Mission Assurance in Joint All-Domain Command and Control

James F. "Frank" Hudson Jr.

Current cybersecurity paradigms are ineffective against most malicious cyber actors. Moreover, the paradigms of old are based on reactive efforts, hardware-based solutions, and paper drills that falsely imply security as the standard. The Department of Defense (DOD) should transition to a more modern framework that implements proactive measures to secure its networks and enables them to operate in a denied, degraded, intermittent, or limited bandwidth (D-DIL) environment, thereby providing mission assurance. The DOD requires a rapid and massive undertaking to revolutionize how cyber defense is planned, executed, and sustained to ensure network availability in the most contested environments and future conflicts. In order to achieve mission assurance and cyber superiority for Joint forces across a multidomain environment, the Department must shift from the current global internet model. Failure to do so will only exacerbate existing problems and create numerous avenues for adversaries to exploit DOD networks to their advantage, leaving these networks ineffective in combat and unable to support the war fighter.

Introduction

One of the most discussed topics within the DOD is the security, or lack thereof, of its networks and the inability to share or protect data. Today the DOD forces the user to conform to an environment of legacy applications and siloed data. Current commercial initiatives in information technology, such as cloud computing and virtualization, render the classic castle-and-moat network security structure obsolete. Technology has advanced past clearly defined perimeters using multiple firewalls to protect data. The DOD continues to acquire weapon systems with stovepiped communications networks and data links that cannot mesh with or talk to other systems to share data. The DOD model of monitor-detect-react enforces a cybersecurity paradigm that is ineffective against most malicious cyber actors and fails to incorporate mission assurance truly.[1]

Security requires more than just building a moat or barrier around networks. The Department has failed to prevent internal and external network threats and

has become a reactive force in protecting its networks and data. The DOD and the commercial industry must strive for a system that delivers mission assurance in the Joint all-domain command and control (JADC2) environment. This article outlines recommendations for the DOD to prioritize and embrace new technology and rethink its current approach to mission assurance.

Today the Department is slowly shifting to a cloud-based model to protect data, one that aligns with the so-called zero-trust model. A zero-trust model involves trusting no one inside or outside the network perimeter—all users must verify their credentials before being granted access to the network and data. Nonetheless, the DOD must move faster in efforts to change how it thinks in terms of technological solutions, adopting the mentality that networks are already compromised and no one can be trusted.[2] The internet was created for efficient information sharing, and security was not an important consideration. The current model does not work in a contested environment; the DOD should move forward with security at the forefront to ensure it achieves mission assurance.[3]

The military has grown accustomed to having an internet connection, and the current model does not adequately consider resiliency or the integrity of information to achieve the mission.[4] The Department operates under a falsehood that the DOD network will always function, but the reality is the network will be ineffective in meeting the requirements for fighting in future highly contested environments. The current DOD strategy falls short. The Department must foster and enforce resiliency and work with private-sector technology development to better align with national security objectives and partners (such as security firms) to eliminate threats.

This research explores three critical areas of concern and provides recommendations for achieving mission assurance in a JADC2 environment. The DOD must take immediate action and enact a change from the current way of thinking. To better understand the current state of security practices and technology, the article will focus specifically on current internet development, security incidents, transports, and policies for protecting the network. The unsatisfactory nature of the current state compels a rethinking of how the Department designs networks and implements security.

The article will first analyze the cloud platform, emphasizing data security and integrity. Next, the article will consider transports of data, critical to survival in a degraded environment. In short, the DOD must modernize the transport architecture to make every system a data node. Lastly, the Department should explore ways to achieve mission assurance by placing security first, leading to a network dependable in a D-DIL JADC2 environment. The DOD must strive to develop

new technology and military mission command systems functional in a contested environment to ensure the success of specific missions and achieve victory. They must proactively defend weapon systems and allow the war fighter to communicate in a D-DIL environment. Now is the time for the DOD to truly consider the suggested recommendations and act on them to maintain its competitive edge over adversaries.

