Vol. 17, September 2018

MITCHELL INSTITUTE
Policy Papers

Key Points

The ability to connect and share information across a large, global membership is transforming semi-isolated weapon systems into an integrated enterprise of great synergy. Sharing is done through physical and logical conduits through which data flows—the network. The network is a physical domain of cyber operations.

All information-age military capability is inextricably linked to networks. The Department of Defense (DOD) must attain network superiority over any potential adversary. However, its network lags far behind what is available on the commercial market, and it will not catch up without dramatic changes in DOD's approach.

DOD's proprietary, hardware-centric, and compliance-based approach, managed by a support agency—the Defense Information Systems Agency (DISA)—is not optimized to deliver network superiority. A whole-of-nation approach is necessary, to include wide area and even end-to-end network services from US-flagged network service providers to deliver superior attributes to US combat forces.

Network Superiority: The Foundation of Future Warfare

By Heather Penney

Senior Resident Fellow, Mitchell Institute for Aerospace Studies

Abstract

Network superiority is the foundation upon which all other military actions depend. Information sharing through physical networks has revolutionized warfare, stimulating new operational concepts. This competitive dynamic will continue. Nations with the most agile and resilient military networks will hold a critical advantage.

The Department of Defense is falling further behind in providing its combatant commands a wide area network with superior attributes. The DOD information network (DODIN), managed by the Defense Information Systems Agency (DISA) support agency, lags far behind capabilities of the commercial market and is more expensive. The DODIN is sub-optimized by a hardware-centric approach where global connectivity is handled as a proprietary commodity. The military services are thus limited from exploiting the power of information with new operational concepts such as the combat cloud that employ networks as weapon systems.

The solution to the challenge currently posed by an anachronistic set of processes and approaches ensconced in DISA may be to incorporate US-flagged network service delivery companies as indispensable partners in network superiority. Using commercial versus current DISA-proprietary standards for military networks, commercial entities could provide state-of-the-art superiority for the military services and combatant commands. The approach recommended in this paper begins with a goal to craft DOD networks that create superior information age effects in peace and war. Recommendations include a determination and findings analysis for network services by each of the armed services to define their own wide area network requirements. Current cyber security structures, standards, and regulations must migrate from compliance to effects-based security processes and technologies. A dedicated intelligence center is also needed for network analysis and assessment to gather relevant intelligence on potential adversary network capabilities to inform military planning and assessment.

Introduction

Today, information and its management are just as important as the traditional tools of hard military power were across the 20th century, hardware such as bomber and fighter aircraft, infantry divisions, tanks, amphibious attack elements, and warships at sea. Powerful advancements in networking—the ability to connect and share information across a large membership—are evolving what once were semi-isolated weapon systems into a highly integrated enterprise of great synergy. As the quality and reach of networks improves, servicemembers are learning to exploit shared information in new ways across the battlespace, changing operational paradigms. In the 21st century, it is the continuous, rich, and unrestricted exchange of information across all platforms, computers, devices, and other end points that will determine success or failure in deterrence and war.

Powerful advancements in networking—the ability to connect and share information across a large membership—are evolving what once were semi-isolated weapon systems into a highly integrated enterprise of great synergy.

The value of information is wholly dependent on the ability to share it, and that sharing is done through the physical and logical conduits through which that data flows—the network. Networks are the key to exploiting the power of information to revolutionize warfare. Tactical datalinks that connected fighter aircraft allowed the pioneering of operational networking, and the immense benefits realized from these networks has created an imperative to expand information sharing across the enterprise. This means expanding beyond a small team of airborne aircraft in close proximity to sharing information across all participants on a global scale and in real time. While senior leadership in the Department of Defense (DOD) has recognized the essential value of information to military operations for nearly two decades, the long-distance network infrastructure that the DOD depends upon lags far behind what is available today on the commercial market, and it is not likely to catch up without dramatic changes to DOD processes.

The DOD gives responsibility to the Defense Information Systems Agency (DISA) for providing global connectivity (once referred to as "long-haul networks") to the whole of the DOD and the National Command Authority. If a data byte travels anywhere beyond its local area network (LAN) or enclave, it rides on the DOD Information Network (DODIN). As the global network the US military depends upon, the DODIN is the foundation of American military power. Yet, the DODIN and the larger joint information environment (JIE) it supports do not reflect state-of-the-art network technology. Shaped by regulation and resulting processes and culture, DISA's hardware-centric, proprietary approach to modernizing, integrating, and managing the DODIN reflects an industrial-era paradigm that is out of step with the information age.

Such an outdated approach to building and sustaining DOD's network architecture poses serious vulnerabilities to the warfighter. The fragmented architecture and systems that comprise the DODIN significantly degrade its performance, directly impacting the Department's opportunity to fully exploit the potential of information in the contested, fleeting, and dynamic battlespace of future warfare. Furthermore, DOD's network defense and information assurance requirements are constantly bumping up against obsolescence, surpassed by both potential adversaries and newer, more resilient security technologies and designs that are already deployed and rapidly refreshed in the commercial sector.

Network capability cannot be separated from the overall military defense capability equation. Despite the goal to maintain superior US military strength, the backbone network architecture to achieve that goal is by approach perpetually second-rate. Constraints, artificial or otherwise, shaping DOD's approach to the JIE, specifically the DODIN, ensure the current network needs of military operations cannot be met. Therefore, using the current DOD processes, it is unlikely ever-growing future requirements can be met.

Again, the performance of the network is inextricably linked with the attributes or value of information in information age warfare. Superiority over adversaries in network performance is a major factor in competitive superiority of information-driven processes. If there is not a dramatic change in how the military departments obtain network services, the nation will be deprived of the decisive edge that information can provide, in both peace and in war.

The Power of Networks and the Requirement for Network Superiority

The DOD has the largest end-point user enterprise network in the world. With over ten thousand operational systems, hundreds of data centers, tens of thousands of servers, millions of computers and IT devices, and hundreds of thousands of commercial mobile devices, the network infrastructure, information assurance, and security demands of the DOD are enormous.[1] Chronic, widespread, and multi-day outages are a routine occurrence in DOD, and even basic administrative information, applications, or services are sometimes not accessible. This impact on operations is even further magnified when it comes to operationally urgent data. It may not seem significant when computer workstation access to the Non-classified Internet Protocol Network (NIPRNet) or the Secret Internet Protocol Network (SIPRNet) goes down, but these failures of connectivity impact more than just email systems.

Historically, wide area networks (WANs) that provide global connectivity have enabled command, control, and communications (C3) from higher headquarters throughout the national security enterprise. The Defense Communications Agency (DCA), the predecessor to DISA, was established in 1947 specifically to address the needs of national leadership to provide better command and control for the US military. Dissatisfied with his personal experience with the natural tensions and competition that existed between military components, regions, and theaters in the common-user communication system of WWII, President Dwight Eisenhower formalized authority for long-distance networks with specific responsibility for C3 within DCA. This global network function is even more important in today's dynamic and uncertain security environment where the scale and scope of American security commitments is vastly expanded. Without global connectivity, C3 functionality is lost. Whether shaping theater environments, conducting deterrence operations, or fighting across the spectrum of conflict, global networks of superior performance, reliability, and security enable decision superiority over adversaries.

Chronic, widespread, and multi-day outages are a routine occurrence in DOD, and even basic administrative information, applications, or services are sometimes not accessible. This impact on operations is even further magnified when it comes to operationally urgent data.

As networks have become more capable and robust, they have also become necessary for more than C3. To access and share information, the DOD has been moving data bases and applications to the cloud. Taking programs and data from locally-based storage services and moving them to a cloud service improves access to geographically-dispersed military users, decreases overall cost and duplication, and facilitates real-time user collaboration. But for any cloud to work, there must exist a robust network. If the cloud isn't accessible, neither are the applications nor the information. Simply degrading the network can adversely impact both the normal business and combat operations that depend on cloud services for everything from personnel management to mobility cargo manifests to operational mission planning.

The utility of networks is not limited to command and control or even cloud services. Modern networks allow the US military to create effects from the tactical to the strategic level anywhere across the globe. Operational weapons systems are becoming more and more connected beyond tactical ranges; the value of information is not limited to proximity. The operational necessity and urgent value of information networks are obvious when considering the advantages that tactical networks like the F-15 Eagle's intra-flight data link (IFDL), the ubiquitous Link-16, and the F-35's multifunction advanced data link (MADL). These networks have improved the quality of situational awareness, enabling more effective combat operations at a tactical level. Whether correlating and cross-checking information to refine position data, cutting through deception and jamming, or helping fighters maintain hostile identification and tracks, these tactical data link networks are a preview of the future. Connecting individual platforms with the entire Air Force or DOD enterprise presents a strategic potential far beyond tactical coordination or even multi-domain command and control (MDC2). Network superiority that ensures robust, rich connectivity

across the whole of the enterprise will be necessary to transform coordinated and synchronized actions into a true combat cloud concept of operations.[2]

The combat cloud is an emerging concept that envisions how a rich and robust connection can amplify tactical to strategic operations, making them more resilient and effective in a contested environment. Ambivalent to whether specific platforms are sensors or shooters, weapons could receive their cueing, targeting, and guidance data from alternate or even multiple entities via the combat cloud. If cuing data from one platform is lost, it could instantaneously be replaced by another. In a similar manner, the network could facilitate a weapon launch from a more kinetically or tactically advantageous position than where the targeting data was generated. Such a concept also exponentially complicates the adversary's problem set, because the kill chain is no longer linear.[3] It cannot be broken or defeated at a single link, nor is the chain even obvious to the adversary. Such a rich and robust network could enable a bomber to receive cuing from a space asset, for example, then guide a submarine-launched cruise missile to the target. Clearly, the combat cloud promises a revolution in maneuver, resilience, effectiveness, and efficiency, and it requires a network that exceeds the reach of tactical datalinks through critical wide area network services.[4]

…the combat cloud promises a revolution in maneuver, resilience, effectiveness, and efficiency, and it requires a network that exceeds the reach of tactical datalinks through critical wide area network services.

Within this context, the "tyranny of distance" problem that the Indo-Pacific and Eurasian theaters pose demonstrates how the role of wide area networks encompasses more than just connecting everyday workstations and computers at a base with the internet. Wide area networks are essential to countering long range, hypersonic, and mobile threats, or adversary initiatives in contingency and combat operations. In highly contested operations, wide area network superiority can facilitate multi-axis, multi-platform operations and the ability to maintain integrity in the kill chain. Sensors that provide threat warning and whose data is used for targeting may not be onboard the shooter. This data may need to be passed or shared between multiple entities near-simultaneously to assure desired outcomes.

Given the territory of the Indo-Pacific or Eurasian theaters, long-distance networked warning and weapons-quality fire-control data are required to mount a timely and effective defense. Similarly, information must cross those same expanses to provide US and coalition forces offensive initiative. Against global competitors, networking will be the essential capability that will enable US and coalition forces to exploit the advantages of synchronized, integrated, and interdependent operations, complicating the adversary's problem set to provide strategic advantage for outnumbered blue forces. Just as tactical datalinks have transformed and dramatically improved US military tactics and operations, wide area networks will be absolutely essential to effective operations across the globe.

But networks are also about more than just building and sharing an accurate battlespace picture or fire control for weapons cueing data or kinetic effects. The importance of cyber operations in future wars will require even greater levels of connectivity based on networks that are superior to our adversaries' networks. The effectiveness of cyberoperations will rely not just on advanced cyber applications, technologies, and the cunning and competence of cyberwarriors, but also on the ability the DOD to achieve network superiority.

Network superiority is not information superiority. While related, they are distinctly different. Information superiority depends on network superiority. Information superiority underpins decision superiority and implies the ability to have more and higher quality information than the adversary. That is, having more and better information than the enemy enables better decisions—thus the emphasis on increasing intelligence, surveillance, and reconnaissance (ISR) capabilities and capacity. However good and plentiful ISR information may be, the data collected must maintain its integrity in order to retain its decisional value. Information superiority, however, is more than just information assurance. Even if the data is unmolested (that is, complete, robust, and true), it must reach the right end point at the right time to enable either a decision or action. Superior information is meaningless unless it can be acted upon, and for that it must be shared. Information superiority depends upon network superiority.

Network superiority is about transport, connections, and destinations—that is, the physical infrastructure, the architecture (design), and the end-point users. While a network could be as rudimentary as a hand-written note transmitted by a horse-back courier (and such a low-tech option may still be a viable course for some specialized operations), the focus of this paper is the physical and logical domain of information and maneuver in cyberspace. Network superiority is a competitive assessment; it is contextualized within the information demands of friendly operational constructs and relative to the capabilities of the adversary. It must both meet the needs of US operations and be better than the adversary's network.

