Industry Study Report

Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR)

A View of the C4ISR Industry in the Combined Joint All-Domain Command and Control (CJADC2) Environment

C4ISR Titans
2023

May 2023

The Dwight D. Eisenhower School
for National Security and Resource Strategy
National Defense University
Fort McNair, Washington, D.C. 20319-5062

Executive Summary

The 2022 National Security Strategy (NSS) illuminates China's economic rise and newfound global influence, underpinning the Chinese Communist Party's (CCP) ambitions of challenging the free and open international rules-based system. After decades of studying the United States, the CCP has undergone a sustained effort to bolster its military to disrupt the U.S. ability to project power. Simultaneously, the CCP is pursuing a concept called "informatized" war to replicate the U.S. approach to network warfare. Both nations rely on their defense industries to outpace their adversaries in this pivotal aspect of great power competition.

Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) is a broad and cross-disciplined industry focused on integrating technology and information systems to enhance a commander's situational awareness and decision-making. Combined Joint All Domain Command and Control (CJADC2) is the DoD's concept to integrate partner nations and service Command and Control (C2) and Intelligence, Surveillance, and Reconnaissance (ISR) systems, thereby allowing commanders to sense, make sense, and act at the speed of relevance. The C4ISR Industry Study examined the health of the U.S. C4ISR industry and its ability to enable CJADC2 technologies relative to its adversaries and propose recommendations for assisting the U.S. effort.

Great power competition has led to the continued growth of the global C4ISR industry. The U.S. market alone is valued at $61.51 billion and covers 678 programs. Comparing the U.S. C4ISR industrial base with that of China and Russia through Porter's Five Forces model, we determined that the United States holds a slight advantage over China due to the competitive forces amongst rivals and the fact that China's technological advancements and industrial base have yet to ween their dependency on foreign technology, although they are aggressively pursuing self-sufficiency.

Despite a robust C4ISR industry, the United States faces many challenges to achieving CJADC2 due to its policy and doctrine, communications environment, and institutional culture. The national security environment demands innovation, speed, agility, and affordability. However, the systemic forces underpinning the balance amongst these factors need to be addressed to adapt to the unprecedented rivalry in global competition.

From a policy and doctrine perspective, the cycle of requirements tied to CJADC2 capabilities and funding continues to fuel the C4ISR industry, but inflexible funding and the requirements-based acquisition strategies are directly opposed to innovation. The Federal Acquisition Regulations dissuade innovation among large defense primes and challenge start-up companies. Additionally, stakeholders across the ecosystem need help to work together because CJADC2 is a process rather than a product. To date, the DoD has accepted many definitions and embraced a federated approach to capability development in the interest of speed. However, a more coherent integration plan is required to tackle the challenge of "making sense" of the voluminous data available as networks proliferate. Finally, two of the primary offices integrating efforts, the Chief Digital and Artificial Intelligence Office (CDAO) and Joint Staff's Command, Control, Communications and Computer/Cyber Directorate (J6), are not responsible for establishing or monitoring the commander's informational requirements leading to an

understanding of the operational environment. As a result, they continue to focus on establishing connectivity between communication nodes rather than the broader effort of delivering decision superiority. To bridge these gaps, we recommend:

- CJADC2 implementation should be owned by the Operations Directorate (J3) and supported by the Combatant Command and Service's Operations Directorates;
- The DoD should focus on its role in the innovation ecosystem rather than trying to recreate an internal ecosystem; and
- Leverage Small and Medium-sized Enterprises to promote competition among firms.

The DoD continues to struggle in the communications environment. It has yet to create an optimal Planning, Programming, Budgeting, and Execution (PPBE) process for fielding interoperable C4ISR systems that satisfy CJADC2. It continues to lag behind the commercial market in developing, fielding, and modernizing cutting-edge technologies with the agility necessary to continue the CJADC2 evolution. It continues to invest in hardware-centric systems to enable decision-making instead of leveraging the software acquisition approach that can deliver the speed of information required for tomorrow. To bridge these gags, we recommend:

- Adopting a C4ISR As-A-Service model (C4ISRaaS) as a cost-effective solution to rapidly upgrade capabilities by leveraging advancing commercial sensors, communication pathways, data management/integration platforms, and user interfaces to satisfy C2 and ISR requirements; and
- Prioritize acquiring advanced software-driven technologies and platforms.

The DoD must shift from a culture that assumes freedom of action in a unipolar world to understanding the need for alliances and partnerships. As such, CJADC2 efforts must prioritize interoperability with mission partners and alliances to ensure rapid and widespread information sharing as a foundational pillar of the CJADC2 implementation strategy. The current practice of over-classification inhibits internal efforts for joint interoperability and presents significant obstacles to working with allies and partners. Furthermore, the DoD must recognize that it is not the global leader in every technology. To bridge these gaps, we recommend:

- Writing data-centric policies for information release at different classifications;
- Assist with building partnerships amongst Indo-Pacific, Euro-Atlantic, and other regional partners;
- Find opportunities to link our defense industrial base with partners;
- Create a fully proven trust chain and data highway to safeguard and verify data sources, vehicles, and receivers; and
- Align structural incentives to streamline acquisition processes.

The U.S. C4ISR Industry possesses the capability and capacity to deliver CJADC2, but it will take leadership to develop, communicate, and acquire the required technical solutions. The federated approach to date has been helpful in determining the requisite technologies and increasing connectivity. Still, it is ready for an evolution toward a more deliberate approach that pursues an initial solitary vision.

Table of Contents

Industry Study Overview

Core Problem Statement

Combined Joint All Domain Command and Control (CJADC2) is DoD's concept to integrate Command and Control (C2) and Intelligence, Surveillance, and Reconnaissance (ISR) systems across services, joint formations, and allies and partners, allowing commanders to "sense, make sense, and act" in a faster decision cycle. Deputy Secretary of Defense Kathleen Hicks directed Department leaders to "ensure all DoD data is visible, accessible, understandable, linked, trustworthy, interoperable, and secure" in her 2021 "Creating Data Advantage" memo.[1] For two years, joint and service commanders and leaders have sought to operationalize the JADC2 concept at the tactical, operational, and strategic levels. This has materialized in short-term band-aids, mid-term testing and evaluation, and long-term intentions to connect everything to everyone by breaking down the proprietary walls around the defense industry's data and architecture to ensure systems produced by multiple vendors can be seamlessly integrated.

In May 2023, the DoD officially changed JADC2 to CJADC2 to emphasize the importance of interoperability with partners and allies "from the beginning," according to Lt. Gen. Mary O'Brien, J6 Director and Chief Information Officer.[2] Across DoD and industry, each stakeholder had a different interpretation of the problem CJADC2 intended to solve, what it would mean for their organization, and how each would solve those problems. As each stakeholder examines the problem from their lens, they naturally come to different conclusions. Additionally, each acute conflict will present new and different challenges for integrating with partner nations. We came to understand that defining CJADC2 across differing DoD and Industry organizations is a challenge, but perhaps an even greater challenge is creating an architecture for CJADC2 that allows it to evolve over time.

Methodology

The Seminar analyzed the Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) industry through a broad lens with visits to various government defense organizations driving requirements and developing new capabilities along with the many industry partners seeking to meet their needs. We then used CJADC2 as a medium to examine the market forces. Finally, we conducted field studies with stakeholders across the ecosystem to gain a deeper understanding of the defense industry's relationships.

Who We Are

The AY 2022-23 C4ISR Industry Study Seminar is comprised of twelve Eisenhower School students from DoD and the Department of State, representing diverse functional backgrounds. COL Karen Briggman (USA) and Mr. George Laskey (NSA) directed the academic program. We also analyzed prominent C4ISR firms as part of a companion course, Industry Analysis, conducted by COL Steven Hanson (USA, ret.) (See Appendix B for Industry Analysis Brief).

Figure 1: C4ISR Industry Study Participants

Summary of Field Studies

We visited organizations and firms in the National Capital Region, Norfolk, VA; Boston, MA; San Diego, CA; Las Vegas, NV; Dallas and Austin, TX; and Honolulu, HI. Additionally, we had virtual engagements with Thales, UK and The French Institute for International and Strategic Affairs. Discussions engaged representatives from a wide range of industries, including several of the large publicly traded defense primes, medium-sized firms looking to expand, and smaller private start-ups seeking to determine government requirements. We also visited several Federally Funded Research and Development Centers working with academia to solve discrete problems and develop emerging technologies to meet the DoD's needs. Finally, we visited INDOPACOM, joint components, and industry partners to understand the emergent challenges in the context of the pacing threat, and how the lead combatant command and services are solving for a solution.

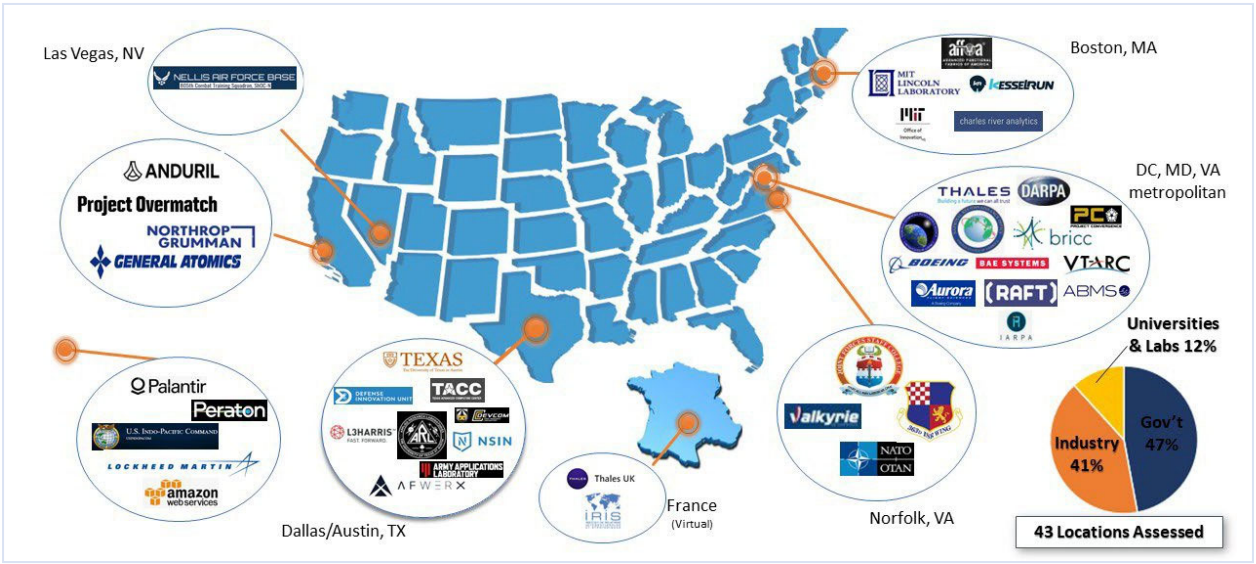

Figure 2: C4ISR Industry Study Field Visits

C4ISR Overview

"C4ISR involves integrating technology and information systems to enhance decision-making and situational awareness on the battlefield."[3] The C4ISR industry provides the critical enabling technologies to ensure U.S. national security leaders have access to the right data at the right time and delivered in a manner to enrich the planning and decision-making cycle.

C4ISR encompasses several inter-related spatial and temporal warfighting functions. *Command and Control* is the art and science of synchronizing joint warfighting functions to maximize "[t]he exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission."[4] In plain language, C2 can be understood as authorities to conduct a mission (the "who"), the forces to execute the mission, the technology, and platforms for the forces to use on the mission (the "how"), the time and schedule for mission execution ("when"), and the geographic area in which the mission will be conducted ("where").[5] According to the DoD dictionary, *Intelligence, Surveillance, and Reconnaissance* is an integrated intelligence and operations function that "synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations."[6] Commanders issue intelligence needs, and the assigned intelligence collection and analysis forces attempt to answer those questions using organic, theater, and national intelligence assets.

The remaining "C's" in C4ISR are Communications and Computers. *Communication* is the throughline for all warfighting functions and exists in many modes, from morse code and semaphore to fiberoptic and satellite communications. The architecture must be scalable, secure, resilient, and redundant to ensure commanders and forces are always connected to pass information and orders. Finally, if *Communication* is the throughline, *Computers* are the physical infrastructure that enables it. Advanced computing is the new disruptive technology of the 21st century. Computers today include the vast new capabilities that exist in virtual servers ("the cloud") and also the new high-speed semi-conductor computer chips that drive the latest artificial intelligence and machine learning (AI/ML) capabilities to process, store, and analyze the data. Advanced computer networks and multiple communications paths ensure information is available at the time of need so commanders and U.S. senior leaders can achieve decision superiority over adversaries.

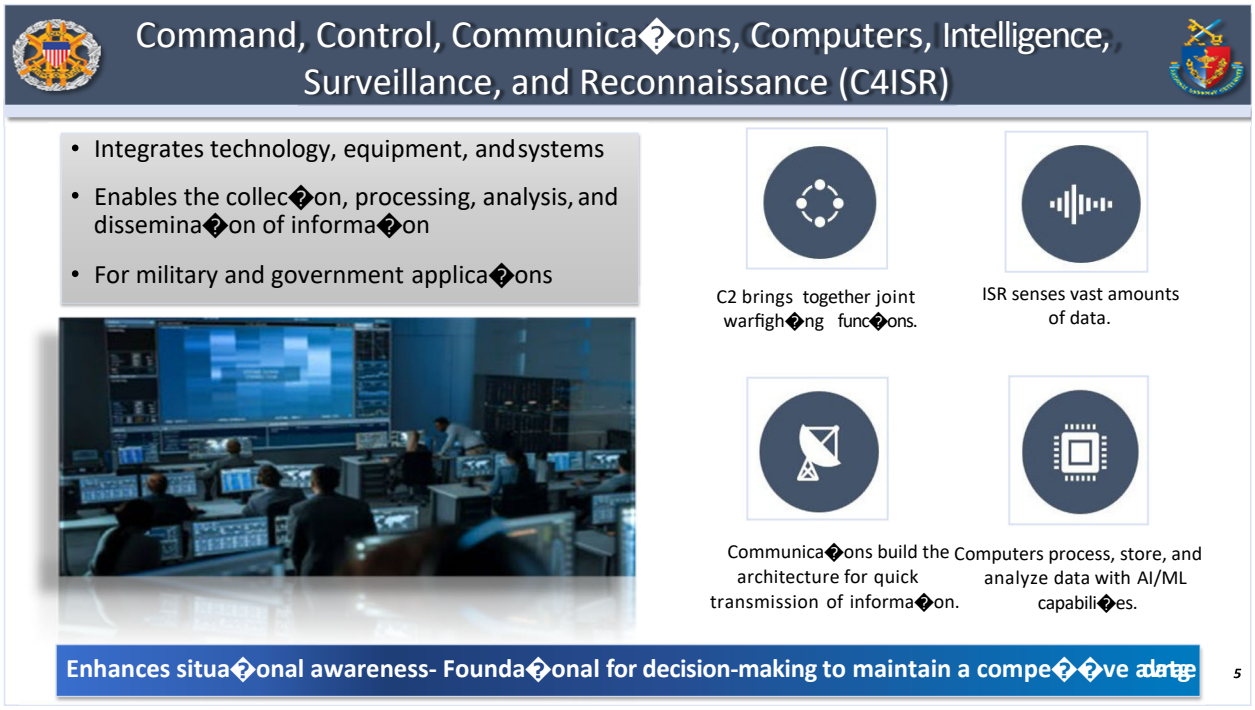

Figure 3: C4ISR Systems Overview

DoD Environment

Even before Advanced Research Projects Agency (ARPA) created the precursor to today's internet and the corresponding network-centric approaches employed during Operation Desert Storm, former Secretary of Defense Robert McNamara approved and pressed for one of the earliest electronic experiments during the Vietnam War. These actions enabled automated decision-making, creating one of the first electronic battlefields using sensors (acoustic and seismic), Air Force aircraft, and a computerized command center, highlighting the importance of leveraging novel technology to create strategic decision advantages.[7] That ARPA scientific experiment was called the "ARPA Barrier" (also known as the "McNamara Line," referencing to the French Maginot line).[8] Though not entirely successful, this technological advance was instrumental in rapidly increasing the ability to take battlefield changes and targets and synthesize them into kinetic decisions and actions.

However, senior DoD leaders inconsistently supported testing and utilization of advanced technologies. In a 2002 article, then-Vice Admiral Robert "Rat" Willard cautioned against relying on the new technologies that were being introduced within the C2 arena when he stated, "the root tenets of command and control are timeless—but they have been lost in the chase for new technologies."[9] Yet, by this time, the People's Republic of China (PRC) was already developing the advantages of building a force around "informatized" warfare.[10] DoD leadership has since attempted to synchronize disparate service systems and technologies through a number of operational concepts, like the Joint Fires Network (2003) and the Air-Sea Battle Concept (2013), none of which have achieved the desired end state.[11][12]

As part of the Joint Chiefs of Staff (JCS) efforts to align resources across the DoD, the JCS published an overall JADC2 Strategy Implementation Plan in March 2022, documenting the

"urgent need for a focused Departmental push on actions and to empower our Joint Forces Commanders with the capabilities needed to command the Joint Force across all warfighting domains"[13] Based on our field studies; however, the predominant aspect that seemed to be constant across governmental agencies, the services, and industry is that there is still not one focused effort to achieve CJADC2. Indeed, one Joint Staff representative highlighted that they continue working to "flip from Service Perspective to an Enterprise Perspective." Still, this goal and vision have yet to materialize from our research visits.

