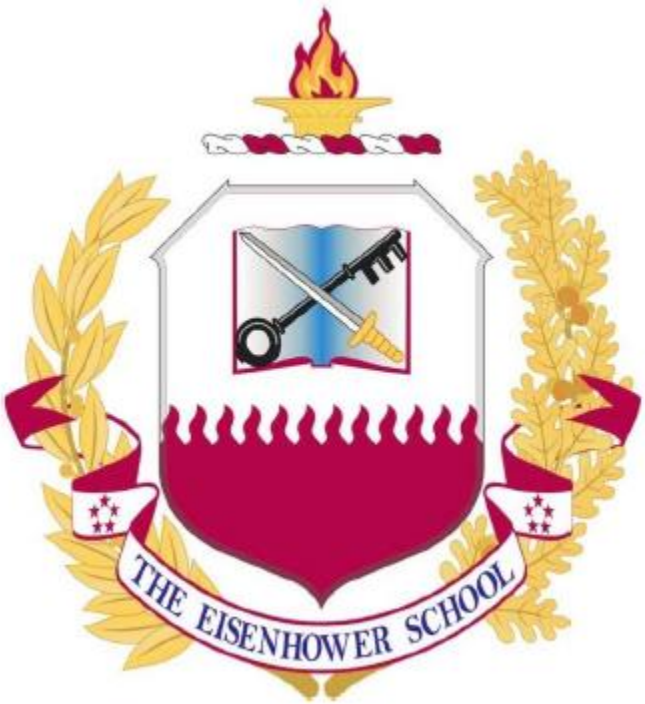
Spring 2021

Industry Study

Industry Report

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

Industry Study of Joint All-Domain Command and Control (JADC2): Competition, Culture, and Complexity



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

Table 1: C4ISR Seminar Members

C4ISR Seminar	
Name	**Organization**
Lt Col John Anderson	U.S. Air Force (USAF)
Lt Col Aaron Capizzi	USAF
Ms. Leah Cook	National Security Agency (NSA)
Col Fernando Cruz	USAF
LTC Julia Donley	U.S. Army (USA)
Mr. Trent Gallant	NSA
Mr. Christopher King	Defense Security Cooperation Agency
Lt Col Michael Kruk	U.S. Space Force
COL Charles Lockwood	USA
Lt Col David Madson	USAF
LTC Daniel Poole	USA
LTC Thomas Potter	U.S. Army National Guard
CAPT William Reed	U.S. Navy (USN)
COL Michael Shouse	USA
Lt Col Clifford Taylor	U.S. Air National Guard
CDR Richard Yeatman	USN

Table 2: C4ISR Faculty Members

C4ISR Faculty		
Name	**Organization**	**Position**
COL Karen Briggman	USA	IS Faculty
RADM (RET) Roseanne LeVitre	Defense Intelligence Agency	IS Faculty
Ms. Candy Green	Department of State	Industry Analysis Faculty
Lt Col John McAfee	USAF	Strategic Acquisition and Resourcing

Executive Summary

For the third year, the Eisenhower School (ES) for National Security and Resource Strategy studied the Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) industry. The focus for the academic year 2020-2021's C4ISR Industry Study is the Department of Defense's (DoD) Joint All-Domain Command and Control (JADC2).

C4ISR systems are critical for enabling an operational all-domain command and control system. Considering the Joint Force will face acute time, distance, and anti-access/area-denial (A2/AD) operational challenges as described in the 2018 National Defense Strategy (NDS), it is all the more imperative that the DoD be ready for high-end conflict against great power competitors, China and Russia.[1] To deter Chinese or Russian aggression and degrade their A2/AD networks, the U.S. must be able to rapidly plan and execute operations across all domains, services, and allies in a synchronized and cooperative manner.[2] To counter its evolving GPC (GPC) competitors, the U.S. is pursuing the JADC2 initiative. JADC2 is the "DoD's concept to connect sensors from all of the military services - Air Force, Army, Marine Corps, Navy, and Space Force - into a single network."[3]

Making decisions within minutes or seconds instead of the current 72-hour operational planning cycle is critical in delivering JADC2. Future conflicts require speed and agility, and the DoD has also noted that its existing C2 architecture is insufficient to meet the demands of the NDS.[4] Planners hope JADC2 will apply technology to speed the military science of decision-making, translating those gains to aid decision-makers and effectively defend and deter GPC threats.

