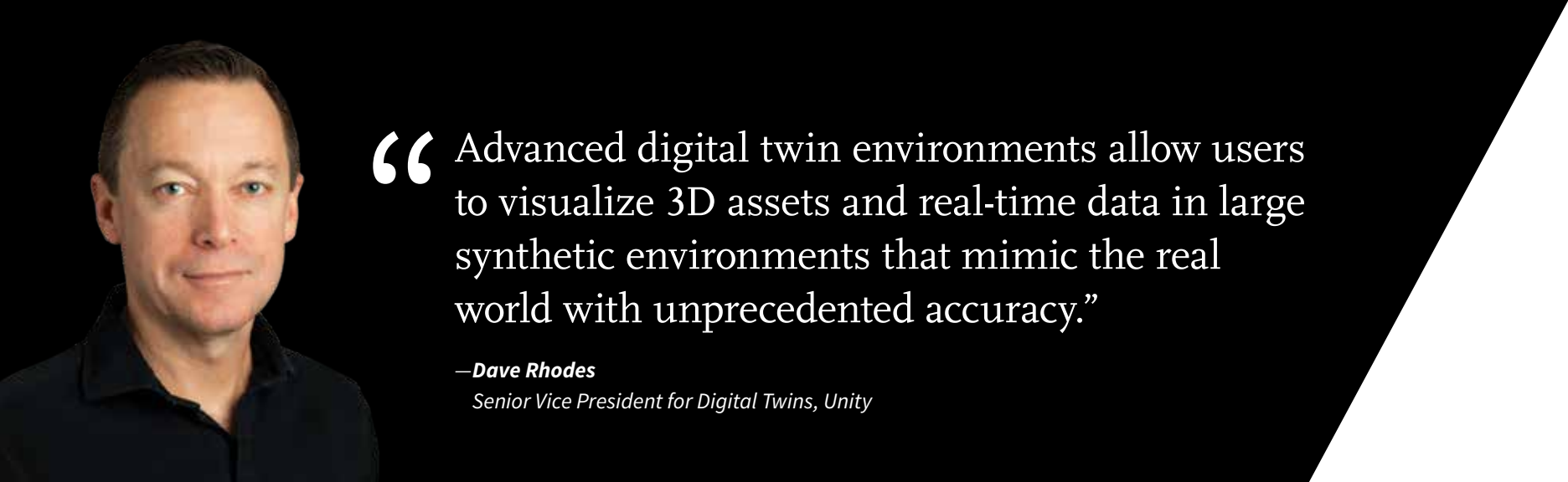
To achieve this unified experience, the digital twin architecture must include and connect a myriad of digital and physical infrastructures. Figure 1 illustrates the integration necessary between cybersecurity, systems integration, digital engineering, data management, platforms,

and analytics and AI to design and deliver comprehensive and valuable information to end users.

Integrating System of Systems—From Hardware to Humans

Digital twins enable new levels of resilience and agility—that is, if they can effectively access and integrate data in a complex digital ecosystem. When backed by thoughtfully designed digital threads, digital twins can advance organizations beyond traditional, siloed approaches to problem solving. They offer the ability to view different yet interrelated systems (each with a seemingly different function and nature) through a comprehensive “system-of-systems” lens. These digital threads that unite data between systems create a streamlined, interoperable view to achieve new insights and enable traceability across the lifecycle of a product or process.

Defense organizations are already taking on this integration. They are adopting digital twins to change the way they field, design, and integrate new systems into the soldier combat ensemble, which includes equipment, weapons, power sources, protective gear, and more. Soldiers today carry more technology on their person than ever before, which can be a major burden and distraction when many of these devices require different cables, interfaces (physical and network), and power sources. Digital twins inform smarter fielding requirements that enforce integration by bringing together these disparately fielded soldier systems (each with unique functions and characteristics) into one authoritative set of blueprints. From there, stakeholder communities can collaborate to assess new technologies, inform system design, and identify impacts to existing fielded configurations.



“Advanced digital twin environments allow users to visualize 3D assets and real-time data in large synthetic environments that mimic the real world with unprecedented accuracy.”

—**Dave Rhodes**
Senior Vice President for Digital Twins, Unity

While this highly complex system-of-systems integration is a challenge in any digital twin environment, imagine if an engineering team had to design a digital representation of you. The potential applications for digital twins now extend beyond the equipment to the individual soldier wearing it. Agencies and organizations increasingly need to understand human performance considerations—specifically, the impact of the uniform and equipment loads individuals are carrying on mobility and muscle strain, stress, training, and environment. Analyzing this information is critical to better serving soldiers as well as astronauts, first responders, and others. From designing custom-fit uniforms and equipment to integrating physical, cognitive, and genetic modeling, organizations are using digital twins of humans, paired with performance insights,

to prepare individuals and teams physically and mentally for the next mission.

As with digital twins of soldier systems, digital twins of humans require sophisticated integration of data, tools, and models into a highly visual environment. Information for a digital twin of a human may be collected through connected wearable devices and Internet of Things sensors alongside anatomic, physiological, and clinical sources. To bring it all together, these tools and data must be wrangled from siloed, server-based systems into cloud-based services to integrate and interface with other cloud-based tools. There is no shortage of technical challenges for IT teams as they refactor and test codebases to ensure interoperability with all modules, review security requirements and address them with the migration from on-premises to cloud-based solutioning.

The integration of so many systems, models, and data sets—especially those with proprietary information, personally identifiable information, and personal health information—creates unique challenges related to data ownership, security, and privacy. Government agencies will need to design solutions that not only protect sensitive data, providing the right permissions and levels of access depending on the system and the data sets involved, but also foster trust with the public. It becomes critical, then, to think of security and trust as synonymous, from protecting sensitive information across a digital thread to fostering trust in the safety and security of the data needed to create a digital twin of a human.

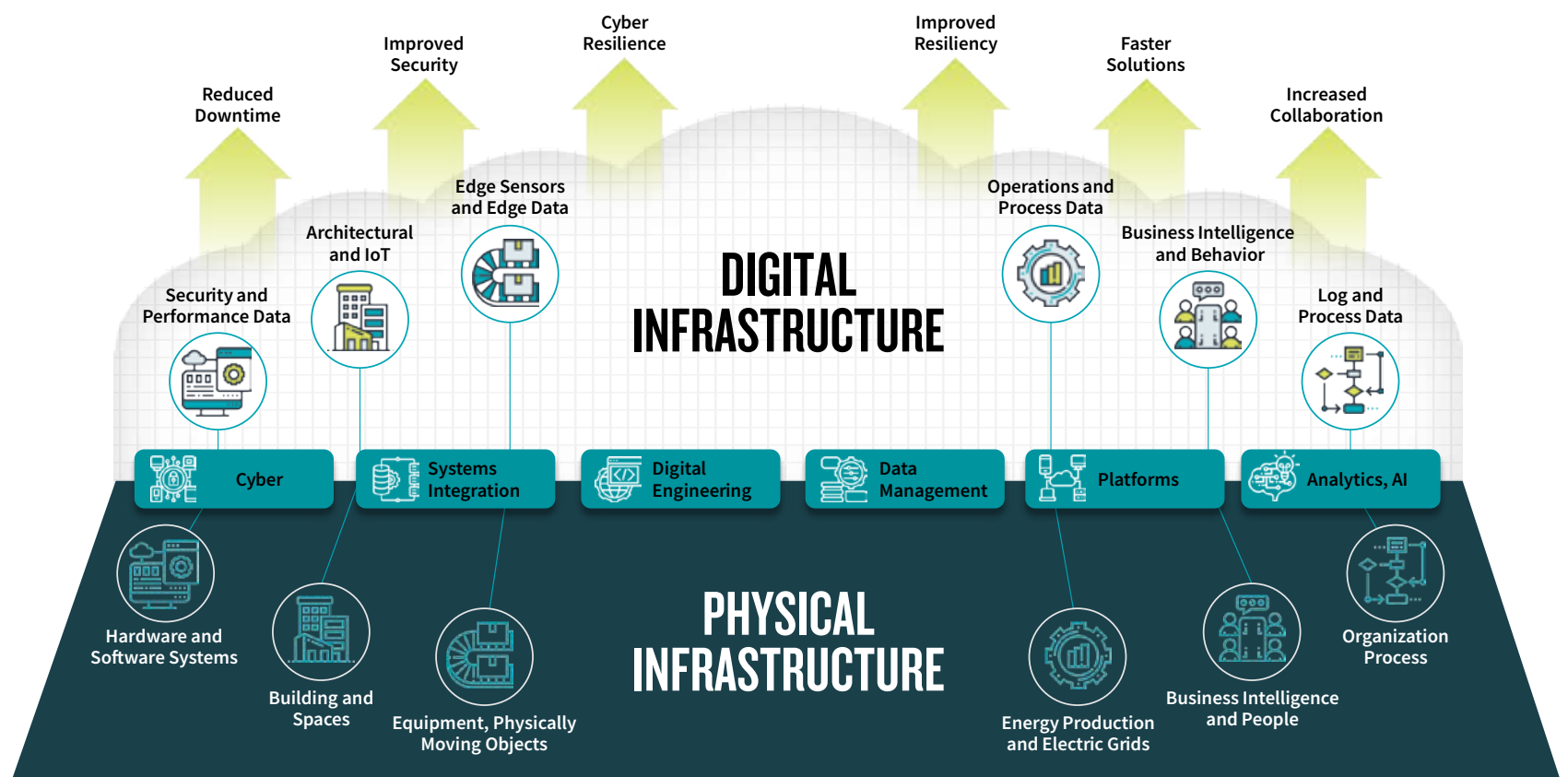


Figure 1: Approach for a Digital Twin Framework

To fully embrace the power of human-machine teaming through digital twins, **human-centered design principles** must be central to the integration, standards, and data orchestration of digital twin development.

Whether it's a digital twin of a human or not, agencies will need to regulate stakeholders' access to information at different levels. By establishing digital ownership, introducing local and multifactor authentication, and managing the traceability among multiple technical products, the Federal Government can use system-of-systems and human-centered digital twins across the lifecycle to enhance mission effectiveness.

Establishing New Standards for Scale

Digital twins are demonstrating promise to help federal agencies improve the development, operations, and sustainment of critical infrastructure. To make this possible at scale, industry and government have an opportunity to reimagine a more flexible, universal approach to digital twins of the future.

Data standards are one of the most critical places to start. For example, some military services (like many organizations) leverage Building Information Models (BIMs) to organize and leverage facility data from design and construction to operations and maintenance. BIMs can be found in large-scale digital twins used to make massive, multimillion-dollar decisions on critical infrastructure. This requires data sets to be standardized and accurate to ensure these decisions are valid and trusted. Any gaps in BIM data standards or inconsistencies in nomenclature, units of measure, or center points to anchor the models can lead to imprecise analytics and data visualization for users. When critical infrastructure decisions need to be made—for example, when using a digital twin for traffic flow simulations to optimize road design—having shared BIMs in the right locations is critical to accurate and safe projections.

A BIM is just one example of how the challenge of bringing together data created by multiple groups and vendors into a

connected system-of-systems digital twin requires the development of key data standards in the digital world.