Industry Environment

Lockheed-Martin's public facing website indicates, "C4ISR is the foundation of every mission."[14] This statement codifies how integral and important C4ISR capabilities are to today's industrial sector components as they support the U.S. defense market. Large Defense Industrial Base (DIB) firms, such as Lockheed Martin, General Dynamics, Boeing, Raytheon, and Northrop Grumman primarily provide 'capability' to fulfill DoD's vision of interconnected sensors and data processing enabled by AI/ML computing technologies, resulting in decision superiority for commanders. As such, the DoD has a monopsonistic effect on these larger companies and, to a degree, adds complexity and barriers to entry for smaller C4ISR firms with some of the latest software and innovative technologies that may benefit the DoD.

In a review of the overall C4ISR sector, an industry analysis firm predicts expansion in the C4ISR market given the dual-use nature of the components and capabilities within the industry will "grow at a compound annual rate of 4.2% through 2021 to 2029, reaching nearly $166 billion."[15] One of the critical areas of our visits highlighted that large prime contractors are vertically aligning to CJADC2, with applicable changes and updates to their niche legacy capabilities to maximize their past investments. In contrast, small-to-medium-sized companies were interested in gaining knowledge on how to integrate into the larger DoD acquisition and procurement processes for their innovative capabilities and efforts. They were not consistently associated as a subcontractor on a prime contract and thus could not afford the initial effort to develop and then subsequently submit their proposals for review by the DoD.

Within the C4ISR industry, technological advancement around data-centric systems carried the most interest for both large and small companies. Hence, strategies to leverage the DoD research, development, and test and evaluation (RDT&E) funds, currently at a record $145 billion, are critical for firms of all sizes.[16] Though most firms are aligning their business segments to produce CJADC2 solutions, many are taking a cautious approach. Industry needs to see DoD tie CJADC2 money to a specific program objective memorandum located in the President's Budget. Additionally, firms likely would be more willing to commit R&D risk to developing CJADC2 capabilities when they see Congressional authorizations and appropriations in the annual National Defense Authorization Act (NDAA).[17] Ultimately, the cycle of requirements tied to CJADC2 capabilities and funding continues to fuel the strategic environment and stronger stakeholder interests within the C4ISR industry.

Strategic Environment

Building cohesive security strategies is increasingly difficult in today's complex global security environment. The 2022 NSS characterized the next ten years as the "decisive decade," which will set the terms of our strategic competition with the PRC, Russia, and other geopolitical threats.[18] Globalization through the post-Cold War years increased interconnectedness among countries and the recent rise of autocracy and nationalism is threatening to upend decades of relative peace between world powers.

Nations are deeply connected through open trade, supply chains, and financial markets subjecting them to conflicts, natural disasters, or mishaps a world away. This was evident as the COVID-19 pandemic ravaged the world, disrupted global supply chains, induced economic hardship, and elevated inflation, which persists to this day. The United States realizes it can no longer pursue a policy of uncontested dominance in the Indo-Pacific, and it must work by, with, and through our allies and partners to increase national security capabilities and capacity in response to shared challenges.[19]

The Russian Federation's escalating aggression since 2008 is forcing national security changes among liberal democracies, following decades-long post-Cold War peace. Vladimir Putin's actions seek to upend the liberal democratic world order. China's economic rise has increased its global influence, fueling the CCP's ambitions of challenging the free and open international rules-based system. The CCP has put economic power at the core of its strategy achieved through significant investments in disruptive technical innovation and advanced manufacturing, of which a significant amount is acquired through intellectual property theft or coerced hand-over. Former National Security Administration director and U.S. Cyber Command commander, General Keith Alexander, once called the CCP's efforts the "greatest transfer of wealth in history."[20] China's economic plan is driven by two major programs: **"The Belt and Road Initiative (BRI)"** envisions the integration of Europe, Africa, Asia, and even Latin America into an economic system with China at its center, and **"Made in China 2025"** envisions manufacturing dominance in strategic industries from robotics to shipping and aerospace.

Stakeholder Interests

The current national security environment demands innovation, speed, agility, and affordability.[21] Notably, the ways to achieve these are inherently challenged by the U.S. acquisition system or the innovation process itself. The system necessitates flexibility in funding and requirements, a vision for innovation, funding for development, competition, and persistent pursuit of an innovation. Fundamentally changing how the DoD pursues capability development could address these internal challenges and acknowledge stakeholder interests.

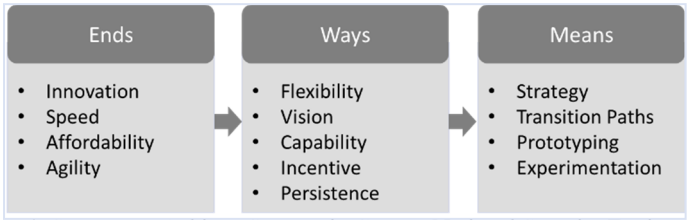

Figure 4: Strategy to Achieve Success in Current National Security Environment

The Joint Capabilities Integration and Development System is a capability-driven requirements process used by the DoD to identify, assess, and prioritize military capability requirements. Within this process, the Joint Requirements Oversight Council aims to validate, prioritize, and resource joint military requirements.[22] This centralized process produces platform-centric requirements rather than defining capabilities at a higher level. Defining capabilities at a higher level, or simply defining the problem, risks a lack of specificity that Joint and service requirements authors struggle to embrace.[23]

Congress is granted the authority to authorize and appropriate money in the Constitution. However, it is unlikely Congress will provide sufficient funding to support innovation.[24] This dynamic drives a deeply entrenched platform-centric budget development process. Prototyping requires an iterative development approach that fuels the majority of successful innovation, yet necessitates flexibility in funding and requirements that is directly at odds with the current budget approach. Although reforming the budgeting process could grant flexibility for innovation, any change could compromise the transparency Congress requires.

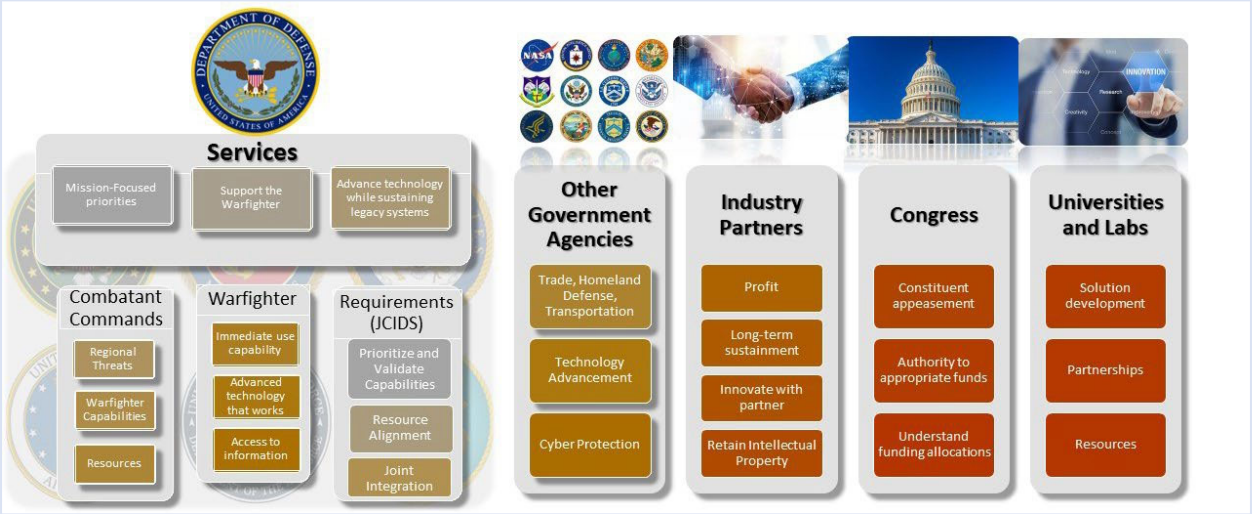

Figure 5: C4ISR Key Stakeholders Overview

The customer's lack of vision is a well-recognized challenge inherent to innovation and represented in the quote often misattributed to automobile innovator Henry Ford, "if I had asked people what they wanted, they would have said faster horses."[25] The late Harvard economist Clayton Christensen explained that good business decisions hinder innovation as businesses overlook disruptive innovations in part because the tools and metrics for analysis are inadequate to convince decision-makers of the value of innovation.[26] If people are challenged to recognize the value of innovation, they cannot be expected to articulate requirements for innovation.

The capability to innovate refers to the adequate capital to invest in innovation while incentive refers to the competition to fuel innovation. Industry determines investment strategies based on where the potential profit merits the risk. R&D efforts generate minimal profits, even when subsidized or funded by the DoD, and firms are more inclined to chase major acquisition programs with large production numbers and long-term sustainment, where most profit potential resides.[27] As the defense industry strives to understand whether the return on investment is worth

the risk, it requires both sufficient competition and funding to justify the investment. The government can reduce the risk to industry by supplementing innovation investments and providing clear, persistent indications for future profit opportunities.

The defense industry responds directly to government inputs and strives to echo the same message when offering examples of how a firm can satisfy government requirements. Industry leaders dissect speeches, articles, budget documents, and conversations trying to understand the evolving priorities and vocabulary to help their company grasp what products and technology it can leverage to meet pending requirements. The challenge related to CJADC2 is that the concept is a process, not a product. It is a process that involves the entire kill chain or kill web in all domains and all services at the tactical, operational, and strategic levels. While DoD looks to industry to develop innovative technologies and solutions, DoD must provide problems to solve, requirements to be satisfied, and capabilities to be developed. Consequently, industry is struggling to infer what DoD desires because the government is struggling to translate the CJADC2 concept into a business line in which firms can justify risk and compete for profits.

C4ISR Competitive Assessment

I. Assessment Overview

The C4ISR industry generates the applications that equip modern militaries. As such, an intense competition has developed among the major global powers for dominance over frontier technologies. In 2017, Russian President Vladimir Putin declared "the one who becomes the leader in [AI] will be the ruler of the world."[28] And Beijing has set 2030 as the year by which it will emerge as the global AI leader.[29] For its part, the United States is well placed to win the AI race and is increasingly funding indigenous talent and hardware, according to Center for a New American Security Paul Scharre.[30] To assist with understanding the relative capability of each country's capacity to reach its goals, we conducted a competitive assessment of the domestic C4ISR industries of the United States, Russia, and China using Harvard Business School Professor Michael Porter's five force forces model.[31] The model encompasses the following critical strategic factors: the Bargaining Power of Buyers, the Bargaining Power of Suppliers, the Threat of New Entrants, and the Threat of Substitute Products or Services.[32]

II. U.S. Overview (C4ISR Growth Around CJADC2)

Complexity within the C4ISR industry stems from the fragmented, yet symbiotic interplay between seven market segments – C2, communications, computers, intelligence, surveillance and reconnaissance, and finally, electronic warfare.[33] Further, the military domains of air, land, sea, space, and cyberspace complicate the product offerings for the firms competing within the C4ISR sector. Market fragmentation has led most large firms to leverage their commercial and defense portfolios to offset downturns that arise from uncontrollable external events (e.g., Russia's invasion of Ukraine, increased tensions with the PRC, or climate change). Even with the uncertainty within the industry, industry experts such as Frost and Sullivan remain upbeat over C4ISR's growth trajectory given the duality and segmentation across the market. C4ISR programs grew to a $61.51 billion industry in FY 2023 covering 678 programs. Additionally, U.S. budget documents over the past two years indicated the DoD has received more than $130 billion in RDT&E funds,[34] with the President requesting $145 billion for the upcoming fiscal year. In 2023, the Navy and Marine Corps have made the plurality of C4ISR investments (i.e., 32.5%; $19.94 billion – See Figure 1).[35] Overall, profit opportunities for C4ISR firms remains promising.

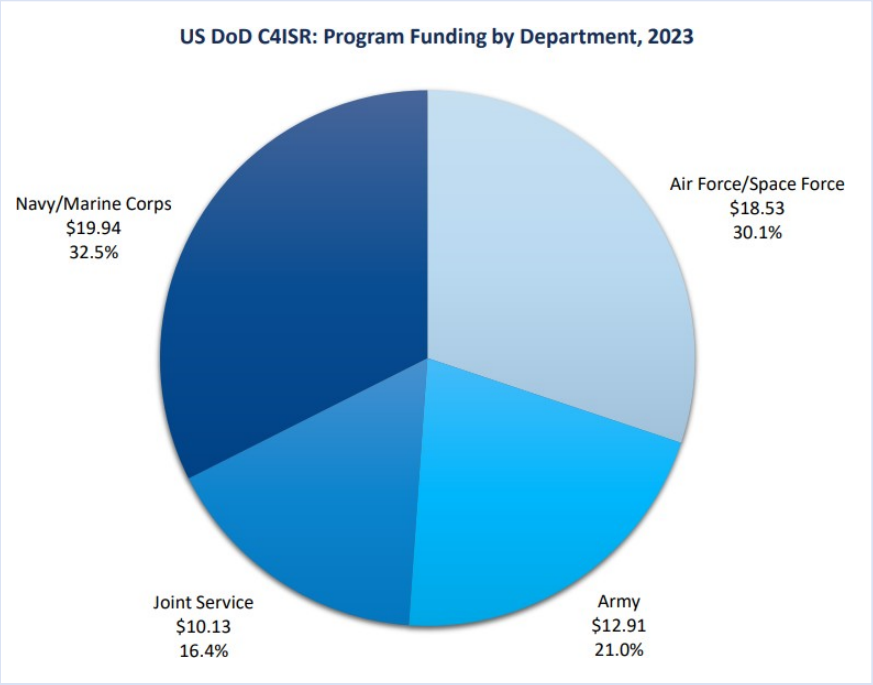

Figure 6: Source: DoD Comptroller; Frost & Sullivan

Porter's Five Forces Analysis: U.S. C4ISR Market

The U.S. C4ISR industry faces many diverse and daunting challenges. Internally, it is competing with the wider commercial technology sector for talent skilled in advanced programming and engineering. Externally, the industry is striving for technological advantages against the growing technology prowess of autocracies such as Russia and China. Therefore, U.S. actions to expand its capacity, capability, and resiliency within the C4ISR industrial base are crucial as the DoD continues to leverage CJADC2 to modernize the joint network for its continued shrinking and technology-dependent military forces. The critical task for the DoD is to use innovation and practical science and technology improvements to accelerate, outmaneuver, and overmatch U.S. adversaries to deter conflict and win if needed.

Following 20 years of low-end counter-terrorism conflicts and rebuilding efforts in Iraq and Afghanistan, the U.S. military is refocusing on advanced threats in the C4ISR environment. DIB firms of all sizes are adapting and developing new technologies and products to meet the military's needs to deter and defeat peer adversaries. CJADC2 demands new methodologies and advanced technologies from the C4ISR market to address our adversaries' technical and warfighting advancements. The primary challenge for the C4ISR industry at this point is managing risk and maintaining profitability while balancing production and support to legacy systems that have yet to reach end of service life and developing new systems that meet CJADC2 concept needs.

Porter's Five Forces are best viewed as the competitive interactions between buyers and suppliers, and similarly, the competitive struggle between new entrants and potential for new substitutes within the C4ISR marketplace. Intermixing within these interactions is the intensity of the rivalry between the overall stakeholders. The DoD maintains a relatively monopolistic

hold over the C4ISR DIB and like other defense sectors, the big five defense prime contractors have a dominant presence competing for large contracts. Importantly, these contracts are the primary demand signal for C4ISR firm to balance profitability risk against investments in maintaining product development and critical resources such as skilled labor. As such, if the demand signal for novel technologies is not communicated to and interpreted by the C4ISR industry as profitable, these vital capabilities will remain aspirations for the CJADC2 vision.

Turning to the interaction between the new entrants and substitutes, this dynamic is of **low to moderate** threat, primarily due to the legacy and expensive platform nature that exists within the DoD for C4ISR capabilities. Indeed, expert C4ISR industry analysts have articulated that the C4ISR market is primed for "collaboration between previously disparate industries," which is currently taking place in the Ukrainian war effort.[36]

Summary of Five Forces Analysis: U.S. C4ISR Market

Threat of New Entrants: The U.S. C4ISR market presents a *low to moderate* threat of new entrants due to specific barriers to entry. Establishing a presence in this market requires significant investments in R&D, specialized knowledge of defense regulations, and access to advanced technologies. The presence of established defense contractors with historical customer relationships and expertise creates a challenge for new entrants to gain market share. Additionally, Defense primes often acquire smaller companies to reduce competition or to gain sector expertise in desired expansion areas. There are some markets, like satellite communications, which benefit from dual-use technologies, miniaturization of computing power, and the decreasing costs of space launch. Dual-use companies such as Starlink, Anduril, and Palantir continue to push into the DIB by augmenting and in some cases replacing legacy systems, the threat will become more prominent. However, DIB profits remain slow and steady and the opportunity cost for startup companies trying to enter the C4ISR market with cutting-edge software or data management tools could be a 10x-20x growth valuation in the commercial sector.