The questions used to identify the problem and guide this study are: 1) What are specific challenges identified by DoD stakeholders in designing and integrating technologies to deliver JADC2 (i.e., competition, complexity, and culture). 2) What competitive advantages does the U.S. enjoy in C4ISR industries that support JADC2? 3) What is the capability and capacity of the U.S to sustain its C4ISR technology advantages within GPC? 4) How will acquisition and security processes and policies adapt to: support multi-domain operational constructs, integrate/support inclusivity with coalition partners, incentivize innovation rather than sustainment within the Defense Industrial Base (DIB) and across industry, support rapid and iterative development (Agile), and increase competition?

The Joint Force faces many challenges in planning and implementing JADC2, but contrary to popular belief, funding is not its most significant hurdle. DoD's 2021 budget includes $58.21 billion for C4ISR programs, an increase of $1.37 billion, or 2.4% over the 2020 request, and DoD spending for 2020-2025 is estimated to grow at a compound annual growth rate (CAGR) of 1.5%.[5]

JADC2's primary issues are the challenges that arise with most institutional change; technical, policy, and process challenges that come with the adoption and implementation of JADC2. These challenges are all rooted in cultural and doctrinal differences. The services, Congress, and industry each have unique cultures, bureaucracies, and operational structures that inform their vision for JADC2 and drive their development of material solutions.

America's C4ISR manufacturers can develop technologies for JADC2 and are working to deliver tools to enable joint multi-domain operations in a synchronized, cooperative, and efficient manner. However, the integration of these technologies and capabilities across all

domains, services, and allies are challenges that cannot be overcome by industry or technology alone.

To successfully implement JADC2, the DoD should look for more solutions than simply bigger budgets and new exquisite platforms. The Joint Force must leverage the existing technologies within the U.S. C4ISR industry and America's competitive tech industry and innovative spirit to design a user-focused JADC2. DoD leaders, at all levels, must work to ensure that process challenges and cultural challenges, and aversion to risk inhibit the adoption of JADC2. A truly joint (and combined) warfighting concept must also leverage warfighter expertise and build trust across departments, services, partners, and allies.

To ensure the successful implementation of JADC2, the C4ISR Industry Study submits the following four recommendations and bold actions: **1) the Joint Staff should undertake an evaluation of the market strengths and weakness of its great power competitor to leverage U.S. dominance and hedge against GPC advantage; 2) the DoD must implement reforms to the its acquisition policies and processes to encourage competition in the C4ISR market; 3) the DoD should develop agreements and standards that enable a trust-based culture for joint and coalition warfighting; and 4) the DoD should continuously evaluate security/classification requirements to remove hurdles that prevent effective interoperability and delegate an authorized board of senior stakeholders that can adjudicate hurdles beyond the scope of individual services.**

Implementing these proposed recommendations will require bold actions:

1) Joint Staff understand the market strengths and weakness of its great power competitor,

    - U.S. Strengths – Innovation culture, Technology Industry, “Fail Fast Fail Often” culture, DevSecOps model of rapid application development and deployment, and a vast network of partners and allies.

    - U.S. Limitations – Federal acquisition process, inefficient communication between DoD, Congress, and industry; and diminishing STEM labor force (quantity and quality).

    - China Strengths – Military-Civilian Fusion strategy, large manufacturing workforce, the dominant supplier of rare-earth materials; 5G technology leader; and robust R&D capital investments.

    - China Limitations – Centralized party control of industry hinders innovation, a vast unskilled labor force, and reliance on foreign technology and systems.

    - Russia Strengths – Clear demand signal from central government and skilled technical workforce in software development and space launch.