To summarize the power of networks and the need for network superiority, network superiority is the foundation of 21st century warfare both in the physical and cyber domains. Robust, resilient, and reliable networks are essential to US national security. A superior network has specific qualities that meets the needs of our forces and exceeds the capabilities of the adversary's network.

Network superiority is a competitive assessment; it is contextualized within the information demands of friendly operational constructs and relative to the capabilities of the adversary. It must both meet the needs of US operations and be better than the adversary's network.

That said, this is not the network that DOD is building. On the current path, DOD is not creating the foundation for wide area network superiority. Given the inherent qualities of airpower—flexibility, range, and speed—which demand long-distance connectivity, it is imperative that the US Air Force modernize its approach to building, maintaining, and modernizing their global information networks. But, this will be a significant organizational challenge. Since 1960, the responsibility for wide area networks has been removed from the military services and handed to DISA.

Originally created for and charged with centralizing DOD C3 for national leadership, DISA has gained expanded authority for the entire DOD wide area network affording global connectivity through a series of directives, regulations, and statutes. These directives, regulations, and statutes, however, exempt DISA from accountability to the US military services for network requirements and performance, setting the conditions for network mediocrity.

It is essential to understand how such a limiting factor to US military superiority occurred, and why stewardship over a critical network capability over time lost connection with contemporary warfighting needs.

The Legacy Approach to Defense Networks Ownership

In response to President Eisenhower's desire to reduce the duplication of military communications facilities and develop a DOD telecommunications system that was interoperable, efficient, and economical, DCA was established by DOD Directive 5105.19. At that time, DCA appeared to be a prudent compromise towards centralization to mitigate inter-service rivalry, and it avoided appointing a single military department (the Army) as the sole communications manager.[5]

DCA's purpose would be to manage the new Defense Communications System (DCS), simultaneously created by DOD directive. Merging the military services' communications systems into one common-user system, DCA assumed service authority to establish and manage its own "long-distance, point-to-point, government-owned and -leased defense communications services."[6] By centralizing those authorities, DCA would streamline DOD communications systems through the efficiencies of consolidation and scale. More importantly, it would create an integrated command and control system that would be more effective and cost efficient for senior Department leaders.

But the establishment of DCA and the DOD's new communications system was in direct conflict with the individual organizational and mission interests of the military services. While it may have appeared parochial, each military service communications system reflected the demands of its unique domain and mission needs. Further exacerbating the military services' reluctance to merge their communication systems was their experience with common systems during World War II. The common-user systems of that era that supported large-scale, global coordination "were designed to serve the communication needs of

others and were thus not fully under one's own respective control."[7] As such, individual service message traffic did not always receive the priority that users thought was appropriate. A major issue was the sheer volume of traffic. The system often choked at key nodes, incentivizing servicemembers to "inflate" the priority of messages in order to speed the processing of their message. These attempts to game the system in actuality only contributed to demand volume, exacerbating delays. Alternately, the military services could be frustrated as their messages were downgraded in precedence and sent to the bottom of the pile, doomed to languish until messages of higher priority were processed.

Because of the dysfunction that the individual services perceived in the WWII common-user systems, they developed separate global communications systems after the war to ensure their individual mission effectiveness.[8]

From DCA's organizational perspective, these failures were directly attributable to the military departments' federated systems, incompatible networks, and lack of unified standards.

Through the 1960s DCA worked to consolidate responsibility and management for a growing portfolio of communications systems. Initially focused on voice, secure voice, and digital telecommunications—DOD's Automatic Voice Network (AUTOVON), Automatic Secure Voice Communications Network (AUTVOSECOM), and Automatic Digital Network System (AUTODIN)—DCA expanded into the Defense Satellite Communications System (DSCS), White House communications to include the Cold War "Hotline," and the World Wide Military Command and Control System (WWMCCS).[9] Assuming responsibility for large numbers of incompatible, service-specific systems that required multiple manual processing steps caused misconnects with serious and sometimes tragic consequences.

From DCA's organizational perspective, these failures were directly attributable to the military departments' federated systems, incompatible networks, and lack of unified standards. The only way to counter such chaos would be to continue to expand DCA's organizational role and authorities over communications and other information technology (IT) systems within the DOD. Over the course of the next 30 years, DCA would assume responsibility for the Minimum Essential Emergency Communications Network (MEECN), act as the systems architect for all defense satellite communications, take over the Joint Tactical Command, Control, and Communications Agency (JTC3A), and establish the Joint Interoperability Test Command (JITC) to perform interoperability compliance testing and certification. These formative experiences would shape DCA's (and now DISA's) approach to systems and technology—an approach which endures today.

Agency Evolution—Purge of Service Authority, Expansion of Scope, Growing Antiquation

The Air Force does not own the entirety of its network or its management. In fact, no military service does. DISA holds the vast scope of responsibility for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions "to serve the needs of the Secretary of Defense, and the DOD components, under all conditions of peace and war."[10] DOD expanded DISA responsibilities well beyond the wide area networks originally tasked to its predecessor, DCA. As data centers, applications, and other capabilities are now moving to the cloud (and therefore "outside the fence line" of military service purview), those activities now also fall under DISA, creating greater service dependency on the organization for effective network services.

Creating the seamless information environment of the future has not been easy, and will not be in the future. The historically fragmented approach to developing military IT capabilities "has resulted in layers of stove-piped systems that are difficult to integrate and not as effective as needed," according to former DOD Chief Information Officer Teri M. Takai.[11] To its credit, DISA has proactively taken on the challenge to consolidate DOD IT across the entire enterprise, aiming to remove the many seams.

With the authority to articulate and provide computing, cloud, and application services, information assurance and security, overarching standards, interoperability, and more, DISA has developed the joint information environment to describe and capture all of these responsibilities.

The JIE is an ambitious vision to provide a single joint enterprise IT platform "that can be leveraged for all DoD missions."[12] The JIE will connect any and all IT devices across the entirety of the DOD and consolidate all "communications, computing, and enterprise services into a single joint platform" to "reduce total cost of ownership, reduce the attack surface of our networks, and … more efficiently access information resources of the enterprise."[13]

As owner and manager of the JIE, DISA is the service provider to the services. That is, DISA is not bundling DOD needs to achieve economies of scale through service contracts to commercial companies. Rather, DISA is the prime contractor, acquiring components and treating companies as suppliers and subcontractors, integrating disparate parts and pieces together to provide IT services through inter-department contracts. It is almost as if DISA is taking on the role of the old US Army Ordnance Department (now the Ordnance Corps), becoming a turn of the (19th) century production arsenal for IT. But DOD's use of DISA as prime contractor, integrator, and IT service provider to the military departments is not cost effective, and it certainly is not best of breed when it comes to IT.

DOD has already recognized that in many technological sectors, the civilian commercial market is outpacing and out-innovating traditional defense companies. The same is true in networks.

Today's overall IT paradigm is outdated. Instead of taking a whole-of-nation approach to leverage cost efficiencies, advanced technologies and capabilities, as well as the expansive reach of US-flagged technology and telecom companies, DISA is building, integrating, and operating not just the DOD Information Network (DODIN) but the entire JIE as a system integrator of hardware. It is an industrial-era paradigm to an information-age imperative. Perhaps at one time it was appropriate to a develop proprietary, hardware-centric networks to manage the larger DOD common-user IT needs. But now that approach is less capable, less responsive, less secure, takes longer, and is more expensive than what domestic US network and cloud services can offer today.

DOD has already recognized that in many technological sectors, the civilian commercial market is outpacing and out-innovating traditional defense companies. The same is true in networks. Commercial telecoms and cloud providers have advanced their network capabilities far beyond what DISA is able to develop as the de facto prime contractor. While the intent of the JIE and DOD's Global Information Grid (GIG) project reflects the demands of the military services' future concepts of operations, the means through which DISA and the DOD is attempting to manifest this vision is not. Network superiority is the foundation of future warfare. The DODIN, DISA's wide area network, all but guarantees that DOD networks are based on obsolete technology, have low bandwidth and high latency, lack agility and resiliency, utilize outdated security paradigms, do not meet even commercial availability standards, and have limited reach. At the same time, cost efficiencies available on the commercial market are left untouched.

Insights from the Regulatory Structure Guiding DISA

While well-intentioned in pursuing its charge, DISA's expansive ownership of the network enterprise may be in violation of the spirit if not the letter of the Economy Act of 1932 (31 US Code §1535). Furthermore, DOD Directive 5101.19 may unduly restrict the rights and responsibilities of the military department heads (service secretaries and their chiefs of staff) to organize, train, and equip their forces by transferring certain authorities to DISA without reasonable approvals or accountability. Complicating network and cyber mission effectiveness are obsolescent security policies, standards, and complex regulations and instructions on the larger IT infrastructure. The result of all of these policies and programs is that the wide area network provided to the US military services cannot meet the demands of current operations, and it risks failing the information and network demands of future warfare.

Military Service Responsibilities and The Economy Act of 1932

A review of The Economy Act and other related legislation demonstrates how, through a somewhat labyrinthine set of guidance, DISA is exempt from the determination and findings requirement mandated by the Economy Act of 1932. Without this check and balance, there is no

accountability for DISA's network performance. Thus, while nothing improper has occurred, there is an absence of the normal due diligence typically performed in the course of inter-agency or inter-departmental ordering. Instead, DISA's role as the wide area network services provider for the military departments is more the result of organizational inheritance and role expansion than a deliberate decision by the military services. More importantly, due to the regulations and policies that mandate DISA's role as DOD's wide area network provider, the military service secretaries and chiefs of staff have no recourse to hold DISA accountable for its performance, and as a result cannot fulfill their obligations to organize, train, and equip.

The Economy Act of 1932, 31 US Code §1535, describes the conditions for agency agreements: when a government agency can or cannot contract another government agency for goods and services. Assuming that funds are available, the head of the requesting agency would need to decide that the order is in the US government's best interest, that the agency requested to fill the order is capable of doing so, and that the goods or services cannot be as conveniently or economically provided by commercial companies.[14] The provisions of this statute are important, because they require the head of the ordering agency to provide rigor behind an affirmative and deliberate decision to make an inter-agency or inter-departmental order.

There must be a significant advantage to making an inter-agency order for it to comply with the Economy Act.

There must be a significant advantage to making an inter-agency order for it to comply with the Economy Act. Without that advantage, if all things are equal, the US government is required to make the desired order directly to a commercial company. But the military department secretaries and chiefs do not even have the option to make that determination and finding when it comes to their own network services.[15]

The Code of Federal Regulations, specifically 48 CFR §17.502-2 "The Economy Act," imposes a more detailed requirement that a determination and findings (D&F) must accompany any Economy Act order and be approved by an authorized contract officer or agency head. The D&F will certify that the interagency acquisition is in the government's best interest, and that commercial companies cannot provide the goods or services as conveniently or economically as the servicing agency. But the determination and findings may not apply to DOD intra-agency orders. Paragraph (a) specifically reinforces 10 USC 1535's provision of authority "for placement of orders between major organizational units within an agency" and further clarifies that those "intra-agency transactions are addressed in agency regulations." Paragraph (c), which stipulates requirements for determinations and findings, applies to "Each Economy Act order… by inter-agency acquisition"—not intra-agency.[16] It appears that for orders within the Department of Defense, DOD regulations and instructions take precedence.

DOD Financial Management Regulation "Economy Act Orders" reinforces 31 US Code §1535's stipulation that for a major organizational unit to place an order with another within the same agency, the head of the requesting agency must determine that the order is in the best interest of the US government, the serving agency is capable of filling the order, and also decide that the "ordered goods or services cannot be provided as conveniently or economically by a commercial enterprise."[17] While this regulation does not mention any determination and findings, its exact reference to the language in the Economy Act appears to provide some clarification as to the prerequisites for an intra-agency order. Less helpful is its pointer to DOD Instruction 4000.19, "Support Agreements."