Bargaining Power of Suppliers: Suppliers in the U.S. C4ISR market hold *moderate* bargaining power. The market relies on various suppliers for components and technologies, leading to a diverse supplier base. Suppliers with specialized technologies have greater bargaining power, especially when they provide critical components or systems.

Bargaining Power of Buyers: The U.S. government holds *significant* bargaining power as the primary buyer in the C4ISR market. The government's defense budget and procurement policies shape the market's demand and size, and a contracting emphasis on cost-effectiveness and value for money provides leverage in negotiations. Furthermore, the government's strict requirements and regulations limit the bargaining power of individual contractors.

Threat of Substitutes: The threat of substitutes in the U.S. C4ISR market is *low*, but could change to moderate in the mid-term. C4ISR capabilities are essential for effective military operations and cannot be easily replaced. While some components or systems may have alternatives, the comprehensive integration and effectiveness of the C4ISR architecture make it challenging for substitutes to replicate its exquisite capabilities thoroughly. As the C4ISR

industry shifts from 'network-centric' to 'data-centric,' prime contractors could encounter new challengers that are marketing "C4ISR As A Service" like Kratos, Maxar, Hawkeye360, Dataminr, and Starlink, that instead of selling hardware and software for the DoD to purchase and maintain, provide services like secure communications and intelligence analysis from commercially-owned space and terrestrial sensors, along with publicly available information.

The Intensity of Competitive Rivalry: The U.S. C4ISR market experiences ***high*** intensity in competitive rivalry. Established defense contractors compete for contracts and market share, continuously innovating to offer advanced solutions and maintain a competitive edge. Competition is primarily based on technological capabilities, performance, reliability, and cost-effectiveness. However, rivalries are often satiated through "competimate" strategies, where one prime wins the overall contract, but sub-contracts portions to other prime contractors. The C4ISR market is platform dependent, and the overall defense market is platform limited. Therefore, several opportunities exist on every major platform contract for firms to contribute with sub-system capabilities, thus creating access to potential profits.

III. Russia Overview (Superiority of Management Doctrine)

Russia has a long history of leveraging regional conflicts for testing operational capabilities. In Syria, Russian forces sought to increase their "Superiority of Management," defined as making better decisions faster than opponents.[37] This concept compares to the U.S. network-centric warfare, vice the newer data-centric view of CJADC2. Superiority of Management includes internal C2 and countering adversary C2 capabilities and the objective is to gain battlefield awareness from the tactical to the strategic at the National Defense Control Center (NDCC) in real-time. The NDCC is a central hub to operate with unified data and communications and includes military and other government agencies responsible for national security.

'Superiority of management' developmental goals include creating a unified information space, planning operations, fostering operational creativity and initiative, gaining advantage in information warfare, and conducting electronic warfare. Russian forces in Syria displayed two capabilities essential for future wars: (1) a whole of government-integrated command structure; and (2) an expeditionary military headquarters. Tactical drone imagery feeds were piped into the Kremlin, allowing battlefield information to be viewed and acted upon by senior leaders. Historically, Russia's command structure divided the country into geographic sectors, a construct not designed for power projection. The 'superiority of management' succeeded in Syria by transforming the command structure into a central, single commander directing all aspects of Russia's national security apparatus. Russia's success in Syria did not translate to Ukraine, where its central command model undermined its battlefield operational command.

Russian C4ISR Military Industrial Base

Until the 2022 Ukrainian invasion, the world perceived Russia as a Great Power. Russian President Vladimir Putin's desire to rebuild the Soviet-era sphere of influence seemed almost within reach. Through 2021, Russia experienced 15 years of growth under Putin's regime, prompted by the investments, privatization, and free-market capitalism installed under his

predecessor, Boris Yeltsin. Russia's economy grew an average of 7% per year, and its booming oil revenue allowed Russia to repay all Soviet Union debts by 2006.[38]

Although Russia rejoined the World Trade Organization in 2012, a decline in oil prices and the COVID-19 induced health crisis sent the Russian economy into recession. Then in February 2022, Russia invaded Ukraine and came under withering criticism and economic sanctions that compounded its already challenging financial environment. Other factors influencing Russia's economic standing include reduced and aging population rates that potentially lower future gross domestic product (GDP), high inflation rates further affecting elevated poverty levels, and unreliable court systems driven by widespread corruption. Russia enacted monetary and fiscal policies to aid and maintain a surplus cash reserve ratio. Nonetheless, it is a closed market with systemic issues due to the strong capital-controlled government regime.

Limited access to reliable financial data makes a U.S. comparative analysis somewhat circumspect for public consumption. For the C4ISR market, the Ukrainian invasion revealed critical gaps in Russia's technological capabilities. Increased sanctions by Western countries decreased Russia's access to supplies and materials to replace articles damaged in the war, further challenging Russia's technological advancements. Russia still maintains some comparative export advantages for oil, minerals, and precious stones. Interestingly, per Trading Economics, Russia's Purchasing Managers Index factor is expanding greater than both China and the United States.[39] Leveraging publicly available data available, below is a structured market analysis using Michael Porter's Five Forces Framework.[40]

Summary of Five Forces Analysis: Russian Market

Threat of New Entrants: The threat of new entrants in the Russian C4ISR market is *low* due to the monopolistic environment by state-owned corporations. Prior to the Russian's Ukrainian invasion, the country contained a well-established industrial base, a skilled workforce, and extensive natural resource reserves, including oil, gas, and minerals. The country's 2019 roadmap described the adoption of information and communication as the groundwork foundation of artificial intelligence.[41] However, the invasion changed the landscape, in part due to surprisingly large military losses, expanded conscription, and a mass exodus of technically skilled Russian labor emigrating to safer countries. These combined factors specifically affect men in the 18-27 age group, which will adversely affect future population growth in the outyears, as well as decrease industrial workforce capability.

Russia's ability to foster opportunities for new entrants and capabilities is increasingly hindered by the government's prioritized focus on the war. Combined with the multitude of sanctions, the market is hampered by the lack of focus on technology advancement research. A Yale analysis identified more than one thousand companies suspended or limited actions with Russian technology companies.[42] Many were crucial to the country's R&D activities in the C4ISR and artificial intelligence market.[43] The Russian government implemented protectionist policies making it even more difficult for foreign companies to enter the already limited market.

Bargaining Power of Suppliers: The Russian government maintains strict controls over the production market, both in price levels and output expectations, ***limiting*** the bargaining power of suppliers. The Kremlin forces suppliers to maintain prices, regardless of inflation, and directs companies to produce specific commodities, even if they are not additive to GDP. Compounding the inefficient financial controls, Russia also faces significant challenges related to corruption, bureaucratic inefficiencies, and geopolitical tensions that discourage foreign investment and foreign military sales.[44] The Ukrainian invasion further disrupted supplier capabilities because of the extensive international sanctions placed against the government, affecting access to critical manufacturing material.

A comprehensive evaluation conducted by former Russian Deputy Energy Minister Vladimir Milov identifies the supplier approach as failing, addressing inferior manufacturing and quality control as a significant factor, with manufacturing contracting by 4% in late 2022. This is partially due to complex product development that requires significant international cooperation to ensure cost competitiveness and satisfactory quality outputs.[45] One positive trend is Russia's closer ties with China and other emerging economies, such as India, which could provide alternative markets for its suppliers and result in technology sharing between countries.

Bargaining Power of Buyers: The bargaining power of buyers is ***high*** in Russia due to limited consumer purchasing power and the dominance of state-owned enterprises in many sectors. The challenges for suppliers also impact buyers that are not state-owned corporations. The Russian government is the primary defense equipment buyer, providing substantial bargaining power over the manufacturing industry focus and direction. Russia does not import many military systems, so there is strong buying power over foreign military equipment suppliers. The result of the dwindling global capital for Russian buyers is a reduction of companies that choose to operate within Russian state-owned enterprises.

Threat of Substitutes: The unique nature of C4ISR capabilities results in a relatively *low* threat of substitutes, especially for a network-centric Russian military that still relies on iterative improvements to legacy systems. If the Russian government regulations allow businesses to operate more freely, there is a better chance for innovative technologies to offer value to Russian consumers. A recent report on Russia's artificial intelligences development concludes that the market sanctions and "cascading effects of Russia being cut off from semi-conductor and microprocessor imports" continue to degrade internal production capability.[46] Therefore, advancing technologies for renewable energy, artificial intelligence, quantum computing, and other digital platforms is increasingly difficult. Continuing to support R&D efforts and data sharing presents a unique opportunity for the U.S. to expand and dominate intelligence technology gaps from Russia's isolationist approach.

Competitive Rivalry: The rivalry between Russian companies is a *low* threat to the energy, defense, and technology sectors that comprise major pieces of today's C4ISR markets. While Russia is a significant producer of military equipment and technology, it cannot increase competition for contracts and market share in software development, cybersecurity, and artificial intelligence. Since the Ukrainian invasion, Russian defense companies maintain presence in the C4ISR industry. The Russian government prioritizes domestic suppliers over foreign competitors and is monopolized by a few state actors, favoring domestic companies vying for shares. Further,

Russian lack of market transparency and its highly regulated system make it challenging to conduct an authoritative competitive analysis.[47]

IV. PRC Overview (Systems Confrontation and Destruction Warfare)

The National Security and Defense strategies identify China as the U.S. pacing threat. China's economic rise has increased its global influence, fueling the CCP's ambitions of becoming the dominant global superpower to replace the U.S.-led international rules-based order.[48] The CCP's People's Liberation Army (PLA) has experienced a meteoric build-up of capabilities and end-strength over the past 20 years and has reorganized itself into geographically based joint commands at the operational level. The PLA's asymmetric answer to U.S. military power has been to develop a sophisticated layered defense comprised of highly capable anti-access aerial denial (A2AD) weapon systems to protect its sea lines of communications and future territorial expansion. In addition to A2AD capabilities the PLA consolidated information-enabling units under the Strategic Support Force (SSF) in 2015. The SFF encompasses space and aerospace, cyber, and electronic warfare forces under a single joint commander to mitigate historically parochial priorities within the PLA land, sea, and air services.[49]

The PLA has transformed from a defensive doctrine to a power projection focus and is also evolving its warfighting doctrine toward systems destruction warfare, refocused on disrupting or destroying the adversary's system of systems while protecting its own.[50] The key to winning a systems-of-systems conflict is information dominance, and the PLA doctrine states that achieving and maintaining information dominance is the only way to succeed in the other warfighting domains.[51] Simply put, the PLA seeks to disrupt, degrade, or destroy an adversary C4ISR systems during war at the tactical, operational, and strategic levels. PLA's doctrine calls for degrading information flow over communications and tactical data networks via jamming or compromising data integrity; using counterintelligence and misinformation to undermine intelligence gathering and assessments; targeting the physical infrastructure like power and ground control stations, data processing centers, cable landing sites, and satellites that facilitate C2, ISR, and communication; and finally disrupting the targeting and weapons engagement cycle at the tactical edge of the battlefield.[52]

Matching the DoD's effort to command and control across all domains through the CJADC2 concept, the PLA ultimately seeks an "information confrontation system" capable of large-area multi-domain jamming across wide bands of the radio frequency spectrum, rendering useless its adversary's C4ISR systems.[53] Understanding this strategically important PLA capability is paramount to DoD's future C4ISR system advancement and architecture. The goal of CJADC2, to "sense, make sense, and act at all levels and phases of the war, across all domains, and with partners, to deliver information advantage at the speed of relevance,"[54] is directly challenged at the tactical and operational levels by PLA's information confrontation system.

To deter CCP's ambitions, the U.S. military must be able to penetrate the A2AD defenses with credible combat capabilities. To achieve this, the U.S. military must adapt from its historical combat power generated by sheer mass to generating combat power by integrating and converging dispersed joint forces, performing effects at a decisive time and space. The CCP and

the United States have come to similar conclusions that "informatized" war, applying information technology to all military operations, is the key to future military victory.[55] CJADC2 is the DoD's solution to penetrate the CCP's A2AD defense and achieve an "informatized" war to deter CCP territorial expansion and win future military conflicts.

PRC Civil-Military Fusion

The PRC's Military-Civil Fusion effort has rapidly advanced the country as a technological powerhouse.[56] CCP leaders drew lessons from Operation Desert Storm on using innovative weapons systems on the battlefield. These conclusions shaped the Central Military Commissions 1993 strategy to "strengthen the army through science and technology."[57] The PLA's assessment encouraged Chinese leaders to develop a grand strategy to break down military and commercial barriers and link China's military development to its technological capability.

Hu Jintao and later Xi Jinping would formally apply the term "Military-Civil Fusion" (MCF) to China's approach. Though progress has been slow, the MCF seeks to achieve a state-led, state-directed "deep fusion" of China's defense industrial base and the civilian industrial manufacturing base.[58] And while the MCF has consolidated cooperation in the civ-mil sectors with a few state-owned conglomerates dominating China's defense industrial base, CCP leaders acknowledge that the lack of genuine competition and diverse viewpoints has hindered technological innovation.[59] Execution challenges aside, Beijing views the MCF as essential in its long-term effort to surpass the United States as a technological superpower by operationalizing frontier technologies for military and civilian purposes.[60]

MCF highlights the growth of a skilled workforce with expertise in both civilian and military sectors. China is seeking to attract and train talent to advance defense-related technologies and projects further. This includes sponsoring partnerships between universities, research institutes, and the military to promote talent development in science, engineering, and other relevant fields.[61] The synergy of the MCF aspires to leverage intellectual property and innovations from the civilian sector for military technological advancements and modernization efforts.

PLA C4ISR Military Industrial Base

The PLA is rapidly adopting C4ISR technology to achieve an advantage in the information warfare domain. The Asia Pacific region is projected to be the largest market for C4ISR technologies by 2025, largely due to China's accelerated development, procurement, and fielding C4ISR capabilities on its ever-expanding fleet of platforms.[62] However, it is widely known that Chinese state-owned enterprises (SOE), or the PLA, have a long history of foreign intellectual property theft from the United States and other Western countries. China has increased investments in R&D and created measures to safeguard intellectual property rights. Technology developed for military use in China requires a military license only offered to Chinese domestic companies, building both a vulnerability and a strength for China.[63]

Despite these efforts toward self-sufficiency, China's technological advancements and industrial base have yet to ween its dependency on foreign technology. China relies greatly on component imports from the United States. That it cannot manufacture domestically.[64] The United States has placed regulatory restrictions on China's access to semiconductors and the equipment necessary to manufacture them, including by adding several Chinese companies to the U.S. Department of Commerce's Entity List.[65] This dependency on external sources could lead to vulnerabilities in its supply chain, restrictions on technology transfer, or access to technology components. While China has made strides in developing its defense industrial base, there is still an apparent quality and innovation gap between Chinese defense technology and those of more advanced countries.

The PLA has developed its Multi-Domain Precision Warfare concept to counter CJADC2, however it has not publicly demonstrated its new systems and tactics, techniques, and procedures, so it is challenging to assess PLA C4ISR capabilities.[66] In 2022, RAND's "*Assessing Systemic Strengths and Vulnerabilities of China's Defense Industrial Base*" study could not obtain data to determine the size and quality of China's defense industrial base software industry.[67] Furthermore, RAND concluded that "software tied directly to hardware systems, such as a guidance system for a missile, assumptions could be made about the software's quality based on the effectiveness of its accuracy, and for software not associated with one system, such as applications for integration in C4ISR systems, we could draw no conclusions."[68] Even with the PLA's comparatively tighter grip on its defense industrial base through SOEs, integrating systems in a data-centric architecture is incredibly complex and likely experiencing challenges similar to the U.S. CJADC2 effort.

Summary of Five Forces Analysis: PRC Market

The CCP's control over the defense industry, emphasizing self-sufficiency and innovation, forms China's competitive dynamics and market structure. This presents unique challenges and advantages to China's C4ISR market since it is primarily state-funded and based largely on technology theft. Combined with limited available data on China's C4ISR market, those factors challenge a reliable Five Forces framework analysis.

Rivalry among existing competitors: Competitive rivalry is *low*, given CCP's ten major defense SOEs are the primary players in the defense industry, with limited participation by foreign companies.[69] Historically, the SOEs receive government support and special treatment, while foreign companies must meet the CCP's stringent requirements to conduct business.