Now consider the requirements for system security. Emerging digital twin commercial software often uses basic role-based security credentials, but agencies will need to adopt more secure multifactor authentication that incorporates federal common access card security requirements. Each government entity also has different requirements across varying on-premises, cloud, and hybrid environments. To meet the myriad security needs in government while enabling the ability to scale, digital twins must run in a secure cloud environment. Implementing microservices with containers provides developers the ability to increase scalability and to deploy and deliver code more quickly and efficiently. Looking ahead, to do this at scale and in an efficient manner, government agencies will want to explore authorization for continuous authority to operate to enable ongoing development and deployment of containerized and authenticated digital twins. This will allow agencies to deploy and begin harnessing the value of digital twins sooner while continuing to build on and mature the digital twin to support additional integrations and use cases across a lifecycle over time.

Finally, to scale performance, digital twins will need fast, high-capacity, highly resilient networking. 5G networks enable large-scale, real-time analysis and bidirectional sensor connections. 5G infrastructure outperforms 4G networks by supporting enhanced mobile broadband and wireless connectivity up to 100 times faster than 4G. 5G optimizes the processing of very large amounts of data with minimal delay and 99.999% reliability through ultrareliable low latency while allowing for massive machine-type communications at nearly 1 million connected devices per square mile. This

capability enhances data quality and allows users to interact with digital twins through analytical simulations and operational usage in a variety of environments—from labs and training ranges to field operations in remote and contested environments.

Orchestrating Data to Address World-Scale Challenges

Calls to action around data standardization are accelerating the adoption of digital twins to address some of the world's most daunting problems. Take climate change, for example. Vast amounts of data from a wide variety of sources need to come together to help solve these complex issues. Governments around the world are beginning to tackle these problems through the use of digital twins:

- Agencies, including the National Oceanic and Atmospheric Administration (NOAA), are exploring the development of a digital twin for Earth observations and to help streamline data processing to users and applications.
- The European Union has an initiative known as Destination Earth to develop digital twins of the planet to better understand climate change and to use simulations to predict future hazards.

These initiatives are just two examples of how data orchestration, when done thoughtfully, has the potential to tackle

“Digital Thread”

A data pipeline that enables a digital twin by collecting and unifying diverse, interrelated datasets (whether they are historical, contextual or real time) across the lifecycle of a product or process, providing a single source of truth.

Booz Allen and Unity are working with the U.S. Air Force to develop a 3D, IoT-connected digital twin at significant scale, as the platform to support the design, reconstruction, operations, and sustainment of the Tyndall Air Force Base. This is providing the Air Force with a digitally connected, resilient, and operationally effective Installation of the Future.



some of our world's greatest challenges. However, it will require stringing together data from siloed sources, which is no small feat. For example, the Destination Earth initiative will use environmental, socioeconomic, and satellite data to help anticipate events like droughts, storms, and sea-level rise so that governments and other entities are better prepared for emergency response. Digital twins have the power to help model global issues, but there are significant complexities to think about, from data ingestion through visualization and usability.

Efforts within the U.S. Government to understand and predict environmental conditions involve collecting multiple petabytes of geospatial and satellite imagery data in varying formats (e.g., raster, NetCDF, tabular, vector). Well-developed data pipelines and processes for standardizing, parsing, enriching, and validating this data are required to ingest, fuse, and process it from multiple sources—atmospheric, oceanographic, cryospheric, land, and hydrologic.

But collection is just one hurdle. Once you have the data, what do you do with it? For example, while satellites and other earth observation sensors generate more environmental data every hour, only 10% to 20% of this data is currently used because there's so much to contend with.

As data sources like this proliferate, the next challenge lies in data integration and fusion to produce and validate artificial intelligence (AI)/machine learning (ML)-ready data sets in real time and at scale. Integration requires a data platform that can feed into any digital twin (i.e., visualize data when plugged into a variety of models with differing metrics/parameters); use AI/ML to build predictive models; and support the streamlined ingestion, parsing, and codifying of the data. Overall, as the influx of integrated data for climate digital twins grows, quantum computing capabilities will be critical to provide the computational power needed to support simulations and assessments (read more on quantum computing on page 6).

Finally, agencies will need to translate digital twin data into meaningful and intuitive visualizations that resonate with end users and encourage adoption. To fully embrace the power of human-machine teaming through digital twins, human-centered design principles must be central to the integration, standards, and data orchestration of digital twin development. Currently, there is not a set of standards for how to interact with digital twins. Since digital twins can be deployed on desktop, mobile, or in extended reality environments, organizations can start to draw user experience and user interface design standards from those platforms to ensure that the applications make sense to

the user and that they achieve tasks with ease to mitigate barriers to adoption.

Realizing This Broader Vision

From living models of whole factories and hospitals to precise replicas of entire cities, the future of digital twins will be large-scale, networked twins. Rhodes emphasizes that this future “offers the advantage of understanding and testing the potential outcomes of something before you ever try it in the physical world.”

Built on comprehensive, trusted data, digital twins will help enterprises optimize operations, detect and predict anomalies, pivot to prevent unplanned downtime, enable greater autonomy, and dynamically adjust their designs and strategies with every new piece of data they collect or every new test they run. While each of these capabilities can save money and increase efficiency, the ultimate benefit lies in what they represent together: a new way of understanding and improving the world around us.

Sandra Marshall, Trishna Lovley, Jennifer Jenkins, and Colin Corridon are part of Booz Allen's Bright Labs incubator, an experimentation organization designed to develop, test, and incubate mission-centric solutions rooted in emerging technology. Their team focuses on the application of digital twins for client missions.

SPEED READ

Digital twins are fast becoming a cornerstone in the design, manufacturing, and operations of products and infrastructure.

Federal agencies, from defense to critical infrastructure, are increasingly exploring this technology to test innovative approaches and solutions (and prepare for emergencies) without ever reaching the limits of the actual world.

As more organizations embrace large-scale, networked digital twins—and as they integrate more users and more disparate data for complex mission areas—technical leaders need to consider and navigate a host of investment decisions. These range from ensuring that the technology meets user needs and expectations to connecting vast amounts of data in a meaningful way and integrating digital models across a product lifecycle.

Putting Zero Trust into Practice

FITTING THE PIECES TOGETHER FOR ADVANCED CYBER DEFENSE

Authors: Imran Umar, Michael Lundberg, and Matthew Snyder

Contributor: Kelly Rozumalski

Federal agencies are racing to adopt a zero trust architecture to comply with urgent cybersecurity requirements. Some are further along than others in this journey, but all face the same questions: Where do we start? And how do we move our organization to the necessary architecture?

To answer these questions and pinpoint where improvements are needed, organizations must first step back and review their existing cybersecurity posture and technology roadmaps through a zero trust maturity assessment. This in-depth look at organizational and architectural issues—which provides deeper insights than typical cyber risk reviews—is designed to help organizations identify and address their zero trust gaps.

Understanding the Pillars of Zero Trust

Identifying zero trust gaps as early as possible will help organizations meet upcoming deadlines. Based on Executive Order 14028 and the federal zero trust strategy, agencies must achieve specific zero trust security objectives by the end of fiscal year 2024. To that end, they have been drafting implementation plans, which need to be refined and resourced to accomplish “ambitious, achievable goals,” according to the White House’s FY24 cybersecurity budget guidance.

Evaluating the current state of the enterprise’s capabilities and gaps is the first step. This enables the security team to weigh priorities and craft tailored implementation guidance to achieve focused improvements over time.

This evaluation requires a framework—a basis for rating capabilities, setting targets for improvement, and achieving measurable

progress. To that end, Booz Allen developed a maturity assessment model: It aligns to the Department of Defense (DoD) and Cybersecurity and Infrastructure Security Agency (CISA) maturity models, but provides a more granular look at an organization’s capabilities across the seven pillars defined in the DoD reference architecture. For more detail on the pillars, see Figure 1 for a visual summary and examples of capabilities along the spectrum.

The model helps put the principles of zero trust—assume a breach; never trust, always verify; and allow only least-privileged access based on contextual factors—into action. It lets organizations rate their capabilities in all seven dimensions of zero trust using the five maturity levels: initial, minimal, basic, innovative, or leading. Insights from such an assessment can help an agency work toward deploying comprehensive security monitoring, granular dynamic and risk-based access controls, and system

Elevate Security By Design With 7 Pillars Of Zero Trust

Maturity model enables focused improvement, in several steps, from initial practices toward leading capabilities

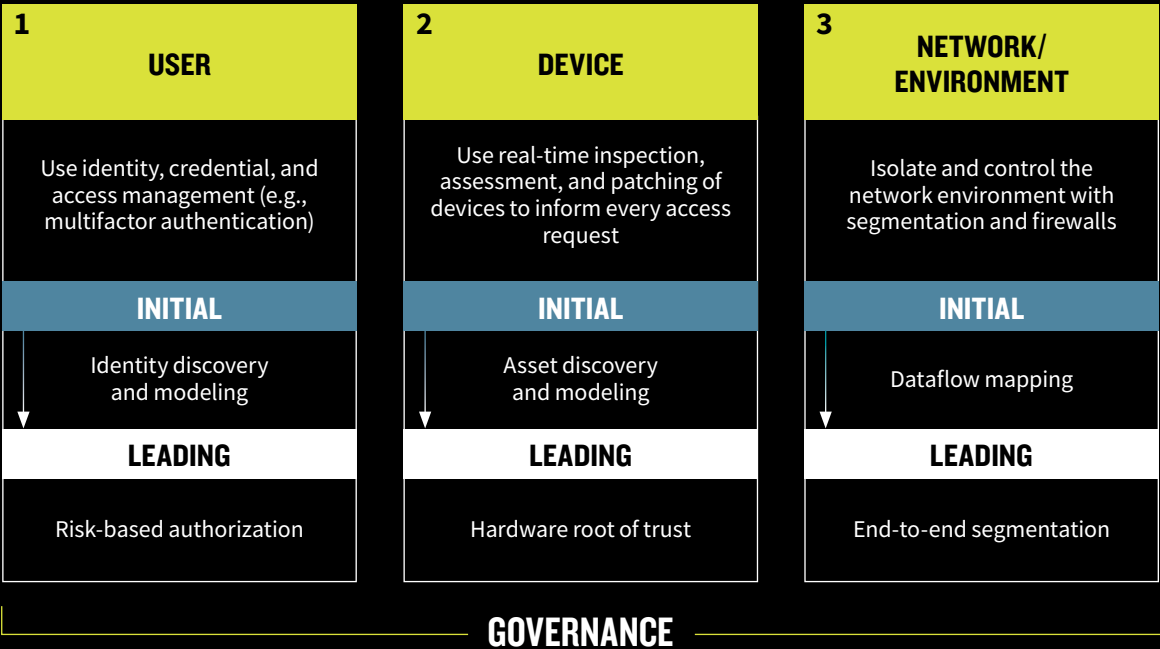


Figure 1

Evaluating the current state of the enterprise's capabilities and gaps is the first step. This enables the security team to weigh priorities and **craft tailored implementation guidance** to achieve focused improvements over time.

security automation in a coordinated way throughout infrastructure.

Armed with a threat-centric understanding of where an organization is along the spectrum, it's possible to set future targets that help drive down operational risk and give rise to new solutions for pressing needs.

Over time, organizations can continuously use the maturity assessment model to conduct follow-on assessments whenever they need to refresh their approach. The first step is always to diagnose challenges across the seven pillars by examining how people, process, and technologies form the organization's security solution. Next, organizations design a zero trust strategy, develop new fixes in the safety of a lab, and deploy new solutions.

