

Deloitte.
Insights



Information at the edge

A space architecture for a future battle network

About the authors

Justin Reed | jtreed@deloitte.com

Justin Reed is a partner with Deloitte & Touche LLP specializing in helping clients improve their enterprise business operations' processes, data, and systems. He has more than 25 years of federal and aerospace and defense experience with enterprise financial operations, enterprise resource planning, asset valuation, cost accounting, acquisition processes, and logistical systems. His clients over the years have included the US Air Force, Navy, Army, Office of Secretary of Defense, NASA, and other federal agencies, as well as major defense system integrators, manufacturers, and government contractors.

Adam Routh | adrouth@deloitte.com

Adam Routh is a research manager with the Deloitte Center for Government Insights and a PhD student in the Defence Studies Department at King's College London. His research areas include emerging technologies, defense, and security, with a focus on space policy. Routh previously worked for the Defense Program at the Center for a New American Security (CNAS). Prior to CNAS, he worked in the private sector, where he facilitated training for Department of Defense components. He also served as a team leader with the US Army's 75th Ranger Regiment.

Joe Mariani | jmariansi@deloitte.com

Joe Mariani leads research into defense, national security, and justice for Deloitte's Center for Government Insights. His research focuses on innovation and technology adoption by both commercial businesses and National Security organizations. Mariani's previous experience includes work as a consultant to the defense and intelligence industries, high school science teacher, and Marine Corps intelligence officer.

Contents

Warfare has changed	2
The requirements for a future battle network	4
Poor resilience, lower responsiveness, outdated ways of operating	6
Solving for shortcomings	8
Making the vision a reality	11
Making the changes stick	14
Endnotes	15

Warfare has changed

DURING THE PERSIAN Gulf War in 1990, the US military linked data with combat operations like never before. Through satellites, stealth aircraft such as the F-117 Nighthawk, and precision-guided munitions, US military commanders were able to coordinate complex air campaigns against Iraqi military command centers, leaving the latter largely without critical early warning and communications just hours after the start of combat operations.¹ With much of Iraq’s military blind to the situation, the US military was able to utilize advanced intelligence, communication, navigation systems, and weapons to jointly coordinate a decisive ground campaign.

What the US military had done was leverage information better than its adversary. It did this by having a superior battle network capable of

collecting, analyzing, fusing, and acting on information more effectively—and by denying Iraq the use of its own battle network. Overall, the United States was able to gain a better understanding of the operational environment and more effectively delegate and realize US leaders’ battlefield intent.

Today, technological and conceptual developments have now put militaries on the cusp of yet another breakthrough in the pursuit to leverage information better than their adversaries. Often called “convergence,” this breakthrough seeks to make information from every sensor available to every shooter. Importantly, convergence for modern military is expected to require use of electromagnetic spectrum (EMS) for communication, targeting, navigation, situational awareness, and early warning.²



Achieving convergence for the US military would depend on possessing a superior ability to maneuver through EMS—while denying that freedom to the enemy—to guarantee the flow of information despite distance and enemy attacks. Ultimately, the United States needs an entirely new battle network—one that masters the use of EMS to offer global reach; is highly resilient in the face of enemy attack; and is responsive to the fast-paced, high-tech nature of future near-peer warfare. In

turn, to achieve this reach, resilience, and responsiveness, the United States will likely need to rely, in large part, on the space segment of its battle network. However, today's space segment—comprising spacecraft, ground stations, and the data links connecting them—seems to fall short of US needs; to develop the right space segment, the US military may need to develop, train, and operate differently.

WHAT MAKES A BATTLE NETWORK VALUABLE?

A battle network allows commanders to understand the battlespace, develop more informed conclusions, and communicate their intent to the force. Possessing a superior battle network can provide a military with the ability to take rapid, decisive action.

Data fuels the battle network, which is why data has become the currency of warfare.³ These networks now typically rely on:

- Advanced sensor suites spread across air, land, sea, space, and cyberspace
- Novel data analysis using artificial intelligence (AI) and automation
- Secure digital networking
- Communications and precision, navigation, and timing (i.e., GPS)
- Command and control (C2)⁴

Each individual network node, be it a satellite, ground station, plane, or C2 hub, can be critical to the network's success.