    - Russia Limitations – Competition-limiting firm structure and an innovation-stifling cultural environment and reliance on foreign suppliers and foreign financing.

2) Implement reforms to the DoD's acquisition policies and processes that encourage competition in the C4ISR market.

    - Modernize program life cycles to focus on rapid development and deployment rather than long-term sustainment of outdated systems and divest antiquated legacy programs.

    - Educate workforce on effective risk management; balance risks against rewards to deliver minimal viable products and support rapid development and deployment cycles.

3) Develop a trust-based culture for joint and coalition warfighting.

    - Implement, train, and trust the Joint Warfighting Concept.

    - Break down service-centric silos at all levels across all domains.

    - Encourage healthy interservice competition and innovation to develop JADC2.

    - Immediately Integrate partners and allies into JADC2 concept development.

4) Continuously evaluate security/classification requirements to remove hurdles that prevent effective interoperability and delegate an authorized board of senior stakeholders to adjudicate hurdles beyond the scope of individual services.

    - Include American partners and allies from the start; not including them creates weakness.

    - Sharing classified information across a coalition network is more a cultural hurdle than a protecting classified data challenge.

    - Invest in partnerships with international partners to ensure U.S. and partners and allies industries support emerging technological development and provide additional industrial output in the event of a contingency.

Disclaimer: The 2020-2021 academic year at the Eisenhower School was virtual due to the COVID-19 pandemic. In March 2021, the C4ISR IS was approved for a limited in-person classified sessions, and in April 2021 was approved to conduct in-person site visits to a limited number of C4ISR companies. Due to the COVID-19 restrictions, the IS had limited access to classified information and discussions hindering the TS/SCI component of the IS. Therefore, research and analysis conducted used open-source data, and classified programs supporting C4ISR and JADC2 are not addressed in this industry study.

Table of Contents

(use hyperlinks below to select any section of the paper)

Introduction

This is the third year an Eisenhower School Seminar researched the Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Industry Study. The scope of this report covers the Joint All-Domain Command and Control (JADC2) component of C4ISR. C4ISR systems are critical for enabling an operational all-domain command and control system. Considering that the Joint Force will face acute time, distance, and anti-access/area-denial (A2/AD) operational challenges as described in the 2018 National Defense Strategy (NDS), it is more imperative that the DoD be ready for high-end conflict against great power competitors, China and Russia.[6]

Since the end of the cold war, the U.S. and its partners and allies enjoyed the ability to deliver overwhelming military force across the world and dominate any opponent via conventional warfighting techniques. This freedom of movement and economic leverage allowed the U.S. to maintain its "command of the commons" in nearly every corner of the globe.[7] However, with the emergence of GPC, the paradigm has shifted. China and Russia have established themselves as near-peer competitors. The U.S. and its partners and allies no longer have an uncontested military and economic advantage in this new geopolitical environment. While neither competitor is equipped or postured to supplant the U.S. and its partners and allies' global presence, they have taken steps to expand their military presence (i.e., China in the South China Sea and Russia in Crimea) threatening world order, peace, and democracy. Furthermore, China and Russia have implemented Civilian-Military Fusion (MCF) strategies that harness investments in dual-use technologies to grow their economies and field technically advanced military capabilities.

Historically, the U.S. has leveraged its technological innovations and superior defense industrial base to provide strategic offsets against its major rivals. Today, DoD is developing joint all domain capabilities to counter the aggressive expansion efforts of its great power competitors. Under this context, JADC2 can be understood as the DoD's attempt to implement Former Deputy Defense Secretary Bob Work's Third Offset initiative. Work described his initiative as the means to offset adversary advances in A2/AD weapons and other emerging technologies.[2] JADC2 envisions becoming the architecture of this third offset strategy. The DoD defines JADC2 as a "concept to connect sensors from all of the military services - Air Force, Army, Marine Corps, Navy, and Space Force - into a single network."[8]

The criticality of delivering JADC2 is evident as future conflicts within the GPC may require decisions to be made within minutes or seconds instead of the current 72-hour operational planning cycle. The DoD has also noted that its existing C2 architecture is insufficient to meet the demands of the NDS.[9] Planners hope JADC2 will apply technology to speed the military science of decision-making, translating those gains to aid decision-makers and effectively defend and deter GPC threats.