DODI 4000.19 is largely a process instruction; a how-to checklist and manual on the contracting legalities of intra- and inter-service transactions. The instruction, however, does not apply to Defense Working Capital Funds (DWCF)—which is how DISA is funded by the military departments.[18] Instead, 10 USC §2208 "Working-capital Funds" is relevant. In addition to reporting and accounting guidance, this statute specifically addresses the "establishment of working-capital funds in the Department of Defense" and purposes those monies for "such industrial-type activities, and such commercial-type activities that provide common services within or among departments and agencies of the Department of Defense, as he [the Secretary of Defense] may designate."[19]

Does this mean that DOD defense working capital funds can be used for intra-agency transactions that could be obtained on the commercial market? Does it supersede the intent behind the D&F requirements of the Economy Act? It appears that the Secretary of Defense does indeed have the authority to circumvent Economy Act determinations and findings by fiat—designating DISA as the support agency responsible for the entire vast DOD IT enterprise, and funding the organization through DWCF.

The Commoditization of Network Capability and Recapturing Warfighting Priority

The trend for DCA to take on increasing authorities for information systems only continued over time. In 1991, the Defense Communications Agency (DCA) was renamed the Defense Information Systems Agency (DISA) in recognition of its "expanded role in implementing the DoD's CIM [Corporate Information Management] initiative, and to clearly identify DISA as a combat support agency."[20] CIM would identify and implement "management efficiencies in DoD information systems",[21] and add responsibility for tactical IT system standards, and support to the JCS and OSD staff.

While each military service may continue to develop, field, and manage tactical networks and the infrastructure inside their services (in accordance with DISA enforced standards), all DOD network elements outside of the service bases, posts, camps, and stations are DISA's territory.

The further expansion of DISA's roles and tasks continued this trend. While each military service may continue to develop, field, and manage tactical networks and the infrastructure inside their services (in accordance with DISA enforced standards), all DOD network elements outside of the service bases, posts, camps, and stations (B/P/C/S) are DISA's territory. DISA also does not just own the long-haul networks. In 2006, DOD Directive 5105.19 granted DISA broad authorities and powers in the following "broad core areas":

1. Communications
2. Command and Control (C2) Capabilities
3. Information Assurance (IA)
4. Computing Services
5. Interoperability, Testing, and Standards
6. Global Information Grid Enterprise Services
7. Engineering
8. Acquisition

Taken together, these assignments constitute nearly the whole of the DOD IT domain. It is not necessary to go into each of the areas at length, but several beg greater consideration, especially when taken in aggregate.

The "Global Information Grid Enterprise Services" sets the context for the others. DISA is charged with providing "the DoD enterprise with a net-centric, service-based, shared enterprise structure that supports ubiquitous user access to reliable capabilities and decision-quality information."[22] This articulation is the connective tissue between all of DISA's other core areas. In order to be able to create the GIG as defined here and envisioned in other key DOD documents, DISA would have to be the network provider, secure the whole of the enterprise, define the standards, engineer the GIG, and then acquire and integrate all the various components to make it happen. On one hand, this expansion of authorities appears to simply be on the trend line that decades of DCA and DISA growth has demonstrated. On the other, given the essential nature of information and networks in current and future wars, the authorities granted in DOD Directive 5105.19 represent not a linear progression but expansion that is orders of magnitude beyond what seems reasonable for common defense services or supply.

There is no mention in DOD Directive 5105.19 of any requirement for the DOD component heads or any military service authority to review or approve DISA's actions. In fact, DODD 5105.19 places DISA is a position of functional authority over the military departments. Although DISA is to consult with the military departments to analyze their requirements, it is not DISA that shall be responsive to the requirements and operational needs of the services, but the services that shall be responsive to the direction of DISA. The military departments must coordinate and obtain approval from the director of DISA prior to any "programmatic or technical changes impacting the funding or interoperability of [command, control, communications, and computers] and

information systems for which DISA has primary responsibility." Furthermore, the departments must coordinate with DISA on all draft acquisition plans.[23] This might seem like a reasonably bounded requirement, but given the ambitious vision of the GIG, the requirement for both approval and coordination will only expand. Conversely, there is no requirement for DISA to coordinate with or obtain the approval or concurrence of the military department heads for DISA programs, plans, or standards.

Network superiority, in particular, will be far more than just a C3 function in future wars, or even assured access to cloud data storage or applications; the network will be a wholly integrated element of combat operations and delivering effects.

The Goldwater-Nichols Act vests the Secretary of Defense with the power to create defense agencies to "provide for the performance of a supply or service activity that is common to more than one military department" when the agency can be more effective, economical, or efficient.[24] But the activities and Global Information Grid enterprise that DISA has been charged with creating seem to extend far beyond common services and supply. Given the critical nature of information and network superiority to military operations, networks are no longer a commodity. The GIG is not the same as the Defense Logistics Agency (DLA) buying jet fuel in bulk.

All these regulations, directives, instructions, and statutes must be contextualized within operational considerations. Goldwater-Nichols provides for defense agencies to conduct common supply and services, and even the military departments' authority to organize, train and equip is at the discretion and control of the Secretary of Defense.[25] Taken with DOD Directive 5105.19, the Secretary of Defense has done nothing improper in restricting the rights of the heads of the military departments to organize, train, and equip when it comes to IT, long-haul networks, and cloud applications and services. The question is not can, but should?

Network superiority, in particular, will be far more than just a C3 function in future wars, or even assured access to cloud data storage or applications; the network will be a wholly integrated element of combat operations and delivering effects. The ability to execute highly agile, resilient, flexible, and precise combat operations that are sensor and shooter agnostic will depend on the quality of both tactical and wide area networks. Networks will also facilitate offensive and defensive cyber maneuver and operations. As the operational concept of combat cloud and cyber tactics, techniques, and procedures mature, the line dividing tactical and long-distance networks will blur.

The value of network superiority is not as a "common service" that can be provided, like a commodity in bulk for a discount. Networks cannot be evaluated as low-cost, technically acceptable competition. Such an approach would diminish the potential of the entirety of joint force operations, force structure, and capability investments. A more appropriate test of "should" would be an operationally-focused analysis that harkens back to the Economy Act:

1. **Has the head of the ordering agency or unit (in this case, the military department secretaries and chiefs of staff) determined that the order is in the best interest of the US government?** The question here is not whether network services are in the best interest—the question is whether providing those services through an inter-agency or inter-department order is in the best interest of the government, and therefore the best interest of the United States. This requires a complex and multifaceted analysis. Is the actual current performance of the DODIN and the JIE capable of establishing the high performance and quality network the military services will need for current operations, and to further develop new operational concepts that can fully exploit the power of networked information?

2. **Is the agency or unit (DISA) able to provide or get by contract the ordered goods or services?** Because DISA is designing and building the DODIN/JIE as a prime integrator, the real issue is DISA's ability to provide the DODIN/JIE both in part and in whole. Is DISA technically and programmatically able to provide the quality of network required by the military departments to meet their obligations to the United States? Will DISA

be able to modernize and field these vital capabilities on a rapid technology cycle that meets or exceeds the pace of commercial or global competitors? Is DISA able to adapt to and respond to the evolving requirements of cyber operations and the cyber component commands of the military departments?

3. **Has the head of the agency (the military department secretaries and chiefs of staff) decided that the ordered goods and services cannot be provided by contract as conveniently or cheaply by a commercial enterprise?** Although it is not required, a determination and finding analysis should be conducted as to whether DISA is less expensive and more convenient than US-flagged commercial alternatives. This D&F should be approved and certified by the heads of the military departments. Are the goods and services provided by DISA convenient, or do they levy additional service changes to hardware, configuration, and other integration demands that drive additional costs internal to the military departments? Is DISA able to modernize and field capabilities as quickly as commercial industry?

The historic and technical discussion that follows only begins to scratch the surface of the magnitude of the technical challenges facing this enterprise—and what is at stake for the US if DOD's current approach remains unable to ensure network superiority in future wars.

Evaluating the Global Information Grid

Early GIG capability documents recognized that the value of connectivity was more than simple command and control, or even the communications that DCA had previously provided. "The real demand for a GIG has been driven by the requirement for information superiority and decision superiority … as expressed in Joint Vision 2020," declared a forward-looking document by the Joint Chiefs of Staff in 2000, that described early concepts for net-centric warfare. Anything and everything that could be connected by any means would be part of the GIG, a massive network and information infrastructure necessary to "deliver the power of information out to the forward edge of the battlespace, thereby enabling decision superiority"—the combat advantage that future warfare would demand to provide "full spectrum dominance."[26] Information would create a common operating picture, improving shared increase situational awareness along with the "resulting increase in combat power."[27]

DISA's first articulations of the Global Information Grid were relatively modest. The services would still have their own networks, identity and access management processes, data centers, mission and business applications, commercial-off-the-shelf (COTS) hardware, and IT procurement services, but connect through emerging standards.[28] But almost a decade after the GIG had been articulated as an information superiority concept, it was still too federated and, according to DOD's chief information officer in 2011, did not "effectively support the joint warfighting environment."[29] The GIG's development had been too "incremental and [the] evolutionary manner in which DOD develops information (IT) technology has resulted in layers of stove-piped systems that are difficult to integrate and not as effective as needed."[30] For DISA, this was not its fault; it was clearly the failure of the military departments to converge their own networks and standards—a situation that clearly demanded intervention, from the organization's perspective.

A central integrator like DISA was deemed necessary because Joint Vision 2020's network-centric vision of warfare had pointed to more than just connectivity. Early capabilities documents define the GIG as "globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel."[31] Such a mammoth effort would require a large, centralized organization to enforce a singular vision, and for DISA, the executor role of the GIG was an incredible organizational opportunity. First steps toward the GIG simply sought to connect those military service-specific systems, but as an information-focused combat support agency overseeing wide area networks essential to future combat outcomes, DISA would rise in prominence within DOD.

And this vision has indeed grown. Today, DOD's network strategy is for the GIG to encompass everything that computes, processes, stores, communicates or transports, presents at the application level (human-computer interaction), or includes network operations such as management, monitoring, dissemination, or assurance and security.[32] That said, this is not simply about creating the US military's own "internet of things." The service warfighting aim is to revolutionize warfare in an information age.

DISA's joint information environment is a natural growth and expression of the GIG as outlined in DOD Directive 5105.19. In 2011, DISA embarked on building the joint information environment, a "single joint platform" that converges all "communications, computing, and enterprise services."[33] The JIE would deconstruct the service network fiefdoms, reduce network vulnerabilities, reduce IT cost, and guarantee interoperability to "enable DISA's mission partners to more efficiently access the information resources of the enterprise to perform their missions from any authorized IT device from anywhere in the world."[34] The JIE would deliver the GIG, and all that it promised to be, to the US military services.

transitioning to thinking about IT as a capability rather than as a program."[36] As right-thinking as these vision documents sound, DOD continues to treat the JIE as an industrial-era program where DISA is assigned as the prime integrator. A closer analysis of the JIE and the DODIN that supports it reveals just how wide the gap is between language and execution.

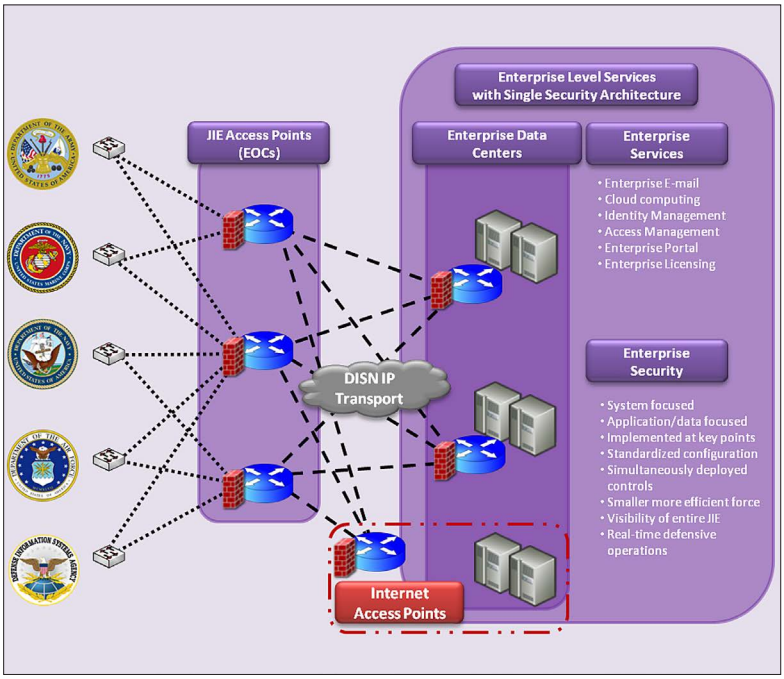

Figure 1: DISA's vision of the Joint Information Environment. Source: Defense Information Systems Agency.