Current State

> *The fundamental problem is that security is always difficult, and people always say, "Oh, we can tackle it later," or "We can add it on later." However, you cannot add it on later. You cannot add security to something that was not designed to be secure.*
>
> —Peter G. Neumann, *RISKS Digest*, 1985

The Internet of Things we know today is not the internet developed more than 60 years ago as a US government Cold War weapon. The focus on science and technology ramped up quickly in the US after the launch of Sputnik with the creation of the DOD Advanced Research Projects Agency to further develop weapon and computer systems. The engineers developed ARPAnet, which evolved into what we know today as the internet. The original model never considered security but instead emphasized the openness of the Transmission Control Protocol/Internet Protocol (TCP/IP) Protocol Suite used universally today. The vision of connecting without dedicated circuits created an environment of good intentions and unforeseen bad intentions as the internet evolved.[5] Addressing the innately insecure TCP/IP model requires the US to improve the engine that continues to fuel the modern-day internet more than 30 years after its inception.[6]

The Department's answer to securing an internet is to apply a security layer to the stack; however, this does not protect the other layers from vulnerabilities or attacks. Simply throwing security at a layer can induce other unforeseen flaws within other protocols. Further, this solution reveals the security manager does not have a real grasp of cyber risk to the actual mission and instead is attempting to protect all assets essentially equally.

The DOD continually works hard from within to defend the Department of Defense Information Network (DODIN) and its vulnerabilities, but it is not making gains where truly needed to assure the mission. The US Cyber Command's new vision states, "adversaries exploit our dependencies and vulnerabilities in cyberspace and use our systems, processes, and values against us to weaken our democratic institutions and gain economic, diplomatic, and military advantages." This vision recognizes development of cyber defense lags behind cyberat-

tack capabilities. Preventive defensive measures cannot keep up with malicious programs, viruses, or other attacks against DOD networks.[7] Previous approaches to cleaning up the mess after the spill are ineffective in today's environment.

Philosopher David Hume wrote, "there can be no demonstrative arguments to prove, *that those instances, of which we have had no experience, resemble those, of which we have had an experience*."[8] Hume's unassailable logic implies the Department will never get ahead of the threat based on reactive practices and technology. Known (much less unknown) cyber threats increase every year. The DOD cannot prevent every cyber threat under the current construct, and its current defensive mindset does not come close to mission assurance.

Defenders of DOD networks react to attacks after the attack versus looking for a new solution that guarantees cyber superiority. The Department patches and uses firewalls and intrusion-detection tools, but it does not stop attackers who want to do damage. These tools are add-ons to the network and create a greater surface-attack area. These actions are decidedly tactical, defensive, and reactive. The effectiveness of current defensive tools is questionable and illustrates a much broader phenomenon proving current reactive measures to secure DOD networks do not work and do not enable them to operate in a D-DIL environment. Some abbreviated vignettes illustrate the gravity of the issues.

In 2015, Russian hackers implemented a cyberattack on the Joint Chiefs of Staff. The attack affected 4,000 personnel, and the email system was down for 11 days. The DOD cannot even determine how much sensitive data was collected.[9] Then in 2017, BGPMon identified a "suspicious event where 80 prefixes normally announced by organizations such as Google, Apple, Facebook, Microsoft, Twitch, NTT Communications, and Riot Games were not detected in the global Border Gateway Protocols routing tables with an origin out of Russia."[10]

Lastly, in 2018, an operational assessment conducted by Joint Interoperability Test Command validated the US Air Force's inability to defend against cyberattacks using the Joint Regional Security Stack (JRSS). To add further insult, the JRSS provided little improvement from the operational assessment conducted in 2017.[11]

Clearly, cyber defense has failed DOD networks, and many will argue the Department is one attack away from losing the entire DODIN used for mission command. Former Defense Secretary Leon Panetta stated, "a cyber-attack perpetrated by nation-states or violent extremist groups could be as destructive as the terrorist attack of 9/11."[12] The word *could* is not the right word; instead, such an attack *will* be at the time and place of an adversary's choosing if the DOD does not change its current defensive paradigm. The Department needs to recognize the enemy will inflict harm to win, even if this means forcing the DOD to

"unplug" from the world to achieve its mission. The DOD is sadly mistaken if it believes current defensive cyber operations are sufficient.