The questions guiding this study are: 1) What are specific challenges identified by DoD stakeholders in designing and integrating technologies to deliver JADC2 (i.e., competition, complexity, and culture). 2) What competitive advantages does the U.S. enjoy in C4ISR industries that support JADC2? 3) What is the capability and capacity of the U.S to sustain its C4ISR technology advantages within GPC? 4) How will acquisition and security processes and

policies adapt to: support multi-domain operational constructs, integrate/support inclusivity with coalition partners, incentivize innovation rather than sustainment within the Defense Industrial Base (DIB) and across industry, support rapid and iterative development (Agile), and increase competition?

Planners envision that JADC2 will apply technology to speed the military science of decision-making, translating those gains to aid decision-makers and effectively defend and deter GPC threats. This report focuses on the competition, complexity, and cultural factors impacting the definition, development, and implementation of JADC2. Specifically, the cultural differences within and between services, Congress, and industry; the technological complexity and policy requirements of interoperating with partners and allies; the complexity of outdated technology and the cultural mindset hindering the divestment of legacy systems; and the culture and complexity of burdensome security/classification requirements and acquisition policies and processes. Once DoD and the services understand and define the problem, they can achieve progress towards a joint solution.

The Joint Force faces many challenges in planning and implementing JADC2, but contrary to popular belief, funding is not its most significant challenge. DoD's 2021 budget includes $58.21 billion for C4ISR programs, an increase of $1.37 billion, or 2.4% over the 2020 request, and DoD spending for 2020-2025 was estimated to grow at a compound annual growth rate (CAGR) of 1.5%.[10] Furthermore, research and development test and evaluation (RDT&E) funding is projected to account for the largest portion of the 2021 budget, totaling $24.55 billion.[11]

JADC2's primary issues are the challenges that arise with most institutional change; there are technical, policy, and process challenges that come with the adoption and implementation of JADC2. These challenges are all rooted in cultural and doctrinal differences. The services, Congress, and industry each have unique cultures, bureaucracies, and operational structures that inform their vision for JADC2 and drive their development of material solutions. These visions and associated material solutions are all being programmed while the Joint Staff is attempting to formalize the policies, doctrine, and requirements for the JADC2 concept.[12] Concurrently, America's C4ISR industry is viewing the DoD's efforts and is working to develop technologies to help the department rapidly plan and execute joint multi-domain operations in a synchronized, cooperative, and efficient manner. However, the integration of these technologies and capabilities across all domains, services, and allies are challenges that cannot be overcome by industry or technology alone.

The DoD, spearheaded by Joint Staff J6, leads a Joint Cross-Functional Team to steer the disparate efforts as the concept evolves.[13] However, the lack of a singular vision has led services and industry to build their JADC2 roadmaps and all efforts leave Congress in an unsettled position. Committees and Representatives understand the need to modernize the force to deter GPC competitors but feel underinformed and uncertain about efficiently spending taxpayer money.

In parallel to U.S. efforts, America's partners and allies also understand the need to modernize and support All-Domain Operations. America's partners and allies are focusing on modernizing their industries, systems, and processes so they can contribute and connect in future

all-domain coalitions. However, the DoD has not established clear guidance on how this will occur. Absent a clear understanding of the direction and implementation, partners and allies are left with a conundrum: modernize now and hope they will connect to future coalitions or wait for the DoD to provide clarity before a contingency arises. Neither of these two options is satisfactory, as partners and allies and GPC industries look to reduce U.S. exports and global market share.