Booz Allen uses this same approach internally to improve our own security posture. The firm is committed to making Booz Allen "client zero" for the development of all kinds of innovative new solutions as

we operate and defend a global enterprise with more than 30,000 users supporting a wide range of critical missions.

Technical Challenges to Focus On

Operationalizing a zero trust architecture along the path to maturity brings a host of technical decisions. Amid the multitude of potential priorities, here are three notable areas of focus for cyber and data practitioners.

Dealing with Data

Every organization is unique. But the aspect of zero trust where most organizations tend to be the weakest is the data pillar. This area involves using end-to-end encryption, data rights management, and data tagging to protect data. Organizations should prioritize fixes in the area of data management to ensure the success of broader objectives.

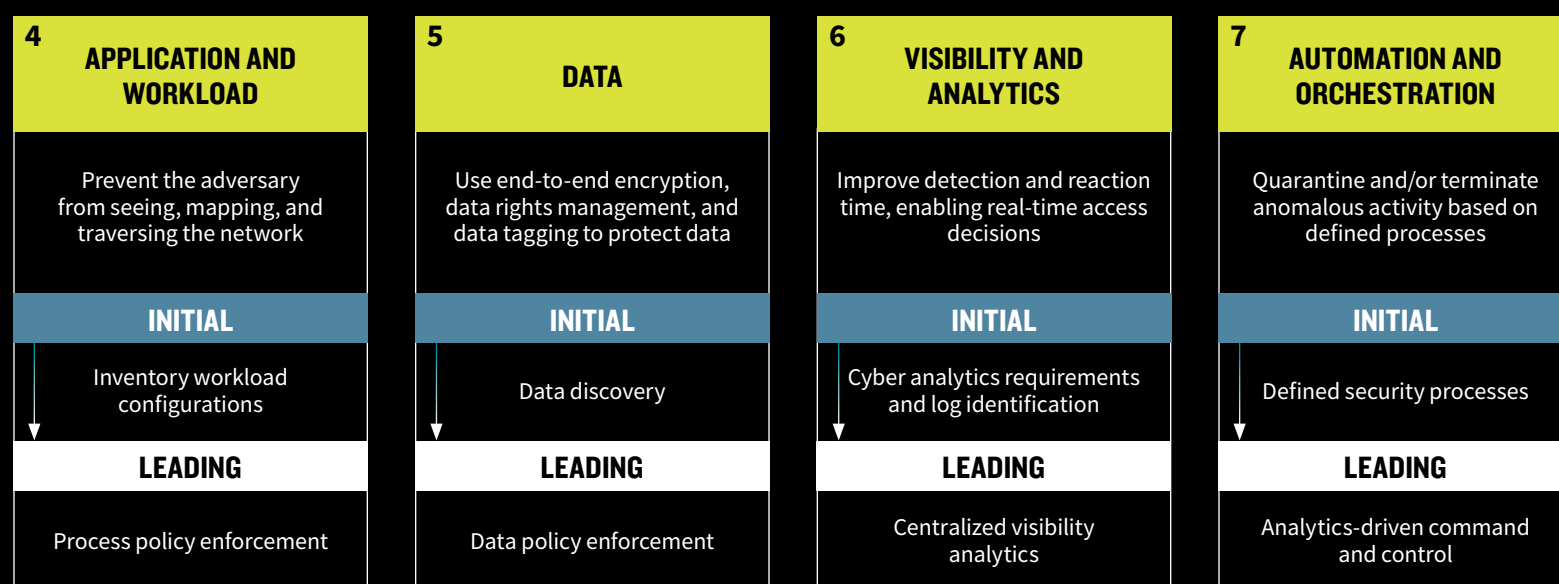
For instance, as organizations try to conduct data discovery and classification,

the first area they are looking to modernize is secure access to their networks (cloud and on-premises), otherwise known as zero trust network access (ZTN). To enable restricted access by default as desired, they first need to figure out how to classify and handle their data.

Implementing Identity

Another big hurdle for enterprise cybersecurity is implementing identity in an unfamiliar way. To achieve the federal vision for zero trust, agency staff need to use enterprise-managed identities to access the applications they use for work. However, employees change roles, routinely in some organizations. It is important, yet challenging, for security teams to maintain awareness of what these individuals should and should not be able to access based on their new position.

The identity management piece is a vital enabler for all zero trust principles. Strong authentication is also important to provide assurance around identities. Focusing



In a survey Booz Allen commissioned of 175 individuals involved in the development, analysis, and review of U.S. cybersecurity practices and policies, 60% of respondents said they had limited knowledge of cyber data analytics. In addition, respondents were roughly split on whether they had limited or substantial knowledge of zero trust and cyber-focused AI and ML.

on these areas from the start can set a strong foundation for further zero trust improvements. Also, organizations should establish a single source of truth for identity credential and access management (ICAM)—one tool that systems can rely on to verify that particular people should have access to particular functions or features. In some cases, based on the size of the organization, federated ICAM solutions are needed.

Making the Most of Logs

Another major challenge is the proliferation of logs driven by zero trust's strong emphasis on continuous monitoring. Amassing countless new logs could overwhelm relatively small security teams. Organizations need to be smart and efficient in how they handle all that data.

Although the administration has introduced new advanced logging requirements, agencies aren't yet using all that data effectively within their security operations centers. On a continuous basis, it's important to evaluate what data is useful and what isn't—for instance, focusing on relevant data elements within broader data feeds.

What's more, organizations need to move away from retaining data in ways that are less cost effective for the long term. By adopting a data-driven cybersecurity approach, organizations can start using cloud-based solutions to store massive quantities of cybersecurity data for longer periods in a more cost-effective manner, which unlocks the benefits of security analytics at scale in real time. And this, in turn, can enable advanced cybersecurity that uses predictive analytics and turns threat intelligence into actionable insights.

Making investments in advanced technology like artificial intelligence (AI), machine learning (ML), and streaming analytics can help security teams make the

most of their data, identify aberrant trends in network traffic, and get ahead of threats. For now, federal and defense agencies are just starting their efforts on this front, but increasingly they will be looking to the private sector to leverage such capabilities.

Over time, organizations can work toward implementing the architecture for a cloud-native, cyber-focused data pipeline for streaming analytics (threat hunt, detection, and compliance) and start to apply the principles of zero trust and data-driven cybersecurity to protect 5G and cloud-based networks.

What's Next? Zero Trust in 5G and Beyond

Imagine an adversary is out to steal and sabotage sensitive technology that underpins a major defense acquisition program designed to meet urgent military requirements. It could all start with a threat actor using 5G threat vectors to conduct espionage, compromise the supply chain, infiltrate a network, and move toward the target. Applying a zero trust mindset, however, could counter such threats with stringent authentication measures, network segmentation, and evolved threat hunting. This is one of two hypothetical scenarios our team developed using tactics and techniques from the MITRE ATT&CK® knowledge base to show the potential of zero trust in 5G.

Operators of 5G ecosystems need holistic security that includes zero trust architecture, 5G development, security and operations (DevSecOps), and a 5G workforce, as well as vulnerability research and embedded security. Zero trust principles can spread through the entire 5G architecture when analytics and automation

are used to drive security improvements over time with policy updates aligned to the other pillars. The continuous development and deployment of new policies protects application authentication and access into the 5G network.

Embrace Zero Trust with Confidence

The journey to zero trust starts with evaluating an organization's cybersecurity against a maturity assessment model and then designing, developing, and deploying solutions that are fit for purpose. Along the path to maturity, organizations may find certain zero trust capabilities already in place and can leverage near-term opportunities to make headway without significant investment. For more substantial zero trust efforts, there is the ability to request funding via the Technology Modernization Fund (TMF).

Importantly, security leaders can look to zero trust efforts at other agencies to glean lessons learned. For instance, the Defense Information Systems Agency (DISA) is developing a scalable prototype of a zero trust security solution known as Thunderdome. Also, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Institute for Standards and Technology (NIST) have recently published several pieces of zero trust guidance. As organizations leverage the growing body of federal guidance on zero trust and share lessons learned, U.S. national and economic security is sure to benefit.

Imran Umar, Michael Lundberg, and Matthew Snyder work with defense and civil clients to advance the adoption and fusion of zero trust, ML, and AI to improve cyber resiliency.

SPEED READ

Agencies are drafting zero trust implementation plans to meet specific zero trust security mandates by the end of fiscal year 2024.

The path to developing tailored solutions for zero trust starts with evaluating the current state of the enterprise's capabilities and gaps. Armed with a threat-centric understanding of where an organization is along the spectrum, it's possible to set future targets that help drive down operational risk and give rise to new solutions for pressing needs.

Amid the multitude of priorities along the journey to operationalize zero trust, three notable areas of focus for cyber and data practitioners are 1) dealing with data, 2) identity management, and 3) smart, efficient handling of logs and data.

Metaverse and Web3: Hype vs. Reality

COLLABORATION, EXPERIENCE, AND TRUST ARE KEY TO THE NEXT WAVE OF INTERNET TECHNOLOGIES

Dan McConnell, Elliot Mandel, and Chris Hample

In the pantheon of buzzwords and technological jargon, the “Metaverse” holds a special place, embodying both the promise of the next internet and the perils of hype exceeding reality. Though the term has recently seen a resurgence in the public consciousness, it originated in Neal Stephenson’s 1992 *Snow Crash*, a science fiction novel that conceived the term as a portmanteau of “meta” and “universe.” Thirty years after the publication of *Snow Crash*, Facebook changed its name to Meta and began the new Metaverse trend, as seen by the internet search volume of “Metaverse” increasing 7,200% after Facebook’s rebranding (Zenou, 2022).

This renewed focus on the concept of the Metaverse has accelerated the development and investment in technologies that are integral to the ecosystem of the Metaverse—cloud computing, artificial intelligence (AI), Internet of Things (IoT), extended reality (XR), and Web3, among others. Both public and private institutions are facing the challenge of understanding these new technologies and separating the hype from the reality of the Metaverse to establish effective strategies for integrating new capabilities to best prepare for the digital future. However, the Metaverse and its associated technologies are nascent and often more nuanced than these headlines purport.

Metaverse Movers

Many commercial companies are allocating significant resources to become early adopters of Metaverse and Web3 ahead of competitors, prioritizing speed and first-mover advantage in a rapidly crowding space. For the Federal Government however, it is critical to move quickly while thoughtfully assessing the protection of digital citizens—especially given the vast amount of data produced and collected by these technologies and the cybersecurity implications of that data as it is produced,

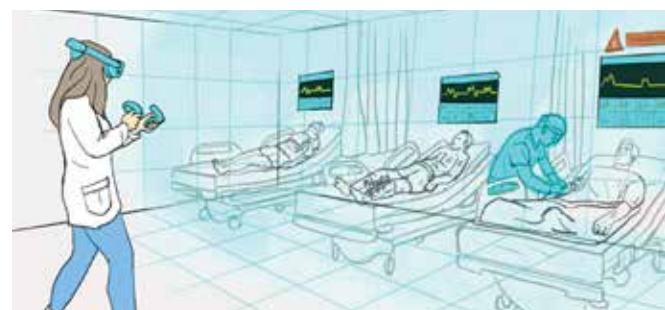
tracked, and leveraged by a whole host of emerging stakeholders, including large technology firms vying to be the Metaverse platform operators of the future.