The requirements for a future battle network

AS THE UNITED States moves toward a future vision of “every sensor to every shooter,” its battle network should be **global**, **resilient**, and **responsive** if it is going to deliver war fighters the edge they need. Space affords these qualities more efficiently and effectively than other domains.

Global, resilient, responsive

In future high-tech warfare, it's likely that the United States will have to operate **globally**. Separated by oceans on both sides, the United States is expected to continue to need to collect, analyze, fuse, and act on information around the world—whether it's providing critical communication to ships at sea or navigation data to planes en route to resupply troops. Global operations are dependent on using EMS.

An essential element of success in warfare is ensuring a battle network can share necessary information around the world without interruption. For this to happen, the network must be **resilient** to an intense barrage from the enemy through a host of threats, including physical threats such as kinetic attacks, electronic warfare (EW) attacks such as signal interference, and cyberattacks.⁵

Though a battle network's resilience is important, it means little if the network is not responsive. This is because a key characteristic of warfare in a digital age is just how dependent modern militaries, and specifically weapon systems, are on data.⁶ But more than raw or unrefined data, weapon systems and troops need refined data that is easy to act upon. Delivering the right data means quickly collecting, analyzing, fusing, and sharing information. Battle networks must be able to expedite the flow of useful information to enable troops to make better and faster decisions.

An essential element of success in warfare is ensuring a battle network can share necessary information around the world without interruption.

Because warfare occurs in the air, land, sea, cyber, and space domains, achieving global reach, resilience, and responsiveness requires a complex battle network architecture of sensors, data processing, and communication spread across each domain. Though space is just one of many operational environments a battle network must operate in and through, it is becoming increasingly important for the US battle network.

Commercially enabled

Earth's orbit provides an ideal place for collecting and sharing information around the globe. So, ever since the US Air Force launched the first communications satellite in 1958, creating a battle network with the ideal reach, resilience, and responsiveness has all but required the use of space. Similarly, as commercial companies began requiring large amounts of data delivered responsively all around the globe, space systems again provided ideal solutions. Commercial space capabilities eventually became ubiquitous enough that they began supplementing military assets in peace and wartime, allowing the US military to more effectively operate globally.

Now, new space technologies—such as small satellites, rapid launch, internet from space, novel earth imagery, and AI—and lower launch costs are all essential elements of the emerging commercial space sector and future battle networks. Given the overlap between commercial and battle network requirements, commercial technology can supplement the military space segment in interesting ways. For instance, unlike a fighter

aircraft or an aircraft carrier, which are purpose-built for the military, many of the elements needed in the space segment of a battle network could be commercial during peacetime but serve military purposes during periods of conflict. Just as the United States used commercial imagery and weather forecasting to enable combat operations during the Gulf War, commercial satellite communication, imagery, data processing, and other capabilities critical to the future battle network could be utilized as a service when the US military needs them. The military will likely require some military-specific space segment assets, but commercial capabilities can offer a highly efficient and effective way of augmenting military systems to provide a future battle network with the ideal reach, resilience, and responsiveness.

Space offers an unparalleled ability to enhance a battle network, which is why the US military has been investing in space systems. However, despite the commercial capabilities being developed or the sophisticated and expensive capabilities the US military has in orbit today, the current military space architecture appears to fall short of what is needed for future warfare.