Today, the DOD is heavily invested in commercial off-the-shelf equipment (COTS) versus government off-the-shelf equipment. Commercial equipment is here to stay—the DOD will not reverse the course as it is too costly to do so. Guaranteeing COTS supply chain security is unrealistic, however, and a monitor-detect-respond model will not find the security flaws, forcing the Department to use untrusted components—hardware, software, networks, protocols, users, and operators.[13] Using COTS creates many more vulnerabilities within the DODIN that will worsen over the next decade as the DOD lacks the strength to mandate greater security in COTS products.[14]

Huawei, a Chinese telecom company, is quickly becoming a dominant global competitor, and the US can expect more companies from China to emerge in other communication networks. Huawei, currently subject to undue influence by the Chinese government, has signed more than 45 commercial 5G contracts worldwide, including with European countries such as Germany. The company plans to ship more than 100,000 base stations to countries free of cost to gain business.[15]

Equipment vulnerabilities are a part of the equation, but commercial transports carrying the critical information are just as important. In 2008, 14 countries lost access to the internet when two undersea cables were severed.[16] The severed lines caused Egypt to lose almost all internet services, and traffic had to be rerouted through other countries including the US. At first glance, the incident seems unimportant because the network traffic rerouted through other commercial transports. But what if the alternate lines were too congested, or slowing or delaying mission-critical information? In 2006, a 7.0-magnitude earthquake struck off the coast of Taiwan, severing eight cables in multiple places. The damage caused disruptions of information flow to and from China and required 49 days to repair.[17] Most alarming, China Unicom, China Telecom, and China Mobile own a 20 percent and growing share of the market today as the companies recently connected Europe, the Middle East, and Southeast Asia.[18]

Space presents the same concerns posed by ground-base transports but for different reasons. Satellites are susceptible to jamming and targeting. The use of kinetic weapons in space has not occurred outside of testing, but it may be only a matter of time. Even though space debris fields and possibly killer satellites pose threats, DOD continuously protects our nation's most vital assets in space: intelligence surveillance and reconnaissance assets, global positioning satellites, mission command satellites, and the Missile Warning System.[19] China has an edge in hypersonic and space technologies as it launched more satellites than any

other country in 2018 and launched the first quantum communications satellite in 2016.[20] Transports are just as vital as creating a network with security first; developing a sensor-driven transport network in a JADC2 environment is essential to achieving mission assurance.

The Path to Mission Assurance

The DOD Directive 3020.40 defines mission assurance "as a process to protect or ensure the continued function and resilience of capabilities and assets, including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains, critical to the execution of DOD mission-essential functions in any operating environment or condition."[21] According to Joint Publication 3-12, cyberspace consists of the interdependent networks of information technology infrastructures and resident data including the internet, telecommunications networks, computer systems, and embedded processors and controllers.[22] If cyberspace remains a critical tenet to achieving military objectives or end states across all war-fighting domains—air, land, sea, cyber, and space—then the DOD cannot rely on the current DODIN defense model or network.

The DODIN is the mission command, but current actions taken to secure the DODIN do not guarantee mission success. These actions fail to protect the integrity of information needed to make timely tactical decisions across all domains. The current cybersecurity paradigm is not reliable and will not allow forces to execute missions in a contested environment. The DOD must engage other means and strategies to deny adversary attempts to access and threaten the DODIN in cyberspace.[23]

Achieving mission assurance in a JADC2 will not happen if the DOD continues to use prescriptive cyber policies enforcing monitor-detect-react constructs on information technology systems.[24] In particular, the desired end state remains war fighting systems that prioritize security, thus ensuring mission success in contested environments and future conflicts. But the DOD must adopt new, commercial-driven technology with a premium on security—an intelligent network that absorbs damage and recovers instantaneously, one that is self-healing. To map the way, the Department can start by developing a secure cloud to provide maximum data access, sensor-driven transports, and a wartime "milnet."

Cloud and Data

No 1960s engineer imagined the military walking around with a COTS handheld device sending information globally. Ensuring the integrity of information

is paramount when traversing COTS systems to carry out military missions. To ensure mission assurance across JADC2, the DOD must embrace the confidentiality, integrity, and availability (otherwise known as the CIA Triad) of information within the commercial cloud. Secured information must flow unimpeded across all transports, or the DOD will fail to achieve national security objectives in peacetime and wartime.

Data resides in various formats on AOC proprietary systems. But navigating through the legacy proprietary systems requires owners agree to merge their data with other AOC systems to create quality data management. The AOC has more than 80 systems, from command and control systems such as Theater Battle Management Core systems, Joint Automated Deep Operations Coordination systems, and the Master Air Attack Planning Toolkit, to Oracle and Microsoft SQL servers.