Threat of New Entrants: The CCP controls the defense industry, and entry into the market requires a significant investment, access to advanced technology, and an influential relationship with the government. These policies impose barriers to entry for new competitors, so as a matter of policy, the threat of new entrants in China's C4ISR market is *low*.[70]

Threat of Substitute Products or Services: The limited data available to assess China's C4ISR market would indicate that the threat of substitute products or services is *low or unknown*. However, as China continues to aspire towards a data-centric architecture, new data-rich technologies could replace legacy systems or capabilities.

Bargaining Power of Buyers: China's defense industry and PLA are the primary C4ISR system buyers. Therefore, the Chinese government has *substantial* bargaining power as it controls budgets, procurement decisions, and policies.[71]

Bargaining Power of Suppliers: China's C4ISR industry *depends significantly* on advanced technologies and components from domestic and international suppliers.[72] Yet, the CCP's emphasis on technological self-sufficiency and increasing domestic defense production will likely depend on the United States and other foreign suppliers, *decreasing* their bargaining power over time.

Competitive Assessment Conclusion

While acknowledging the difficulty in applying the Porter's market framework to the state-directed economies of China and Russia, the model does help clarify some fundamental dynamics within the C4ISR market. Though Russian and Chinese economic systems maintain advantages in their ability to control and sustain indigenous markets to generate military technology, the DoD benefits from access to a more competitive market, comprised of more than 70 individual companies supplying C4ISR solutions to the U.S. military.[73] The industry's competitiveness will continue develop as demand for commercial and military C4ISR applications increases. A maturing market will create the capability, capacity & resiliency to deliver on near-term CJADC2 goals.

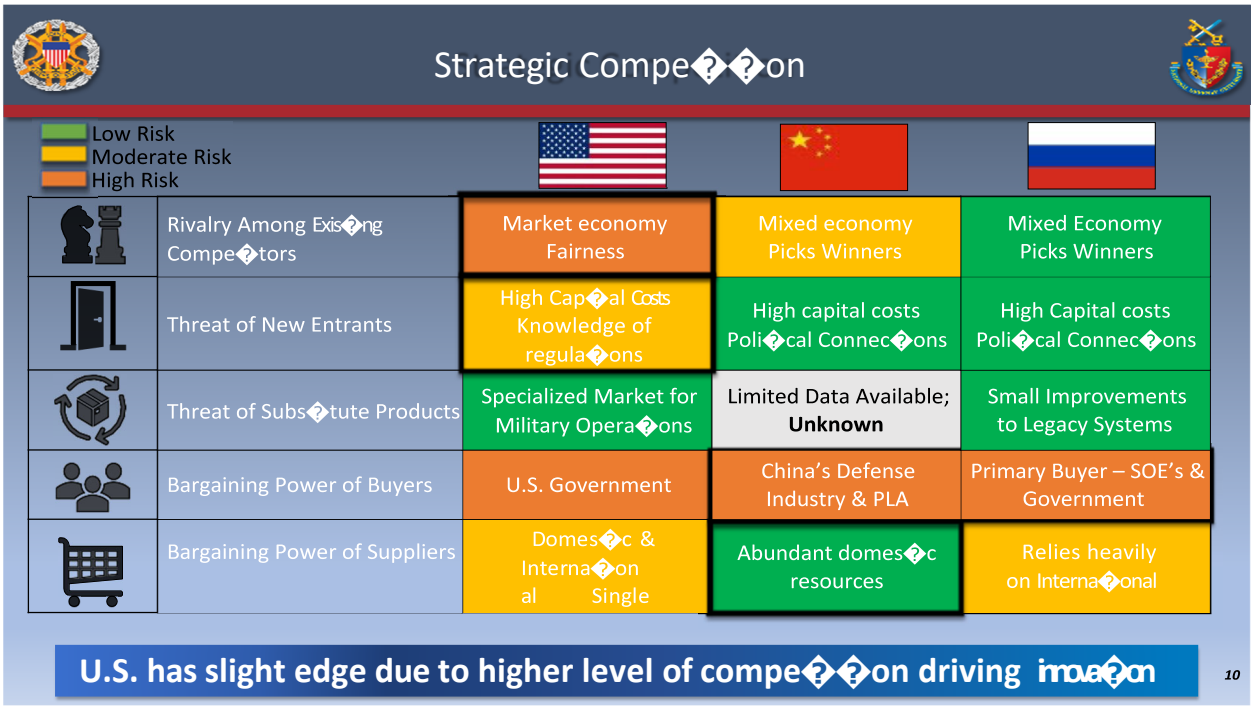

Figure 7: C4ISR Competitive Analysis Overview

CJADC2 Implementation Challenges

Overview of CJADC2 Challenges

The DoD has yet to participate in a conflict requiring full joint integration, and each military service has pursued individual requirements to fulfill its distinctive Title 10 mission. Chief Strategy Officer at Anduril Industries Christian Brose contends, "the military services, Congress, and defense industry conceive of military power in terms of platforms. The ability of these things to share information is often an afterthought."[74] This dynamic creates an environment in which the military services have focused on boosting combat power through advanced platforms, rather than increasing interoperability between existing platforms. DoD funding for CJADC2 continues to increase $650 million annually, dedicating roughly $1.4 billion toward CJADC2 in FY 2023.[75] However, the concept remains challenged by policy, tactics, techniques, and procedures rather than funding shortfalls or technology gaps. These core implementation challenges fall into the following categories: (1) policy/doctrine, (2) communication; and (3) culture.

Policy/Doctrine

DoD has made considerable investments and taken giant strides toward defining how joint warfighters will use the CJADC2 concept in future conflicts. The DoD is doing the right things, yet it continues to stumble in pursuit of this future vision. An incomplete understanding of enabling technologies sets unrealistic expectations and postures the DoD to make architectural and contractual missteps through the existing platform-centric acquisition system and warfighters will be forced to live with the resulting issues for decades. Some critics pejoratively refer to the federated approach as "Service All-Domain C2" or "SADC2," playing off the risk that service-specific pursuits will create new interoperability stovepipes and fail to produce a joint solution. The DoD has accepted this inconsistent definition and embraced a federated approach to capability development in the interest of speed. As the DoD continues through its digital revolution, legacy platforms and systems reaching the end of service life are being replaced by evolutionary platforms with greater connectivity, more capable sensors, and smarter weapons, but still reach technological obsolescence within years of fielding.

Additionally, the Federal Acquisition Regulations, including the defense supplements, govern DoD contracting processes. These complex policies can dissuade innovation among large defense primes and can make it difficult for start-up companies to navigate the acquisition process. The projected C4ISR market growth, both in technological advancements and funding, provides a unique opportunity for the DoD to leverage small business competition. The Chips Act and Inflation Reduction Act drive new industry consortiums to assist small business with infrastructure and investment grants. Venture capital influxes into defense industrial base, especially within the C4ISR market and dual-use technologies, provides opportunities for a stronger, more resilient industrial base.

Communication

The DoD and the DIB are prioritizing immediate efforts on interoperability in CJADC2's "sense" stage specifically, connecting disparate communication, sensor, and shooter systems. Full interoperability assumes that once all systems communicate, one will have access to all the data, resulting in complete situational awareness to facilitate timely and accurate decisions. However, timely and accurate decisions are predicated on information cleanly navigating the fog of war and stepping through the information hierarchy for transformation into understanding. Interoperability will increase the amount of collected raw data at unprecedented levels. Not developing ways to process the data effectively and efficiently into relevant information will overload CJADC2's "make-sense" stage, leading to paralysis. Even more concerning than processing the enormous amounts of data is that this warfighting decision-making process is not being led by operators and warfighters who are responsible for setting information requirements and priorities, but by enabling organizations who are staffed with and led by communications officers.

An organization or command's communication department or directorate is typically comprised of and run by technical experts. They plan, coordinate, and establish the technical communication systems to support the C2 system. Their responsibilities include ensuring the commander can communicate securely, determining the supportability and feasibility of the signal plans, managing communications assets, determining specific or unique communications and network requirements, and securing the network. The section is not responsible for establishing or monitoring the commander's informational requirements that lead to understanding the situation or a decision. Communication sections also inherently lack the authority to drive and hold the other staff sections accountable. According to a May 2023 Joint Staff briefing to the Chairman and Service Chiefs, CJADC2 is defined as "the Joint Force Commander's ability to C2 across warfighting domains and with Allies and partners," and historically the coordinating authority to inform and enable commander's decision is outside the role of the communication department.[76] Because the Joint Staff and military services have assigned the CDAO and the J6 to lead CJADC2 implementation, the sections have focused on what they know and do best, establishing connectivity between communication nodes.

Culture

The CJADC2 concept requires an unprecedented effort to integrate systems across the services and challenges DoD's "jointness" culture and statutory authorities. Since the National Security Act of 1947 was signed into law to formally establish the Office of the Secretary of Defense (OSD) and the Joint Staff, the organizations have strained to establish a unity of effort among the parochial services amidst a competitive environment for resources, personnel, roles, and missions. While many rightfully laud the operational alignment resulting from the 1986 Goldwater-Nichols Act, it did not break service-led programming and acquisition strategies. Although this continues to plague joint acquisition programs compared to service-led major defense acquisition programs, Congress has repeatedly rebuffed coalescing more power in the hands of OSD. It is inherently designed neither to be efficient nor speedy, but rather to distribute political power and resources. OSD's role is to coordinate, rather than direct, the services – despite the efforts of some Secretaries of Defense over the years.

Moreover, combined warfighting interoperability requires rapid, widespread sharing of information with like-minded nations. The ability to share is dependent on the cyber security of those systems. Indo-Pacific countries struggle to build multilateral information-sharing capabilities at the unclassified level. Key Indo-Pacific allies such as Japan and South Korea remain outside of arrangements such as the Five Eyes, through which the U.S. shares its most sensitive intelligence with close allies. Currently, INDOPACOM uses 13 separate networks to communicate with regional allies, partners, and friends.

Fully Resourced Recommendations

The following section outlines a series of policy recommendations aimed at supporting DoD's CJADC2 implementation. The recommendations are keyed to the core implementation challenges related to (1) policy/doctrine; (2) culture; and (3) communication.

Policy/Doctrine Recommendations

Operational Ownership of CJADC2

Starting with the Joint Staff, CJADC2 implementation should be owned by the Operations Directorate (J3) and supported by the Combatant Command and Service Operations Directorates (i.e., J3/G3/N3/S3/A3), which manage commander's informational requirements and has the authority to drive the other staff sections. C2 supports the commander's ability to understand and accomplish mission objectives. Information transformation through the information hierarchy is designed, constructed, and implemented to support the commander's information requirements for making those decisions. The operations section executes the C2 system by developing plans, monitoring operations, and conducting unit/combat assessments.[77] Operations sections can determine future processed data requirements commanders require for timely and accurate decision-making. The other staff functions can support the operations section to ensure requirements are met for manpower (J1), intelligence (J2), network connectivity and security (J6), training (J7), etc.

Promoting an Innovation Ecosystem

The DoD needs to focus on its role in the innovation ecosystem rather than trying to recreate an ecosystem from within the DoD. Problem definition, capital to seed innovation, experimentation opportunities, paths to transition and fielding, and enabling policy and doctrine changes must be the DoD's focus. The DoD must lay out a simple and accessible definition of how service programs, joint efforts, and various supporting experiments and activities align. The DoD must embrace "under-promise, over-deliver" and avoid combining technology horizons.

Industry leaders with direct warfighter access and those closely studying and following CJADC2 as it unfolds understand the Joint Warfighting Concept and CJADC2 vision. However, this limits access to many in the industry that may have a more mature understanding of software solutions than traditional defense contractors. The federated approach to capability development

is essential for rapid development, but this approach will become inefficient if a succinct explanation of how these efforts align is not broadly communicated.

Leverage Small and Medium-sized Enterprises (SMEs)

Growth in the C4ISR market provides a unique opportunity for the DoD to leverage SME competition. While the defense industrial base should attract diverse small businesses with its large budgets and various requirements, barriers challenge small business participation in government contracts, especially for the DoD. Complex contract submittal processes, delayed contract awards, security classification requirements, and large defense prime integrators hinder small business participation even though there are significant government grants and programs attempting to incentivize new entrants.

The DoD must continue to streamline contracting processes, working to reduce administrative time between solicitation and contract award. Security procedures to gain access to networks, computers, and facilities must be reduced to a week, not a month or longer. The DoD should consider partnerships using government or commercial security facilities for those companies that need these resources. Contracting strategies should consider long-term relationships, optimizing contracts' size and scope to be conducive to a small business and awarding follow-on contracts to avoid devastating gaps in revenue flow. Finally, government personnel need more training on how to assess small business solvency, national security, and performance risk reducing hesitancy of using a non-traditional defense company. (See Appendix E for additional context for SMEs in the C4ISR industry.)

Communication Recommendations

C4ISR-as-a-Service

DoD should adopt C4ISRaaS as a cost-effective solution to rapidly upgrade capabilities by leveraging advancing commercial sensors, communication pathways, data management/integration platforms, and user interfaces to satisfy C2 and ISR requirements. The commercial world is rapidly adopting the "as-a-Service" business model in which firms provide the most up-to-date product for a consumer to use, with no strings attached for operational management, maintenance, updates, accessibility, and scalability. The subscription-type model has been around for decades but has expanded as a result of the digital revolution that grants near instant access to information through wide-spread internet connectivity and portable devices.

C4ISRaaS offers flexible, advanced capabilities that can satisfy C2 and ISR requirements through commercially available hardware, software, communication networks, and intelligence collection and analysis products that can be purchased as a service, reducing the lengthy traditional timeline for requirements development to capability fielding timeline. Much like the commercial "as-a-Service" model, defense firms will deliver capabilities to the warfighter on a subscription-like contract that offers long-term financial stability to the firms and minimizes maintenance, sustainment, and upgrade costs for the DoD.

C4ISRaaS Options: C4ISRaaS can play a pivotal role in the near-term because it can be implemented nearly seamlessly in a number of different strategies to answer capability requirements. One strategy would use C4ISRaaS as a bridging solution while DoD gains understanding of how to plan, program, budget, and execute a plan to field interoperable C4ISR systems to satisfy the CJADC2 concept. Another scenario could be that DoD realizes that the commercial world is far more capable and agile in developing, fielding, and modernizing cutting edge technologies that will satisfy the vast majority of C4ISR requirements. In this strategy, DoD would outsource for C4ISRaaS to deliver the majority of warfighter needs at the tactical and operational levels, while maintaining only the exquisite strategic level capabilities in-house. Finally, and likely the most resilient and capable strategy, would be leveraging C4ISRaaS throughout the DoD C4ISR enterprise where it makes most sense as a primary, alternate, or tertiary capability. Most importantly, warfighters and decision makers would maintain proficiency with both DoD and commercial C4ISR communications and ISR systems so that in the event of a conflict, the right systems can be used in the right situations to gain and maintain information dominance over the adversary.

Developing Software-Defined Communication

CJADC2 must prioritize acquiring advanced software-driven technologies and platforms, vice hardware-centric systems, to enable decision-making at the speed of information need that future missions will require. The Joint Staff must develop a "joint mission priority" approach, considering applicable policy and doctrine, along with the new software technology, and clearly articulate a digital transformation strategy whereby the missions are prioritized with the National Military Strategy and National Defense Strategy (NDS). In doing so, some outdated and antiquated large platforms can be phased out systematically, with specific thought and, more importantly, resources aligned to new attritable, lower cost, advanced soft-ware defined technologies that enable the C4ISR-as-a-Service approach.

The intersection of big data, cloud/GPU computing, multimodal ISR sensors, and AI requires a robust and resilient network to pass data seamlessly from one system to another. Yet, application programming interfaces (APIs) still require and deserve a standardized strategy for the future next-generation networks and communication mediums, allowing for security and capacity. Current data standards and open architecture documentation are available; however, the Joint Staff should focus on gaining ground on the awash of generated and exposed APIs, moving away from the representational state transfer models of today to cloud-native models across the joint domains.

Culture Recommendations

Increase Intelligence Sharing

Modernizing mission partner information sharing is a pillar of the CJADC2 implementation strategy. Multiple partners collecting the same intelligence information in disparate network systems results in decision making delays and the inefficient use of resources. Ideal mission partner system integration is realized when data from each partner's C2 system can be accessed, viewed, and acted upon by every other approved partner.[78] **When decision makers**

think of the CJADC2 framework, they should also think of mission partner environments (MPE) and champion writing data-centric policies for information to be eligible for release at different classifications.