The Federal Government is already entering the Metaverse arena. In May 2022, the U.S. Department of Defense (DoD) announced that it is building its own Metaverse that will include F-35 fighter jet helmets with built-in augmented reality (AR) head-mounted displays (HMD) to display telemetry and target data over live video. The U.S. Army also awarded \$22B to Microsoft to develop AR fighting goggles. Most recently, at the forefront of such a transformation is the U.S. Space Force, which recently trademarked the name SpaceVerse™ for the organization’s branded Metaverse. As DoD’s only digitally native service, the Space Force is taking an organized, methodical approach to experimenting with new use cases for the SpaceVerse focused on “leapfrogging ahead and designing the future technologies that the Space Force will need” to realize a shared digital and physical workspace and partner ecosystem (Underwood, 2022).

Foundations of the Metaverse: Definition and Technical Capabilities

Many popular definitions of the Metaverse focus on a narrow and static view of the future: technologies and standards that are mainly dedicated for creating persistent, immersive 3D experiences. However, the definition of the Metaverse is constantly evolving, with different elements and components of the broader ecosystem being leveraged for new and emerging use cases and experiences as the capabilities grow. Rather than focusing on a specific definition, an effective process for engaging with the Metaverse is to understand the distinct elements that comprise the whole.

Article illustrations by Booz Allen



Elements of the Metaverse

The rise of Metaverse and Web3 technologies has been enabled by the ongoing advancement and innovations in different layers across the entire technology stack. This emerging architecture will be the foundation at the intersection of our future digital and physical worlds, extending across institutional boundaries to create increasingly seamless and immersive experiences. Capability areas describing these future experiences can be segmented into eight components (see Figure 1).

While the technological promise of these elements paints an idyllic picture of the future Metaverse, there remains a large distance to cover between the world of today and that of tomorrow.

Putting Your Money Where Your Metaverse Is

In January 2022, Microsoft made the largest acquisition of a gaming company to date, purchasing the game studio **Activision Blizzard** for \$68.7 billion explicitly to provide “building blocks for the Metaverse.” In April 2022 **Epic Games**, the American video game company, raised \$3 billion to fund a Metaverse strategy for the future, including a partnership with **LEGO** to build a Metaverse for kids.

Eight Components of the Future Metaverse

COMPONENT	DESCRIPTION	TECHNICAL FOCUS AREAS
Experience	The expected Metaverse experience will be one that cuts across industry and use cases, where a single user experience could integrate into multiple capabilities like a “one-stop-shop.”	Designing experiences to leverage IoT sensors; haptic clothing; and AI, allowing users to sense space and time in XR.
Content Creation	The ability to create content will continue the shift toward democratization and decentralization of digital content creation.	A robust creator economy will be supported by advanced technologies such as AI/ machine learning (ML) and low-code/no-code authoring tools.
Discovery	Discovery of information ensures that content is open and tagged with appropriate metadata so it can be found by users across a variety of user interactions.	Automated service and content discovery powered by personalized AI algorithms tailored to a user based on the local hardware and software paired with the supporting infrastructure.
Human Interface	From a user perspective, the experience layer will be the most apparent transformation of how someone interacts with a digital space. XR enhances an individual’s perception of the world, allowing for new ways of interacting with people and things.	Developing differentiated capabilities for creating mature HMDs for new human-computer interaction techniques.
Infrastructure	As the data evolves from flat, 2D representations to 3D, the infrastructure must not only be able to account for the increased storage requirements and throughput of multiple dimensional data, but it also needs to be able to capture an ontology and relationships of 3D synthetic and real-world environments.	Investment in creating the AR Cloud infrastructure, “a collection of billions of machine-readable datasets, point clouds, and descriptors, aligned with real-world coordinates; a living, shared, ‘soft copy’ of the world created by scanning physical features around us in which persistent augmented reality experiences reside.” (Open AR Cloud Association)
Spatial Computing	The ability to seamlessly mesh digital space with physical space will require real-time spatial alignment capabilities, enabling Metaverse applications to leverage 3D image generation and geospatial data. This extends across a wide range of sensory input including gestures, voice, audio, and even neural, supported by Metaverse optimized chipsets.	AR Cloud will also deliver the necessary persistence that spatially locates digital assets and localizes using the user device’s precise geolocation. It will leverage geospatial positioning to create a 1:1, dynamic point cloud, or digital twin, of the physical earth, while localization services enable AR content to be placed in a specific place on earth and persist there.
Decentralization	The Metaverse is decentralized and its digital assets, such as avatars, cryptocurrency, and NFTs, are user controlled and span applications that are not centrally governed.	Web3 and development of distributed ledgers to enable decentralized distribution of data, assets, and computing resources.
Standards and Protocols	In the same way HTML, HTTP, and URL standards defined the internet, future underlying standards and protocols must ensure cross-platform translation and communication across the 3D Metaverse with its myriad of experience designs, interfaces, and applications.	Interoperability between technologies built on different platforms, programming languages, and data structures to enable seamless transition between virtual worlds.

Figure 1

The rise of Metaverse and Web3 technologies has been enabled by the ongoing advancement and innovations in different layers across the entire technology stack. This emerging architecture will be the foundation at **the intersection of our future digital and physical worlds**, extending across institutional boundaries to create increasingly seamless and immersive experiences.

Barriers for Adoption

Technology leaders in public and private sectors should follow and understand the impact that emerging Metaverse and Web3 technologies, such as XR, digital assets, and distributed ledgers, will have on their organizations and the users they serve. As these technologies mature, CIOs and CTOs need to recognize barriers to adoption across people, processes, and technologies at the intersection of these capabilities and their real-world usage.

See Figure 2 for a summary of the top barriers to adoption for Metaverse and Web3 technology and a forecast for when these barriers will be overcome.

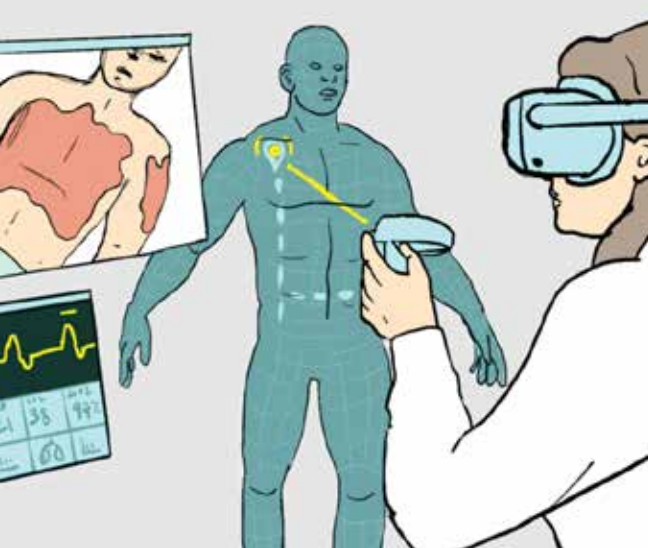
For teams interested in experimenting with Metaverse and Web3, new skill sets will be needed to prototype and build capability in this space. Related fields such as 3D modeling and design, XR software development, and distributed ledger development are growing rapidly, while more traditional technical capabilities such as data engineering, user interface (UI) and user experience (UX) development, and cybersecurity and privacy become even more important when building in the Metaverse.

For organizations interested in experimenting with emerging Metaverse technology, learning new skill sets and refreshing current ones will be necessary

to prototype and build capabilities in this space. Hardware remains a significant blocker to user adoption, despite price reductions and new market entrants in recent years. Current XR HMDs, however, are not ready for mass adoption due to limitations, including form factor, SWAP (size, weight, and power), field of view, and cost. While some sectors may choose a “wait and see” approach, early adopters are experimenting with capabilities such as remote rendering, a service that uses the computing power of the cloud to render high-quality 3D content and deliver immersive XR experiences directly to a user’s HMD.

BARRIERS TO ADOPTION	FORECAST	RECOMMENDATION	METaverse ELEMENT IMPACT
New technical skills and competencies critical to building the Metaverse	2–5 years	Invest in training on COTS gaming engines such as Unity or Unreal, digital twin and IoT platforms, and spatial 3D data pipelines.	Content Creation; Discovery
Scaling user adoption to reach critical mass	5–10 years	Identify and pilot early use cases that are engaging, relevant, and that cannot be experienced without the technology.	Experience; Discovery; Human Interface
Common frameworks for managing internal governance	5–10 years	Adopt user-centric guidelines for data privacy and technology governance covering different aspects of the Metaverse.	Experience; Human Interface; Standards and Protocols
Standards and protocols	5–10 years	Pursue collaboration across government, industry, and nonprofits to cooperate on the development of interoperability standards for an open Metaverse.	Standards and Protocols; Decentralization
XR hardware limitations	5–10 years	Identify XR hardware requirements for mission-focused use cases and focus experimentation on improving SWAP tradeoffs across mission areas.	Human Interface; Infrastructure; Spatial Computing
Interoperability in the AR Cloud	>10 years	Invest in efforts and partnerships to experiment with digital twins, localization services, and creating 3D content that is interoperable across multiple Metaverse platforms.	Standards and Protocols; Decentralization; Infrastructure

Figure 2: Summary of Key Barriers to Adoption of Metaverse and Web3 Technology



While somewhat nascent in their development cycle, technologies such as Remote Rendering provide the critical component needed to scale XR experiences from single-point AR/VR solutions tailored to specific devices to a secure, managed, and easy-to-distribute enterprise spatial ecosystem. Multiple players are currently investing large amounts of research dollars into this technology, and it is unsure what standards will emerge. Organizations must become comfortable with rapid prototyping and iterating in an ambiguous space to better understand the design challenges and patterns that will inform their future enterprise IT architecture.

With the expansion of Metaverse competencies, new interface capabilities and rapid prototyping processes will require existing IT governance frameworks to consider the exponential increase in recorded spatial and personal data and the additional attack surfaces that new applications and interface devices will bring. New risks related to privacy, data ownership, acceptable use, identity, and trust also present themselves in the Metaverse. It is incumbent on technology leaders to keep other leaders aware of these risks and how to continually manage them through technology adoption.

Policy and Safety in the Metaverse

As technology advances and exciting new use cases grow by the day, it is imperative that leaders place a premium on the safety of users and supporting policies as the Metaverse expands into daily life.

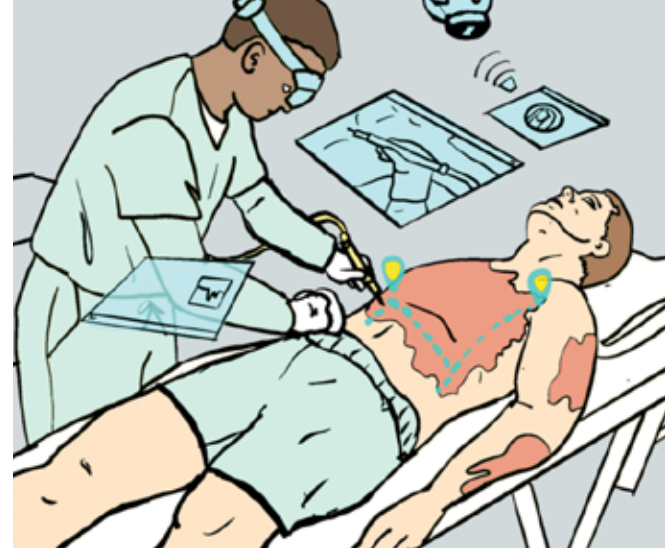
The consequences of not establishing these types of protections early on will amplify and replicate the safety issues of the internet of today at the Metaverse scale. As such, public policy and standards in the Metaverse must keep pace with its emerging technical capabilities, and leaders



in all industries and organizations must take an active role in ensuring the Metaverse is safe and reflects the values of equity and inclusion for all. In particular, leaders need to be aware of the following issues:

- **Content Moderation.** Bullying and harassment is already an issue on the internet and in the Metaverse, and public policy on content moderation needs to extend to text, speech, and behavior of users' avatars and digital assets.
- **The Digital Divide.** The Metaverse threatens to increase the existing gap between those who have access to digital technology and those who do not. To access the Metaverse, users will need broadband download and upload speeds that are possible on a wireless 5G network. However, in 2020 only 3% of mobile connections in the U.S. were on 5G and geographic availability is ambiguous and fluctuating (Zhu, 2022).
- **Privacy.** Some Metaverse technologies, such as VR, could give various vendors access to immense amounts of personal data, such as body and facial movements and biometric data, that could reveal a user's identity and even emotions and intent in new and unsuspecting ways.