Evaluating the Department of Defense Information Network

From the start, DISA understood that 21st century military operations "require an agile information environment to achieve an information advantage."[35] Subsequent vision documents would continue to hit the right targets: the JIE would decrease cost, reduce attack surface, synchronize command and control, streamline decision making, ensure cyberspace sovereignty, be agile, adaptive, fast, and accessible. A 2016 strategy document even states that DOD is moving "from a culture of compliance to one of risk assessment,

The first and most critical step in building the DODIN (and therefore the JIE) is fully fielding and integrating each of the military services into the joint regional security stacks (JRSS) that support the JIE architecture. The "near-term focus" of the JIE, the JRSS, are a "regionally based, centrally managed suite of network security appliances that will help simplify and secure the current DOD IT environment," according to the DOD's chief information office.[37]

The joint regional security stacks are the entry points for the services to access the DOD's information network (DODIN) and then the larger joint information enterprise. Each individual military department has the responsibility for managing and maintaining their network to the edge of their individual enclaves, but if they want to access any point beyond, they must pass through the JRSS. Service enclaves

are any of the tactical networks and networks on any base, camp, post, or station (B/C/P/S). At an almost-literal fence line, information packets pass through a service gateway to the JRSS, for entry into the DODIN.

A helpful analogy to understand the DODIN is that of a road network. If a packet of data (information) is a car, then the road system that it drives across is the network. The service enclave can be envisioned as a gated community. The homeowner's association (military department) designs the community inside the gates, builds and connects discrete sections (tactical network architecture), names the roads (message traffic standards), sets speed limits (bandwidth), and provides security (authentication and encryption). No car gets in or out of this community unless they first pass through a security gate (gateway).

Once outside the gate, all cars must first pass through a customs checkpoint (the JRSS). At this checkpoint, all cars must present their license and registration (accreditation and authentication). Like verifying a license with a department of motor vehicles (DMV), the JRSS will verify the accreditation with the service authentication proxy. Cars must also provide their intended destination and routing (end-point destination or address), and be inspected. During this inspection, all suitcases must be removed and opened (break and inspect), and all riders interrogated (fine grain content filtering). Cars must go through several inspectors at the checkpoint before passage; this "defense in depth" concept is a cornerstone to DISA's security paradigm.

Like a GPS-guided traffic navigation application such as Waze, software defined networks (SDNs) can real-time redirect data packets to faster roadways and streets based on traffic.

After the car has passed through the customs checkpoint (JRSS), it must go through the tollbooth (router). If the car has an electronic toll collection device like an E-ZPass (the data packet has been encoded using multi-packet label switching, or MPLS standards) and the booth has the equipment to recognize the pass (a MPLS router), the car may quickly enter the highway. But if either of those are not in place, then the car must take the time to stop at the tollbooth (router) to pre-pay for its intended route and destination. Finally, the car must know the route it must take to get to its destination. Like a GPS-guided traffic navigation application such as Waze, software defined networks (SDNs) can real-time redirect data packets to faster roadways and streets based on traffic. Without SDN, message traffic must remain on a preplanned routing, regardless of whether a faster (lower latency) route exists.

The value of networks is not just about getting from point A to point B, though. As DOD moves more to cloud services (whether it be for data storage, computing, applications, or combat weapons data), the ability to exploit the value of the cloud is all dependent on network superiority.

DISA has not yet fully deployed either multi-packet label switching or software defined networks on the networks it leases from telecoms. Although these technologies and other advanced capabilities are now developed and routine tools used by the large telecoms, DISA does not leverage this potential in their contracting. In fact, the only element that DISA leases from telecoms is the most basic level of the network—the physical "layer one." Literally, the fiberoptic cable, copper wire, or cellular tower link.

As the prime integrator for DOD IT systems, DISA is using commercial-off-the-shelf hardware from numerous vendors to build a DOD-unique network. Being DOD-unique, though, is not necessarily attributed to military necessity, nor is it in the best interest of the United States. DISA policy and vision documents have all the right intent, but the reason that the DODIN is unique is because within its hardware-centric approach, DISA has attempted to reverse-engineer commercial networks by using an obsolescent security model. The DODIN is several generations behind the current state of modern commercial service.

Because the JIE is not a program of record—and therefore no individual element or subsystem is either—DISA is able to circumvent many of the reporting, review, and other milestones associated with government defense acquisition. This should speed the fielding of the JIE and the mature DODIN, but progress is years behind state-of-the-art capabilities. Although DISA is purchasing all commercial-off-the-shelf (COTS) technologies to create the JIE and DODIN subsystems, DISA then spends months to years integrating those pieces,

whether processors, racks, or software, into the larger enterprise. After integrating the hardware, DISA must test the subsystem before it can field. That DISA is already using mature technologies means that, when fielded, these new systems are already out of date. Add to this problem the fact that the military services must then react with their own network and system upgrades. Modernization and associated warfighting utility are therefore further delayed.

Integrating commercial technologies may appear to take advantage of the robust research and development investments made by the IT industry. However, IT technology advances quickly. The lag time induced by DOD's model at best delivers systems with limited relevance, and at worst, systems that are already outdated. In a field where advances occur at a dizzying pace, DOD's focus on hardware, using DISA as the integrator, works against the needs of the military services for network superiority.

Networks do not exist for their own purposes. Transporting information is not the value of a network. Rather, value is about what the end point user can do with the information.

For example, DISA has only begun to introduce MPLS and software defined networking to the DODIN, and has not yet fully fielded either capability. These technologies are robust capabilities today, but tomorrow they may be as dated as dial-up internet access. The true measures of the network are its qualities. Yes, the technology must be sound, but it is the effect that technology delivers that makes the network capable of allowing warfighters to leverage the true potential of information. As new technologies field, they provide a qualitative and quantitative improvement over older technologies. This is why focusing on hardware or even software is not sound approach to network superiority. All pathways concerning the JIE must both begin and end at the same place—warfighting effectiveness that is superior to any potential adversary.

Network Attributes and Network Superiority

Networks do not exist for their own purposes. Transporting information is not the value of a network. Rather, value is about what the end point user can do with the information. It is a complex system where advancements are a result of both "pull" and "push." Users articulate requirements for networks based on new needs. These needs may be in response to new threat capabilities, improvements in weapons, or new concepts on how to exploit information to gain initiative in the battlespace. Users pull the network technology forward by making demands on the system that exceed current performance. Alternately, network engineers can push technology to users, providing a quality of network that goes beyond what current weapons and platforms can use, stimulating the user to innovate new ways to take advantage of improved qualities. Those who can both transport and employ richer information with lower latency and a greater reach begin to achieve network superiority in relation to an adversary.

Richness is an "aggregate measure of the quality of information," not the network.[38] Richness is important to the warfighter because the level of detail information is more robust, making it both more useful and more valuable. Richness can mean the difference between a target location located somewhere within a mile or having precise enough coordinates to deliver a GPS-guided weapon. Richness is the difference between a radio or voice talk-on to a target, and the ability to live-stream color video from a fighter aircraft to a joint tactical air controller (JTAC) to more precisely integrate kinetic or other effects in a dynamic area of operations. Because richness is a qualitative measure of value and utility to the user, it is necessarily subjective in content—what richness generally implies, though, is a volume, context, and complexity that requires bandwidth to transmit. The degree of richness depends on the network.

Because of bandwidth limitation—that is, the maximum number of bytes per unit of time that can flow through a transmission line or network—richness historically had to be traded off for reach. Bandwidth dictated an inverse relationship between the richness of the information that could be exchanged with the number of individuals it could be exchanged with.[39] This was also true for time and distance. The faster or further the information had to be transmitted, the less rich it could be. Richness is useless if the size of the data packet is so large that it exceeds the network's ability to process and transport it in a timely manner to the appropriate end point user. Overly rich information packets can jam the system

and impede the transport of other data, just like congestion slows traffic flow on a busy highway. Similarly, if the network is so limited that the information conveyed is of no practical utility, that information can act as noise, detracting from mission accomplishment. Thus, while richness is not an inherent quality of the network per se, it can be enhanced or constrained by the network's attributes related to capacity or speed.

The network must also have attributes that provide right information to the right person at the right time.

Network Attributes

Network superiority must both meet the information needs of US and allied weapon systems, while also exceeding the capabilities of the adversary's network. Future wars will require high-performing networks with the following qualities:

- **Reach:** Both the physical range that a network extends, and the number of end points.
- **Accuracy:** The ability of a network to deliver data to the correct and intended end point.
- **Availability:** The percentage of time the network is available to its users.
- **Bandwidth:** The volume of data a network is able to process and transport without incurring degradation of operations.
- **Latency:** How quickly a network is able to move data between two end points.
- **Integrity:** The ability of a network to protect the veracity of a data packet throughout processing and transport, without molestation or alteration.
- **Richness:** A qualitative measure of value and utility to the user.
- **Resilience:** The ability of a network to sustain damage and still function effectively.
- **Awareness:** The ability of the network manager to monitor and have high-fidelity knowledge of network performance and operations.
- **Security:** The ability of a network to detect, repel, and repair intrusions or attacks by the adversary.
- **Control:** The ability to control all the functions of the network and the information riding on the network.

First, the network must be able to reach the right entity or end points across the battlespace. The attribute of reach includes the physical range the network spans and the number of end point users within the network. None of the other network qualities matter if the network does not extend throughout the battlespace. For deployed operations, this can be problematic. Because DISA is responsible for wide area networks, it must ensure deployed network connectivity to austere or pop-up locations. Often, these bases have no real option to connect to terrestrial networks because of how DISA manages and integrates long-haul services as the prime service provider. DISA only leases the physical layer of network transport and may not have the contracting mechanisms or relationships in place to facilitate unanticipated locations in the event of contingencies. Akin to resorting to helicopters to provide lift to deliver suitcases and other contents of the cars in the previous analogy, satellite links become the default for these deployed locations, with the potential to strain or overload a system that is limited and already in high demand. It does not matter how robust the tactical or base network is if the information cannot get through the link, or if there are unintended imposed costs or liabilities associated with satellite communications.

It is from those base edges that the military service base-area networks and tactical networks then go the last mile. Regardless of whether the edge is a long-established facility or "off the grid," accuracy is the ability of the whole network to deliver data to the correct and intended end point. Accuracy is not simply ensuring the right data gets to the right person, like delivering a package to the correct address. Accuracy also prevents accidental delivery to an unintended recipient or its diversion or loss. Often taken for granted in today's networks, accuracy enables the correct end point to use the information transmitted through the network.

A corollary to reach and accuracy is availability. The network that is not reliably accessible is not useful, and in military applications even dangerous. Measured in percentage of the time the network is available to its users, DISA's objective availability is anywhere between 98.5 percent and 99.9 percent.[40] The sheer volume of data transactions going on every second means that even at 99.9 percent, such an objective goal for availability is not actually an impressive metric. For every million transactions, the system is unavailable for 1,000 of them. But which 1,000? When compared to commercial levels of service of at least 99.999 percent, that number drops to only 10. Given how essential the role of information is in current and future operations, availability is a crucial metric for measuring network quality—

and will only grow in importance in contested environments.

How much data a network can process and transport without incurring degradation of operations is the quality of bandwidth. Bandwidth is not an unlimited network feature. In older networks, it can be constrained by how the message traffic and network itself is structured (like the Link 16 data link, with predetermined network membership and a limited number of message data types). Alternately, bandwidth can be conceived as simply the number of lanes on a highway. Tradeoffs can be made between how robust a data packet is (a wide-load tractor-trailer truck), or how many data packets can travel on the highway. But there are only so many lanes to accommodate traffic, and too many of either can slow down the entire system. Future operational concepts will require massive bandwidth to support the rich data needs of warfighter situational awareness, maneuver, and targeting.

The speed of the network between two end points is its latency. Speed can be limited by the bandwidth of the network, the architecture of the system, and the infrastructure of the network. The architecture of the network is somewhat similar to a city street network and its many avenues, control measures, and traffic rules. Latency is impacted by available routing, traffic lights, posted speed limits, and the numbers of inspections message traffic must process through. The physical transport layer can also impact latency. Like the difference between smooth asphalt versus a gravel road, fiber optics can support faster transmission than copper wire and therefore has lower latency. Speed is important to ensure that the information conveyed is still relevant to the end user. In a highly dynamic battlespace, it does no good to receive targeting data on a mobile target that has already left the messaged location.

The speed of the network between two end points is its latency. Speed can be limited by the bandwidth of the network, the architecture of the system, and the infrastructure of the network.