A MPE is a C4ISR framework that improves joint force capabilities and supports CJADC2 by enabling trusted allies and strategic partners to share information in a common environment. Dynamic MPEs combine the effect of joint tactics and training, trust, policy sharing agreements, and the ability to share (zero trust, encryption, technology). DoD MPEs provide seamless information-sharing capabilities such as real-time online chat, email, and file sharing, along with collaborative intelligence sharing and analysis of technologies between U.S. commanders and their counterparts in partner countries, in the Secret and below releasable environment. Recently, U.S. Army units have begun using a new MPE across service formations deployed in United States Army Europe and Africa, allowing service commanders to exchange data more freely with allies and partner country forces downrange.[79]

DOD should continue to develop MPEs to facilitate information sharing with partners, coordinate operations, and enable high-end weapon system integration. In April 2023, the INDOPACOM commander stressed the need for a new secure MPE for U.S. partners and allies in the Pacific to Congressional appropriators. "Part of my unfunded list is something called a Mission Partner Environment to talk to allies and partners. What we are attempting to deliver is a single pane of glass that allows us to communicate securely in a cyber safe way with all of our partners across the region, regardless of classification."[80] INDOPACOM's MPE, a zero-trust architecture model created in partnership with U.S. Cyber Command, modernizes 13 separate coalition command, control, communication, computer, and information technology network systems into a single cyber-safe system to deliver a resilient, secure, combined C2 capability, and allows all participants to share a common operational picture. The INDOPACOM MPE remains an unfunded priority in the FY 2024 budget.

Encourage Allies and Partners to Strengthen Ties With Each Other

U.S. diplomacy must continue to build bridges between the Indo-Pacific, Euro-Atlantic, and with other regions. Modernizing mission partner information sharing also requires a commitment to participate in global CJADC2 innovation efforts with allies and partners. At the 2021 NATO Summit in Brussels, Allied leaders agreed to launch the Defense Innovation Accelerator for the North Atlantic (DIANA) to foster transatlantic cooperation on critical technologies, promote interoperability and harness civilian innovation by engaging with academia and the private sector. Through competitive challenge programs, DIANA works directly with leading entrepreneurs, from early-stage start-ups to more mature companies, to solve critical problems in defense and security through cutting edge science and engineering. Accepted innovators gain access to a network of innovation hubs across the NATO Alliance and receive non-dilutive investment capital, with the possibility for development and adoption contracts with Allies for dual-use technologies. DIANA begins pilot activities in summer 2023.[81] Indo-Pacific allies such as Australia, Japan, and South Korea could be incorporated in this initiative through their role as NATO "global partners."[82]

Link Defense Industrial Bases of Allies and Partners

The United States and its Allies must find opportunities to link our defense industrial bases and prioritize rapid identification, development, and adoption of new, attritable C4ISR capabilities that give combat advantage and replaced at low cost. America's acquisition and innovation processes need an alliance-centric approach from inception, rather than treating allies as add-ons to existing American plans. Working with allies and partners to harness and scale new technologies will anchor an allied techno-industrial base; especially microelectronics, advanced computing and quantum technologies, artificial intelligence, biotechnology and biomanufacturing, advanced telecommunications, and clean energy technologies. Partnering with like-minded nations to co-develop and deploy technologies builds robust and durable supply chains so aggressors, like China, cannot use economic warfare to coerce others. [83]

Integrating our defense supply chains, and co-producing key technologies shores up our collective military advantages. [84] The United States should accelerate region-wide consultations regarding developments in such critical areas as nuclear and missile technology (e.g., hypersonic weapons), cyberoperations, counterspace, and autonomous systems and their contributions to China's coercive and warfighting capabilities. These discussions should explore cooperative options with U.S. allies and partners through measures such as strategic reassurance, joint deterrence, and counterproliferation.

Implementing a Zero-Trust Architecture

For the frameworks of CJADC2, zero-trust, and MPE to be successful against cyber-attacks, a fully proven trust chain, and data highway must be created to safeguard and verify the original data source, the data vehicle, and the data receiver. This will ensure that no seams are left open during the communication and maintains data integrity. Regular network penetration exercises will test the zero-trust architecture to ensure that current procedures and policies are resilient against an evolving cyber threat.

Current budgetary shortfalls due to the PPBE process do not align with the ambitious timeline for zero-trust implementation. Congress must prioritize funding appropriations to fully employ the zero-trust model and zero-trust architecture over continued support of legacy systems. This will require an analysis of zero-trust implementation milestones across the federal government to develop funding distribution streams.[85] Zero-trust implementation cannot be realized without prioritizing funding to buy down the technology debt, and the software and hardware required.

Furthermore, talent acquisition is required for long-term institutional cyber resilience. The DoD has struggled with hiring strong acquisition talent. A technically knowledgeable workforce is fundamental to implementing zero-trust and zero-trust architecture. Creating a tech-savvy workforce through hiring strong talent that embraces innovation, disruption, and diversity in talent and skills will foster the right working culture and environment.[86] This moves the perception from "failure is unacceptable" to the "fail fast, recover faster" approach used by industry.[87]

Building a zero-trust architecture that never trusts, continuously verifies to grant access, and assumes an adversary always threatens every user and system leads to a highly resilient, flexible ecosystem designed to thwart cyber-attacks. Without a successful zero-trust strategy and zero-trust architecture implementation across the DoD enterprise, the success of CJADC2, MPE, and other future programs will fail. Congress must fund the DoD to acquire the required technology and software to meet the FY27 deadline for long-term cyber security and resiliency against the U.S.'s adversaries.

Streamlining the Acquisition Process

DoD must look at the structural challenges to interoperability and make a focused effort to align incentives and streamline processes.[88] Examining the history of acquisition reform reveals no shortcuts to the iron triangle of cost, schedule, and performance.[89] While reform efforts will ebb and flow with the political tenor of the day, no Americans will tolerate military failure. The historical record shows that when OSD oversight has been the most lax, poor decisions have led to the most dramatic growth costs.[90] Efficiencies gained by streamlined processes can be quickly lost by a few poorly considered program decisions.[91] However, we must be willing to accept some cost inefficiencies to increase our acquisition speed and performance. Acknowledging that no system can optimize performance across every parameter, it is time to shift the paradigm for speed and performance rather than continuing to attempt economic efficiency through onerous oversight and management processes.

The model for successful acquisition reform entails three components. First, the reform must target a specific set of related problems.[92] Second, it must gain support from all stakeholders, to include Congress and the Executive Branch.[93] Third, it must endure over time with committed and sustained leadership.[94] The 1986 Goldwater-Nichols Act, often pointed to as the gold standard for military reform, is a testament to this model. It tackled a specific and well-defined set of problems, identified a root cause, and then accomplished the laborious work of championing and sustaining a course of action to address the root cause.[95] Subsequent defense reforms over the years have not been as successful. Although some current reforms, like the PPBE commission mandated in the FY 2022 NDAA, show promise in tackling the problems of speed and performance.[96] Still, there are other recommendations for consideration.

Two additional recommendations for reforming the defense acquisition system to support CJADC2 include employing joint capability budgets and reattempting the biennial budget process.[97] Shifting a significant portion of the defense budget to delivering and maintaining a joint-capability portfolio would decrease overlapping service-led acquisition programs and allow for greater flexibility in deploying capital. This kind of shift would increase the linkage between procurement and strategy by allowing OSD to clearly link procurement dollars to achieving its goals for national defense. Furthermore, it would help to erode the service chief consensus which has largely led to parity amongst the funding levels of each service despite radical differences in national objectives and adversaries.[98] Finally, reducing the various "colors of money" would empower program managers to incorporate new and emerging technology as it advances along with program maturity rather than continuing to build new equipment with dated technology.

Another way to increase acquisition speed it to shift from an annual to a biennial budget process.[99] More significant than the lost funding is the lost time that results from a continuing resolution. The DoD has lost over 1,600 days through continuing resolutions since FY2010.[100] The most recent continuing resolution from October 1 to December 23, 2022 also cost $17B.[101] Although politically challenging, this is low hanging fruit and would allow the DoD to employ more consistent funding streams which are most critical to the small businesses that can deliver the greatest value to achieving CJADC2. Finally, a two-year budget would align with each Congressional session, thereby maintaining their oversight responsibilities.

The current acquisition processes offer the services avenues for accepting greater risk than they have in the past but are mired in regulations and changing guidance that hamper program managers. In addition to the expense, these processes add program execution time. Instead of focusing on laborious management practices that add little value, the acquisition system must empower its program managers and hold them accountable. In the words of then Army Chief of Staff, Mark Milley, "Empower the PEOs, empower the Heidi Shyus of the world, empower the service chiefs…Cut us loose and see what happens. If we fail, fire us."[102] Accepting risk is necessary, but insufficient; we must shorten the acquisition timelines by revamping existing management processes and incentives.

Concluding Thoughts

C4ISR is the backbone of military operations from the tactical to strategic levels, throughout all phases of conflict. The C4ISR industry underpins the technical capabilities that enable commanders and senior leaders to understand the operational and strategic environment, communicate orders, move forces, and close kill webs. Single pathway communications and legacy systems based on network-centric warfare are increasingly challenged in today's global security environment.

Despite operational challenges against a tougher-than-expected Ukrainian military and supporting defense industry in a less-conventional fight, Russia maintains robust electronic and cyber warfare capabilities that can challenge U.S. C4ISR in a conventional fight. However, the Russian defense industry will be challenged to recover lost years of future development and capability due to a mass exodus of technical talent seeking to avoid conscription into the Ukrainian battlefield. The PLA continues to resource its services to become one of the most capable and largest militaries on earth and orient the force towards systems confrontation and system destruction warfare, with informatized warfare being the key enabler. This meteoric growth in size and capability has only been possible due to systematically stealing advanced U.S. and other western military technology, allowing the PLA to leapfrog past decades of R&D and almost straight into advanced weapon system production.

Following multiple attempts to refocus the U.S. joint force back to preparing for high-end conflict against a peer adversary with like-capabilities, the 2018 NDS and 2022 NSS firmly pivoted the national security apparatus towards the pacing threats challenging the rules-based international order. In a conflict between adversaries with comparable weapons capabilities, battles are won by the side that observe, understand, and act most effectively. The CJADC2 framework is how DoD intends to gain decision advantage for commanders in the next high-end

conflict, and it requires service, joint, and partner C4ISR systems integration to "sense, make sense, and act" in a faster decision cycle. To achieve this, a healthy relationship between DoD and the C4ISR industry is vital to developing the technology needed to connect the combined, joint force.

The U.S. C4ISR industry is at an inflection point facing the challenges associated with transitioning from legacy network-centric systems to more resilient and capable data-centric systems. The shift to software-based digital systems puts the C4ISR industry in direct competition with the commercial tech industry for attracting and retaining the required engineering and computer programming workforce. The industry is facing external threats as well in securing networks and technology from being breached and stolen by unprecedented Chinese espionage efforts.

Therefore, DoD, industry, and international partners must jointly expand capacity, capability, and resiliency to field systems that enable commanders to CJADC2 in a contested or denied communications environment. DoD's CJADC2 effort must be led by warfighters that can define prioritize information requirements. Additionally, DoD leaders need to foster the existing U.S. commercial technology innovation ecosystem, rather than try to create one focused on DoD needs. Critical to succeeding in this effort is adjusting the requirements and acquisition processes to leverage small and medium-sized firms that often develop the most cutting-edge C4ISR technologies needed to gain a competitive advantage on the battlefield. DoD must also explore novel means to acquiring cutting edge technologies in a way that it can forces are always leveraging the most advanced technologies. C4ISRaaS is a cost-effective solution to rapidly upgrade C4ISR capabilities without the infrastructure overhead of purchasing and maintaining traditionally acquired platforms and hardware. When security risk and operational sensitivities require full DoD communications custody, the joint force must acquire advanced software-driven technologies and platforms to ensure interoperability and resilient communications across all service and allied networks.

The first letter of CJADC2 stands for combined, and its placement deservedly defines a most critical aspect of how the U.S. is going to fight future wars – with international allies and partners. Beyond the acronym and operational intention, there is much work to be done to realize this critical need. Mastering the basics of information sharing is a foundational step, and most of the friction is with restrictive DoD and IC computer network and information sharing policies, along with a culture of over classification. Increased proliferation of zero-trust architecture amongst U.S. and partner networks will eliminate significant risk for data spillage and network espionage. In addition to improving information and intelligence sharing, the U.S. can lead the way in the Euro-Atlantic and Indo-Pacific by leveraging technology and innovation to strengthen cross-border industrial base development.

Finally, the DoD, Executive Branch, and Congress must enact serious and sustainable changes to build trust, but also address significant budgeting and acquisition shortfalls that could sabotage the already very lofty goals for the CJADC2 concept. Clear signals to industry through a more predictable budgeting process, realigning service appropriations to joint accounts to reduce redundancy, and allowing some discretion to service comptrollers for appropriated funds could unlock synergy and efficiencies previously unseen in the Joint-force era. CJADC2 is a

revolutionary concept that could be largely achieved with some evolutionary policy changes. The C4ISR Industry can produce the needed technology, and much of it is already on a warehouse shelf. Failing to put all the pieces together now could, following a near-term conflict with a very capable and determined adversary, change the entire picture on the puzzle.

Appendix A – Capstone Question Paper Response

Question: China and the BRI: Short and long-term implications on our Allies, Partners, and the United States. What can the United States do to present viable non-BRI options globally?

Introduction: Lula's Huawei Embrace

Brazil was one of the world's fastest-growing countries between 2000-2012.[103] Analysts often attribute Brazil's average 5 percent annual growth during this period to then-president Luiz Inácio Lula da Silva's spending and poverty reduction programs.[104] So when da Silva launched his bid to return to the presidency in 2022, he campaigned credibly on a platform of restoring Brazil to its previous era of economic prominence. And it worked. After defeating incumbent Jair Bolsonaro in a tight run-off in October 2022, da Silva began a frenetic international travel schedule to bolster Brazil's economic position, meeting his South American neighbors in January 2023 followed by U.S. President Joe Biden in February. However, da Silva's most highly-anticipated trip was his four-day swing through the PRC, where he met Chinese leader Xi Jinping and toured the Huawei Shanghai Research Center in April.[105]

Some within the Washington policy establishment expressed apprehension over da Silva's public embrace of Huawei after his predecessor had been so critical of the CCP.[106] In reality, Lula's 'Huawei embrace' does not signal any lack of friendliness in the U.S.-Brazil relationship. Brazil is one of only 18 countries designated as a major non-NATO ally and remains a major diplomatic and trading partner of the United States.[107] But the embrace does highlight Brazil's broader reliance on the PRC's 5G infrastructure. It also points to a glaring gap in the U.S. diplomatic strategy: the United States offers no alternatives to the PRC's digital and physical infrastructure projects while admonishing recipients of BRI and Huawei assistance programs. Instead, the United States should supply global partners with competitive alternatives to the assistance approach it condemns while not criticizing developing countries that do accept the only option available. The United States can leverage its C4ISR industry for diplomatic advantage through the concept of "networked interference," a diplomatic strategy introduced in this paper that attempts to mute China's provocative global activity by building out the military and civilian C4ISR infrastructure of U.S. partners and allies.

Defining the Toolkit: C4ISR and 'Networked Interference'

Traditionally, one thinks of C4ISR in the context of military battlespace management and multi-domain, joint command and control.[108] Undoubtedly, C4ISR presents opportunities to revolutionize defense system integration and accelerate warfighting decision-making. But the C4ISR market also includes systems that have civilian government and commercial applications. While military forces can utilize Common Operating Picture (COP) programs to coordinate joint-multi-domain operations, civilian agencies can also deploy COP for disaster response and border security. Geographic Information Systems (GIS) designed to help warfighters visualize and analyze geospatial data also have public safety and emergency management applications. AI programs designed to assist military intelligence with weeding out noise and focusing target selection can help public health officials identify patterns and surge healthcare during outbreaks and pandemics.

Notably, the answer to 'What is C4ISR?' can scale according to the objective, given the wide range of products on the market. For example, Lockheed Martin has developed the RQ-170 Sentinel, a low observable unmanned aircraft system (UAS) for use by FVEY partners to perform time-sensitive targeting. But the C4ISR defense industrial base also produces surveillance UAS that benefit civilian operators conducting humanitarian crisis response. Lockheed Martin is also developing the Command, Control, Battle Management & Communications platform to support ballistic missile defense, while modified versions of this technology can support law enforcement and other domestic public safety agencies. This ability to scale per customer need expands the scope of C4ISR applicability, allowing the United States to leverage this industry as a counterweight against the PRC.

But what is 'networked interference?' As we will explore in a subsequent section, the PRC has built a foreign aid strategy to support its military expansion outside the first and second island chains. With the lack of alternatives from the West[109], the BRI has gained prominence, particularly among 'global south' countries, and helped expand China's infrastructure footprint in Asia, Africa, Europe, and Latin America. The BRI has the added benefit of buying silence among countries that might otherwise criticize China's attacks on international norms.[110] Effective U.S. diplomacy can disrupt this practice. Within the information technology environment, "network interference" occurs when distribution hubs are degraded by multiple devices tapping into the same physical infrastructure. The United States can apply this concept diplomatically by degrading China's BRI network with C4ISR engagement through foreign military sales or financing scaled appropriately to the bilateral partner. In some cases, the engagement might be limited to the sale of commercial C4ISR equipment for use by a state's civil authorities. In other cases, a C4ISR initiative might lead to an advanced military partnership that presents a deterrent effect against China. The point, however, is that engagement, either narrowly or broadly tailored, provides an entry point for C4ISR collaboration and adds networked interference to China's expansionary vision. Of course, this would not be the only tool in the toolkit, but it could help produce networks for the United States diplomatically, economically, and militarily to degrade PRC influence. This is the concept of C4ISR-enabled networked interference.