Unique among all the various stakeholders defining the future of the Metaverse, government stands to serve as a trusted institution and key enabler going forward. In democracies such as the U.S., the government will play three key roles in the development of the Metaverse with respect to privacy and safety: protecting each citizen online, defending the nation from foreign cyberattacks in the Metaverse, and ensuring the economy remains open and free from anticompetitive behaviors. Look to publications from organizations such as the National Institute for Standards and Technology (NIST) for ongoing guidance and discussions.



The Federal Government in the Metaverse

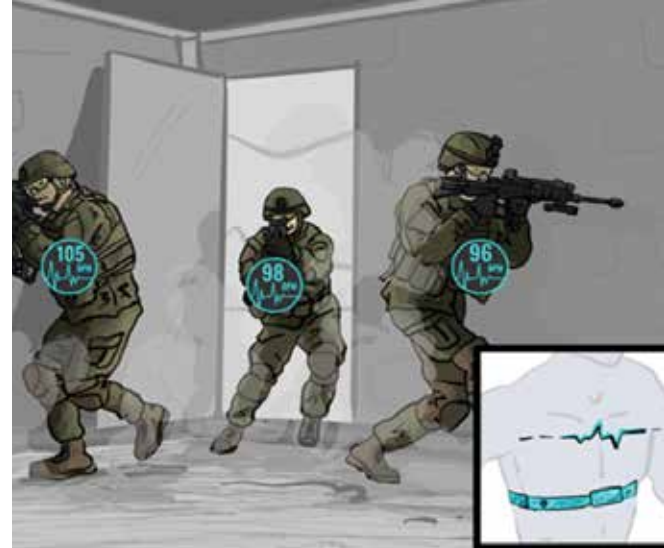
With the growth and rapid adoption of Metaverse and Web3 technologies across commercial industry, the Federal Government has started seeing significant intersections and opportunities to leverage these technologies to better serve the American people.

In the defense space, early military applications of the Metaverse are focused on enhanced individual and group training. The evolution of these technologies will yield increasingly advanced capabilities extending from training to operational use cases across the digital battlespace. A clear example is a Metaverse capability that will add value for the DoD by enabling servicemembers to “train as they fight,” aligning training and operational domains to significantly increase effectiveness. These platforms will create a foundation for multi-domain communication, establishing seamless standards and data exchange pipelines for information sharing between DoD units and with other critical stakeholders.

Key Recommendations

As use cases for the Federal Government proliferate—spanning next-generation digital currency, realistic combat training at scale, and healthcare delivery for underserved and vulnerable populations—the following areas will need to be addressed.

- **International Relations and Global Governance.** Federal agencies should position the U.S. at the table in establishing global standards and technical protocols for technologies that will ultimately enable the Metaverse. Additionally, agencies should partner closely with allies, particularly those in the European Union (EU), as foreign



governments participate in the emergence of standards around the Metaverse. The European Commission's evolving digital policy roadmap, "Shaping Europe's Digital Future," is designed to encourage innovation, promote competition among the large technology platforms, and protect the privacy of Europeans. There is a risk to U.S.-E.U. cooperation should they establish and adopt fundamentally different rules and regulations.

Recommendation: Agencies and industries should embrace partnerships with standards organizations such as Institute of Electrical and Electronics Engineers (IEEE), OARC, and 3rd Generation Partnership Project (3GPP) for 5G and next-generation mobile telecommunications. The Metaverse Standards Forum provides a venue for cooperation between standards organizations and companies to foster the development of interoperability standards for an open and inclusive Metaverse and accelerate their development and deployment through pragmatic, action-based projects. Federal agencies should also collaborate closely with their European counterparts to address common areas of concern.

• **Commercial Regulation.** Beyond the established technology firms going "all in" on the Metaverse, an entire new ecosystem of companies and capabilities is emerging to build the Metaverse, such as industry-leading game engines; cryptocurrency exchanges backed by blockchain; and new hardware manufacturers, to name a few. Federal agencies will have difficulty ensuring the responsible growth of these large platforms while discouraging anticompetitive behaviors.

Recommendation: First, government agencies should bolster antitrust regulation to account for growth in these new industry verticals. More importantly, agencies that have a stake in the Metaverse beyond regulatory jurisdiction can collaborate with these large digital platforms and their technologies that are shaping the Metaverse. The best way for the government to anticipate the future and remain agile will be to experiment with these technologies to better understand the benefits and risks associated with their adoption.

• **Public Policy Support for Individuals.** Arguably, the most important role for government will be to work with industry and other stakeholders to establish common standards around how privacy, trust, access, inclusion, and equity will be protected in the Metaverse.

Recommendation: Federal agencies should identify current technology limitations that could adversely impact the Metaverse and create standards that promote ideals such as trust and inclusion. Specifically, organizations can address issues such as working to remove biases in ML algorithms that reflect human biases and building diverse networks of talent to help them succeed.

This is a time for experimenting, learning, and preparing for the future. Organizations succeeding in the fledgling Metaverse will require flexibility and agility to pivot as Metaverse and Web3 technologies mature, new use cases emerge, and we close the gap between the physical world and the Metaverse.

Dan McConnell, Elliot Mandel, and Chris Hample lead digital and immersive capability development in Booz Allen's Bright Labs incubator, an experimentation organization designed to develop, test, and incubate mission-centric solutions rooted in emerging technology.

SPEED READ

A renewed focus on the concept of the Metaverse has accelerated the development and investment in technologies such as cloud computing, AI, and Web3, among others. Public and private institutions are struggling to understand these new technologies and must establish effective strategies for integrating new capabilities to best prepare for the digital future.

As the Metaverse expands to daily life, leaders should prioritize the safety of users and supporting policies. Leaders in all industries and organizations must take an active role in ensuring the Metaverse is safe and reflects the values of equity and inclusion for all.

In the defense space, early military applications of the Metaverse are focused on enhanced training. The evolution of these technologies will yield an increasingly advanced capability that extends from training to operational use cases across the digital battlespace and beyond.

INVEST,
ACTIVATE,
AND S



Emerging Investment Models to Accelerate Mission Execution

Brian MacCarthy, James Gadea, and Helen Phillips

CALE

The United States is at a crossroads of rapid technological change amid mounting worldwide challenges: a global pandemic, rising geopolitical threats from foreign adversaries, and newly exposed vulnerabilities across supply chains and critical infrastructure. To maintain an advantage against the evolving challenges that the nation faces at home and abroad, the Federal Government is increasingly looking to startups and commercial partners for rapid innovation through dual-use technologies.

With access to a rich commercial ecosystem aligned to mission outcomes, the Federal Government can unlock critical, emerging capabilities that level the global playing field.

“Over the next 30 years we will see emergence of a highly distributed and edge-AI-enabled conflict threatening our national security,” said Bilal Zuberi, a general partner at Lux Capital. He describes a future where “human decision making will likely be almost entirely absent from the decision loop—be it in battlefields, in our communication networks, food and water supply chains, health systems, or in the very air we breathe. Nations that excel in AI, autonomy, quantum computing, brain-computer interfaces, and resilient self-organizing swarm systems, etc., will have distinct advantage.”

To prepare for this future, there is momentum to build meaningful, clear pathways for technology primarily serving commercial markets to be tested and adapted to government missions. Agencies across government are increasingly using venture-like approaches to test and deploy new technologies by way of accelerators, new partnerships, and alternative acquisition models. Still, federal organizations continue to face enduring obstacles to acquiring the right commercial technology for their mission needs.

“Over the next 30 years we will see emergence of a highly distributed and edge-AI-enabled conflict threatening our national security. ... Nations that excel in AI, autonomy, quantum computing, brain-computer interfaces, and resilient self-organizing swarm systems, etc., will have distinct advantage.”

—**Bilal Zuberi**, General Partner at Lux Capital

The Role of Venturing

Several organizations, such as In-Q-Tel and the Department of Defense (DoD) Defense Innovation Unit, have vastly improved the Government’s ability to buy commercial technology or work directly with startups, and the use of Other Transaction Authorities (OTAs) has increased 712% from fiscal years 2015 to 2019, according to the Center for Strategic and International Studies. However, mission execution for commercial innovation on a broad scale has inherent challenges—and the cumbersome and sensitive government acquisition process can be difficult for startups to navigate.

Ultimately, startup technology needs to be strategically integrated into broader solutions for mission impact at scale. However, the startup ecosystem has limited experience and insight regarding federal acquisition, the unique preferences of target customers and buyers, and the relevant environments to test and validate new capabilities. Founders are not inherently versed in how to navigate government or access real end users, and they need support to

Spotlight: Booz Allen Ventures

In 2022, Booz Allen launched an initial 5-year corporate venture fund of \$100 million. The program furthers the firm’s commitment to investing in dual-use technologies that will provide federal clients high-impact technology. This fund is established to support America’s national security efficiently and cost-effectively by streamlining access to a supply chain of critical technologies.

Booz Allen Ventures invests in software, hardware, and deep-tech startups, enabling the firm to advance companies with the most promising solutions to address complex mission challenges. The program also provides founders with access to mission expertise, client use cases, and acquisition support.

To date, the program has facilitated more than 30 teaming agreements for its portfolio companies.



translate and guide their journey into federal programs while seeking funding to further their business (read our interview with Latent AI on page 18). Similarly, government acquisition officials often lack visibility across the full breadth of venture-backed capabilities available to them. As a result, dual-use technology frequently fails to proceed past the prototyping phase, and companies with promising capabilities to support mission use cases often struggle to demonstrate value and utility in the field and at scale.

Venture capital funds increasingly play a critical role in providing inroads for startups to integrate into government environments and enable government acquisition officials, decision makers, and end users better access to emerging technology.

Since 2021, newly established entities include Harpoon Ventures, Andreessen Horowitz’s American Dynamism, Shield Capital, and America’s Frontier Fund. There is a related emergence of corporate venture capital funds, such as Lockheed Martin Ventures and RTX Ventures (a division of Raytheon Technologies). These programs are enabling corporations and system integrators who have access to large-scale federal contracts to serve as a bridge between the U.S. Government and the technology ecosystem, deploying capital to guide startups so they can accelerate innovation for mission relevance.