To overcome the complexity of implementing JADC2, the DoD must do more than simply request larger budgets to build exquisite new platforms. To successfully conduct Joint, All-Domain operations, the Joint Force must develop a coherent vision that incorporates warfighting capabilities across all domains, services, allies, and partners. This vision should leverage the existing and emerging technologies within both U.S. and friendly C4ISR industries to harness innovative capabilities for JADC2. DoD leaders, at all levels, must work to ensure that process challenges, like federal acquisitions, and cultural challenges, like service cultures and aversion to risk, do not inhibit the adoption of JADC2. It must continue to develop a truly joint (and combined) concept of warfighting by leveraging warfighter expertise and building trust across departments, services, partners, and allies.

While this report presents bold actions to shape the development of JADC2, the authors agree that its goals must not change. To deter Great Power Competitors, the U.S. and its allies and partners must not delay bringing JADC2 to fruition. The development and implementation of combined capabilities will ensure the U.S. and its coalitions can successfully deter and defend against China and Russia and ensure that Great Power Competition does not lead to Great Power Conflict.

The Great Power Competition in the C4ISR industry

The U.S.' robust Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) industry develops the technologies and capabilities needed for JADC2. However, it is not enough for the U.S. C4ISR industry to be capable of delivering innovative C4ISR solutions to the warfighter with alacrity; it must be *more* capable and *more* rapid than its great power competitors.

The U.S. innovation ecosystem has developed and advanced defense technologies since World War II. These Defense Industrial Base (DIB) created groundbreaking technologies such as jet aircraft, radar, GPS, the Internet, networked computers, and wireless communications[14] that provided the U.S. with a marked advantage over its competitors. They also allowed the U.S. to meet its national security requirements while supporting the growth and advancement of the nation's economy, and the U.S. C4ISR industry is no different.

Using Porter's Diamond Framework to evaluate the great power competitors' C4ISR industries, we can characterize the national environment in which they compete. Porter's Diamond posits that "four broad attributes…attributes that individually and as a system constitute the diamond of national advantage, the playing field that each nation establishes and operates for its industries. These determinants create the national environment in which companies are born and learn how to compete."[15] The attributes are:

1. *Factor Conditions.* The nation's position in factors of production, such as skilled labor or infrastructure, necessary to compete in a given industry.
2. *Demand Conditions.* The nature of home-market demand for the industry's product or service.
3. *Related and Supporting Industries.* The presence or absence in the nation of supplier industries and other related industries that are internationally competitive.
4. *Firm Strategy, Structure, and Rivalry.* The conditions in the nation governing how companies are created, organized, and managed, as well as the nature of domestic rivalry.[16]