Each weapon system provides its own proprietary data, making it increasingly harder to unlock and then determine the correct data in a clean state. One approach with legacy systems is using the data as is, but again, in most cases, this does not provide clean, usable data. The DOD must break away from the current proprietary model and move toward a commercial model of open-architecture utilizing apps. To do this, the Department must work hand-in-hand with commercial industry and recognize the commercial world has achieved cloud data integrity.

The DOD has evolved in a defense industry that develops platform-centric systems; instead, industry must design a buffering system or median that can take various data inputs and convert them into an interface understood by all weapon systems and sensors. This buffering system requires a standardized set of entities or data fields where the interface or application correctly accepts the input and creates a common data relationship across the systems, matching and merging all data. The deciphering median is created around a common data standard that allows for cross-utilization among proprietary weapon systems and sensors. This common data standard enhances the DOD's ability to make timely decisions.

It will not be simple, and there is no straightforward solution; however, DOD must identify data as a strategic asset. As the Department builds new weapon systems, it must place interoperability first and identify the right data standard within a modular open system. The DOD needs data; how much is still the unanswered question. Large amounts of useful data are necessary for machine learning and enable the Department to develop a more intelligent network able to heal itself and anticipate the adversary's next attack. Future wars will only become more complicated and complex. Data is a strategic asset in its own right.

The DOD must prioritize interoperability at the start with a metadata standard and a modular open-systems architecture.

The commercial cloud provides the ability to scale and secure both the collection and the analysis of data stored in an enterprise DOD cloud.[25] The cloud provides the operator with the ability to make decisions with the most relevant information. The DOD would no longer maintain a costly data silo infrastructure across commands, and such storage would increase a combatant command's ability to share data enterprise wide. The cloud would eliminate costly proprietary data systems and data silos, making it possible to achieve real-time information and infuse data in a JADC2 environment.

Further, the DOD could increase or decrease the information flow, and cloud computing provides the platform for machine learning (ML) and artificial intelligence (AI). An enterprise cloud has lower upfront costs and reduced legacy infrastructure costs, but most importantly, an enterprise cloud works in every environment, across all military operations—from the tactical edge to the home front—and at all classification levels.[26] A commercial cloud ensures availability and increased security and data protection, and it reduces infrastructure cost, enhancing the DOD's ability to collaborate worldwide. If implemented across the DOD, an enterprise cloud will increase the ability of the Department to operate in a JADC2 environment. Commercial cloud storage will improve tactical effectiveness and efficiency while in a D-DIL environment, allowing war fighters in every JADC2 environment to make data-driven decisions. This capability will also enhance the ability of the DOD to share data with allies and operate as a coalition force.[27]

Transports

Information must flow unimpeded and remain confidential and accurate across all transports, or the DOD will fail to achieve national security objectives in peacetime and wartime. As the Department moves toward AI and ML, many assume the DOD will always have the available bandwidth even in a degraded state. The highly sophisticated and expensive satellites used by the Department will not work in a JADC2 environment. Data availability is vital to achieving national interest in the future crossdomain/multidomain collaboration within a JADC2 environment. High data availability in a degraded environment is the difference between winning and losing. Developing a security-first architecture not only provides confidentiality and information integrity, but it ensures a transport system will overcome power outages, commercial circuit outages, or satellite failures to deliver the right information unimpeded to the right personnel on demand.

To enhance network resiliency, the DOD must increase the number and diversity of transports, thus exponentially increasing the probability of connecting. The DOD is currently at risk because it relies on an aging communication satellite infrastructure augmented by commercial satellites. Overwhelming multiple types of transports also creates greater confusion and costs to the adversary as the DOD can decrease the predictability in data traffic routes. Currently, the Air Force is conducting real-world experiments to achieve this vision as they connected F-35 and F-22 stealth fighters to share data without divulging their location.[28]

Ultimately the DOD must develop a transport-agnostic approach where all systems in every domain become transport nodes to move data, giving the DOD "a seamless battlefield presence crossing the air, land, sea, space and cyber domains where troops and weapon systems are connected 24/7 to ubiquitous sensors and can react almost instantly to put effects on targets."[29]

The DOD's highly sophisticated and powerful communication satellites are costly and take years to launch into space, labeling them a critical center of gravity in a wartime environment. Understanding this critical vulnerability and working with the commercial sector to create cheap minisatellites with the ability to launch instantaneously will help achieve JADC2.[30] Looking ahead, partnering with companies like Amazon and SpaceX is critical. Currently, Amazon plans to launch 3,236 satellites over the next decade and create 12 ground-station facilities.[31] Like Amazon, SpaceX is mass producing and launching thousands of minisatellites within the next five years.[32]

To build the right constellation for communicating in a D-DIL environment, the DOD should consider a new satellite communications enterprise vision that addresses the current aging system and creates a roadmap to a seamless network of military and commercial communications satellites. The Department must designate war-contingency bandwidth reservations across all transports, better understand Wi-Fi signals or low-level cellular, or advance strategies in space through satellites.