Poor resilience, lower responsiveness, outdated ways of operating

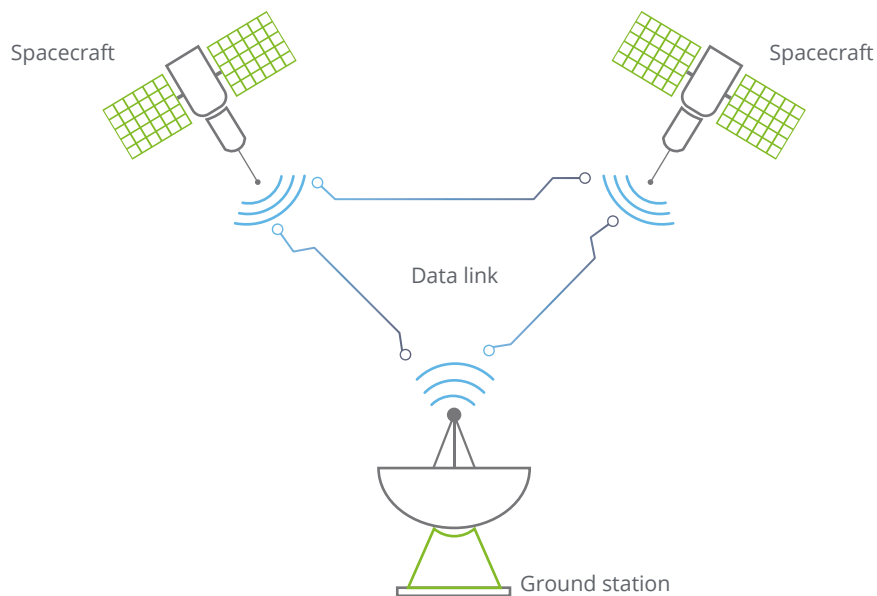
THE UNITED STATES possesses an impressive set of satellites, ground segments, and supporting networks that provide its battle network with formidable capability. However, many of these assets are aging, vulnerable, and less responsive than what future high-tech warfare is expected to necessitate. If the US military wants its battle network to meet future demands, it would likely need to overcome deficiencies in resilience and responsiveness, and develop the right concepts

of operation to quickly provide military forces spread around the world with the right information.

Over the last several decades, the United States has invested billions of dollars in very complex and capable satellites and associated infrastructure. These very large, very expensive satellites provide much of the functionality the US military requires, but they may not be fit for **resiliency** in future fights. In fact, they've been described as "large, big,

FIGURE 1

The space segment comprises the spacecraft, ground stations, and the data links connecting them



Source: Deloitte analysis.

fat, juicy targets.”⁷ This is due, in part, to the limited number of satellites supporting the US battle network. With roughly 208 operational military satellites, as compared with the thousands likely to be set up by new commercial constellations, a US adversary would be able to destroy or disrupt the US space segment by targeting only a few satellites.⁸

Fewer assets can make the entire architecture less **responsive** as well. With relatively few space assets to serve the entire Joint Force, demand for battle network resources can often exceed supply, hindering responsiveness of the battle network; and since the assets are so complex and expensive, they cannot be quickly upgraded or replaced. If the goal is to connect every sensor to every shooter, there will likely need to be more space assets providing sensors, communication, and other critical battle network functionality to achieve the proper level of responsiveness for a large force.

Developing the space segment for a future battle network could also require a new approach to how the US military thinks about **operating** in and through space. Today, for example, overclassification of many space activities and systems can make it difficult for the US military to work effectively with allies or the commercial sector.⁹ In addition to overcoming the capabilities of a high-tech adversary, future warfare could require greater interoperability with allies and partners, both of which may require new strategies and ways of operating. While the U.S. Space Force’s recent *Space Capstone Publication* was designed as a foundational doctrine, additional tactical concepts of operation for using a future space segment as part of a battle network are likely necessary, such as how gaining an advantage through EMS can affect the use of space systems.¹⁰