The network must have integrity, that is, information must arrive to the intended end user without molestation or alteration. As the data packet moves through the network, routers, and processing stations (such as the JRSS), it must not be altered, hacked, degraded, or infected. Integrity assures that the data has remained secure and as intended throughout transmission. To continue with the vehicle analogy, it means that as a car moves from point A to point B and makes its stops and turns along the way, without any nefarious packages being slipped into the trunk, or suitcases switched out. Integrity ultimately refers to the trustworthiness of the network—that data arrives whole and secure throughout its transport.

Resilience is the ability of a network to sustain damage (through either physical or network attack) and still retain network superiority. This requires the network to continue to function effectively for end users while also outperforming adversary networks. The cars must still get to their destinations, whether through detour routing, by crews repairing pot holes quickly, or by driving on the shoulder, and arrive in time with the right content to be operationally effective.

Resilience also depends on both how the network is designed and built and how it is operated. Network management elements like awareness, security, and control are critical resilience factors. That is, a resilient network must provide operators situational awareness so that they can positively control the network and provide security. High-fidelity awareness of network performance can provide early indicators of subsystem failures, intrusion attempts, malware, or other important network performance and activity. Commercial operators build sensors into their networks to monitor the traffic, health, and other real-time qualities of their networks, and that information can provide incredible insight to savvy operators. It allows them to proactively manage information flows and all other functions of the network. Additionally, network awareness can alert both defensive and offensive cyber operations to enhance security. Inspection of data packets is not the best or only way to detect adversary activity on a network; sometimes traffic flow or other signals can be more revealing. This kind of awareness is more valuable than simply knowing from highway camera footage where traffic jams have already occurred. More like the Waze smartphone application, which alerts a driver as to how traffic activity will impact their route, network awareness can show areas of high activity,

where accidents have occurred (and prompt the deployment of a crash response), or other "pattern of life" monitoring that can either make network flow control more effective or facilitate anomaly detection.

These network attributes have been broken out separately, but in practice they are interrelated and interdependent. One attribute can positively, adversely, or inversely affect the others. Of relevance here is how DISA's hardware-centric approach as a prime integrator impacts the quality of DODIN attributes.

A case study of the joint regional security stacks—the "customs checkpoint" of the vehicle and road analogy—offers great insight into the network attributes of the DODIN and the larger DISA enterprise. Representative of DISA's overall approach to developing, fielding, and managing the JIE, the JRSS are important because they provide insight into the failures of architecture and engineering, programmatics, and interface with the military departments. Furthermore, a study of the JRSS demonstrates the inefficient, fragile, and vulnerable state of the networks that the success of future military operations will depend on. The JRSS is a critical node in the DODIN. Described as the customs entry or check point above, the JRSS is both the entry point to the DODIN and the primary defense mechanism for all DOD networks. But DISA's approach to the DODIN is not on a path to achieve and maintain network superiority. If the US military departments cannot dramatically change how they obtain wide area network services, they will be unable to exploit the power of information in future military operations.

The fielding of JRSS first began in 2015, years after the effort was first initiated. It is still not yet complete… As of mid-2018, only 13 NIPR stacks were operational, and no SIPR stacks were operational.

The Joint Regional Security Stacks: A Case Study of the DODIN

The fielding of JRSS first began in 2015, years after the effort was first initiated. It is still not yet complete. Of the 48 planned joint regional security stacks, 23 will support the NIPRNet and 25 SIPRNet. As of mid-2018, only 13 NIPR stacks were operational, and no SIPR stacks were operational. To date, none of the military services have completed their transition to the JRSS. What was supposed to have been a complete transition for the DOD network in 2017 is now programmed for the end of 2019. This delay alone is enough to bring doubt regarding the technological currency (and therefore value) of the JRSS. Given Moore's Law, which stipulates the number of transistors in an integrated circuit will double about every two years, and the rate of technological progress, at least three technology generations will have passed since fielding began, clearly putting the DOD behind the state-of-the-art of commercial networks—with any delay to fielding only leaving the DOD even further behind in the network and cyber competition.

Part of the delay is due to the complexity of the stacks. Although each stack is composed of mature commercial racks, the stacks involve more than 50 different vendors, which has resulted in a complicated and fragile configuration.[41] An Air Force official who was working in the JRSS program office in 2015 criticized the technical approach as lacking in systems engineering. This official's critique was both specific to the JRSS and the larger JIE program. Citing the lack of functional systems engineering analysis for the overarching and subsystem architectures, the lack of larger vision created what was described as a "list of materials" approach. JIE subsystem program managers separately acquired commercial racks and processors in isolation from the larger system vision. Without considered design on how these subsystems would integrate or function as a whole, the JRSS is just one of the many subsystems where lack of coordination created large, embedded inefficiencies in the functionality of the JIE.[42] It should be noted that program managers were doing their best to provide effective technologies at their level. But without a larger integrated master plan or schedule, these managers were set up for failure. The dysfunction caused by a lack of a unified vision has necessitated work-arounds or side programs to compensate for gaps both within DISA and the military departments.

The first order of business for JRSS evolution is simply to meet the baseline military service requirements to connect. Version 1.0 of the JRSS "was the minimum capability needed for the Army to do its consolidation … Version 1.5 is not

a whole new thing…. [it] will accommodate the baseline requirements for the Air Force," DISA's division chief for JIE solutions said in 2016.[43] Similarly, Version 2.0 will facilitate the Navy and Marine Corps migration. Accommodation, though, does not mean that the JIE is "plug and play." Each military department will have to make significant hardware, software, and configuration changes to their own networks so that their systems are interoperable with the JRSS. In the Army's case, millions of dollars of recently acquired equipment is incompatible with the JRSS and will have to be replaced. It is up to each service to fund the adaptation of their networks to ensure configuration compatibility with the JRSS.

The JRSS approach to security is described by DISA as a "defense in depth." In this scenario, the multiple stacks are a virtue, not a vice, as they force the message traffic to be filtered and sifted a number of times before progressing beyond the stacks.

Unfortunately, even though the first version of the JRSS was designed to enable the Army to integrate their networks onto the JIE, the Army still has not connected through the JRSS and currently is pausing these efforts. The Army has not funded the modification of its networks to comply with the JRSS standards and may choose not to migrate. At issue is the service's desire to monitor and manage their networks on "one pane of glass"—that is, to be able to consolidate all network metrics, health, status, management, and control tools into a single screen that captures the entire network from beginning to end. Operating the JRSS system itself is complex and unwieldy; JRSS operators must manually "integrate and configure the complex, room-sized suite of JRSS hardware and associated software," according to DOD's director of operational test and evaluation.[44] Although this is standard for network operations centers in various domestic technology and telecom companies, the JRSS is not able to provide both network status or control in a single view.

The JRSS approach to security is described by DISA as a "defense in depth." In this scenario, the multiple stacks are a virtue, not a vice, as they force the message traffic to be filtered and sifted a number of times before progressing beyond the stacks. If one stack misses something, another has the opportunity to discover it. One of the functions of the JRSS is to "break and inspect." The JRSS opens each data packet to identify any potential malware or virus. Problematically, DISA is logging all the data, but there is no concept on how to operationalize those findings. Unlike electronic intelligence (ELINT) that can transform recordings of enemy radar systems into effective jamming techniques, there is no exploitation of malware findings. Furthermore, the JRSS does not have malware handling capability, as commercial IT or telecom companies do. The best the JRSS can do is quarantine the message and not let it through—it cannot destroy the malware and let either innocuous or mission-relevant data go forward. Bluntly, DISA's commitment to defense in depth is an obsolescent security strategy that lacks flexibility, adaptability, or maneuver. It reflects a bureaucratic approach rather than a warrior-minded urgency to operate a superior network.

JRSS modernization will not accelerate or solve any obsolescence problem for the JIE. Once true modernization kicks in, it will still take 12 to 18 months to field a new update. As it is not a DOD program of record, the JRSS is not subject to the approval and review process that a traditional acquisition program faces. Logically, as an information technology system, DISA should be able to rapidly acquire and field modernization versions. But even though the JRSS is comprised of commercial, off-the-shelf units, the integration and testing of the complicated stack will occur at a glacial speed compared to commercial industry standards. By the time mature, advanced stacks are fielded, they will already be obsolete. This clearly is not in the best interest of the military services, nor will it meet their warfighting requirement for network superiority.

Delays in reaching operational status are not only due to internal JRSS issues. To connect to the broader transport network, the JRSS depends on the readiness of other JIE subsystems. For example, the multi-protocol label switching (MPLS) router, two logically and physically separate 10 gigabyte stacks, is a separate DISA program that is necessary to connect the JRSS to the backbone of the JIE.[45,46] As a newer program, the programmed fielding schedule of the MPLS stacks is not the same as the JRSS, and some sites do not even have the requisite

infrastructure to support the MPLS. Clearly, it is not just the number of racks in each JRSS that makes for a complicated program.

Integrating these disparate technologies has not been easy, nor is the operation or management of the stacks. As of this report, the total number of people who can operate and manage a JRSS is around 10 persons, and to optimize system performance, those individuals should be teamed in groups of two or three in order to take advantage of their personal areas of expertise.[47] JRSS has been a DISA program for at least five years, and in that time the organization has not developed the manpower, concept of operations, or training programs to make the hardware useful. This oversight betrays the hardware focus of DISA. Even if the JRSS were fully fielded, it is unclear how DISA expects to employ the JRSS to win network superiority without the requisite cyber manpower, expertise, training, or procedures to operate the system.

Even if the JRSS were fully fielded, it is unclear how DISA expects to employ the JRSS to win network superiority without the requisite cyber manpower, expertise, training, or procedures to operate the system.

The 2017 annual report by DOD's Director of Operational Test and Evaluation (DOT&E) was highly critical of the failure to mature the JRSS as holistic system. An operational assessment of the JRSS Version 1.5 found that the system "is unable to help network defenders protect the network against operationally realistic cyber-attacks."[48] In large part, DOT&E attributed this to the complexity of integrating technologies from a large number of vendors (over 50). Additionally, the DOT&E evaluation found that both DISA and the Air Force were undermanned at the JRSS, with the Air Force manning at only 50 percent. Yet, lack of personnel may not be as significant of a factor in the efficacy of the JRSS, as DOT&E also found that operator training lagged far behind the deployment of the JRSS. This training deficit may be reflective of a larger operational shortfall, in that the military services, DISA, and US Cyber Command (CYBERCOM) have "not codified JRSS joint tactics, techniques, and procedures to ensure unity of defensive effort and enhance defensive operations."[49] One cannot train to what does not exist.

Tactics, techniques, and procedures (TTPs) are the essential foundation of operational advantage in any weapon system. TTPs are designed to exploit and maximize US advantages against specific adversary systems and tactics. More than just best practices or how-to, they are developed and validated through rigorous operational experimentation and testing. Once refined, these TTPs are codified to ensure they can be trained to and employed as a set of standards. It is important to emphasize that TTPs are not static. They are continuously updated as potential adversaries field new capabilities and evolve tactics, or when new US and allied capabilities are fielded. TTPs are then documented and disseminated through a series of manuals colloquially called "the 3-1" (referring to the Air Force manual numbering system), providing servicemembers the best proven methodologies to employ their particular weapon system across a range of scenarios and to integrate with other US military communities. Together with training, TTPs can make the difference between operational success and failure when faced with an adversary that possesses relative capability parity.

The DOT&E was so dismayed by the findings of their JRSS operational analysis that it recommended that the DOD CIO and the military services "should discontinue deploying JRSS until the JRSS demonstrates that it is capable of helping network defenders to detect and respond to operationally realistic cyber-attacks."[50]

The notable absence of JRSS tactics, techniques, and procedures identified by DOT&E is indicative of the larger problem in DISA's approach to networks. There is a poorly defined vision regarding employment of the JRSS, the DODIN, or the JIE as an operational weapon system. This demonstrates the gulf between well-intentioned rhetoric and actual execution. Hindered by custom, culture, regulation, and the disjointed nature of how DISA has structured the JIE, even conscientious employees cannot overcome bureaucratic constraints to deliver network superiority to the military services.

The joint regional security stacks enterprise is a Rube Goldberg-like overly-complex system of racks and processors—the focus is hardware. Representative of DISA's broader approach

to the DODIN and the JIE, the JRSS clearly demonstrates the inability of DOD to deliver the network capabilities that 21st century warfare will require. But even the development and fielding of tactics, techniques, and procedures for the JRSS would not solve the fundamental liabilities posed by a hardware-centric, compliance, and checklist-oriented approach to a consolidated architectural paradigm.