Achieving Mission Assurance

Developing a scientific approach with industry forces the DOD to comprehend the utilization or effects of innovation across all domains and how the innovation will attain mission-essential functions in conflict. Driving technological complexity through mission assurance will produce exponential challenges and vulnerabilities to our adversary, causing confusion and overwhelming effects in conflict.[33]

Moreover, mission assurance requires the DOD to conceptualize and focus within a realistic framework considering actual adversaries with realistic capabilities and real strategic objectives.[34] The DOD cannot continue to paper-drill exercises and assume everything will work but instead should introduce real anomalies, incorporate outside the box thinking, and force consideration of worst-case scenarios. Testing aircraft systems' resistance to cyber threats and the ability to operate in a contested environment to achieve mission assurance is a start. Introducing a new type of wargaming to thoroughly exercise networks, computers, satellites, facilities, tanks, aircraft, or ships in a JADC2 environment through nonkinetic and kinetic means allows the DOD to understand where changes are needed to achieve success. Also, this testing is critical for the DOD to implement a smart, self-healing, and proactive defensive network utilizing AI and ML.

As the Department embraces AI and ML fully, the hardest decision for the DOD is how much data it truly needs in a JADC2 environment. Large video files not only take up tremendous bandwidth but are also a hacker's dream as they can easily hide malicious code. Giving up bandwidth-hungry features may not sit well with all stakeholders, especially in today's world where users are accustomed to seeing massive amounts of information with no restrictions. In a time of war, standard peacetime capabilities like PowerPoint and video teleconferences may not be absolutely necessary, but determining the right information needed to make timely decisions is vital.

Just last year, the Air Force began to recognize the importance of data in a JACD2 environment and is now leading the way within the DOD to create a strategy to exchange data between platforms, address data management, and standardize data policies. As the network grows smarter through ML, and the DOD designs a buffering system that takes various inputs from proprietary systems and converts the data into a similar standard for all, bandwidth utilization may continue to be an issue. Bandwidth is critical, and even as a smart network predicts the right path or sensor to transmit data for the highest probability of success, it will require a DOD communications transport strategy to mesh military and commercial transports.

The Air Force Research Lab is developing a network that puts security first, and understanding bandwidth utilization is critical to this effort. This network will provide a user the ability to share necessary data similar to telegraphic transmissions using plain-text data. The lab network uses low-bandwidth transports to access critical mission data segmented across multiple regions worldwide, creating a "milnet" that brings together requested data from the cloud to the user as needed. The critical information is transmitted in multiple data packets across

the JADC2 architecture sensors and assembled again at the next user point, making it virtually impossible to intercept and capture the full data transmission and leaving the adversary with only bits at best. The bottom line: the data is never fully compiled until it reaches the user's point of presence.

Another unique feature of this network allows the user to carry a dongle as their computer to connect to the internet of things globally, while the data itself does not reside on any local computer or laptop used to connect to the cloud. It affords the DOD the ability to access data at all classification levels and places security first. This innovation may force the DOD to rethink command and control to support forces using applications with less bandwidth like multiple miniaturized versions of combined air and space operations centers within a theater; however, this article cannot go into the possible new C2 support.[35]

Finally, as the DOD moves forward to achieve mission assurance in a JADC2 environment, it must develop a culture of change. Many organizations, especially the DOD, do not accept change well and are unwilling to accept the resulting risk. Program managers have focused on the system life cycle and now need to focus not only on the system but on the data, too. Current DOD leadership backs multidomain communications using a mission assurance model, but this effort will require a significant culture change within the DOD. Shifting from a reactionary defensive posture to virtualization, fob technology, zero-trust, or consolidating data across all security platforms introduces new ways of thinking. Promulgating these new ways of thinking means focusing on mission assurance, which takes time and requires personnel to work outside their comfort zone.