Solving for shortcomings

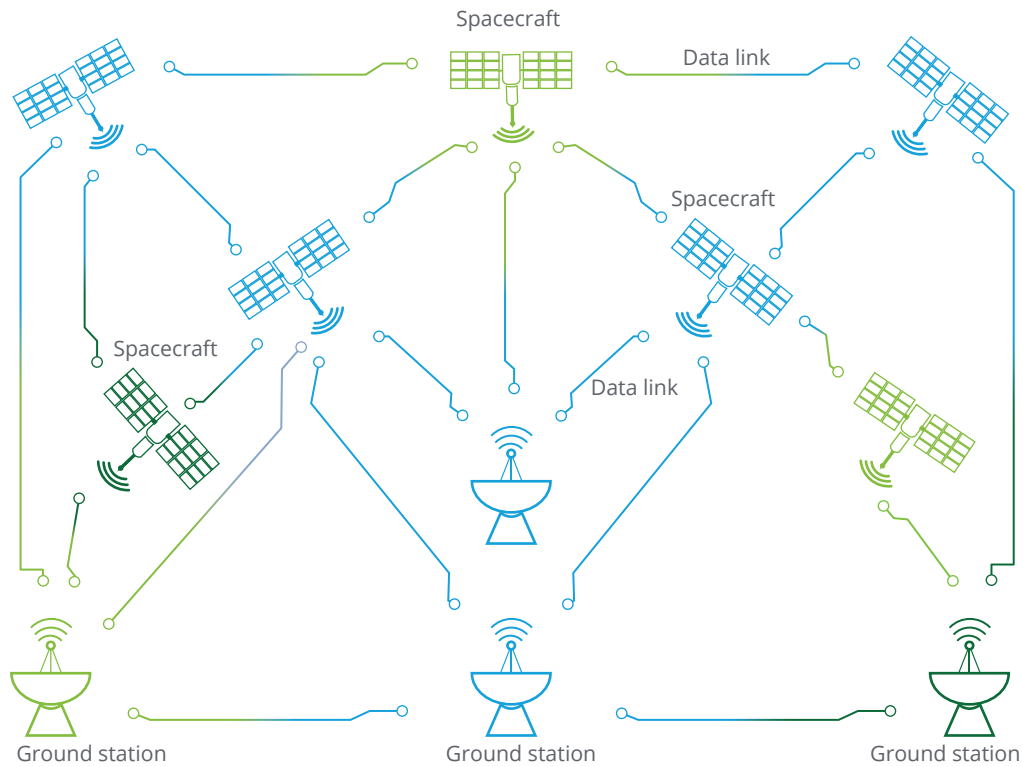
HOW WOULD A future space architecture need to look in order to be global, responsive, and resilient? Space almost innately provides global reach; satellites orbit around the Earth after all. Resilience and

responsiveness are not qualities that come naturally to space, however. They must be purposefully developed based on the needs of the force and the character of warfare (figure 2).

FIGURE 2

An example of a multinodal, interoperable (commercial, US military, and allied) space segment

■ Commercial ■ US military ■ Allied



Source: Deloitte analysis.

Building in resilience

Each space segment node—spacecraft, ground station, or data link—presents an opportunity for an adversary to target the US battle network. A resilient space segment must therefore be defensible against kinetic, EW, and cyberattacks, while avoiding single points of failure. Given the number of ways the space segment can be attacked, resilience ultimately comes down to quantity, variety, and dispersal of nodes and communication channels.

Like a school of fish overwhelming a predator, presenting an adversary with too many targets of different types and in different locations can make battle network disruption more difficult. For the space segment, this translates to placing satellites with different purposes and capabilities in different orbits—from low Earth orbit to geosynchronous orbit. Similarly, because satellites are wholly dependent on over-the-air communication, each satellite should have the ability to intuitively find available communication pathways within the network to guarantee the flow of data despite crowded frequencies or enemy EW attacks. A satellite might leverage various radio frequencies or even reroute data through optical intersatellite links to find a clear channel to communicate. Ground stations would also need to be dispersed geographically with the ability to effectively navigate any challenges posed by a congested or contested EMS. Other factors include diversifying software and hardware so that they aren't all susceptible to the same means of attack, and interoperability in connecting to and sharing information across each asset so that each node can operate with another regardless of type or configuration.

Resilience also demands being able to replenish or repurpose various space segment nodes quickly, through launching new satellites, deploying new ground stations, or retasking existing assets.¹¹ These assets may come from existing military

stockpiles, commercial providers, or allies. Newly deployed ground segments or spacecraft should be able to “plug and play” with older systems regardless of whether they are commercial or allies.