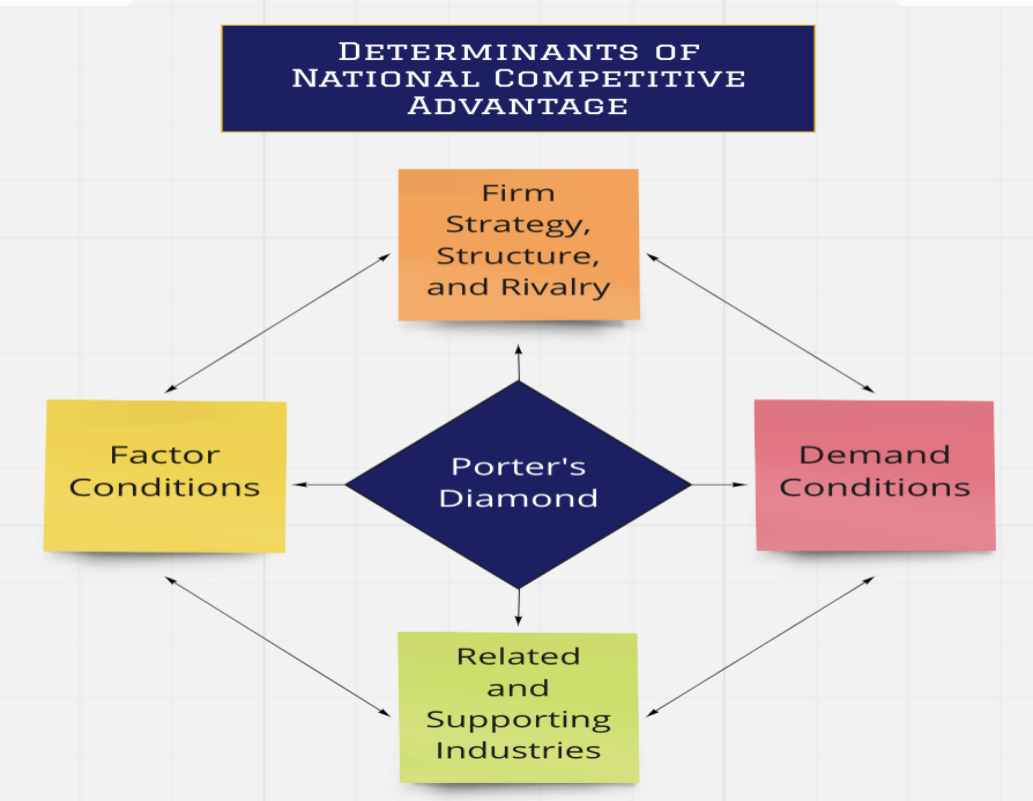


Figure 1: Michael Porter's Diamond
Source: The Competitive Advantage of Nations, Porter, 1990

Employing Porter's four attributes, we assessed how Chinese and Russian C4ISR companies develop and compete to achieve international competitive success. These characterizations provide the contextual backdrop against which to compare the U.S. C4ISR industry. In contrast, by investigating Russia's competitive advantages, historical events that have shaped Russia's prioritization of C4ISR over the last 30 years emerge. Further, Porter's framework demonstrates the value of China's civil-military synergy policies. These policies, first envisioned in the late 1970s and1980s, have created the foundation upon which China pursues C4ISR efforts today. While both China's and Russia's C4ISR industries are continuously evolving to meet increasing demand, Porter's framework demonstrates critical limitations that can be exploited to ensure they are denied a significant competitive advantage in C4ISR. The following sections provide an overview of the Chinese, Russian, and U.S. C4ISR industries through the lens of Porter's Diamond.