Through corporate venturing programs, prime contractors are joining traditional venture funds on the cap table and are gaining equity in the long-term success of these companies. Some corporate programs invest opportunistically off the parent company’s balance sheet, while others have dedicated funds with a clear investment horizon and a committed pool of capital. Advantages for corporate venture capital funds include:

- Enabling parent companies to lean into disruptive innovation and establish incentive-aligned partnerships
- Shortening the time to market in critical areas for mission modernization
- Prioritizing internal research and development in areas where the company has a market advantage
- Improving company services and offerings for customers through codevelopment with startup partners

Unlike mergers or acquisitions, corporate investments enable startups to continue to operate independently, maintaining their speed and culture, and minimizing risk to both entities.

An Evolving Ecosystem of the Future

The National Security Commission on Artificial Intelligence (NSCAI) 2021 Final Report put out a very clear call to action around the role of industry to innovate through integrated partnerships, sponsoring and supporting new technology startups. Corporate venture programs have a key role in doing just that. For federal clients, it is a model that provides new access to technology startups and can dramatically streamline and transform how agencies carry out essential mission processes. Mission-focused investments help decrease the time it takes the government to source and adopt next-generation capabilities in areas from artificial intelligence (AI) and machine learning to cybersecurity and defense system technology.

Acquisition officers need the ability to access high-potential startups and shepherd commercial technology out of a lab, across the “Valley of Death,” and into the hands of mission operators. This closer collaboration happening between systems integrators, the startup ecosystem, and the Federal Government helps address historical challenges related to interoperability, lack of reusability, and slow cycles of adoption.

Ultimately, the U.S. cannot afford to be out-invested and out-innovated by adversaries. Commercial technology built by industry and the startup ecosystem, spurred by financial and strategic investments, offers critical capabilities for the U.S. to maintain technical advantage and address evolving and increasingly advanced challenges. With mission-aligned venture programs, agencies across the board—not just within DoD innovation units—have accelerated access to the next generation of technology architects who are pushing the boundaries of digital government.

Brian MacCarthy is vice president of technology scouting and leads Booz Allen Ventures, a \$100 million fund to invest in and integrate commercial technology into Federal Government missions.

James Gadea and **Helen Phillips** scout dual-use commercial technologies for Booz Allen clients.

SPEED READ

The U.S. faces increasing foreign and domestic challenges, as AI and quantum computing define national security. To maintain advantage in the global technology race, the Federal Government is partnering with the startup industry to accelerate the application of dual-use technology.

Startup technology needs to be strategically integrated into broader solutions for mission impact at scale. An emerging breed of mission-focused venture capital funds is serving as a bridge between the U.S. Government and the technology ecosystem, deploying capital to guide startups so they can focus on high-impact innovation aligned to large-scale federal contracts.

The state of the world and the advancement of foreign powers demands more viable paths for the acquisition and investment of emerging commercial technology. The closer collaboration happening between systems integrators, the startup ecosystem, and the Federal Government helps address historical challenges related to interoperability, lack of reusability, and slow cycles of adoption.



CIO CORNER

VIEWS

From Our Modern Lakehouse

INSIDE BOOZ ALLEN'S ENTERPRISE DATA PLATFORM

Brad Stone, Marisa Santisi, Matthew Langevin, Michael Tsyvine, and Ramy Mansour

Across all federal and commercial sectors, data continues to grow in volume, velocity, and variety—with some organizations processing multiple petabytes of data every day. Although new technologies have made this deluge of data easier to store, harnessing that data to help meet mission and business objectives is a more complicated endeavor. To succeed in today's complex mission environments, organizations must have the right platform, processes, people, and algorithms to turn data into insights and—more importantly—*actions*.



At Booz Allen, our IT organization grappled with business pressures to fully harness the power and potential of our data at speed and at scale. Although we had a large data warehouse and several business intelligence (BI) tools for our business systems, we were primarily developing backward-looking dashboards instead of providing the self-service data access and advanced analytics that our customers demanded.

In 2020, we reached an inflection point: Previous investments in modernizing our infrastructure and core business applications were accelerating business processes for individual functions, such as Finance and Human Resources, but our data and analytics capabilities were still lagging. Thus, in collaboration with these business teams, we set out to develop a new data platform that could support Booz Allen's complete data-to-decision lifecycle by meeting the needs of three primary customers:

1. **Builders:** developers and data scientists who create new data products (dashboards, data sources, analytical models)
2. **Analysts:** functional analysts who review existing data products, create new ones, and derive insights to help inform business decisions
3. **Leaders:** functional owners in the business who review those insights and use them to make decisions and take action

Combining feedback from this customer collaboration with lessons learned from Booz Allen client engagements, vendor partnerships, and industry best practices, we developed and deployed a novel data platform to deliver the following key capabilities:

We chose to implement a data lakehouse architecture. ... This platform allows us to capture full data sets of all sizes and formats from our business systems while maintaining fast data query performance, compatibility with common query languages, and support for advanced analytics.

Faster and Broader Access to Data

The most common request from builders, analysts, and leaders was to make more data available to them more quickly and in a self-service manner. Our new platform satisfies this request by combining several new products and technical features.

- **Analytics hub:** An intuitive web portal that allows users to view enterprise dashboards, curated data sets, and analytical models developed, certified, and published by analytics teams across the organization
- **Rapid ingestion:** Automated data acquisition pipelines that do not require upfront data analysis or schema development, and are able to onboard data from an entirely new business system in as little as 1 hour
- **Data catalog:** Automated collection of all data in our platform that allows users to find and understand data, provenance, and lineage down to the individual field level
- **Analytics workspaces:** Sandboxed working environments that give individual teams access to analytics tools and certified data, providing the freedom to experiment with new analytics, introduce custom data, and share results

Enablement of Advanced Analytics

Analysts and leaders wanted to supplement traditional BI reporting with new artificial intelligence (AI) and machine learning (ML) models that can predict future outcomes, detect anomalous events, and make recommendations for actions. Our platform brings together the right tools, data, and compute environment to enable builders to develop advanced analytics that can be delivered directly or integrated seamlessly into existing BI products.

- **Support for data science tools:** Notebooks (e.g., Python, SQL) provide a centralized location for data analysis and code development, while built-in Spark support accelerates processing of large data sets
- **More model training data:** We ingest all available data from our source systems, including structured, unstructured, and semi-structured elements, to enable more robust training of AI ML models and to broaden the range of potential analytical insights
- **Accelerated model delivery:** Streamlined machine learning operations (MLOps) processes (e.g., feature stores, MLFlow) and multiple delivery mechanisms enable rapid development, deployment, and management of production-ready AI/ML models

New Data Lake Platform

FEATURES

Modern, scalable cloud platform for data storage and compute

Flexible, rapid data ingestion

Comprehensive datasets for advanced analytics

Automated data catalog to easily find and understand available data

Centralized, policy-based security

Consolidated data storage for all business systems

Structured and unstructured data

Scalable, Secure, and Flexible Operations

In addition to meeting the needs of our customers, we built this platform to satisfy key IT requirements as well. More specifically, we focused on the following areas:

- **Scalable, vendor-managed infrastructure:** We use cloud-native tools and services that scale resources automatically based on our capacity demands and receive automatic updates to provide new features and mitigate security vulnerabilities.
- **Secure data enablement:** We use automated, centrally managed data access policies that integrate with our enterprise identity management solutions.
- **Open standards:** We use tools that support open standards, scripting languages, and data formats to improve the portability of our overall platform and mitigate vendor lock-in.

What We Learned: Takeaways for IT Leaders

Here are three strategic takeaways we identified during our data modernization:

1. The views are better from a lakehouse. While a *data lake* excels at helping organizations store large amounts of diverse data, it is not as optimized as a *data warehouse* for rapid data queries and robust data management. We knew that we needed the best of both worlds to be successful, and so we chose to implement a *data lakehouse* architecture.

This platform allows us to capture full data sets of all sizes and formats from our business systems while maintaining fast data query performance, compatibility with common query languages, and support for advanced analytics. And, since our data lakehouse runs in the cloud and emphasizes process automation, we're able to deploy new capabilities and pipelines in a matter of hours instead of days.

2. Control the data, democratize the insights. In today's highly decentralized organizations, it is no longer feasible for only one team to build data products for an entire organization. However, without a predefined approach and architecture for decentralization, an organization will struggle with inconsistent user experiences and, most critically, multiple versions of the truth.

At Booz Allen, we decided to enable distributed self-service analysis of trusted data, accelerating creation and consumption of analytics while ensuring enterprise data integrity. We do this in two primary ways: (1) curated data products and (2) analytics workspaces. Curated data products, such as dashboards and data sets, are developed by enterprise and functional analytics teams, certified for accuracy, and made available for consumption via our Analytics Hub. This meets the needs of most leaders and analysts, but builders often require more interactivity with the data. For those use cases, we create sandboxed analytics workspaces, which provide access to governed, enterprise data and advanced tools that promote responsible experimentation, collaboration, and analytics development. The work done in these workspaces can stay private to a particular team or be submitted for certification and inclusion in the shared data platform for broader consumption. This approach takes us beyond sharing data extracts with only a few users to enabling teams to develop predictive models and other innovations on trusted data that can be shared across the enterprise.

3. Data modernization requires cross-functional delivery.

Ultimately, collaboration across technical and business functions is key to the success of any data modernization effort. Primary teams can include specialists in technical platforms, data engineering, analytics, and data governance, while the extended group can include data analysts from business units that can help pioneer new capabilities. Every team brings a unique set of priorities and constraints to the table, and when all are working toward the common goal of data modernization, this collaboration ensures the most efficient prioritization of activities and early identification and remediation of any issues.

The Ultimate Goal: Seamless, Augmented Intelligence

When data modernization is done right, we've seen how analytics use cases multiply and innovation flourishes in a frictionless data environment. We have already come a long way: from generating static monthly reports to using AI/ML models that help us remove bottlenecks from the talent acquisition process, automate quarterly financial forecasting, and apply natural language processing to match employees with new projects.

On our data modernization journey thus far, we've learned that our success is not measured by the complexity of our platform but by the speed and simplicity with which it enables the business. Our ultimate goal is to provide a kind of "second brain" to leaders across the firm, helping them make better decisions that are informed by insights, recommendations, and predictions. As we continue to evolve our new data platform and analytical use cases to achieve that goal inside Booz Allen, we will apply our lessons learned to help our clients accelerate their own critical journeys from data to seamless, augmented intelligence.

Brad Stone is Booz Allen's chief information officer.

Marisa Santisi, Matthew Langevin, Michael Tsyvine, and **Ramy Mansour** lead enterprise analytics within Booz Allen's Office of the CIO.

Today, we're using **insight-driven analytics and AI/ML applications** to remove bottlenecks from the talent acquisition process, automate quarterly financial forecasting, and apply natural language processing to guide technical communication and match employees with new projects.



SPEED READ

Storing and querying data is not enough to succeed in today's complex mission environments. Organizations must have the technology, processes, people, and algorithms to turn data into insights and actions.

Booz Allen reached an inflection point for its own data transformation and set out to build a data lakehouse—designed for builders, analysts, and leaders—to support the firm's entire data-to-decision lifecycle across critical business functions, such as managing our people, finances, operations, and portfolio of work.

As we develop, test, and refine new ways of managing data and new analytical use cases, we get to translate what we learn to help clients accelerate their own critical journeys from data to insights to action.