Framing the Argument

The path toward C4ISR-enabled networked interference in the great power context is rooted in the themes explored in the succeeding literature review. The argument is then framed in three parts. Part I conducts a comparative analysis of the U.S. and PRC development frameworks and underscores the strategic challenge. Part II builds on the governance theme detailing how democratic systems produce a C4ISR industry that can serve as a competitive diplomatic tool. Finally, Part III outlines specific policy options for leveraging C4ISR as a political-military tool to build partnerships to deter aggression and prevail in the event of war.

Literature Review

There is no shortage of literature defining the contours of the great power competition with China. In *The Return of Great Power Rivalry*, Matthew Kroenig thoroughly assesses the

relative strengths of democracies when engaging in diplomatic and economic competition with autocracies.[111] Kroenig reaches practical conclusions on how the constraints of democratic governance facilitate diplomatic and military advantages. He raises the importance of America's democratic traditions in an age when 21st-century national security policymakers frequently characterize U.S. foreign engagement nearly exclusively in terms of security and economic interests. These are worthwhile considerations given that the case for sustained U.S. leadership is rooted in preserving a rules-based international system that benefits not just the United States but the broader global community. The CCP-led autocracy is hard-pressed to make a similar argument.

Among the multiple works offering insight into the PRC's ideological outlook, two books provided extensive background in framing this paper's theory. Examining the political viewpoint, Jonathan D.T. Ward's *China's Vision of Victory* covers the CCP's historical underpinnings and the vision that undergirds Xi's "China Dream."[112] Providing a military perspective, M. Taylor Fravel captures 70 years of the People's Liberation Army (PLA) military history in *Active Defense: China's Military Strategy Since 1949.*[113] Most usefully in this sphere, Rush Doshi's *The Long Game* provides one of the seminal pieces examining the PRC's grand strategy.[114] Doshi focuses on the post-Tiananmen period of China's grand strategy formulation, in which CCP leaders conclude the PRC must at least "share" the 21st century with the United States if not outright seek to dominate. *The Long Game* describes the PRC's three-phased displacement strategy that sets out to (1) blunt U.S. power over China; (2) build the foundation of regional hegemony in Asia; and (3) expand power globally. The book concludes by outlining an asymmetric strategy for competition that pulls in aspects of alliance building and C4ISR resilience.

Writing about the information space, U.S. Institute of Peace's Dean Cheng has published a series of papers on the nexus between emerging technologies and PLA development. Cheng's *Cyber Dragon: Inside China's Information Warfare and Cyber Operations* provides context on how the PLA views future warfare and outlines policy options for C2 resiliency in a future fight.[115] Cheng also sets up the concept of "informational mercantilism," which he defines as the CCP's approach to rebalancing the global power equilibrium through information dominance. 'Informational mercantilism' clarifies the objectives of PRC assistance programs like the BRI and helps elucidate themes in this paper. Finally, as foreign military sales and financing (FMS/FMF) will provide the principal mechanism for the United States to deploy C4ISR capability for diplomatic advantage, context into the history of the security assistance process is helpful. Military officers and researchers David Anderson and Randall D. McCauley detail the evolution of FMS and FMF programs from 1950-2007.[116] Additionally, the Congressional Research Service report on foreign assistance is a preeminent source document in understanding the security assistance process.[117]

Part I: From Industrialization to Donor – A Comparative Analysis

When formulating how to deploy an industry, such as C4ISR, as a competitive tool against the BRI, it is helpful to conduct a comparative analysis of the United States and China to understand how each country arrived at its assistance framework.

Industrialization (United States): For the United States, the journey began in the small town of Pawtucket, Rhode Island, which sits strategically along the upper tidewaters of Narragansett Bay against the Blackstone River basin. Owing in part to these rich geographic features, Pawtucket gave birth to the first commercially-successful, mechanized U.S. production process in 1793 when English-American industrialist Samuel Slater constructed a textile mill powered by the force of the Blackstone River. Slater's template eventually paved the way for the American industrial revolution transforming an agrarian 18th-century nation into the world's leading industrial economy.[118] By the end of the 19th century, U.S. industrialization had eventually outpaced the rest of the world, and it would go on to generate decisive advantages for the United States that helped it power the "arsenal of democracy" in World War II[119] and bankrupt the Soviet Union during the Cold War.[120]

Assistance Framework (United States): America's road to industrialization as a liberal, free-market economy fueled its leaders' desires to remake the world in its image. To achieve this objective, the United States structured its foreign assistance around governance and human capital development. Today, Congress appropriates the plurality of U.S. foreign aid (31 percent) to bilateral assistance programs administered by State and US Agency for International Development to improve economic development, most of which is devoted to global health.[121] Coupled with economic assistance, Congress appropriates military and non-military security assistance (29 and 6 percent, respectively) administered by State and usually implemented by DoD designed to train, equip, and professionalize foreign military and law enforcement agencies.[122] The experience of 20th-century wars taught the United States to elevate global partnership development as a cornerstone of its foreign policy. Central to these partnerships is the security and assistance relationship through which the United States believes it can fashion a more secure and democratic world.[123] The United States approaches development assistance wholistically rather than as one component of a transactional relationship. As we will see, the PRC takes a very different approach.

Industrialization (China): The CCP began pulling its nation out of its "century of humiliation" after taking power in 1949 following a more than 20-year civil war. Roiled by its initial failures of the Great Leap Forward and the Cultural Revolution, the CCP launched an economic liberalization project in 1978 that expanded China's economy by double-digit rates for three decades.[124] After China acceded to the World Trade Organization in 2001, CCP leaders quietly began economic interventions to artificially devalue the yuan and utilize technology transfers to grow its domestic capability at each stage of the value chain.[125] Simultaneous with this economic growth, the PRC unleashed a massive military modernization program and eventually abandoned its previous "hide and bide" strategy. With the tragedy of Tiananmen behind it, the CCP developed a new compact with its subjects: ideological compliance in exchange for individual prosperity.[126]

Assistance Framework (China): Chinese leaders dating to Deng Xiaoping recognized that the PRC's growing global aspirations would eventually require a commensurate expansion of its military footprint.[127] The CCP looked to ancient China to provide a blueprint for this growth. Beginning in the 2nd century BCE, China's Han Dynasty opened a network of overland trading routes linking China with ancient Persia, India, and the Mediterranean. Chinese merchants traded silk, spices, tea, and other goods in exchange for horses, furs, and jade through

routes that would later be termed "the Great Silk Road." So when Xi Jinping traveled to Astana, Kazakhstan in 2013 to outline a new global trade and cooperation framework, his "One Belt, One Road" vision evoked images of the ancient routes that made China the dominant economic power of the pre-industrial world.[128]

Renamed in 2016, the BRI has become China's 21st-century global grand strategy.[129] The initiative connects the PRC to the most strategic logistic nodes throughout South Central Asia, East Africa, Europe, and Southeast Asia. Through the BRI, China has built infrastructure projects prominently along these nodes or in countries rich in natural resources.[130] For recipient countries, this assistance often carries the perception of having little to no conditionality.[131]

The Strategic Challenge: PRC public diplomacy has framed the BRI as an economic initiative to enhance global cooperation.[132] But at the 2017 Belt and Road Forum, the PRC released a white paper entitled "Vision for Maritime Cooperation under the Belt and Road Initiative," which outlined plans to build infrastructure at strategic locations that could be used to secure PLA sea lines of communication.[133] While couched as an overseas infrastructure development program, this 'vision of cooperation' seemed to tackle the challenge that Deng Xiaoping-era military planners identified, who viewed China's geographic constraints inside the first and second island chain as an Achilles' heel.[134] BRI initiatives also bring concerns of entrenched Chinese surveillance, particularly in resource-rich Africa, where SOEs have constructed at least 186 government buildings across 40 of the continent's 54 countries, and Huawei has built out more than 70 percent of its 4G telecom infrastructure.[135]

This transactional approach to overseas development underscores Dean Cheng's previously discussed 'informational mercantilism.' Cheng testified before Congress that an emergent CCP views information as currency, and state power is now more a function of its ability to gather, analyze, and exploit information rather than generate raw output, as was the case during the industrial age.[136] The PRC facilitates its information dominance through programs such as the BRI and Huawei's supply of telecom infrastructure, which it deploys to gain access to foreign information while closing off its own markets to others.[137] These efforts to shape the interpretation of information represent a threat to the United States, its allies, and the integrity of the entire international system. Yet emerging countries do not want lectures from U.S. diplomats on the dangers of Huawei and information security. They prefer alternatives, which the United States currently has in short supply. The United States needs to provide options rooted in democratic values that counter the PRC's authoritarian view of the international system. Part II tackles that challenge.

Part II: Understanding the Democratic Advantage

Democracies are falling out of vogue. Sixty-eight percent of the world's population now lives under the grip of an autocratic government.[138] The 21st century has thrown challenges that have tested the resilience of the democratic system. CCP leaders interpreted the two decades of American-led war on terror and the calamitous 2008 financial crisis as the end of the American-built international world order. The PRC positioned itself as the savior of the global financial

system by quickly injecting liquidity into the market when the West appeared trapped in political and economic turmoil.[139] Separately, autocratic governments like the Russian Federation have weaponized disinformation, engaged in political interference, and conducted cyberattacks against voting software, further weakening the case for democratic political systems.[140]

Yet the fundamental case for democracies remains strong. Democracies produce more resilient economies, stronger diplomatic alliances, and greater human prosperity than their autocratic counterparts.[141] The constraints democracies put on governing authorities encourage the free flow of capital and business confidence, empowering markets to innovate and respond to consumer needs. The lack of capital restraints has secured the dollar's position as the world's reserve currency despite attempts by China, Russia, and others to diversify away from the dollar.[142] In fact, the PRC's history of currency manipulation has undermined its efforts to substitute the yuan for the dollar. Democracies also encourage immigration, which has provided the foundation for American innovation for more than a century. These factors have helped produce the most innovative defense industrial base on the planet.[143]

This democratic advantage transfers to the C4ISR industry. From radars and sensors to space communications, electronic warfare, and ISR assets, the United States has produced some of the most innovative C4ISR products on the market. According to business research firm Marketline, three of the top five C4ISR firms are headquartered in the United States.[144] Though the U.S. C4ISR industry is moderately concentrated,[145] more than 70 individual companies are currently supplying C4ISR solutions to the U.S. military (see Figure 1).

By contrast, the PRC only has seven state-owned defense enterprises supplying weapons to the PLA.[146] As a result, the PLA does not have access to the same heterogeneous product offering as the U.S. military. Only 2 percent of Chinese private sector firms supply the PLA despite the PRC's military-civil fusion approach. And as expected within an autocracy, SOE reform within the PRC has been slow.[147] According to primary source documents from the PRC, CCP leaders are seeking to inject genuine competition into their system and encourage the diversity of views that occurs naturally in a democracy such as the United States.[148] While there is growth and the Chinese defense SOEs are increasingly finding their way onto the list of top 20 global defense firms (see Figure 2), PRC-based firms lack transparency, making it difficult to assess their financial health.[149]

China's state-led economic system conducts anti-competitive practices, limits market access, and manipulates its currency valuation. These tactics threaten U.S. technological leadership. Yet, labeling these schemes as 'unfair' will do little to win the strategic competition. The United States instead must find ways to build resilient partnerships and alliances that deter these maneuvers. This is the subject of the next section.

Part III: Leveraging C4ISR for Diplomatic Advantage

Johnathan D.T. Ward concludes *China's Vision of Victory* with the following three observations:

1. The contest with China is fundamentally about economic power;

2. A contest with America will be close, but a contest with the entire democratic world would be impossible; and

3. The military power favors the United States and its allies.[150]

These observations are profound as they point to the strengths the United States has leaned on not just during the period of great power competition, but for the duration of America's 75-year reign as the world's leading democratic power. The PRC understands these strengths, and the BRI endeavors to break down each of these three levels by (1) promoting exports and Chinese labor overseas; (2) building goodwill by delivering domestic political wins for democratic leaders abroad; and (3) establishing strategic overseas logistics points for the PLA overseas. And as previously noted, what has made the BRI so impactful is the lack of U.S. alternatives. Matt Kroenig accurately summarizes the dilemma, "the U.S. system is competitive, but Washington must still compete."[151]

Policy Recommendations: The following list offers policy interventions to help the United States build out "networked interference" to deter and, if required, counter PRC aggression. This is not a panacea. Some recommendations will require legal or structural changes. But this list recognizes the untapped potential of utilizing the C4ISR industry for diplomatic advantage.

- *C4ISR as an Export*: Many companies have noted the difficulty of exporting C4ISR products through direct commercial sales (DCS) or FMS due to bureaucratic challenges within the Departments of State and Defense.[152] Each sale of a U.S. product disapproved is another opportunity for the PRC to sell a similar, but perhaps inferior, product over which the United States lacks oversight. Moreover, needlessly denying potential partners' FMS or DCS cases promotes a PRC narrative that paints the United States as an unreliable ally. Further, DCS and FMS bolster the defense industrial base and should be encouraged where applicable. Understandably, there will be any number of FMS/DCS cases that Washington must deny on legitimate policy grounds. But U.S. officials should positively orient toward approving FMS and DCS cases that do not compromise U.S. intellectual property or national security concerns.

- *FMF as a Partnership Tool*: As noted previously, the U.S. C4ISR industry is world-class. However, high quality often means high expense, and many emerging economies cannot afford U.S. C4ISR products. The United States should aggressively use its FMF authorities to build the C4ISR capacity of low- and middle-income partners. Congress (through earmarks) or the Executive branch (through policy) should allocate a specific portion of the overall FMF account toward C4ISR. As C4ISR powers the technology that underpins a modern military, applications such as COP and GIS provide entry points for future military collaboration. Additionally, C4ISR software programs carry fewer end-use monitoring requirements on embassy staff, and their operations and maintenance costs on host governments are more manageable.

- *An Asia Pivot for FMF*: President Obama announced the 'Pivot to Asia' in November 2011. Each subsequent NSS and NDS has reflected this change attaching greater emphasis on the

Indo-Pacific. Twelve years later, FMF allocations have yet to make a similar pivot. Apart from Ukraine, Middle East and North Africa (MENA) countries continue to receive the highest proportion of FMF dollars.[153] While there are statutory reasons certain upper- and high-middle-income MENA countries continue to receive significant FMF appropriations, Washington needs to rebalance FMF distributions to align with U.S. national security priorities. Although the two most populous countries in Southeast Asia – Indonesia and the Philippines – are increasingly seeing larger shares of FMF, the broader Indo-Pacific still significantly lags behind MENA and Europe in FMF distributions.[154]

- *Prioritize C4ISR Sales*: Unlike the FMF programs discussed above, FMS in the Indo-Pacific is increasing. For FY 2022, FMS cases in East Asia and the Pacific accounted for approximately 40 percent of total FMS cases, according to reporting in June 2022.[155] Yet, in the same year, C4ISR accounted for only 12 percent of FMS case value, compared to fixed-wing aircraft, which accounted for 65 percent of the overall case value.[156] However, Taiwan notably acquired $406.5 million in radar and surveillance equipment through the FMS program in CY 2022. FMS cases should follow this pattern set by Taiwan as C4ISR equipment, on the surface, is less provocative given its dual-use capability. Yet, it provides a broader foundation for future military cooperation than large air platform acquisitions.

- *Bolster the Indo-Pacific C4ISR Architecture*: As Ward notes, military power favors the United States and its allies in the contest with China. [157] U.S. partners and allies remain the most critical component of the U.S. deterrence strategy. Apart from the newly re-established presence in the Philippines, most U.S. troops in the Indo-Pacific are stationed in Northeast Asia. Beyond the Philippines and Thailand, the United States needs to grow treaty alliances outside this traditional sub-region. It can start by engaging potential allies with dual-use C4ISR systems. By providing surveillance and reconnaissance systems and data-sharing platforms, the United States can begin enabling an Indo-Pacific C4ISR architecture on which to build as military partnerships deepen. Additionally, the United States should ensure the resilience of the C4ISR architecture among its allies by exercising cooperative targeting in contested environments.[158] It should also look to expand its sensor and radar networks among its Indo-Pacific partners to detect and counter China's anti-access/area denial capabilities.[159] Achieving these objectives is essential to the success of networked interference.

Concluding Thoughts

Reflecting on da Silva's travel to Shanghai, it becomes clear that the traction of the BRI is the fact that it provides any option at all. Huawei has a 20-year presence supplying telecom infrastructure in Brazil, primarily due to the lack of alternatives. A common refrain among foreign officials to U.S. diplomats is that 'China is present…the United States is not.'[160] This approach must change.