Transformational change is a long-term investment and introduces two anxieties—transparency and inclusivity—into organization personnel, survival, and learning.[36] People hate change but will follow if adequately informed and coopted from the beginning and educated about where their mission fits into the change. Transparency and inclusivity are crucial tenets to achieving change and avoiding resistance. Leadership must know how to reinforce transparency and inclusivity within a military organization. Resistance to change can be a struggle to overcome. But with a clear focus on goals, reinforcing the desired end state at all levels, transparency, and recognizing that risk and mistakes are acceptable, the DOD will achieve this new implementation of technology, thus gaining mission assurance across all domains.

Conclusion

As the DOD goes through the transformation to proactive security, security first, and mission assurance, it should become creative in testing and evaluating mission command across war-fighting domains. If the DOD's goal is to present

exponential challenges to adversaries, expose their vulnerabilities, and cause them confusion, it should understand the adversaries are trying to do the same. The Department cannot continue to carry multiple systems in war fighting to access different classifications of information. Military members need simple ways to access data at the right time and place. To achieve this, the DOD must shift from defending the current internet to creating a new internet with COTS products built on solid security principles embracing data protection through global cloud storage. The new internet thinking places emphasis on mission assurance across multiple domains and pulls the DOD away from reactive defense of its networks.

Now is the time for the DOD to act and quickly move away from a monitor-detect-react model to one that delivers mission assurance in the JADC2 environment by implementing the following recommendations:

1. Develop a sensor-driven transport network.
2. Develop a secure cloud to provide maximum data access, sensor-driven transports, and a wartime "milnet."
3. Move to a commercial model of open-architecture utilizing apps.
4. Increase the number and diversity of transports.
5. Partner with commercial companies to create cheap minisatellites that can launch instantaneously.
6. Test all aircraft systems' resistance to cyber threats and the ability to operate in a contested environment.

These recommendations will remedy the DOD's current strategy that falls short in adequately addressing security first and mission assurance in a JADC2 environment. Undeniably, cyberspace networks are the center of gravity to deliver mission command in a future JADC2 architecture. Understanding DOD vulnerabilities before they are exploited and identifying new ways of defending a network gets the Department closer to cross-functional success in all domains. The need for immediate changes in network defense in an ever-changing environment can only happen if the DOD fully understands the need for out-thinking the adversary.

The US Cyber Command vision emphasizes the utilization of cross-research and advancements by academic communities, government, and commercial sectors that understand the need for a more robust way of thinking in terms of cyber superiority in a highly contested environment.[37] The network may not be a new internet, but the solution must guarantee security first to accomplish mission-essential functions within a JADC2 environment. In the words of former Secretary of Defense Mark Esper, "You've got to be able to take some risk, and you've got to be able to accept some failure."[38] ✪

James F. "Frank" Hudson Jr.

James F. Hudson Jr. is assigned to the Air War College, Air University, Maxwell AFB, AL. He served in significant leadership positions over the last twenty-seven years; throughout his career, he has assumed assignments of increasing responsibility beginning as an enlisted/officer member of the US Air Force and in supervisory and managerial positions with industry and as an Air Force civilian.