The Case for Change

Horacio Rozanski, *President and Chief Executive Officer*

At Booz Allen, we embrace challenges. For more than 100 years, business, government and military leaders have turned to Booz Allen to solve their most complex problems. From doubling the size of the U.S. Navy fleet during World War II to contributing to the design of the Hubble Space Telescope to accelerating the development and distribution of the COVID-19 vaccine as part of Operation Warp Speed, we have brought mission expertise and technical prowess to bear during some of our nation's most defining moments. Building on this heritage of transformation through innovation, we continue to address the greatest challenges of today—and tomorrow.

We are currently living through one of the most turbulent and uncertain times in recent history. We are coming off the heels of a global pandemic that strained our healthcare systems. Climate change endangers our critical infrastructure and natural resources. Adversaries are finding new and sophisticated ways to unleash cyber-attacks that threaten national security. And the geopolitical landscape is becoming increasingly volatile. These disruptions are happening at an accelerated rate, causing anxiety, instability, and conflict. As a result, the U.S. Government is forced to address a new set of dynamic challenges and reassess mitigation strategies to maintain its competitive advantage and global leadership position.

Against this backdrop, the digital revolution that has already transformed the private sector is fully underway in the public sector. Defense, intelligence, and civilian missions must transform and become more digital, and the Federal Government is relying on industry to help them reach that destination faster. Historical innovation roles and investment boundaries have shifted. Today, private sector investment in advanced technology development surpasses that of the U.S. Government. From small startups to the largest corporations, the cycle of innovation is shrinking from decades to months, and new technologies are being introduced at a staggering pace. The need for scouting and integrating the best technologies to create secure, connected, resilient digital solutions has never been greater. And while corporations everywhere struggle to adapt, the challenge is even greater in government—where the scale and scope of the missions dwarf the requirements of private enterprise.

Reimagining the Future

This shift in innovation and investment is another defining moment, creating an extraordinary opportunity to reimagine how industry will address complex mission needs. Our industry must meet this moment or risk becoming irrelevant. No one company will be able to do this alone—success will rely on our ability to build enduring partnerships into an innovation ecosystem that can move from idea to scaled mission impact at breakneck speed.

At Booz Allen, we aspire to be a leader transforming our industry to better serve our government clients. To get ready, earlier this year, we launched our VoLT (Velocity, Leadership, and Technology) strategy. Through VoLT, we are accelerating the innovation and integration of highly technical solutions in partnership with the very best. We bring the best thinking, technology, and people together to solve some of the government's most critical challenges. We know the value of building partnerships and creating opportunities for organizations with the right technology and vision to have a seat at the table, regardless of their size. By embracing the collective ingenuity inherent in an innovation network, we are leveraging the best of AI, cybersecurity, 5G, quantum, and other technologies to power the U.S. Government's digital revolution.

A Pivotal Moment

I mentioned earlier that we are living in one of the most turbulent and uncertain times in recent history. Everything seems to be changing all at once. In this turbulence, I also see opportunity—for Booz Allen to work with the best companies in our country to create a better future together. This is about the power of technology, of course, and it is also about the power of people, of purpose, and of passion.

Our country is at a pivotal moment. We have an opportunity to inspire our existing teams and to bring a new generation into this cause. We must take everything we have learned and use it to shape the digital future of the Federal Government. Our success will be determined by how well we help our clients to adapt and lead in a changing world. And to do so, we must first change ourselves—to become faster, more agile, and more innovative. The digital future will increase competition, opportunity, and reward—but only for those ready to adapt and meet it.

The topics explored in these pages demonstrate the measure of this innovation already unfolding in the federal sector—proof that change is already underway, and the future is bright. Building an integrated ecosystem will not be easy, but we at Booz Allen are rising to the challenge, and I look forward to embarking on this journey with you.



In this age
of great
uncertainty,
there is
extraordinary
opportunity
to reimagine
how industry
will address
complex mission
needs. Our
industry must
meet this moment.

REFERENCES

6: The Quantum Cyber Threat

“NIST Announces First Four Quantum-Resistant Cryptographic Algorithms,” NIST, July 05, 2022, <https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms>.

9: Enterprise DevSecOps in Action

“F-35 Joint Strike Fighter: Cost Growth and Schedule Delays Continue,” U.S. Government Accountability Office, April 27, 2022, <https://www.gao.gov/products/gao-22-105943#:~:text=DOD%20plans%20to%20acquire%20%2C470,and%20foreign%20military%20sales%20customers>.

David Vergun, “DOD Laser-Focused on Driving Down Costs of F-35, General Says,” DOD News, U.S. Department of Defense, May 14, 2021, <https://www.defense.gov/News/News-Stories/Article/Article/2618253/dod-laser-focused-on-driving-down-costs-of-f-35-general-says/>.

12: Achieving Engineering Excellence in the Race for Talent

Aimee George Leary and Robin Erickson, *Building an Innovative Model for Growing and Inspiring Tech Talent*, The Conference Board, July 28, 2022, <https://www.conference-board.org/topics/hr-transformation/building-innovative-talent-model>.

“Job Postings Dashboard,” Emsi, accessed August 26, 2022, <https://www.economicmodeling.com/job-posting-dashboard/>.

“Technology Transformation Services,” U.S. General Services Administration, last modified February 25, 2022, <https://www.gsa.gov/about-us/organization/federal-acquisition-service/technology-transformation-services>.

United States Digital Corps, accessed August 26, 2022, <https://digitalcorps.gsa.gov/>.

18: Traversing the Valley of Death: A Discussion with Founders

Patrick Ward, “Is It True That 90% of Startups Fail?,” NanoGlobals, Jun 29, 2021, <https://nanoglobals.com/startup-failure-rate-myths-origin/>.

22: Trust: An Imperative for Our Collective Future

Differential Privacy for Census Data Explained, National Conference of State Legislatures, November 10, 2021, <https://www.ncsl.org/research/redistricting/differential-privacy-for-census-data-explained.aspx#:~:text=Differential%20privacy%20will%20mean%20that,used%20to%20protect%20small%20populations>.

Health and Location 5 Data Protection Act of 2022, S. 4408, 117th Cong. (2022), <https://www.warren.senate.gov/imo/media/doc/Health%20and%20Location%20Data%20Protection%20Act.pdf>.

Kyley McGeeney et al., *2020 Census Barriers, Attitudes, and Motivators Study Survey Report a New Design for the 21st Century*, U.S. Census Bureau, January 24, 2019, <https://www2.census.gov/programs-surveys/decennial/2020/program-management/final-analysis-reports/2020-report-cbams-study-survey.pdf>.

“Experts Doubt Ethical AI Design Will Be Broadly Adopted as the Norm Within the Next Decade,” Pew Research Center, Washington, D.C. (June 16, 2021) <https://www.pewresearch.org/internet/2021/06/16/experts-doubt-ethical-ai-design-will-be-broadly-adopted-as-the-norm-within-the-next-decade/>.

“Trust and Distrust in America: 4. Americans’ Solutions for Trust-Related Problems,” Pew Research Center, Washington, D.C. (July 22, 2019) <https://www.pewresearch.org/politics/2019/07/22/americans-solutions-for-trust-related-problems/>.

“Identity Theft Resource Center’s 2021 Annual Data Breach Report Sets New Record for Number of Compromises,” Identity Theft Resource Center (January 2022) <https://www.idtheftcenter.org/post/identity-theft-resource-center-2021-annual-data-breach-report-sets-new-record-for-number-of-compromises/>.

Megan Brennan and Helen Stubbs, *Americans Are Critical of Technology Companies Despite Changes to Misinformation Policies*, Knight Foundation, October 21, 2020, <https://knightfoundation.org/articles/americans-are-critical-of-technology-companies-despite-changes-to-misinformation-policies/>.

“Public Trust in Government: 1958-2022,” Pew Research Center, Washington, D.C. (June 6, 2022) <https://www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022/>.

28: A New Paradigm for National Security Innovation?

Alex Rossino, *Department of Defense 5G Investment in Fiscal 2022*, GovWin, December 8, 2021, <https://iq.govwin.com/neo/marketAnalysis/view/Department-of-Defense-5G-Investment-in-Fiscal-2022/6297?researchTypeId=1&researchMarket=>.

Christopher Darby, “The Unseen Conflict: Strategic Technology Competition,” testimony to the House Subcommittee on Strategic Technologies and Advanced Research, February 12, 2020, <https://www.congress.gov/116/meeting/house/110489/witnesses/HHRG-116-IG10-Bio-DarbyC-20200212.pdf>.

DARPA Contracts Management Office, *Other Transactions Authority*, March 15, 2019, https://acquisitioninnovation.darpa.mil/docs/Training/Other%20Transactions%20Comprehensive_May%202022.pptx.

“David W. McKeown to senior Pentagon leadership, defense agency and DoD field activity directors,” February 3, 2022, Office of the Secretary of Defense, <https://media.defense.gov/2022/Feb/03/2002932852/-1/-1/0/CONTINUOUS-AUTHORIZATION-TO-OPERATE.PDF>.

James Andrew Lewis, *National Security and the Innovation Ecosystem*, Center for Strategic and International Studies, October 1, 2021, <https://www.csis.org/analysis/national-security-and-innovation-ecosystem>.

Rhys McCormick, *Department of Defense Other Transaction Authority Trends: A New R&D Funding Paradigm?*, Center for Strategic and International Studies, December 8, 2020, <https://www.csis.org/analysis/department-defense-other-transaction-authority-trends-new-rd-funding-paradigm>.

34: Achieving Decision Advantage by 2025

Bryan Clark, Dan Patt, and Timothy A. Walton, “Implementing Decision-Centric Warfare: Elevating Command and Control to Gain an Optionality Advantage,” Hudson Institute, March 2021, https://s3.amazonaws.com/media.hudson.org/Clark%20Patt%20Walton_Implementing%20Decision-Centric%20Warfare%20-%20Elevating%20Command%20and%20Control%20to%20Gain%20an%20Optionality%20Advantage.pdf.

Colin Clark, “Gen. Hyten on the New American Way of War: All-Domain Operations,” Breaking Defense, February 18, 2020, <https://breakingdefense.com/2020/02/gen-hyten-on-the-new-american-way-of-war-all-domain-operations/>.

Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People’s Liberation Army Seeks to Wage Modern Warfare*, Santa Monica, CA: RAND Corporation, 2018, https://www.rand.org/pubs/research_reports/RR1708.html.

38: Solving Global-Scale Challenges through a Data Ecosystem

Jackson Barnett, “DoD Platform Made for Financial Data Finds Battlefield Use,” FedScoop, January 5, 2022, <https://www.fedscoop.com/advana-use-in-jadc2-experiment/>.

“Top Technology Trends in Government for 2022,” Gartner Research, n.d., <https://www.gartner.com/en/doc/760926-top-technology-trends-in-government-for-2022>.

“U.S. Customs and Border Protection’s Office of Information Technology’s Border 5/Migration 5 (B5M5) CIO Tech Forum,” U.S. Customs and Border Protection, June 2, 2022, <https://www.cbp.gov/newsroom/spotlights/us-cbp-oit-border5-migration5-cio-tech-forum>.

42: Digital Twins for Modern Government

“Digital Twin for Earth Observations (EO-DT) Using Artificial Intelligence,” National Environmental Satellite Data and Information Service, accessed August 26, 2022, <https://www.nesdis.noaa.gov/events/digital-twin-earth-observations-eo-dt-using-artificial-intelligence>.