Given the number of ways the space segment can be attacked, resilience ultimately comes down to quantity, variety, and dispersal of nodes and communication channels.

Building in responsiveness

In a digital age, information flows quickly, and, on the battlefield, when networks fail to provide information when it's needed, the consequences can be dire. Building responsiveness into a space segment thus requires it to handle raw data effectively and quickly, from collection, to analysis, fusion, dissemination, and action. Therefore, the space segment should also have an intuitive network management system that can help organize and control the highly complex number of nodes, data, and users. Finally, a responsive space segment should have automated defense measures that allow it to respond at speeds characteristic of high-tech warfare.

With every sensor connected to every shooter, a future battle network could have an incredibly large number of nodes collecting and sharing data. If not prioritized properly, the battle network could become overwhelmed with mountains of unrefined data flowing incoherently all at once. To avoid clogging the network, data should be processed closer to the source—rather than stored at the source or passed through it—to ensure only refined,

actionable data is occupying the network while a network traffic prioritization system gives important data precedence over unimportant data.¹² The management system would also need to direct how the data is transmitted throughout the network. This requires an understanding of how existing communication pathways, such as wireless or physical data connections, are being used or attacked, and what the shortest route between the source and destination is.

An architecture management system can also help by making it easy for human operators to understand where assets are, if they are functional, and what they are doing. AI, automation, and smart user interfaces are expected to have a major role to play in managing the architecture.¹³ With AI detecting issues or needs, automation can enable these systems to take necessary action more quickly than if they were controlled by humans, while smart user interfaces keep human operators informed of what's taking place. Responsiveness would also require the management system to play a role defending the network using AI to detect attacks and automation to take defense measures. This defense might also need to cover allies and commercial assets that may not have the same capacity for self-defense as military capabilities.



Making the vision a reality

MANY OF THE capabilities and solutions that would be needed for this new space architecture are very different from how the US military operates today. For example, the capability to rapidly replenish space-based assets contrasts with today's decades-long development of exquisitely crafted, but fewer, space assets. To get the most out of a space segment, the US military would need to change how it works with new space technologies.

Develop differently

With space systems, older procurement practices can often lead to interservice stovepipes, duplicative efforts, and less interoperability.¹⁴ For the future space segment, everything from the technology and partners used to build the space segment to the timeline for deployment, should be reconsidered.

Developing differently requires rethinking how the military creates the complete set of space segment capabilities it requires. Principally, this could mean shifting away from fewer, larger, and more exquisite platforms to smaller, more affordable, but less capable ones. These satellites are less exquisite but produced in large numbers and can provide similar functionality as the larger, expensive platforms the military has traditionally produced. By building the backbone of the space segment with small satellites, the US military can increase satellite numbers and more affordably and routinely upgrade and replace them—all of which improve the resilience and responsiveness of the architecture. This shift would keep pace with the

commercial sector, enabling the military to more easily leverage commercial partners and their capabilities.

For the elements of a space architecture requiring entirely new or military-centric solutions, digital engineering (DE) is another smart development method. It combines data science, advanced analytics, and digital technologies with traditional engineering techniques to improve product design and quality, while lowering costs. In a DE environment, prototype spacecraft can be tested before launch, allowing developers to identify potential issues or failures and make necessary adjustments without the cost or permanence of launching it into orbit.

Smarter development also typically requires partnerships. Alone, the US military would need to design, mature, and integrate a host of new capabilities to develop the right space segment. While the military is certainly capable of doing this alone, it may not be the smartest approach. Partners, whether commercial or allies, often possess a host of useful technology, tools, and solutions that the military should leverage. From offering new talent and alternative points of view to develop cutting-edge solutions, to offering existing capabilities “as a service” to save time and money, partners can help make development faster and more affordable without sacrificing quality. An example of this is the U.S. Space Force's recent choice to leverage a Norwegian satellite as a host for US satellite payloads, saving US\$900 million dollars while deploying needed capabilities much more quickly than if the US had built its own satellite.¹⁵

Finally, developing differently can mean doing so faster. Developing a battle network for future warfare may imply there is plenty of time to design and deploy the network, but that's simply not true. Many threats to the existing US battle network, such as sophisticated EW, cyber, or kinetic attack, exist today.¹⁶ Ensuring the space segment is sufficiently resilient is an immediate need. In addition, the research and engineering needed to improve essential elements of the space segment, such as AI, space domain awareness, and future concepts of operation and training systems, all take time to develop.