Does DOD's Obsolescent Approach to Cyber Security Increase Risk?

At issue here is whether for security reasons, DISA must develop, integrate, and operate military networks. That is, do the unique security and classification requirements of military information – and the need to protect that information – levy a unique requirement on defense networks that commercial IT and telecoms cannot ensure? By their very nature, are military networks and their security requirements so unique that they cannot be considered "commercially available"?

At issue here is whether for security reasons, DISA must develop, integrate, and operate military networks. That is, do the unique security and classification requirements of military information… levy a unique requirement on defense networks that commercial IT and telecoms cannot ensure?

DISA's defense-in-depth information assurance and network security model has perpetuated the checklist-oriented compliance mindset of the DOD towards cyber security. In this security model, the objective is to consolidate the flow of information through a castle-and-moat approach; for the JIE, that defensive monolith is the JRSS. To maintain our earlier street analogy, defense-in-depth is like a road security checkpoint where multiple streets and lanes neck down into a single road, or single lane series of check points. This approach "reduces the attack surface," conceptually minimizing vulnerabilities by funneling all information through iterative defensive layers. Defense-in-depth depends on ensuring certain hardware configurations and installation of patches or software to provide a layered screening and filtering defense. Adversaries must get across the moat and over the walls to access the system. In many ways, defense-in-depth is "install and trust." Once the configuration and required software is installed, system managers just have to trust that the moat works.

The notion that military network security requirements can only be met through a DISA-proprietary defense-in-depth network and architecture must be questioned, as these layers of screens and filters are not effective for today's cyber threats. That the JRSS represents DISA's most advanced defense technology should already be cause to evaluate the suitability of commercial network services. One real-world analogue may be found in the financial services business sector. Money may be the only similar commodity that requires the same elevated levels of network superiority and information assurance as military information. Supporting financial activities such as trading, mergers and acquisitions, and other transactions requires superior network performance. High accuracy, availability, bandwidth, low-latency, resilience, and security are all elements that a healthy financial industry depends upon. Notably, the financial markets are not in the network business; they rely upon commercial network services. These are not minor stakes. The global economy is highly reactive, and any network hiccup or misstep with respect to money reverberates around the world. The US government, as it turns out, is not the only entity with vital information and data to protect. It may be that commercial IT and telecom companies are leading the technological state-of-the-art when it comes to network superiority.

Cyber adversaries have already learned how to overcome these "castle" barriers and have demonstrated the inadequacies of relying wholly on defense-in-depth. Domestic IT and telecom companies are at the forward edge of the battle area in the cyber domain. Monitoring their global networks, detecting anomalous activity, identifying nefarious patterns of behavior, and discovering malware through an incredible volume of end point users, commercial network service providers have greater reach and richness of data when it comes to the threat environment. As a corollary, these companies also have the business imperative to provide robust network protection to their customers. One commercial IT company representative interviewed during the research for this project indicated that because of their firm's

advanced analytics and the scope of their network, they are often at the leading edge of cyber threat detection for the US government. While defense-in-depth may retain some residual value against less capable threats, it cannot be the entire security strategy. Compliance does not equal security.

The defense-in-depth mentality that defines the JRSS also drive's DISA's requirement for physical separation of all DODIN transport from commercial transport, SIPRNet traffic from unclassified traffic, and JIE applications from other commercial or cloud services. Like defense in depth, this physical separation is also outdated. Advanced cryptology and other software techniques are now able to provide the barriers that in the past only physically separate networks could ensure.

The National Security Agency (NSA) is pioneering a somewhat different approach to protecting classified information. Instead of physical separation, a standing set of standards that comply with a defense-in-depth paradigm is published. Commercial providers can apply to have their systems tested and certified as a "capability package." Called "Commercial Solutions for Classified" (CSfC), this program certifies commercial companies to provide layered capability packages (CPs) across a number of different applications to protect classified information without requiring physical separation. NSA's intent is to accelerate commercial innovation to the government by testing and pre-approving commercial providers' systems to streamline the authorization and contractual process.[51] While this approach does provide more opportunity to the DOD to expand its cloud, application, and network providers, it still retains a configuration compliance and hardware-centric approach premised on defense in depth. Even so, DISA will not embrace NSA's certification of CSfC commercial providers, rather insisting on owning and integrating a system that does not enhance network superiority.

Security, or information assurance (IA), is not simply about filtering, barriers, or physical separation. Security standards are also key to IA.

Security, or information assurance (IA), is not simply about filtering, barriers, or physical separation. Security standards are also key to IA. Again, DISA is responsible for defining those standards and ensuring that they are implemented in all commercial cloud, services, applications, and hardware and software. The commercial interface for these requirements is DISA's Federal Risk and Authorization Management Program (FedRAMP) and the Information Assurance Support Environment Security Technical Implementation Guides (IASE STIG) websites. Like CSfC, the intent behind FedRAMP is to "simplify" certification of cloud, automation, and application service providers by reusing assessments and authorizations across DOD customers, as appropriate, and to ensure "consistent application of existing security practices."[52] DISA's STIG program proactively publishes technical security standards for all DOD devices and systems and applies to both DOD IT and cyber operators, as well as commercial vendors. STIGs provides the "technical guidance to 'lock down' information systems/software that might otherwise be vulnerable to a malicious computer attack," according to DISA.[53] Though these programs, DISA is rightfully trying to decrease the bureaucratic barriers to entry for commercial technology and services.

The challenge is that neither program can truly mandate leading-edge security standards with respect to the cyber threat because the cyber threat is constantly changing. This threat is in fact adapting and changing faster than DISA policy, regulations, and standards can respond. One commercial telecom executive stated that DISA standards are routinely three to four years behind the commercial sector. Although this executive regularly participates in the cybersecurity advisory bodies to the National Institute of Standards and Technologies (NIST) that DISA uses as a standards resource, he stated that his impression was that both government agencies sought to "reverse engineer commercial capabilities," and that cementing technical standards prevented DISA and any of its vendors from providing relevant technologies to US military servicemembers. By codifying certain security standards in policy, DISA is virtually guaranteeing that companies must provide outdated or older technology, and in some cases modify COTS hardware to backwards-comply with their requirements.

Findings

The JRSS represents DISA's organizational commitment to retaining the role of prime integrator and network service provider to the DOD. Of course, there are natural organizational dynamics and interests at play reinforcing this behavior, but DISA is also the charge of DOD Directive 5105.19. That directive mandates that the agency act as the prime integrator for the GIG, and therefore the JIE and DODIN: "DISA shall be responsible for planning, engineering, acquiring, testing, fielding, and supporting global net-centric information and communications solutions…."[54] The military departments have no choice in how they order or manage their network superiority requirements. The Secretary of Defense has directed that the military services' organize, train, and equip responsibilities, as they pertain to wide area networks, be delegated to DISA. Just as networks are becoming more and more integrated into current and future wars, more and more IT services and network architecture and capabilities are being assumed by DISA. To put it another way, information systems are becoming weapon systems, yet are being built, managed, and operated by a non-warfighting support agency. The potential negative consequences of this situation could not be more startling.

Given the necessary and essential nature of network superiority to current operations and future warfare, it cannot simply be assumed that DISA's current path on the JIE and DODIN will provide network superiority to the warfighter.

DISA's broad and expansive network mandate is not just an artifact of DOD Directive 5105.19, but a long-standing inheritance that goes back to 1960. Not even the shortcomings and gaps identified in the JIE are new. Instead, evaluations of past DCA systems sound just as current as today, critiquing DCA's "proprietary low-performing network and mainframe-based hardware architecture, [that] you really could not evolve that into some of the expanded missions…"[55] Without an actual determination and findings to recommend DISA in the spirit of the Economy Act of 1932, the DISA mandate seems more like simple organizational inertia than a real value proposition.

Given the necessary and essential nature of network superiority to current operations and future warfare, it cannot simply be assumed that DISA's current path on the JIE and DODIN will provide network superiority to the warfighter. Wide area networks are not just avenues for the flow of communications to national leadership from the front, or even timely and effective command and control. As warfare becomes more tightly integrated with and dependent on network superiority, these wide area networks must be understood as weapons systems that enable cyber maneuver and other tactical and strategic cyber operations in concert with the US military services, while simultaneously supporting future operational concepts like the combat cloud.

The potential consequences of not establishing network superiority in relation to any competitor or adversary are far too great to continue unexamined. The answer cannot be a simple business case in which networks are treated as a commodity where low priced, technically acceptable is good enough. The more important measure is whether a DISA solution or a commercial solution is more mission effective. That is, which is more able to provide network superiority in a contested environment? To answer the earlier question of should the services be compelled to delegate their network organize, train, and equip duties to DISA, an operationally-focused determination and findings analysis is a valuable guide for a way forward.

Have the military department secretaries and chiefs of staff determined that the inter-departmental network services order with DISA is in the best interest of the US Government?

By virtue of DOD Directive 5105.9 and the other regulations reviewed previously in this paper, the military department secretaries and chiefs of staff have not had the option to certify, assert, or find against an inter-department order to DISA for their wide area network services. It may be implied that the Secretary of Defense has made that determination by virtue of his directive, but a determination by authorization does not make a valid finding.

The "best interest of the government" must mean more than just "cheaper." Especially in the case of network superiority, it must mean that DISA is able to provide a more capable, agile, adaptive,

faster, and robust network than commercial alternatives and adversary networks. Any D&F must be operationally focused. Yet that is not the case at all. This analysis of current performance indicates that the DODIN and JIE lag far behind domestic commercial networks, and that the deficiencies cannot be quickly or easily rectified. The case study of the JRSS, a keystone element in the DODIN architecture, demonstrates the challenges facing DISA in delivering network superiority. The DODIN and JIE is the result of structural, technical, organizational, cultural, and policy obstacles, and cannot support the growing network performance needs of the military services in an efficient or effective way. It is unlikely that DISA will be able to play catch up with the commercial network performance standards of today, much less outpace technological developments that will support network superiority in a near-peer war. A different network services paradigm is required to further develop new operational concepts that can fully exploit the power of networked information both in the traditional military domains and in cyber.

Networks are not a commodity and cannot be treated as such. Network superiority is essential to the evolving way of war; this advantage will directly influence which side prevails in conflict.

Networks are not a commodity and cannot be treated as such. Network superiority is essential to the evolving way of war; this advantage will directly influence which side prevails in conflict. It is increasingly clear that an inter-departmental order for network services is not in the best interest of the military departments or, by extension, the government and the United States. DISA simply does not have the creativity, experience, agility, flexibility, or bureaucratic responsiveness to be able to discard old paradigms or obsolete architectures, develop and exploit emerging technologies, and counter adversary network advances. The DODIN and JIE architecture, hardware, and management do not have the potential to maintain network superiority and services in future combat cloud operations or the ability to effectively cyber maneuver against peer competitors.

As a contrast to inter-departmental contracting, a whole-of-nation approach should be considered with respect to how US power, influence, and reach in both peacetime and war impact a "best interest" analysis. The predatory statecraft of other nations and their corporations begs for a larger aperture in this analysis. Part of the "best interest" determination must include both the opportunity cost of inter-departmental contracting as well as the opportunity lost.

As near-peer and peer competitors identified in the 2018 National Defense Strategy, both Russia and China are using a whole-of-nation approach with their networks. China, in particular, is leveraging the commercial telecom Huawei to expand its national reach and influence across the globe. As a commercial company, Huawei has much more flexibility and maneuver to spread infrastructure and develop network technologies that are also resources for the Chinese government and military. In fact, Article 7 in China's National Intelligence Law, passed in 2017, requires all Chinese companies and citizens to "support, cooperate with, and collaborate in national intelligence work."[56] While this statute focuses specifically on intelligence collection, it clearly sets a trend towards "fuller fusion between the party-state apparatus and commercial enterprises."[57] It is not a broad gulf between intelligence collection and offensive cyber operations or even exploiting those networks for more traditional military actions. The Chinese government is taking full advantage of Huawei's extended reach, robust network, technological innovations, and millions of customers.

DISA's proprietary network simply cannot compete against the capabilities of other nation's commercial companies. Like the inherent value that the US military receives through foreign military sales, taking a whole-of-nation approach to US military-wide area networks would provide the United States reach, relationships, and readiness that DISA cannot create on its own. A whole-of-nation network is more than purchasing COTS racks and processors or leasing layer one physical data transport. Empowering US-flagged telecoms—with their substantial investment and infrastructure—to unleash their creativity, deep experience and expertise, and advanced capabilities to partner and collaborate with the military departments brings all of the best of what the American commercial IT and telecom industry has to bear to ensure network superiority

for US military servicemembers. While it is not the purpose of this paper to delve deeply into a net assessment of DISA network capabilities vis-à-vis the US's global competitors, it must be a consideration in any determination and findings.