Digital Twin Market: Global Opportunity and Trend Analysis, 2020–2035, Research and Markets, May 2020, https://www.researchandmarkets.com/reports/5023844/digital-twin-market-global-opportunity-and-trend?utm_source=dynamic&utm_medium=BW&utm_code=p8khql&utm_campaign=1387606+-+Outlook+into+the+Worldwide+Digital+Twin+Industry+to+2035+-+Featuring+Ansys%2c+Autodesk+%26+Aveva+Among+Other&utm_exec=jamu273bwd.

Jaqueline Feldscher, “Space Force Buys a Digital Twin of Orbital Space,” Defense One, March 31, 2022, <https://www.defenseone.com/business/2022/03/space-force-buys-digital-twin-orbital-space/363858/>.

Sara Schonhardt, “Digital Earth ‘Twins’ Could Help Address Climate Change,” Scientific American, April 8, 2022, <https://www.scientificamerican.com/article/digital-earth-twins-could-help-address-climate-change/>.

Sid-Ahmed Boukabara et al., “Outlook for Exploiting Artificial Intelligence in the Earth and Environmental Sciences,” *Bulletin of the American Meteorological Society* 102, no. 5: E1016–E1032, <https://journals.ametsoc.org/view/journals/bams/102/5/BAMS-D-20-0031.1.xml>.

46: Putting Zero Trust into Practice

Exec. Order No. 14028, Improving the Nation’s Cybersecurity, May 12, 2021, <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>.

M-22-09, Zero Trust Strategy, memorandum, Executive Office of the President, January 26, 2022, <https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf>.

M-22-16, memorandum, Executive Office of the President, July 22, 2022, <https://www.whitehouse.gov/wp-content/uploads/2022/07/M-22-16.pdf>.

“New Technology Modernization Fund Investments to Boost Network Security for Critical Services,” U.S. General Services Administration, June 21, 2022, <https://www.gsa.gov/about-us/newsroom/news-releases/new-technology-modernization-fund-investments-to-boost-network-security-for-critical-services-06212022>.

Patrick Gorman et al., “Building Mission-Driven 5G Security with Zero Trust,” Booz Allen Hamilton, accessed August 26, 2022, <https://www.boozallen.com/insights/cyber/building-mission-driven-5g-security-with-zero-trust.html>.

49: Metaverse and Web3: Hype vs. Reality

Hackl, Cathy, Dirk Lueth, and Tommaso Di Bartolo, *Navigating the Metaverse: A Guide to Limitless Possibilities in a Web 3.0 World* (Hoboken, NJ: Wiley, 2022).

Knight, Will, “The US Military Is Building Its Own Metaverse,” *Wired*, May 17, 2022, <https://www.wired.com/story/military-metaverse/>. Labonte, M. (2022). *Central Bank Digital Currencies: Policy Issues*. Congressional Research Service.

Labonte, Marc, and Rebecca M. Nelson, “Central Bank Digital Currencies: Policy Issues,” Congressional Research Service, updated February 7, 2021, <https://crsreports.congress.gov/product/pdf/R/R46850>.

McArdle, Jennifer, and Caitlin Dohrman, “The Full Potential of a Military Metaverse,” *War on the Rocks*, February 18, 2022, <https://warontherocks.com/2022/02/the-full-potential-of-a-military-metaverse/>.

“Microsoft to Acquire Activision Blizzard to Bring the Joy and Community of Gaming to Everyone, Across Every Device,” Microsoft News Center, Microsoft, January 18, 2022, <https://news.microsoft.com/2022/01/18/microsoft-to-acquire-activision-blizzard-to-bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/>.

Balaban, Mariusz Adam, “Privacy Concerns with Big Data Analytics: US DoD/Army Landscape,” Interservice/Industry Training, Simulation, and Education Conference (IIITSEC), Conference (IIITSEC), Orlando, FL, December 2019, https://www.researchgate.net/publication/338421462_Privacy_Concerns_with_Big_Data_Analytics_US_DoDArmy_Landscape.

“Central Bank Digital Currencies: Foundational Principles and Core Features,” Research and Publications, BIS, October 9, 2020, <https://www.bis.org/publ/othp33.htm>.

Gatto, James G., Yasamin Parsafar, Townsend L. Bourne, “Blockchain and Metaverse Legal Issues for the Government and Government Contractors,” *National Law Review*, May 23, 2022, <https://www.natlawreview.com/article/blockchain-and-metaverse-legal-issues-government-and-government-contractors>.

Stephenson, Neal, *Snow Crash* (New York: Bantam Books, 1992).

“Central Bank Digital Currency Tracker,” Atlantic Council, last modified 2022, https://www.atlanticcouncil.org/cbdctracker/?mkt_tok=NjU5LVdaWC0wNzUAAAF-ahMwPvT7taShD6dOUCyZElHxdkHTeni_SU_V_6KzrLq9AcU4KdcDwVw4sBwD80qmOzYEGtXV-WGy5ObQ8qw.

Underwood, Kimberbly, “Introducing the SpaceVerse: The U.S. Space Force Is Preparing to Create a Converged Digital and Physical Environment,” *Signal*, June 9, 2022, <https://www.afcea.org/signal-media/introducing-spaceverse>.

Zenou, Theo, “A Novel Predicted the Metaverse (and Hyperinflation) 30 Years Ago,” *Washington Post*, June 30, 2022, <https://www.washingtonpost.com/history/2022/06/30/snow-crash-neal-stephenson-metaverse/>.

Zhu, L. (2022). *The Metaverse: Concepts and Issues for Congress*. Congressional Research Service.

54: Invest, Activate, and Scale

Rhys McCormick, *Department of Defense Other Transaction Authority Trends: A New R&D Funding Paradigm?*, Center for Strategic and International Studies, December 8, 2020, <https://www.csis.org/analysis/department-defense-other-transaction-authority-trends-new-rd-funding-paradigm>.

“The Final Report,” The National Security Commission on Artificial Intelligence, March 1, 2021, <https://www.nscai.gov/2021-final-report/>.

BOOZ ALLEN AUTHOR INFORMATION

Special thanks to all of the leaders from within Booz Allen who contributed to this collection and provided technical and mission expertise along the way.

Josh Boyd Boyd_Joshua@bah.com	Jordan Kenyon Kenyon_Jordan@bah.com	Julie McPherson McPherson_Julie@bah.com	Munjeet Singh Singh_Munjeet@bah.com
Paul Chi Chi_Paul@bah.com	Matthew Langevin Langevin_Matthew@bah.com	Beau Oliver Oliver_Beau@bah.com	Matthew Snyder Snyder_Matthew@bah.com
Jennifer Congdon Congdon_Jennifer@bah.com	Ki Lee Lee_Ki@bah.com	Susan Penfield Penfield_Susan@bah.com	Ramesh Soni Soni_Ramesh@bah.com
Colin Corridon Corridon_Colin@bah.com	Trishna Lovley Lovley_Trishna@bah.com	Helen Phillips Phillips_Helen@bah.com	Brad Stone Stone_Brad@bah.com
Frank DiGiammarino DiGiammarino_Frank@bah.com	Michael Lundberg Lundberg_Michael@bah.com	Horacio Rozanski Rozanski_Horacio@bah.com	Josh Strosnider Strosnider_Joshua@bah.com
JD Dulny Dulny_JD@bah.com	Theresa Lynch Lynch_Theresa@bah.com	Kelly Rozumalski Rozumalski_Kelly@bah.com	Prachi Sukhatankar Sukhatankar_Prachi@bah.com
Steve Escaravage Escaravage_Steven@bah.com	Brian MacCarthy Maccarthy_Brian2@bah.com	Dylan Rudy Rudy_Dylan@bah.com	Matt Tarascio Tarascio_Matthew@bah.com
Kathleen Featheringham Featheringham_K@bah.com	Elliot Mandel Mandel_Elliot@bah.com	Haluk Saker Saker_Haluk@bah.com	Steven Terrana Terrana_Steven@bah.com
James Gadea Gadea_James@bah.com	Ramy Mansour Mansour_Ramy@bah.com	Sahil Sanghvi Sanghvi_Sahil@bah.com	Michael Tsyvine Tsyvine_Michael@bah.com
Aimee George Leary George_Aimee@bah.com	Sandra Marshall Marshall_Sandra@bah.com	Marisa Santisi Santisi_Marisa@bah.com	Imran Umar Umar_Imran@bah.com
Chris Hample Hample_Christopher@bah.com	Dan McConnell McConnell_Dan@bah.com	Saurin Shah Shah_Saurin@bah.com	
Jennifer Jenkins Jenkins_Jennifer@bah.com	Adam McCormick McCormick_Adam@bah.com	Vincent Simpson Simpson_Vincent@bah.com	

VELOCITY, A BOOZ ALLEN PUBLICATION

CHIEF TECHNOLOGY OFFICER

Susan Penfield

OFFICE OF THE CTO Frank DiGiammarino Steve Escaravage Julie McPherson Munjeet Singh Brad Stone	EDITORIAL Senior Editors: Abby Vaughan and Sahil Sanghvi Managing Editor: Elana Akman Editorial Consultant: Emily Primeaux, Dragonfly Editorial	DESIGN Art Director: Chris Walker Designers: Brody Rose and David Everett
MARKETING AND COMMUNICATIONS Head of Brand, Marketing, & Media: Sandhya Davis Media Director: Jessica Klenk		
For media inquiries please contact Amanda Allison: Allison_Amanda@bah.com		
COMMUNICATIONS AND DIGITAL Special acknowledgments to individuals across content, digital, creative, brand, media, legal, website, accessibility, and project management for their support of this project.		
NOTABLE CONTRIBUTIONS Jags Kandasamy, Chief Executive Officer, Latent AI “Traversing the Valley of Death: A Discussion with Founders”18 Sek Chai, Chief Technology Officer, Latent AI “Traversing the Valley of Death: A Discussion with Founders”18 Ryan Wright, Professor, University of Virginia “Trust: An Imperative for Our Collective Future”22 Dave Rhodes, Senior Vice President, Unity “Digital Twins for Modern Government”42 Bilal Zuberi, General Partner, Lux Capital “Invest, Activate, and Scale: Emerging Investment Models to Accelerate Mission Execution”54		

ABOUT BOOZ ALLEN

For more than 100 years, military, government, and business leaders have turned to Booz Allen to solve their most complex problems. As a consulting firm with experts in analytics, digital solutions, engineering, and cyber, we help organizations transform. We are a key partner on some of the most innovative programs for governments worldwide and trusted by their most sensitive agencies. We work shoulder-to-shoulder with clients, using a mission-first approach to choose the right strategy and technology to help them realize their vision.

To learn more, visit www.boozallen.com.

*Booz Allen team at the U.S. Space & Rocket Center
(Huntsville, AL)*



The background of the entire page is a dark blue field filled with intricate, glowing patterns. These patterns consist of numerous thin, curved lines that swirl and loop around each other, creating a sense of dynamic movement and complexity. Interspersed among these lines are small, bright blue dots, some of which appear to be part of the swirling paths, while others are isolated. The overall effect is reminiscent of a high-tech or digital environment, possibly representing data flow, network connections, or the intricate nature of modern technology.

Booz Allen®

Velocity, a Booz Allen publication, studies the complex issues that are emerging for mission and technology leaders on the front lines of government innovation.

BoozAllen.com/Velocity