And the evidence suggests change is underway. Recent U.S. government strategy documents acknowledge that the United States can no longer pursue a policy of uncontested dominance in the Indo-Pacific.[161] Countries such as India, Indonesia, Malaysia, the Philippines, Thailand, and Vietnam have and will continue to play significant roles in numbing malign PRC

effects.[162] But many of these countries are small, and China possesses tremendous political and economic sway in the region. Moreover, the degree of apprehension about Chinese intent varies widely throughout the region, so a blanket counter-China policy is destined for failure.[163] Even for small countries that squarely consider the PRC a threat, overt military cooperation with the United States is likely to trigger unwelcome PRC reactions these countries are ill-equipped to confront. Collaboration within C4ISR can scale to meet the needs of a particular bilateral requirement while enabling a framework for future military cooperation. This depends on the ability of the United States to offer C4ISR solutions that foreign governments see as applicable but also promote the rules, norms, and standards that characterize a free and open international system. To do that, the United States needs to provide a better alternative to the PRC's authoritarian view of the system. Networked interference helps address that challenge.

Command & Control	Communications	Computers	Intelligence	Surveillance & Reconnaissance
• Raytheon	• Raytheon	• Microsoft	• General Dynamics	• Raytheon
• LinQuest	• BAE	• Cisco Systems	• Actionable Solutions	• L3 Harris Technologies
• Lockheed Martin	• Cubic Corporation	• Perspecta	• Fulcrum IT Services	• Boeing
• Inmarsat	• UTC	• Leidos	• Engility	• Northrop Grumman
• Leonardo	• DynCorp	• Brit Systems	• Metis Celestar	• ERAPSCO
• MetTel	• General Atomics	• HPI Federal	• Assured Information	• General Atomics
• Sprint/T-Mobile	• Data Link Solutions	• Leonardo	• BAH	• Sierra Nevada Corporation
• Boeing	• Assurance Technology	• ICF	• G2 Global Solutions	• Lockheed Martin
• Centurum	• MicroTechnologies	• Parsons Corporation	• Dynetics	
• G2 Software Systems	• L3 Harris Technologies	• BAE	• CWU Inc.	**Electronic Warfare**
• Geocent	• Boeing	• IBM	• L3 Harris Technologies	
• CACI	• ViaSat	• NCI Information	• Northrop Grumman	• Northrop Grumman
• Forward Slope	• General Dynamics	• NetCentrics	• The Buffalo Group	• Raytheon
• Iridium Communications	• Lockheed Martin	• Boeing	• The Stratagem Group	• Georgia Tech Applied
• Advanced Sciences	• AEG Group	• Tapestry Solutions	• ManTech	• BAE
• Assurance Technology	• Northrop Grumman	• DTechLogic	• Systems Technology, Inc.	• L3 Harris Technologies
• Solute	• Textron	• SAIC	• Etegent Technologies	• American EW
• Data Intelligence	• Serco	• Dell	• Radiant Solutions	• Black Water Systems
• Motorola	• SAIC	• Oracle	• CoSolutions	
	• Intelligent Waves			

Source: Frost and Sullivan

Figure 1 – Key Competitors in the DoD C4ISR Market (by sector)

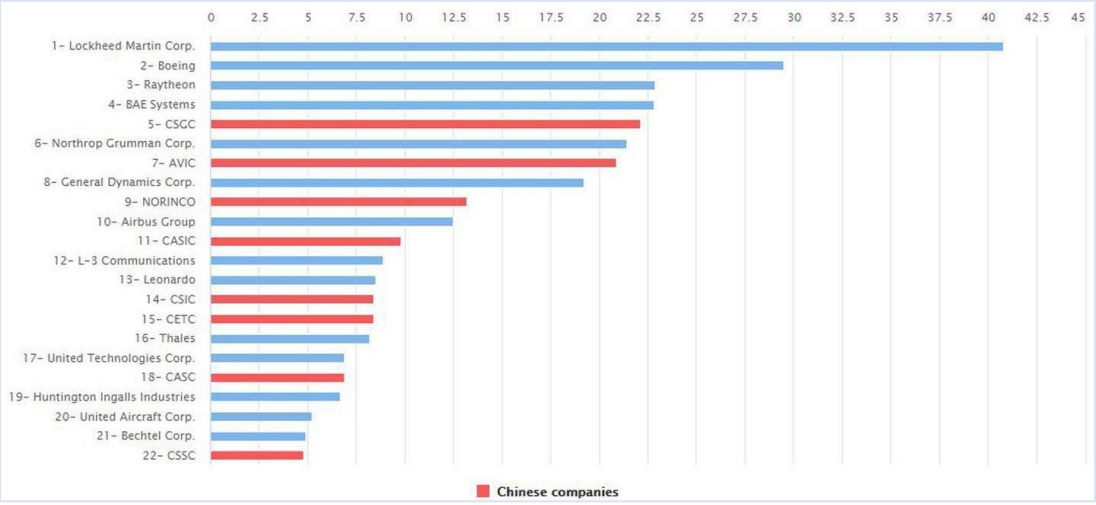

Figure 2 – Top 22 Global Defense Companies in 2016 (by sales)

Source: IISS, a London-based think tank, has calculated defense revenues for the largest Chinese companies to figure out how they stack up against their global counterparts. (IISS)

Endnotes

[1] U.S. Department of Defense, Office of the Deputy Secretary of Defense. 2021. *Creating Data Advantage*, by Kathleen Hicks, May 2021. https://media.defense.gov/2021/May/10/2002638551/-1/-1/0/DEPUTY-SECRETARY-OF-DEFENSE-MEMORANDUM.PDF

[2] Jaspreet Gill, "Return of CJADC2: DoD officially moves ahead with 'combined' JADC2 in a rebrand focusing on partners," Breaking Defense, May 16, 2023. https://breakingdefense.com/2023/05/return-of-cjadc2-dod-officially-moves-ahead-with-combined-jadc2-in-a-rebrand-focusing-on-partners/

[3] Karen Briggman, "C4ISR IS Lesson 1, Introduction to C4ISR Industry Study," accessed May 3, 2023, https://ndu1.sharepoint.com/:b:/s/msteams_1b61ab/EYfqgyiGoTdPtL1FVcgEmdQB0TY-8Hs21SN4QGHkPT-yfQ?e=TuuHQQ.

[4] Computer Security Resource Center. "Command and Control," Glossary, Information Technology Laboratory, National Institute for Standards and Technology. Accessed on May 9, 2023. https://csrc.nist.gov/glossary/term/command_and_control

[5] Hoehn, John, R., Caitlin Campbell, Andrew S. Bowen, 2022. "Defense Primer: What is Command and Control?" *Congressional Research Service*, IF11085, November 14, 2022. https://crsreports.congress.gov/product/pdf/IF/IF11805

[6] Department of Defense. 2017. "DoD Dictionary of Military and Associated Terms." March 2017. https://apps.dtic.mil/sti/pdfs/AD1029823.pdf

[7] Michael Ellmer, "The McNamara Line and The Jason's," *Grey Dynamics* (blog), April 16, 2021, https://greydynamics.com/the-jasons-and-the-mcnamara-line-a-tale-of-innovation-collateral-damage/.

[8] Sharon Weinberger, *The Imagineers of War: The Untold History of DARPA, the Pentagon Agency That Changed the World* (New York: Alfred A. Knopf, 2017), chap. 9.

[9] "Master the Art of Command and Control," U.S. Naval Institute, February 1, 2018, https://www.usni.org/magazines/proceedings/2018/february/master-art-command-and-control.

[10] M. Taylor Fravel, *Active Defense: China's Military Strategy since 1949* (Princeton University Press, 2019), https://doi.org/10.2307/j.ctv941tzj.

[11] Sandra I. Erwin, "Navy, Air Force Team Up in 'Joint Fires Network,'" National Defense Magazine, March 1, 2003. https://www.nationaldefensemagazine.org/articles/2003/2/28/2003march-navy-air-force-team-up-in-joint-fires-network

[12] Department of Defense, "Air-Sea Battle: Service Collaboration to Address Anti-Access & Area Denial Challenges," Air-Sea Battle Office. May 2013. https://dod.defense.gov/Portals/1/Documents/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf

[13] "SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.Pdf," 1, accessed March 14, 2023, https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.

[14] "C4ISR," Lockheed Martin, accessed May 5, 2023, https://www.lockheedmartin.com/en-us/capabilities/c4isr.html.

[15] "C4ISR Market: Global Industry Analysis and Forecast (2022-2029)," *MAXIMIZE MARKET RESEARCH* (blog), accessed May 6, 2023, https://www.maximizemarketresearch.com/market-report/global-c4isr-market/16148/.

[16] "Department of Defense Releases the President's Fiscal Year 2024 Defense Budget," U.S. Department of Defense, accessed May 6, 2023, https://www.defense.gov/News/Releases/Release/Article/3326875/department-of-defense-releases-the-presidents-fiscal-year-2024-defense-budget/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F3326875%2Fdepartment-of-defense-releases-the-presidents-fiscal-year-2024-defense-budget%2F.

[17] Based on seminar's discussions with industry representatives.

[18] The White House. 2022. "National Security Strategy." https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf.

[19] U.S. Department of Defense, "Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked." June 1, 2019. https://media.defense.gov/2019/Jul/01/2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF. (Accessed April 28, 2023

[20] Josh Rogin, "NSA Chief: Cybercrime constitutes the "greatest transfer of wealth in history," Foreign Policy, July 9, 2012. https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

[21] "National Security Strategy." Accessed November 9, 2022. https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf.
[22] "Charter of the Joint Requirements Oversight Council and Implementation of the Joint Capabilities Integration And Development System." Joint Chiefs of Staff, October 30, 2021. https://www.jcs.mil/portals/36/documents/library/instructions/cjcsi%205123.01i.pdf.
[23] Wolak, "Accelerating Progress: Transforming Capability Development Through Prototyping."
[24] "Article 1 Section 9 Clause 7." U.S. Constitution Annotated - Congress. https://constitution.congress.gov/browse/article-1/section-9/clause-7/.
[25] Vlaskovits, Patrick. "Henry Ford, Innovation, and That 'Faster Horse' Quote." Harvard Business Review, July 23, 2014. https://hbr.org/2011/08/henry-ford-never-said-the-fast.
[26] Christensen, Clayton M. The Innovator's Dilemma. New York, NY: Harper Business, 2011
[27] "Operating and Support Cost-Estimating Guide." Cost Assessment and Program Evaluation. Office of the Secretary of Defense, September 2020. https://www.cape.osd.mil/files/OS_Guide_Sept_2020.pdf.
[28] The Associated Press, "Putin: Leader in artificial intelligence will rule world," September 1, 2017, https://apnews.com/article/technology-russia-business-artificial-intelligence-international-news-bb5628f2a7424a10b3e38b07f4eb90d4.
[29] Paul Mozur, "Beijing Wants A.I. to Be Made in China by 2030, The New York Times, July 20, 2017, https://www.nytimes.com/2017/07/20/business/china-artificial-intelligence.html.
[30] Paul Scharre, America Can Win the AI Race, Foreign Affairs, April 4, 2023.
[31] Michael E. Porter, "The Five Competitive Forces That Shape Strategy," Harvard Business Review, January 2008 (15 pp.). https://nduezproxy.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,url,uid&db=bth&AN=28000138&site=ehost-live&scope=site
[32] Michael E. Porter, "The Five Competitive Forces That Shape Strategy," Harvard Business Review, January 2008 (15 pp.). https://nduezproxy.idm.oclc.org/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,url,uid&db=bth&AN=28000138&site=ehost-live&scope=site
[33] Global Aerospace & Defense Research Team at Frost & Sullivan, "US DoD C4ISR Growth Opportunities: The Shift to Multi-Domain Operations Will Open Up More Opportunities for Commercial Product Manufacturers," https://ndu-libguides-com.nduezproxy.idm.oclc.org/ld.php?content_id=65960353.
[34] Global Aerospace & Defense Research Team at Frost & Sullivan, *US Department of Defense C4ISR, 2022–2027*, K7C9-22 (Santa Clara, CA: Frost & Sullivan, 2022), https://ndu1.sharepoint.com/sites/UserCreated-Library-AS-ALL/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FUserCreated%2DLibrary%2DAS%2DALL%2FShared%20Documents%2FEarly%20Bird%2FDocuments%20for%20EB%2FU%2ES%2E%20Department%20of%20Defense%20C4ISR%2C%202022%E2%80%932027%2Epdf&parent=%2Fsites%2FUserCreated%2DLibrary%2DAS%2DALL%2FShared%20Documents%2FEarly%20Bird%2FDocuments%20for%20EB&p=true&ct=1684264229211&or=OWA%2DNT&cid=9a2e5807%2D95c3%2Dc1c3%2D8426%2D3c32faa91e8f&ga=1.
[35] "Pentagon Boosts Spending on R&D, JADC2, and Cybersecurity in $145B Budget," Breaking Defense, accessed March 18, 2023, https://breakingdefense.sites.breakingmedia.com/2023/03/pentagon-boosts-spending-on-rd-jadc2-rapid-experimentation-and-cybersecurity-in-fy24-request/.
[36] Global Aerospace & Defense Research Team at Frost & Sullivan, "Assessment of the US DoD C4ISR Market, Forecast to 2025: DoD Is Continuing Standardization and Qualitative Improvement Efforts by Expanding and Adopting More Innovative Commercial IT Technology," https://ndu-libguides-com.nduezproxy.idm.oclc.org/ld.php?content_id=65960355.
[37] Clark, Mason. "Institute for the Study of War Report Part Title: Russia's Main Lesson from Syria: Improving Command and Control Report Title: The Russian Military's Lessons Learned In Syria Report Subtitle: Military Learning And The Future Of War Series," 2021.
[38] Ashley Seager, "Russia pays off its Soviet era debts to the west," The Guardian, August 21, 2006. https://www.theguardian.com/business/2006/aug/22/russia
[39] Trading Economics, "Russia Indicators," accessed May 11, 2023, https://tradingeconomics.com/russia/indicators.
[40] Michael E. Porter, "The Five Competitive Forces That Shape Strategy," *Harvard Business Review* 86, no. 1 (January 2008): 78–93.
[41] Samuel Bendett, "Russia's Artificial Intelligence Boom May Not Survive the War."

[42] Yale School of Management, “Over 1,000 Companies Have Curtailed Operations in Russia—But Some Remain,” May 14, 2023, Accessed on 5/22/2023, https://som.yale.edu/story/2022/over-1000-companies-have-curtailed-operations-russia-some-remain."
[43] Masha Borak, “How Russia Killed Its Tech Industry,” MIT Technology Review, April 4, 2023, Accessed on 5/22/2023, https://www.technologyreview.com/2023/04/04/1070352/ukraine-war-russia-tech-industry-yandex-skolkovo/
[44] Vladimir Milov, “Beyond the Headlines: The Real Impact of Western Sanctions on Russia,” *European View* 22, no. 1 (April 2023): 149–50, accessed 5/11/2023, https://doi.org/10.1177/17816858231162460.
[45] Vladimir Milov.
[46]
[47] Vladimir Milov, “Beyond the Headlines.”
[48] Jonathan Ward, "China’s Vision of Victory," (*Ambassador’s Brief*, 2019), https://static1.squarespace.com/static/5925ea8d20099ef1f41e895f/t/5d70486a3abbbf0001aeaad0/1567639658708/J Ward+Ambassador+Brief+Final.pdf.
[49] Costello, John, 2016. “The Strategic Support Force: Update and Overview,” China Brief Volume: 16 Issue 19. *The Jamestown Foundation*, December 21, 2016. https://jamestown.org/program/strategic-support-force-update-overview/
[50] Engstrom, Jeffrey, Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR1708.html.
[51] Ibid.
[52] Ibid.
[53] Ibid.
[54] U.S. Department of Defense. 2022. “DoD Announces Release of JADC2 Implementation Plan.” U.S. Department of Defense, March 17, 2022. https://www.defense.gov/News/Releases/Release/Article/2970094/dod-announces-release-of-jadc2-implementation-plan/
[55] M. Taylor Fravel, *Active Defense: China’s Military Strategy since 1949*, Princeton Studies in International History and Politics (Princeton (N.J.): Princeton University Press, 2019).
[56] M. Taylor Fravel, Active Defense: China’s Military Strategy Since 1945. (Princeton: Princeton University Press), 2019, pp. 187-88.
[57] Fravel, pp. 210.
[58] Alex Stone and Peter Wood, “China's Military-Civil Fusion Strategy: A View from Chinese Strategists,” China Aerospace Studies Institute, Air University, Maxwell AFB, AL, June 15, 2020, pp 6, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2020-06-15%20CASI_China_Military_Civil_Fusion_Strategy.pdf, (accessed January 15, 2022)
[59] Stone and Wood, pp. 59.
[60] Richard A. Bitzinger, “China’s Shift from Civil-Military Integration to Military-Civil Fusion,” Asia Policy, Volume 16, Number 1, (Seattle, Washington: The National Bureau of Asian Research), January 2021, www.rsis.edu.sg/wp-content/uploads/2022/05/Asia-Policy-16.1-Jan-2021-Richard-Bitzinger.pdf, (accessed January 11, 2023).
[61] Weinbaum et al.
[62] “China’s Rise in the C4ISR Race - Defense One,” accessed May 7, 2023, https://www.defenseone.com/insights/cards/c4isr-military-nervous-system/7/?oref=d1-cards-cardstack-toc.
[63] Cortney Weinbaum et al., “Assessing Systemic Strengths and Vulnerabilities of China’s Defense Industrial Base: With a Repeatable Methodology for Other Countries” (RAND Corporation, February 11, 2022), https://www.rand.org/pubs/research_reports/RRA930-1.html.
[64] Weinbaum et al.
[65] Weinbaum et al.
[66] Roy Kamphausen, David Lai, and Andrew Scobell, “The PLA at Home and Abroad: Assessing the Operational Capabilities of China’s Military:” (Fort Belvoir, VA: Defense Technical Information Center, June 1, 2010), https://doi.org/10.21236/ADA525113.
[67] Weinbaum et al., “Assessing Systemic Strengths and Vulnerabilities of China’s Defense Industrial Base.”
[68] Weinbaum et al.