Notes

1. Dr. Kamal Jabbour, "The Post-GIG Era: From Network Security to Mission Assurance," Air Force Research Laboratory, Secretary of the Air Force Public Affairs, *Cyber Defense Review*, November 15, 2019, https://cyberdefensereview.army.mil/.
2. C. Todd Lopez, "Assume Networks Are Compromised, DOD Official Urges," defense.gov, September 24, 2019, https://www.defense.gov/.
3. Jabbour, "Post-GIG Era."
4. Jabbour, "Post-GIG Era."
5. History.com, "The Invention of the Internet," October 28, 2019, https://www.history.com/.
6. Jeff Hussey, "The Fundamental Flaw in TCP/IP: Connecting Everything," May 17, 2019, https://www.darkreading.com/.
7. US Cyber Command (USCYBERCOM), *Achieve and Maintain Cyberspace Superiority: Command Vision for US Cyber Command* (Fort Meade, MD: USCYBERCOM), March 1, 2018, https://www.cybercom.mil/.
8. David Hume, *A Treatise on Human Nature: Being an Attempt to Introduce the Experimental Method of Reasoning into Moral Subjects and Dialogues Concerning Natural Religion* (London: Longmans Green, and Co., 1878), 390 (emphasis in original).
9. Will Robinson, "Russia Hacked Joint Chiefs of Staff and Have Shut Down the Email System of 4,000 Pentagon Employees for ELEVEN DAYS. . . and Counting," August 7, 2015, https://www.dailymail.co.uk/.
10. Richard Chirgwin, "Suspicious BGP Event Routed Big Traffic Sites through Russia, December 13, 2017, https://www.theregister.co.uk/.
11. Office of the Director, Operational Test and Evaluation (DOT&E), *Director, Operational Test and Evaluation: FY 2018 Annual Report* (Washington, DC: DOT&E, 2018).
12. Jim Garamone, "Panetta Spells Out DOD Roles in Cyberdefense," October 15, 2012, https://www.army.mil/.
13. Jabbour, "Post-GIG Era."
14. Robert H. Anderson and Richard Hundley, *The Implications of COTS Vulnerabilities for the DoD and Critical U.S. Infrastructures* (Santa Monica, CA: RAND Corporation, 1998) 1–15, https://www.rand.org/.
15. Michael Nienaber, "Germany Could Still Ban Huawei from 5G Build-Out: Defense Minister," Reuters, November 5, 2019, https://www.reuters.com/.
16. Kim Zetter, "Undersea Cables Cut; 14 Countries Lose Web Updated," December 19, 2008, https://www.wired.com/.
17. Douglas Main, "Undersea Cables Transport 99 Percent of International Data," *Newsweek*, April 2, 2015, https://www.newsweek.com/.
18. Stacia Lee, "The Cybersecurity Implications of Chinese Undersea Cable Investment," East Asia Center, University of Washington, February 6, 2017, https://jsis.washington.edu/.
19. Todd Harrison, "Space Threat Assessment 2019," Center for Strategic and International Studies, April 4, 2019, https://www.csis.org/.
20. David Vergun, "Chinese Set Sights on High-Tech Production," Department of Defense (DOD), 29 October 2019, https://www.defense.gov/.
21. Office of the Under Secretary of Defense for Policy, DOD Directive 3020.40, *Mission Assurance*, https://fas.org/.

22. Office of the Chairman of the Joint Chiefs of Staff (CJCS), Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: CJCS, June 8, 2018), https://www.jcs.mil/.

23. North American Electric Reliability Corporation and US Department of Energy, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," June 2, 2010, https://www.energy.gov/.

24. Jabbour, "Post-GIG Era."

25. John Curran, "DoD Publishes Cloud Strategy With Eye on Modernization," MeriTalk, February 5, 2019, https://www.meritalk.com/.

26. Curran, "Cloud Strategy."

27. Tom Keelan, "The Pentagon's JEDI Cloud Strategy is Ambitious, But Can It Work?," March 21, 2019, C4ISR Net, https://www.c4isrnet.com/.

28. Sydney Freedberg Jr., "F-35 To F-22: Can We Talk? Finally, the Answer Is Yes," World Defense, November 7, 2019, https://world-defense.com/.

29. Theresa Hitchens, "Breaking D's 2019 Top Five: From Multi-Domain Ops to Killer Robots," Breaking Defense, December 27, 2019, https://breakingdefense.com/.

30. Sydney J. Freedberg Jr., "Build Bare-Bones Network & Small Satellites for Multi-Domain Battle," Breaking Defense, July 31, 2017, https://breakingdefense.com/.

31. Michael Sheetz, "Amazon Cloud Business Reaches into Space With Satellite Connection Service," CNBC, November 27, 2018, https://www.cnbc.com/.

32. Eric Ralph, "SpaceX's Starlink Eyed by US Military as Co. Raises $500-750M for Development," Teslarati, December 21, 2018. https://www.teslarati.com/.

33. US Air Force (USAF), *USAF 2030 Science and Technology Strategy: Strengthening USAF Science and Technology for 2030 and Beyond*, April 1, 2019, https://www.af.mil/.

34. Williamson Murray and Allan Millett, *Military Innovation in the Interwar Period* (New York: Cambridge, 1998).

35. Colin Clark, "MDC2: Air Force Works on Huge Command, Control System; Allies Key," Breaking Defense, March 7, 2017, https://breakingdefense.com/

36. Edgar H. Schein, *Organizational Culture and Leadership* (Hoboken, NJ: Wiley & Sons).

37. US Cyber Command, "Achieve and Maintain Cyberspace Superiority."

38. Brian W. Everstine, "Esper: Culture Change in DOD Needed to Improve Acquisition Process," January 24, 2020, *Air Force Magazine*, https://www.airforcemag.com/.