Operate differently

Even if the United States comes to possess an incredibly advanced battle network with all the features described previously, a future near-peer adversary will likely possess the means to disrupt or deny the flow of information at least in part. Being able to communicate despite a high-tech enemy attack reflects a resilient battle network, even if that communication is imperfect.

Against a high-tech adversary, the communication windows in even a capable US battle network might become short, sporadic, or planned, affording only a brief opportunity to upload and download data-rich packets of information. Indeed, persistent communication between forward units and command may not be guaranteed—or even wanted, as the signals from sending and receiving information can inform the enemy of friendly positions.¹⁷ In such a scenario, the military forces operating at the battle front should be able to balance their immediate mission needs with working largely autonomously to meet the

commander's intent to a greater degree than what US troops may be used to today. In the future, troops in combat zones could be given the commander's intent, with leaders on the ground deciding how best to realize it.¹⁸ For example, rather than using a communication window to tell troops on the battlefield to hold adjacent high ground, they may be told to deny the enemy's ability to maneuver, and leave it up to the leader on the ground to decide if the high ground is the best way of doing that.

War fighters responsible for managing a future battle network, and the space segment specifically, will need to offer critical information precisely when troops on the ground need it. Like a football quarterback who may maneuver in the pocket or pump fake to confuse the defense before throwing the ball between defenders, military personnel responsible for coordinating satellites, ground segments, and networks will need to coordinate complex communications campaigns to avoid the enemy and deliver information. These activities may include using EW or cyber tools to thwart enemy attacks on the US battle network and create brief windows at the most advantageous time to share data with troops in combat zones. Similar to forces at the front, these choices will have to be made based on the commander's intent, rather than specific orders. A future battlefield is likely to be too dynamic for stagnant decision-making at the operational level.

Adjusting how the US military conducts combat operations, from centralized and highly managed today to more adaptive and autonomous in the future, will be no small task. It can be done, however. Central to changing how the US military fights could be how it trains and develops its troops.

Train differently

Training future military leaders for high-tech combat against near-peer adversaries requires educating them on the capabilities and limitations of their battle network (and also their adversary's battle network). Central to this training should be creating a culture of trust that their counterparts (allies or otherwise) are also doing what they are supposed to do in a highly decentralized operational environment.

Successfully adapting to the high-tech character of warfare would require service members to have a basic understanding of how battle networks function. From human-machine collaboration, EMS, EW, and cyber capabilities, to the different ways information can be shared via various communication nodes, future combat leaders will need to understand how to leverage the battle network at their disposal and how to operate around their adversary's capabilities. This is not to say future leaders will necessarily need to be computer scientists or engineers. Just as today's military leaders have a basic understanding of the capabilities necessary for success in modern warfare, future leaders will likely need a similar

working knowledge of the technology central to their battle network. Without it, they may not be prepared to leverage the information they receive. This education should not stop with officers either; enlisted leaders should also have a working knowledge of their battle network.

Leadership development should also focus on empowering military personnel to make decisions in a decentralized environment, which comes down to trust. The military is a very hierarchical organization, and for good reason. But a future operating environment likely won't allow for a strict command structure requiring multiple levels of command approval before taking action, to which US forces have grown accustomed.¹⁹ This education should extend to commercial and allied partners as well.

Training doesn't stop with people either. Adversaries will seek to exploit vulnerabilities in the US battle network, which could mean AI algorithms as much as physical hardware or humans. Ensuring both the human and AI elements in the battle network are tested, trained, and capable of operating together can be essential.