Is DISA able to provide the ordered services—that is, network superiority?

The real question about DISA and network services is not whether DISA is able to provide a long-haul backbone but whether DISA is able to provide a wide area network that can ensure network superiority. A network that is merely adequate does not meet the intent of "ordered service," and the foundational nature of networks to current and future warfare means that "good enough" is not in fact satisfactory. DISA is not technically or programmatically able to provide the quality of network required by the military departments to meet their obligations to the nation's security needs.

DISA's hardware-centric, proprietary approach to building the JIE and the DODIN projects tremendous liability for US military servicemembers. The JRSS, the keystone to the DODIN, is a brittle and fragile configuration that does not employ the latest methods and technologies in network security. It cannot monitor, manage, or defend the network as a whole. And because the DODIN relies on a large number of unsynchronized and separate DISA programs to function well, the architecture is cumbersome, imposes cost and inefficiencies on the military services, and has poor functionality. It cannot provide the promised seamless access to and use of cloud services, or other service-specific needs.

The JRSS, the keystone to the DODIN, is a brittle and fragile configuration that does not employ the latest methods and technologies in network security. It cannot monitor, manage, or defend the network as a whole.

This architecture is not easily departed. DISA is not and will not be able to modernize and field advanced technologies or capabilities in a rapid cycle that competition demands. Since they are not a program of record, DISA is dependent on mature COTS technologies, with the resulting limited shelf-life, to construct the DODIN and the JIE. When DISA's time to integrate is layered on top, it drives ever greater delays into the DODIN. Obsolescent security techniques, standards, and policies create vulnerabilities for the US military servicemember, and the overall performance of the DODIN inhibits the military departments' opportunity to exploit the power of information and develop new operational concepts that employ networks as a weapons system. Whether it is supporting new operational concepts like the combat cloud or offensive and defensive maneuver in the cyber domain, by any measure, the DODIN cannot deliver decisive network superiority to servicemembers.

Have the military department secretaries and chiefs decided that network services cannot be provided by contract as conveniently or cheaply by a commercial enterprise?

There are viable commercial service alternatives to DISA being the prime integrator and service provider to DOD's wide area networks, but without the opportunity to make a determination and findings assessment, these network services have not been evaluated with respect to meeting the wide area, end-to-end needs of the military services.

A common objection is that the services have too many different configurations to enable the use of commercial network services. But this challenge is not unique to commercial providers. DISA also must contend with the many disparate configurations of the military services' IT systems. A qualitative difference is that commercial telecom providers are experienced in how to provide effective network services while gracefully transitioning customers to a common, interoperable configuration. Many American IT and telecom providers are experienced in efficiently transitioning the dissimilar configurations of their customers to create automated and mission-effective systems. Furthermore, they can proactively support configuration upgrades as they continue to enhance the capabilities and introduce new technologies to the network.

For US telecom firms, research and development are crucial to maintaining an advantage both against commercial competitors, and outpacing hackers, non-state actors, and other entities who would seek to disrupt or corrupt the network and the information that rides on it for

their own gain. Motivated by market competition, developing advanced capabilities in network services and cyber security are existential issues for these companies. Some executives interviewed for this project indicated that their network investments exceed $20 billion annually. Infrastructure is also another key area of investment. Without high-bandwidth fiber, advanced cell towers, and satellite communications, commercial providers cannot grow their customer base, and risk losing contracts to their competitors. For example, the race is now on for 5G cell network capability. For commercial network providers, network superiority means market share—there is a direct relationship between network quality, superiority, and the bottom line.

With these investments amortized across their commercial customers, domestic IT and telecom companies can offer DOD leading-edge capabilities and innovations at a speed and cost that DISA simply cannot match. DISA cannot produce the same network quality available by today's commercial IT and network service providers, and it most certainly cannot match the speed of their modernization and investment.

It seems intuitive that a US-flagged network provider would be able to deliver network services for less cost than DISA. But for any cost comparison to be valid, the market advantages that commercial business structures have to offer must be allowed.

It seems intuitive that a US-flagged network provider would be able to deliver network services for less cost than DISA. But for any cost comparison to be valid, the market advantages that commercial business structures have to offer must be allowed. Finally, any determination and finding must go beyond a cost-focused business case analysis. An important measure to assess is whether a DISA or commercial solution would be more mission effective in providing network superiority in a contested environment.

In the 21st century, information has become the crucial element to asserting military dominance. Without a strong, robust, and resilient network with reach, the traditional instruments of warfare will be unable to deliver the dominance they once did as individual platforms. Sharing information through networks will have a synergistic impact on the battlespace, with network superiority being the predicate to military superiority. Without one, one cannot have the other. DOD's current approach is not delivering network superiority. The irony is that just as information networks are becoming weapon systems in and of themselves, the entirety of the DOD network—constructing, managing, and operating it—has been bureaucratized by DOD through the use of a non-warfighting agency.

This responsibility must be reexamined. Inheriting defense networks as a legacy of the common communications systems of World War II is not a sufficient reason to continue DISA's role as network provider. As the case study of the JRSS revealed, DISA is years behind network state-of-the-art, and its policies and standards are outpaced by the advancements of technology. The proprietary, hardware-centric way in which DISA is building the wide area networks the US military services depend upon virtually guarantees obsolescence at fielding, and the DODIN is already years behind its intended schedule. While DISA has been empowered through the authorities of DOD Directive 5105.19 and other regulations and guidance, a determination and finding should still be conducted to ensure that the inter-departmental order meets the spirit of The Economy Act. The prime objective, after all, is to secure network superiority for those who would have to fight future wars.

Recommendations

Sharing information has already revolutionized warfare, stimulating new operational concepts, and this competitive dynamic shows all signs it will continue. The goal is to lead in the competition. Network superiority is a non-negotiable requirement for the United States.

As the cycles of technological advancement increases and adversaries close the gaps in long-held US advantages, DOD is falling further behind in its ability to connect the military services across its wide area network. The DODIN is sub-optimized by a hardware-centric approach. Improved systems engineering and a larger network architectural vision is needed that is mindful of keeping pace with the threat against the network. The JRSS case study illuminates these needs and brings to question DOD's ability to deliver network superiority for superiority in information age warfare.

DODIN lags far behind what is available on the commercial market and is not likely to catch up on its present course. DISA's enterprise solutions are less capable and likely more expensive when normalized against what is commercially available. This paper's analysis indicates that DOD's approach may also be in violation of the spirit of the Economy Act when it comes to wide area network services for the military departments.

network superiority must be understood as a critical national resource. Given the essential nature of network superiority to military operations, the DOD must take the lead in assuring network superiority for the United States.

Finally, this paper makes clear that since the 1960s DISA has been executing its mission as DOD and Congress have shaped and instructed the agency to do. That mission is executed around the clock by over 8,000 military and civilian employees who are motivated and dedicated while shouldering an essential part of America's defense. They are constrained, however, by long-term structure and oversight over which they have limited power and authority to change. The critical nature of this paper's findings suggest that change must be facilitated from outside this system.

To provide for the course corrections necessary to deliver network superiority to US servicemembers, the following recommendations are offered for consideration:

1. **Evolve DOD's Understanding of Networks.** The DOD is effectively treating network services as a commodity through the inter-departmental order to DISA. While interoperability and security are stated priorities for the DODIN, this does not mean that the DOD fully understands and appreciates the wide area network as a pivotal warfighting domain. This will require a significant shift in mindset. A bureaucratic, compliance-oriented management culture cannot grasp the network as both a cyber-combat domain and a critical foundation for future operational concepts. Additionally, network superiority must be understood as a critical national resource. Given the essential nature of network superiority to military operations, the DOD must take the lead in assuring network superiority for the United States. This paradigm shift includes treating US-flagged IT companies and telecoms as not just service providers or even as important pillars of the industrial base, but indispensable partners in developing and extending the reach of the nation's network superiority.

2. **Create a Dedicated Center for Network Analysis and Assessment Within the Air Force's National Air and Space Intelligence Center (NASIC).** Network superiority will be a major determining factor in future wars, yet there is no DOD organization dedicated to gathering relevant intelligence on potential adversary network capabilities to inform military planning and assessment. The Air Force should stand up such a center within the National Air and Space Intelligence Center (NASIC) at Wright-Patterson AFB, OH to collect intelligence and make current and predictive assessments on the characteristics, performance, capabilities, and intent of potential adversaries with respect to their wide area networks, and other networks. Similar to how NASIC analyzes foreign air and space capabilities, doctrine, training, and proficiencies, this network analysis center would support the development of operational war plans, network requirements, modernization efforts, and support the maturation of cyber tactics, techniques and procedures—as well as support comparative assessments of US and allied capabilities against potential adversaries.

3. **Revise DOD Cyber Security Standards and Regulations.** Current cyber security structures, standards, and regulations focus on inputs, not effects. Put another way, these standards focus on means, not the ends. The timelines imposed by working group inputs, staffing, approval, publishing, and other normal bureaucratic processes mean that these standards cannot help but be outdated by the time they are released. The cyber threat environment is outpacing these processes. Moving away from a compliance-focused orientation, DISA should refocus on effects-

based security processes and technologies. Such an approach will be more responsive and agile in countering malware and other threats.

4. **Accomplish a Military Department-Specific Determination and Findings Analysis and Recommendation for Network Services.** The current regulatory structure not only fails to require a determination and findings (D&F) to be accomplished for DOD inter-department orders, it empowers the Secretary of Defense to direct the heads of the military services to utilize DISA and fund their defense capital working fund. This may be appropriate for commodity-type orders and services, but the value of information and the networks that allow sharing information goes far beyond commodity status. Any determination and findings analysis must predominantly be an operational evaluation, focused on the qualities of network superiority and competitive advantage, not simply cost. The heads of each of the military departments should be empowered to conduct a detailed D&F in accordance with their own service's current and future network requirements with respect to their unique roles and missions, to include the demands of future operational concepts in contested environments. The determination and findings certified by each of the military department heads should serve to inform their branch's wide area network requirements.

Employing broad, end-to-end network services with US-flagged network providers will provide the military departments greater reach, relationships, and readiness that DISA is fundamentally unable to craft on its own.

5. **Beta Test Commercial End-to-End Network Services.** The liabilities identified in this analysis indicate that DISA has been and will be unable to provide network superiority for the US military departments. Based on determination and findings analyses, each department should have the option to enter into, at a minimum, a beta test of a commercial end-to-end network service contract with the US-flagged commercial provider of their choice. A deliberately scoped beta-test would enable a military department to "walk before running," limit unintended consequences, and develop best practices to extend to the enterprise, while providing data to create an integrated master plan and schedule to successfully expand network services in future option years. In leveraging this comprehensive approach, the departments should seek to cultivate a robust commercial base that strengthens the whole of the domestic IT and telecom industry. Employing broad, end-to-end network services with US-flagged network providers will provide the military departments greater reach, relationships, and readiness that DISA is fundamentally unable to craft on its own.

6. **Embed Cyber Teams in Commercial Network Operations Centers.** A major value proposition for leveraging domestic IT and telecom companies to provide end-to-end networks as a service is that it enables military cyber operators to partner with the provider in military network traffic management and operations. Embedded teams could also have access to global network activity, acting as early warning lookouts, or identifying pattern of life or anomalous activity. Certainly, privacy rights and other legal restrictions must be respected, but even with those limitations there is greater opportunity for network defenders when they partner with commercial providers. Cyber operations require a domain, and that domain is the network. Having embedded cyber teams partner with end-to-end network service providers expands situational awareness, maneuver room, defense response, and operational resiliency.

Conclusion

Network superiority is the foundation upon which all other military actions depend. As stated by Army Gen Martin Dempsey, former Chairman of Joint Chiefs of Staff, "the military that maintains the most agile and resilient networks will be the most effective in future war."[58] Without network superiority, information is degraded, irrelevant, and isolated. It cannot support enhanced situational awareness, cross-targeting, or other advanced operational concepts like the

combat cloud. An inferior network decreases the quality of decision making and command and control, and inhibits the maturation of cyber defense, maneuver, and cyber combat operations. The DOD must challenge its old cyber paradigms and overhaul outdated approaches. If uncorrected, the current course will impede the US military's ability to attain and maintain network superiority.