Analysis of China C4ISR Industry

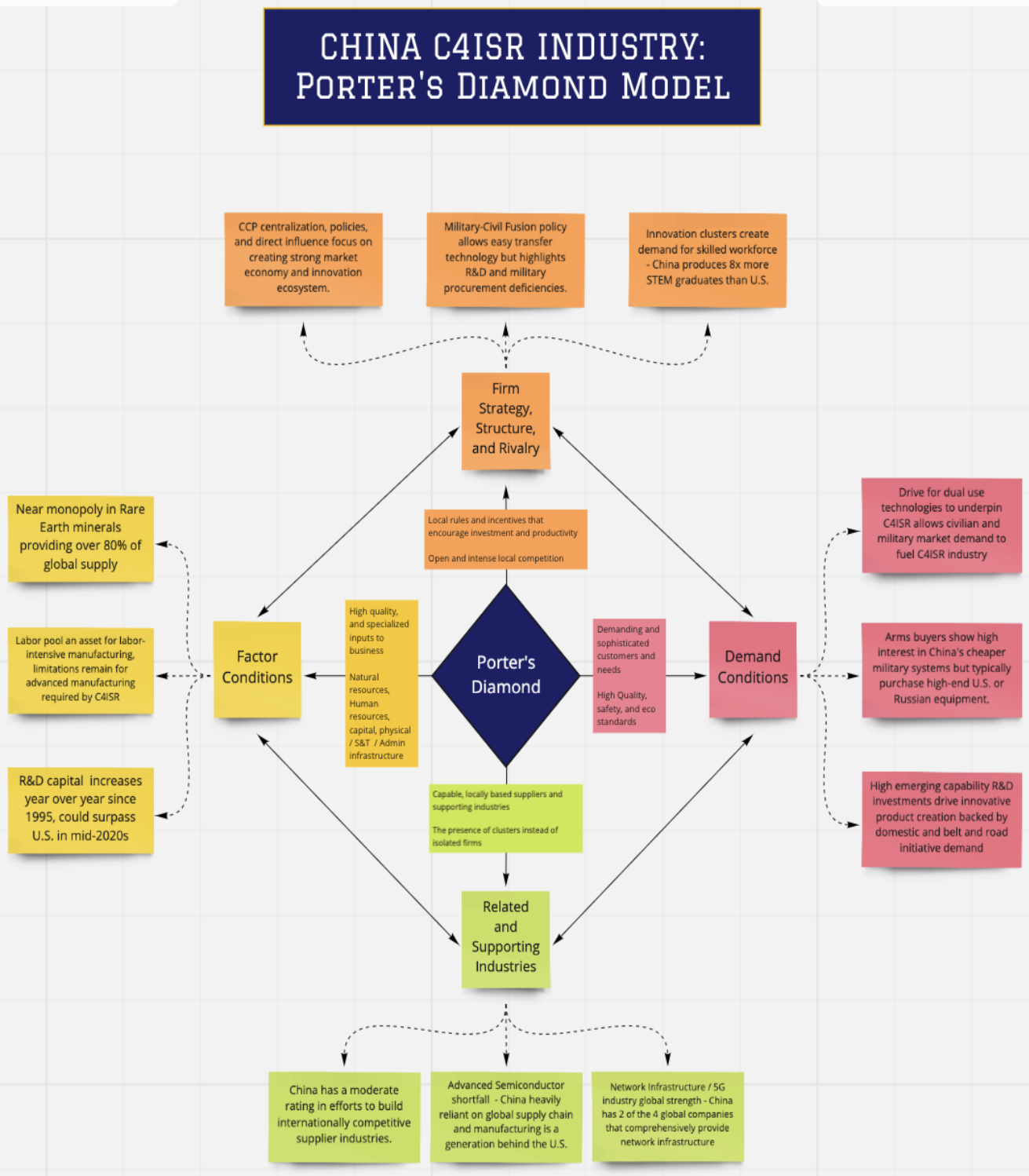


Figure 2: Porter's Diamond Analysis of China's C4ISR Industry

Related and Supporting Industries

In *The Competitive Advantage of Nations*, Michael Porter argues that the presence or absence of related internationally competitive supplier industries determines the country's competitive advantage.[17] Concerning China, multiple related and supporting industries contribute to its attempt to create its C4ISR industry competitive advantage. The two critical supporting industries that have the potential for the most prominent impacts are 1) semiconductors for building C4ISR systems and 2) the (enterprise) information technology that comprises China's network backbone, enabling C4ISR data transfer between collection assets, decision-makers, and shooters. The Chinese Communist Party (CCP) has recognized the importance of investing heavily in these sectors, reportedly dedicating $1.4T between 2020 and 2025 to build the foundation for future success.[18]

The DoD's use of Network-centric warfare (NCW) in the Gulf War inspired China's focus on the C4ISR market.[19] China is developing competitive semiconductor and network backbone industries to create permanent national advantages. This Chinese focus is especially relevant in the C4ISR market segment, as the NCW model generates combat power by effectively linking (or networking) actors, sensors, and decision-makers.[20] Since all C4ISR systems contain semiconductors, they are fundamental to sustaining current equipment and developing emerging technologies. These moves are already bearing fruit: according to a Congressional Research Services report, "China's state-led efforts to develop an indigenous vertically integrated semiconductor industry are unprecedented in scope and scale," and used legal and illegal means to try and establish it.[21]

Additionally, China is pursuing technologies to establish itself as a leader in network infrastructure technologies through investments in 5G technology. It tells that of the four companies currently providing telecommunications equipment infrastructure globally, two are Huawei and ZTE. Both are state-sponsored Chinese companies or colloquially titled 'champions' by the CCP.[22] Despite their state-sponsorship, the fierce national competition between China's tech giants drives innovation and strengthens China's C4ISR diamond despite relying on a global supply chain.