Making the changes stick

THE MILITARY IS no stranger to developing new technologies and implementing new concepts of operation. Yet, even with that experience, adopting new concepts of operation and technologies is rarely easy: Change can be difficult, especially large-scale change across an organization as big and complex as the US military. Our research has shown that large-scale transformations in any area of government are about much more than new tech; [they typically are about changing human behavior](#).²⁰ But providing the right support to the right people at the right time can help shepherd change through even a large organization.

The “conceive, prove, adopt” framework can highlight which elements of the process require attention, isolation, or cooperation, and when to provide the right support to the right step in the process.²¹

- During the **conceive** phase, incentivize small groups to develop new ideas that may run counter to prevailing concepts of operation. These groups should have direct access to senior leaders while sitting outside of the day-to-day needs of the organization. This can help avoid any roadblocks and allow the organization to continue to address the day-to-day requirements.
- The **prove** phase is designed to allow for testing and evaluation of new ideas while allowing the process to slowly consume the ideas that have proven successful. Starting

small and slowly building in scope and scale, testing should be iterative; with each successful iteration and evolution, more of the process can be modified to support the new concept, including career fields, performance evaluation criteria, among other elements.

- Finally, the **adopt** phase allows new ideas to be scaled to the entire organization at the right time. While the prove phase allows for confidence in the new idea, it does not account for whether the organization will be receptive to enterprise change. Determining when is the right time to implement a new idea across the organization requires a strong culture. Tools such as [organizational network analysis](#) and [culture audits](#) can also help.²²

Change can be difficult, especially large-scale change across an organization as big and complex as the US military.

A future-ready battle network will be an essential element for success in future warfare, but it's also an indication that the character of warfare seems to be changing. Timely attention to a space architecture today can help ensure the US military is driving that change rather than responding to it in the heat of the next conflict.

Endnotes

1. James A. Winnefeld and Dana J. Johnson, *Air power in the Gulf War*, Rand Corporation, January 1, 1994.
2. Congressional Research Service, *Defense primer: Military use of the electromagnetic spectrum*, October 8, 2020.
3. David Goldfein and Jay Raymond, "America's future battle network is key to multidomain defense," *Defense News*, February 27, 2020.
4. Ibid; Octavian Manea, "The role of offset strategies in restoring conventional deterrence," Syracuse University, March 19, 2018.
5. For a thorough analysis of different counter-space capabilities, see Secure World Foundation, *Global counterspace capabilities: An open source assessment*, April 2020.
6. Kenny Grosselin et al., *Space power: Doctrine for space forces*, Space Capstone Publication, U.S. Space Force, June 2020.
7. Sandra Erwin, "STRATCOM chief Hyten, 'I will not support buying big satellites that make juicy targets,'" *SpaceNews*, November 19, 2017.
8. For numbers of active military satellites, see Union of Concerned Scientists, "UCS Satellite database," August 1, 2020; for analysis on how adversaries may destroy the US space segment, see Shawn Brimley et al., *Building the future force*, Center for a New American Security, March 29, 2018.
9. Aaron Mehta, "'Unbelievably ridiculous': Four-star general seeks to clean up Pentagon's classification process," *Defense News*, January 29, 2020; Nathan Strout, "Barrett, Rogers, consider declassifying secretive space programs," *Defense News*, December 7, 2019.
10. Grosselin et al., *Space power: Doctrine for space forces*.
11. U.S. Space Force, "United States Space Force vision for satellite communications (SATCOM)," January 23, 2020.
12. *SpaceNews*, "Blackjack: DARPA's big bet on small satellites," August 4, 2020.
13. Theresa Hitchens, "NRO taps AI for future 'hybrid architecture,'" *Breaking Defense*, August 4, 2020.
14. U.S. Space Force, "United States Space Force vision for satellite communications (SATCOM)."
15. General John W. Raymond (chief of space operations, United States Space Force), video interview with Susanna V. Blume, senior fellow and director of the defense program at the Center for a New American Security, July 24, 2020.
16. Secure World Foundation, *Global counterspace capabilities: An open source assessment*.
17. John Cogbill and Eli Myers, "Decentralizing the fight: Re-imagining the brigade combat team's headquarters," *Modern War Institute*, August 5, 2020.
18. C. Todd Lopez, "Future warfare requires 'disciplined disobedience,' Army chief says," *United States Army*, May 5, 2017.
19. Ibid.