[69] "Weighing Giants: Taking Stock of the Expansion of China's Defence Industry," accessed May 8, 2023, https://www.tandfonline.com/doi/epdf/10.1080/10242694.2019.1632536?needAccess=true&role=button.
[70] Tarun Chhabra Kimball Rush Doshi, Ryan Hass, and Emilie, "Global China: Technology," *Brookings* (blog), April 27, 2020, https://www.brookings.edu/research/global-china-technology/.
[71] "Weighing Giants."
[72] Weinbaum et al., "Assessing Systemic Strengths and Vulnerabilities of China's Defense Industrial Base."
[73] Mordor Intelligence "US C4ISR Market Size," Industry Research Report - Growth Trends, 2023. https://www.mordorintelligence.com/industry-reports/united-states-c4isr-market (Accessed April 28, 2023).
[74]Christian Brose, "The Kill Chain: Defending America in the Future of High-Tech Warfare," (New York: Hachette Books, April 2020)
[75] Travis Sharp, "JADC2 spending is sprawling. DoD should keep watch, but Let It Go," Breaking Defense, October 20, 2022. https://breakingdefense.com/2022/10/jadc2-spending-is-sprawling-dod-should-keep-watch-but-let-it-go/
[76] Col(s) Kyle Takamura, "Joint Staff J-6 Command, Control, Communications, & Computers/Cyber" ("While You Were Out" 17X Transition Event, Washington, D.C, May 4, 2023).
[77] United States Marine Corps, *Command and Staff Action,* pg. 48.
[78] "SUMMARY OF THE JOINT ALL-DOMAIN COMMAND & CONTROL (JADC2) STRATEGY." 2022. https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF.
[79] "US Army Running SBU Variant of Mission Partner Environment." n.d. Janes.com. Accessed May 16, 2023. https://www.janes.com/defence-news/news-detail/us-army-running-sbu-variant-of-mission-partner-environment. [80] "United States Committee on Armed Services." n.d. www.armed-Services.senate.gov. https://www.armed-services.senate.gov/hearings/to-receive-testimony-on-the-posture-of-united-states-indo-pacific-command-and-united-states-forces-korea.
[81] NATO. 2022. "Emerging and Disruptive Technologies." NATO. December 8, 2022. https://www.nato.int/cps/en/natohq/topics_184303.htm.
[82] Goldgeier, Lindsey W. Ford and James. 2021. "Retooling America's Alliances to Manage the China Challenge." Brookings. January 25, 2021. https://www.brookings.edu/research/retooling-americas-alliances-to-manage-the-china-challenge/.
[83] The White House. 2022. "National Security Strategy." https://www.whitehouse.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf.
[84] The White House. 2022. "INDO- PACIFIC STRATEGY of the UNITED STATES." https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf.
[85] Harding et al.
[86] Harding et al.
[87] Harding et al.
[88] Levine, Peter. Defense Management Reform : How to Make the Pentagon Work Better and Cost Less / Peter Levine. [EBook]. Stanford University Press, 2020.
[89] Levine, Peter. Defense Management Reform : How to Make the Pentagon Work Better and Cost Less / Peter Levine. [EBook]. Stanford University Press, 2020.
[90] Levine, Peter. Defense Management Reform : How to Make the Pentagon Work Better and Cost Less / Peter Levine. [EBook]. Stanford University Press, 2020. P.145.
[91] Levine, Peter. Defense Management Reform : How to Make the Pentagon Work Better and Cost Less / Peter Levine. [EBook]. Stanford University Press, 2020. P.145.
[92] Ibid.
[93] Ibid.
[94] "Defense Management: Opportunities Exist to Improve DOD's Reform Efforts | U.S. GAO." US Senate: GAO, April 27, 2021. https://www.gao.gov/products/gao-21-532t.
[95] Levine, Peter. Defense Management Reform : How to Make the Pentagon Work Better and Cost Less / Peter Levine. [EBook]. Stanford University Press, 2020.
[96] Cook, Cynthia. "Is the National Defense Strategy Calling for Acquisition Reform?," November 2, 2022. https://www.csis.org/analysis/national-defense-strategy-calling-acquisition-reform.
[97] Mccusker, Elaine. "Reforming Defense Budgeting." Report. AEI Paper & Studies. Washington, DC: American Enterprise Institute, March 2023. Gale Academic OneFile. https://link-gale-com.nduezproxy.idm.oclc.org/apps/doc/A747080452/AONE?u=wash60683&sid=ebsco&xid=dd78d5b8.

[98] Sharon K. Weiner. Managing the Military : The Joint Chiefs of Staff and Civil-Military Relations. New York: Columbia University Press, 2022.
[99] Mccusker, 9.
[100] Ibid.
[101] Ibid.
[102] Levine, Peter. Defense Management Reform : How to Make the Pentagon Work Better and Cost Less / Peter Levine. [EBook]. Stanford University Press, 2020. P.145.
[103] "GDP Growth - Brazil." World Bank Open Data, 2023. Accessed April 23, 2023).https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=BR,
[104] Monica de Bolle, "Lula Is Back, but Can He Fix Brazil's New Problems?" The Peterson Institute for International Economics Monica, November 21, 2022. (Accessed April 22, 2023) https://www.piie.com/blogs/realtime-economics/lula-back-can-he-fix-brazils-new-problems.
[105] Simone Preissler Iglesias, "Lula to Visit Huawei Site in Shanghai, Potentially Irking US." Bloomberg.com. Bloomberg, April 11, 2023. (Accessed April 22, 2023) https://www.bloomberg.com/news/articles/2023-04-11/lula-to-visit-huawei-site-in-shanghai-potentially-irking-us#xj4y7vzkg?leadSource=uverify%20wall.
[106] Ryan C Berg and Carlos Baena. "The Great Balancing Act: Lula in China and the Future of U.S.-Brazil Relations." CSIS, April 19, 2023. https://www.csis.org/analysis/great-balancing-act-lula-china-and-future-us-brazil-relations (Accessed April 22, 2023).
[107] The Department of State. "Major Non-NATO Ally Status - United States Department of State." U.S. Department of State. U.S. Department of State, August 12, 2022. https://www.state.gov/major-non-nato-ally-status/ (Accessed April 22, 2023).
[108] "C4ISR." Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/c4isr.html. (Accessed March 20, 2023
[109] Gisela Grieger. "Towards a Joint Western Alternative to the Belt and Road Initiative?: Think Tank: European Parliament." Think Tank | European Parliament, January 12, 2021. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698824. (Accessed 21, 2023)
[110] Timothy Grose, James A. Millward, Jessica Batke, and Joanne Smith Finley. "Why Aren't More Countries Confronting China over Xinjiang?" ChinaFile, January 14, 2020. https://www.chinafile.com/reporting-opinion/viewpoint/why-arent-more-countries-confronting-china-over-xinjiang. (Accessed April 22, 2023).
[111] Matthew Kroenig. The Return of Great Power Rivalry: Democracy versus Autocracy from the Ancient World to the U.S. and China. New York, New York: Oxford University Press, 2022.
[112] Jonathan D. T. Ward. China's Vision of Victory. Giza, Egypt: Atlas Publishing and Media Company, 2019.
[113] M. Taylor Fravel. Active Defense: China's Military Strategy since 1949. Princeton, New Jersey: Princeton University Press, 2019.
[114] Rush Doshi. Long Game: China's Grand Strategy to Displace American Order. New York, New York: Oxford University Press in the United States of America, 2023.
[115] Dean Cheng. "Cyber Dragon: Inside China's Information Warfare and Cyber Operations." Santa Barbara, California ; Denver, Colorado, California: Praeger, 2017.
[116] David Anderson and Randall McCauley. "Ideology or Pragmatism? U.S. Economic Aid, Military Assistance, and Foreign Military Sales: 1950-2007." Strategic Insights VIII, no. Issue 3, August 2009.
[117] Emily M. Morgenstern and Nick M. Brown, *Foreign Assistance: An Introduction to U.S. Programs and Policy*, R40213, Congressional Research Service, Washington, D.C., January 10, 2022.
[118] "22a. Economic Growth and the Early Industrial Revolution." U.S. History: Pre-Columbian to the New Millennium. Independence Hall Association, (Accessed April 22, 2023). https://www.ushistory.org/us/22a.asp.
[119] Arthur Herman, "Freedom's Forge: How American Business Produced Victory in World War II," New York: Random House Trade Paperbacks, 2012.
[120] John Lewis Gaddis, "In Strategies of Containment: A Critical Appraisal of Postwar American National Security Policy," Chapter 8. Pp. 353–56. New York, New York: Oxford University Press, 2005.
[121] Emily M. Morgenstern and Nick M. Brown (2022)
[122] Ibid.
[123] David Anderson and Randall McCauley, 2009.
[124] Jonathan D. T. Ward, 2019, pp. 17.
[125] Barry Naughton, "In The Rise of China's Industrial Policy, 1978 to 2020," Chapter 4. pp. 86–90. México, D.F.: Universidad Nacional Autónomica de México, Facultad de Economía, 2021.

[126] Jonathan D. T. Ward, 2019, pp. 21.
[127] Ibid. pp. 20.
[128]Jane Perlez, "China Looks West as It Bolsters Regional Ties," the New York Times, September 7, 2013. https://www.nytimes.com/2013/09/08/world/asia/china-looks-west-as-it-strengthens-regional-ties.html, (Accessed April 23, 2023).
[129] Jonathan D. T. Ward, 2019, pp. 81.
[130] Ibid.
[131] Theodor Tudoroiu and Amanda R. Ramlogan, *The Myth of China's No Strings Attached Development Assistance: A Caribbean Case Study* (Lanham ; Boulder ; New York ; London, New York: Lexington Books, 2020), pp. 1.
[132] Turcsanyi, Richard, and Eva Kachlikova. "The BRI and China's Soft Power in Europe: Why Chinese Narratives (Initially) Won." Journal of Current Chinese Affairs 49, no. 1 (2020): pp. 58–81, https://doi.org/10.1177/1868102620963134 (Accessed April 27, 2023).
[133] Richard Ghiasy, Fei Su, and Lora Saalman. "The Maritime Silk Road." The 21st Century Maritime Silk Road: Security Implications and Ways Forward For The European Union. Stockholm International Peace Research Institute, 2018, pp. 8. http://www.jstor.org/stable/resrep24530.5 (Accessed April 27, 2023).
[134] Jonathan D. T. Ward, 2019, pp. 20, 57.
[135] Joshua Meservey. "Government Buildings in Africa Are a Likely Vector for Chinese Spying." The Heritage Foundation. Backgrounder No. 3476, May 20, 2020.
[136] *China's Technological Rise: Challenges to U.S. Innovation and Security*, 150th Congress, 1st Session (2017) Dean Cheng, Senior Advisor the Heritage Institute.
[137] Ibid.
[138] The Department of State. "U.S. Department of State - United States Department of State." The Joint Strategic Plan FY 2022-2027. The Department of State, March 2022.pp. 31. (Accessed April 23, 2023). https://www.state.gov/wp-content/uploads/2022/03/Final-State-USAID-FY-2022-2026-Joint-Strategic-Plan_29MAR2022.pdf.
[139] Xioalan Fu, *China's Role in Global Economic Recovery* (New York: Routledge, 2012) Section 1.7 https://books.google.com/books?id=oGKpAgAAQBAJ&pg=PT38.
[140] David E. Sanger and Catie Edmondson. "Russia Targeted Election Systems in All 50 States, Report Finds." The New York Times, July 25, 2019. https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html, (Accessed April 23, 2023).
[141] Kroenig. pp. 19–35.
[142] Ben Norton. "Brazil's Lula Travels to China and Calls to End US Dollar Dominance." Geopolitical Economy Report, April 16, 2023. https://geopoliticaleconomy.com/2023/04/15/brazil-lula-china-us-dollar-dominance/ (Accessed April 28, 2023).
[143] Kroenig, pp. 32.
[144] MarketLine, "C4ISR Sector Report," MarketLine Industry Profile, April 2023, https://advantage-marketline-com.nduezproxy.idm.oclc.org/Company/Index?recordtype=Companies&q[]=C4ISR&exactword=1&SearchKey=undefined&column=revenue&direction=Descending&pageNumber=1&pageSize=1000 (Accessed April 28, 2023).
[145] Mordor Intelligence "US C4ISR Market Size," Industry Research Report - Growth Trends, 2023. https://www.mordorintelligence.com/industry-reports/united-states-c4isr-market (Accessed April 28, 2023).
[146] Fenella McGerty and Meia Nouwens. "China's Military Modernization Spurs Growth for State-Owned Enterprises." Defense News. Defense News, August 21, 2022. https://www.defensenews.com/opinion/commentary/2022/08/08/chinas-military-modernization-spurs-growth-for-state-owned-enterprises/ (Accessed April 28, 2023).
[147] Alex Stone and Peter Wood, "China's Military-Civil Fusion Strategy: A View from Chinese Strategists," China Aerospace Studies Institute, Air University, Maxwell AFB, AL, June 15, 2020, pp 59, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2020-06-15%20CASI_China_Military_Civil_Fusion_Strategy.pdf, (accessed January 28, 2022)
[148] Ibid, pp. 59.
[149] Mehta, Aaron. "These 7 Chinese Companies Each Topped $5B in Defense Sales - and Could Rival American Firms." Defense News. Defense News, August 17, 2022. https://www.defensenews.com/top-100/2018/08/23/these-7-chinese-companies-each-topped-5b-in-defense-sales-and-could-rival-american-firms/ (Accessed April 28, 2023).
[150] Jonathan D. T. Ward, pp. 229-230.
[151] Kroenig, pp. 217.

[152] Based on author's conversations with C4ISR industry representatives.
[153] "Foreign Assistance." Foreignassistance.gov. https://www.foreignassistance.gov/, (Accessed April 28, 2023).
[154] Ibid.
[155] Lauren Woods. "U.S. Arms Sales: 2021 – Early 2022." Security Assistance Issue Paper, July 2022. https://securityassistance.org/publications/u-s-arms-sales-2021-early-2022/ (Accessed April 29, 2023).
[156] Frost and Sullivan Global Aerospace and Defense Research Team. "U.S. Foreign Military Sales Market Growth Opportunities." K8BD-22, Frost and Sullivan, March 2023.
[157] Jonathan D. T. Ward, pp. 229-230.
[158] Ely Ratner, Daniel Kliman, Susanna V. Blume, Rush Doshi, Chris Dougherty, Richard Fontaine, Peter Harrell, Martijn Rasser, Elizabeth Rosenberg, Eric Sayers, Daleep Singh, Paul Scharre, Loren DeJonge Schulman, Neil Bhatiya, Ashley Feng, Joshua Fitt, Megan Lamberth, Kristine Lee, and Ainikki Riikonen, "Rising to the China Challenge Renewing American Competitiveness in the Indo-Pacific," Center for a New American Security, January 28, 2020, pp. 19 http://files.cnas.org/backgrounds/documents/CNAS-Report-NDAA-final-6.pdf?mtime=20200116130752&focal=none (accessed April 25, 2023)
[159] Ratner et. al, pp. 15-16.
[160] Nahal Toosi, "'Frustrated and Powerless': In Fight with China for Global Influence, Diplomacy Is America's Biggest Weakness." POLITICO, October 23, 2022. https://www.politico.com/news/2022/10/23/china-diplomacy-panama-00062828 (Accessed April 23, 2023).
[161] The White House. Biden-Harris National Security Strategy. October 2022.
The White House. "Indo-Pacific Strategy of the United States." February 2022 https://media.defense.gov/2019/Jul/01/2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF (Accessed April 28, 2023); and
U.S. Department of Defense, "Indo-Pacific Strategy Report: Preparedness, Partnerships, and Promoting a Networked." June 1, 2019. https://media.defense.gov/2019/Jul/01/2002152311/-1/-1/1/DEPARTMENT-OF-DEFENSE-INDO-PACIFIC-STRATEGY-REPORT-2019.PDF. (Accessed April 28, 2023)
[162] Ratner et. al, pp. 4.
[163] Ibid. pp. 4.