Approaching the JIE and the DODIN from a hardware-centric mindset that neglects a whole-of-nation approach, DISA is unable to ensure network superiority for current and future operations. A finding from a nearly 50-year old DCA network congressional committee investigation regarding a command and control network system has surprising relevance to DOD's current approach to wide area networks and the global connectivity it provides. "The task force report's dour conclusion was that the United States had failed to deploy command and control systems 'commensurate with the nature of likely future warfare, with modern weapons systems, or with our available technological and industrial base."[59]

American leadership and American military servicemembers who lifted US military prowess to historic heights over the past 50 years would never allow such an ominous conclusion to go unanswered—this is not the time or place to start. ✪

Endnotes

1 Department of Defense Chief Information Officer, *Department of Defense Information Technology Environment: Way Forward to Tomorrow's Strategic Landscape,* (Washington, D.C.: Department of Defense Chief Information Office, 2016), https://dodcio.defense.gov/Portals/0/Documents/JIE/DoD%20IT%20Environment%20Way%20Forward%20-%20DISTRO%20(Aug%202016).pdf, 3-4.

(All links accessed September, 2018).

2 Author's note: The "combat cloud" is the nomenclature used to refer to a future operational concept developed by Lt Gen David Deptula, USAF (Ret.).

3 Author's note: The "kill chain" references the sequence of events necessary to successfully employ weapons against a target: Find, Fix, Track, Target, Engage, and Assess (known as F2T2EA in military parlance). First, the target must be detected (Find); then its position must be accurately located (Fix); position information must be passed to a fire control system so that a track file (a target's position over time) can be established (Track); that track file is designated and passed to the weapon (Target); the weapon is fired and guides to the target (Engage); and finally, the outcome of the engagement must be evaluated (Assess). This process evaluates whether or not the desired outcome was achieved, if the weapon accurately guided, fused, and if the desired effects were accomplished. If the kill chain is, at any point, corrupted, interrupted, or broken, the engagement will be unsuccessful.

4 David Deptula, *Evolving Technologies and Warfare in the 21st Century: Introducing the 'Combat Cloud*, (Arlington, VA: Mitchell Institute for Aerospace Studies, 2016), http://docs.wixstatic.com/ugd/a2dd91_73faf7274e9c4e4ca605004dc6628a88.pdf.

5 David E. Pearson, *The World Wide Military Command and Control System: Evolution and Effectiveness* (Maxwell Air Force Base, Alabama: Air University Press, 2000), 19.

6 Pearson, *The World Wide Military Command and Control System*, 19.

7 Defense Information Systems Agency, "Our History: The Beginnings - The Creation of DCA, 1947-1960, Post World War II /Cold War," July 6, 2018, https://www.disa.mil/About/Our-History.

8 Ibid.

9 Defense Information Systems Agency, "Our History: 1960s," July 6, 2018, https://www.disa.mil/About/Our-History/1960s.

10 Department of Defense, *Defense Information Systems Agency (DISA)*, DOD Directive 5105.19, (Washington, D.C.: Department of Defense, 2006) http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510519p.pdf, 2.

11 Teri M. Takai, *Department of Defense Information Technology Enterprise Strategy and Roadmap,* (Washington, D.C., 2011), https://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf, iv.

12 Defense Information Systems Agency, *Enabling the Joint Information Environment (JIE): Shaping the Enterprise for the Conflicts of Tomorrow* (Washington, D.C: Defense Information Systems Agency, 2014), https://www.disa.mil/About/Our-Work/JIE, 2.

13 Defense Information Systems Agency, *Enabling the Joint Information Environment (JIE): Shaping the Enterprise for the Conflicts of Tomorrow,* 5.

14 US Government Publishing Office, Agency Agreements, 31 U.S.C. § 1535 (2009), https://www.gpo.gov/fdsys/pkg/USCODE-2009-title31/pdf/USCODE-2009-title31-subtitleII-chap15-subchapIII-sec1535.pdf.

15 Author's note: For the Department of Defense, there is further guidance on interagency orders under the Economy Act provided by 48 CFR §17.502-2 "The Economy Act;" DOD Financial Management Regulation 7000.14-R Volume 11A Chapter 3 "The Economy Act;" DODI 4000.19 "Support Agreements;" and 10 U.S.C. §2208 "Working Capital Funds." These layers of regulations and policy only serve to create ambiguity, muddling the issue.

16 The Economy Act, 48 CFR §17.502-2 (2014), https://www.gpo.gov/fdsys/pkg/CFR-2014-title48-vol1/pdf/CFR-2014-title48-vol1-sec17-502-2.pdf.

17 Department of Defense, *DOD Financial Management Regulation*, DOD 7000.14-R Volume 11A Chapter 3 "Economy Act Orders", (Washington, D.C.: Department of Defense, 2000), https://comptroller.defense.gov/Portals/45/documents/fmr/archive/11aarch/11a_03_Feb08.pdf, 3-1.

18 Department of Defense, *Support Agreements*, DOD Instruction 4000.19, (Washington, D.C.: Department of Defense, 2013), https://comptroller.defense.gov/Portals/45/documents/fmr/archive/11aarch/11a_03_Feb08.pdf, 1-2.

19 Working-capital Funds, 10 USC § 2208 (2011), https://www.gpo.gov/fdsys/pkg/USCODE-2011-title10/pdf/USCODE-2011-title10-subtitleA-partIV-chap131-sec2208.pdf, 1107.

20 Defense Information Systems Agency, "Our History: 1990s," June 30, 2018, https://www.disa.mil/About/Our-History/1990s.

21 Defense Information Systems Agency, "Our History: 1980s," July 12, 2018, https://www.disa.mil/About/Our-History/1980s.

22 Department of Defense, *Defense Information Systems Agency (DISA)*, DOD Directive 5105.19, (Washington, D.C.: Department of Defense, 2006), http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510519p.pdf, 2.

23 Ibid., 4, 8.

24 Goldwater-Nichols Department of Defense Reorganization Act of 1986, 10 USC §191 (1986), https://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf, 1019.

25 Functions of Military Departments, 32 USC §368.6 (2002), https://www.gpo.gov/fdsys/pkg/CFR-2002-title32-vol2/xml/CFR-2002-title32-vol2-sec368-6.xml.

26 Department of Defense, Chief Information Officer, *Department of Defense Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise,* (Washington, D.C.: Department of Defense, 2007), www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484389, 7.

27 US Joint Forces Command, *Capstone Requirements Document: Global Information Grid (GIG) JROCM 134-01,* (Washington, D.C: Department of Defense, 2001), www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA408877, 1.

28 Teri M. Takai, *Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap* (Washington, D.C., September 2011), https://dodcio.defense.gov/Portals/0/Documents/Announcement/Signed_ITESR_6SEP11.pdf, 7.

29 Ibid., 7.

30 Department of Defense, Chief Information Officer, *Department of Defense Global Information Grid Architectural Vision: Vision for a Net-Centric, Service-Oriented DoD Enterprise* (Washington, D.C.: Department of Defense, June 2007), www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA484389, iv.

31 US Joint Forces Command, *Capstone Requirements Document: Global Information Grid (GIG) JROCM 134-01* (Washington, D.C: Department of Defense, 2001), www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA408877, 2.

32 US Joint Forces Command, *Capstone Requirements Document: Global Information Grid (GIG) JROCM 134-01,* 5-6.

33 Defense Information Systems Agency, *Enabling the Joint Information Environment (JIE): Shaping the Enterprise for the Conflicts of Tomorrow,* (Washington, D.C: Defense Information Systems Agency, 2014), https://www.disa.mil/About/Our-Work/JIE, 5.

34 Ibid.

35 Takai, *Department of Defense (DoD) Information Technology (IT) Enterprise Strategy and Roadmap,* 4.

36 Department of Defense Chief Information Officer, *Department of Defense Information Technology Environment: Way Forward to Tomorrow's Strategic Landscape,* (Washington, D.C.: Department of Defense Chief Information Office, 2016), https://dodcio.defense.gov/Portals/0/Documents/JIE/DoD%20IT%20Environment%20Way%20Forward%20-%20DISTRO%20(Aug%202016).pdf.

37 Ibid., 7.

38 David S. Alberts, John J. Garstka, Richard E. Hayes, David T. Signori, *Understanding Information Age Warfare* (Washington, D.C.: DOD Command and Control Research Program, 2007), 46.

39 Ibid.

40 Defense Information Systems Agency, *Infrastructure Executive (IE) Directorate: Telecommunications Service Level Agreement (SLA),* (Fort Meade, MD, 2016), https://www.disa.mil/-/media/Files/DISA/Services/Network-Services/SLA/TelecommunicationsSLA.ashx.

41 Author's note: These insights are from the perspective of a senior DOD information technology official, personal communication, July 13, 2018.

42 Author's note: This individual participated in one of nine tiger teams that lasted for two years (2015-2017) to address the fractured, dysfunctional, and disjointed systems that comprise the JIE. No critical answers or solutions were found to bring the various subsystems together in a more integrated, unified whole or elegant architecture. Instead, both DISA and the military services continued to develop work-arounds and side programs to address the seams, gaps, and shortfalls in the JIE. This in itself creates vulnerabilities and levies additional complexity and unnecessary cost on all the military departments.

43 DISA News, "3 Common Misperceptions About the Joint Regional Security Stacks," *CHIPS: The Department of the Navy's Information Technology Magazine*, April 27, 2016, http://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=7782.

44 DOD Director of Operational Test and Evaluation (DOD DOT&E), *FY 2017 Annual Report* (Washington, D.C.: Department of Defense, 2017), http://www.dote.osd.mil/pub/reports/FY2017/, 71.

45 Author's note: While MPLS is a technology that is broadly used across the telecom industry to streamline the routing of data packets, DISA has only recently begun fielding the capability and is treating it as a separate program within the JIE.

46 Senior DOD IT official, personal communication, July 13, 2018.

47 Ibid.

48 Director, Operational Test and Evaluation, *FY 2017 Annual Report*, 69.

49 Director, Operational Test and Evaluation, *FY 2017 Annual Report,* 71.

50 Ibid.

51 National Security Agency Central Security Service, "Commercial Solutions for Classified Program," June 20, 2018, https://www.nsa.gov/resources/everyone/csfc/.

52 General Services Administration – FedRAMP, "FedRAMP: About Us," July 18, 2018, https://www.fedramp.gov/about/.

53 Defense Information Systems Agency, "IASE Security Technical Implementation Guides," DISA, July 18, 2018, https://iase.disa.mil/stigs/Pages/index.aspx.

54 Department of Defense, *Defense Information Systems Agency (DISA)*, DOD Directive 5105.19 (Washington, D.C.: Department of Defense, 2006), http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510519p.pdf, 1.

55 Pearson, *The World Wide Military Command and Control System: Evolution and Effectiveness*, 365.

56 Elsa Kania, "Much Ado about Huawei (Part 2)," Australian Strategic Policy Institute's *the Strategist*, June 5, 2018, https://www.aspistrategist.org.au/much-ado-huawei-part-2/.

57 Ibid.

58 Martin E. Dempsey and Peter Singer, "Defending the Nation at Network Speed: A Discussion on Cybersecurity with Gen Martin E. Dempsey, US Army," presentation (Center for 21st Century Security and Intelligence, The Brookings Institution, Washington D.C., June 27, 2013), file:///C:/Users/hpenney/Desktop/Network%20as%20IT%20Service%20Paper/20130627_dempsey_cybersecurity_transcript.pdf, 12-13.

59 Pearson, *The World Wide Military Command and Control System: Evolution and Effectiveness*, 204.

About The Mitchell Institute

The Mitchell Institute educates about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Series

The Mitchell Institute Policy Papers is a series of occasional papers presenting new thinking and policy proposals to respond to the emerging security and aerospace power challenges of the 21st century. These papers are written for lawmakers and their staffs, policy professionals, business and industry, academics, journalists, and the informed public. The series aims to provide in-depth policy insights and perspectives based on the experiences of the authors, along with studious supporting research.

About the Author

Heather Penney is a senor resident fellow at the Mitchell Institute, where she conducts research and analysis on defense policy with a focus on leveraging the critical advantage aerospace power affords. Prior to joining Mitchell, Penney worked over a decade in the aerospace and defense industry, where she was responsible for budget analysis activities, program execution, and campaign management. An Air Force veteran and pilot, Penney served in the Washington, DC Air National Guard flying F-16s and G-100s, and has also served in the Air Force Reserve in the National Military Command Center.