20. William D. Eggers et al., *Behavior-first government transformation: Putting the people before the process*, Deloitte Insights, August 25, 2020.
21. Joe Mariani and Adam Routh, "The Henry and the Helicopter," *MilitaryTimes*, August 30, 2020.
22. Tiffany McDowell and Siri Anderson, *Making the invisible visible: How network analysis can lead to more successful organizational redesigns*, Deloitte Insights, February 27, 2019; John Taft et al., *SOF culture is the mission: Culture is key to special operations' transition to great power competition*, Deloitte Insights, July 15, 2020.

Acknowledgments

The authors would like to thank **Zac Crippin, Jeff Matthews, David Goldstein, and Chris Radcliffe** of Deloitte Consulting LLP for their invaluable insight and research support through the writing of this article.

About the Deloitte Center for Government Insights

The Deloitte Center for Government Insights shares inspiring stories of government innovation, looking at what's behind the adoption of new technologies and management practices. We produce cutting-edge research that guides public officials without burying them in jargon and minutiae, crystalizing essential insights in an easy-to-absorb format. Through research, forums, and immersive workshops, our goal is to provide public officials, policy professionals, and members of the media with fresh insights that advance an understanding of what is possible in government transformation.

Defense, Security & Justice services

Deloitte offers national security consulting and advisory services to clients across the Department of Homeland Security, the Department of Justice, and the intelligence community. From cyber and logistics to data visualization and mission analytics, personnel, and finance, we bring insights from our client experience and research to drive bold and lasting results in the national security and intelligence sector. People, ideas, technology, and outcomes—all designed for impact. Read more about our defense, security, and justice services on [Deloitte.com](https://www.deloitte.com).

Contact us

Our insights can help you take advantage of change. If you're looking for fresh ideas to address your challenges, we should talk.

Industry leadership

Mark Nace

Principal | Deloitte Consulting LLP
+1 703 519 2414 | mnace@deloitte.com

Mark Nace is a principal in Deloitte Consulting LLP's US Government & Public Services (GPS) practice and the lead client service partner (LCSP) for the United States Air Force account.

The Deloitte Center for Government Insights

Adam Routh

Research manager | The Deloitte Center for Government Insights
+1 202 220 2633 | adrouth@deloitte.com

Adam Routh is a research manager with the Deloitte Center for Government Insights and a PhD student in the Defence Studies Department at King's College London. His research focuses on the defense and security.

Joe Mariani

Research manager | The Deloitte Center for Government Insights
+1 312 486 2150 | jmariani@deloitte.com

Joe Mariani is a research manager with the Deloitte Center for Government Insights where his research focuses on innovation and technology adoption by both commercial businesses and National Security organizations.

Deloitte.

Insights

Sign up for Deloitte Insights updates at www.deloitte.com/insights.



Follow @DeloitteInsight

Deloitte Insights contributors

Editorial: Aditi Rao, Sayanika Bordoloi, Nairita Gangopadhyay, and Rupesh Bhat

Creative: Sonya Vasiliieff and Juhi Mehrotra

Promotion: Alexandra Kawecki

Cover artwork: Jaime Austin

About Deloitte Insights

Deloitte Insights publishes original articles, reports and periodicals that provide insights for businesses, the public sector and NGOs. Our goal is to draw upon research and experience from throughout our professional services organization, and that of coauthors in academia and business, to advance the conversation on a broad spectrum of topics of interest to executives and government leaders.

Deloitte Insights is an imprint of Deloitte Development LLC.

About this publication

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or its and their affiliates are, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your finances or your business. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

None of Deloitte Touche Tohmatsu Limited, its member firms, or its and their respective affiliates shall be responsible for any loss whatsoever sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.