China's state-sponsored efforts do not always translate to success. Despite the gains in 5G and infrastructure technologies, the country remains woefully behind in semiconductor development. Despite investing nearly $20B in its semiconductor industry is at least a generation behind the U.S.[23] This lagging may indicate the current market for semiconductors and the global diversity of their supply chains. These factors make it virtually impossible for any country to develop them independently. China's forced entry into the market has encouraged competitors from teaming with Chinese industries in the segment.

Factor Conditions

Under Porter's model, military/security disadvantages can act as a fear-based motivator for innovation and upgrades; therefore, they count as competitive factor conditions. China's 2049 goal to produce a "world-class military" combined with its realistic assessment of its current inadequacies are the primary drivers behind its modernization and innovation initiatives.[24] Chairman Xi and the CCP have loudly broadcast their intentions to meet these goals, creating further impetus achieve them by any means necessary and ensure the party does not lose face.

Additionally, China's natural resources, labor pool, and capital investments in C4ISR systems are key factor conditions that hold the potential to creating China's competitive advantage in C4ISR.

Among its natural resources, rare-earth materials prove to be some of the most important resources required to produce modern C4ISR systems. They are also critical for making a range of emerging technologies, including batteries necessary to power everything from military hardware to civilian automobiles. China currently dominates the rare-earth global supply, producing over 80 percent of the global supply. This near monopoly places the country in a prime position in the C4ISR value chain.[25] Despite U.S. and the European Unions' attempts to diversify rare earth supply chains away from China, pollution produced during the refinement process makes it politically challenging to re-shore mining operations.

Conversely, although China's natural resources strengthen its C4ISR competitiveness, its labor pool creates some limitations. China's large population, geared to support labor-intensive manufacturing. This abundance of labor helped fuel the massive economic growth from the 1980s until the 2010s. However, China has modernized its labor pool, facing the same challenges that post-industrial economies face: a shrinking labor pool forced to support an aging population. A lack of specialized education also threatens China's labor pool. Although its graduates three times as many STEM students as the U.S. each year, its large population dilutes these numbers.[26] Many of China's workers are not educated and do not have the specialized skills necessary to work in modern manufacturing. This lack of skilled labor slows the development of advanced manufacturing techniques required for China's C4ISR system production. Despite its limiting characteristics, China's labor pool generates 28 percent of global exports for labor-intensive electronics and optical products, adding some strength to its C4ISR diamond.[27] Although not yet independent in advanced manufacturing required for C4ISR competitive advantage, China overcomes its manufacturing deficiencies by acquiring advanced U.S. and Taiwanese chip technology.[28]

One factor condition China continues to strengthen year over year is its R&D expenditures. According to the Center for Strategic and International Studies, China has increased its R&D investments every year since 1995, reaching almost $426 billion in 2018 for civilian and military R&D combined.[29] In comparison, U.S. R&D spending totaled $580.0 billion in 2018, per the Congressional Research Services analysis.[30] Experts project China's robust R&D capital investments could surpass U.S. R&D funding by the end of 2022.[31] It is important to note that these numbers are estimates; due to China's secrecy concerning military investments, with some foreign estimates claiming that the numbers are closer to double the official tallies.[32] Regardless of the actual dollar figure, China's civil fusion policy ensures that the entire country profits from its R&D spending. The policy directs R&D transfers between the civilian and military sectors to reduce R&D investment redundancy and ensure gains throughout the economy. Additionally, any civilian technological advance could be shared with the military, allowing the defense industry to reap the benefits of civilian R&D investments.

Firm Strategy, Structure, and Rivalry

Many experts describe China's economic and innovation ecosystem development approach as a textbook example of a whole-of-nation effort.[33] Since the early 1980s, China has advanced policies to increase synergy between its civilian and military sectors and gain efficiencies from innovative efforts. President Xi Jinping formally elevated MCF as a national strategy in more recent years. A Massachusetts Institute of Technology defense innovation report argues that the CCP's MCF strategy allows China to remove the barriers between civilian and military R&D ecosystems and enable dual-use technologies to transfer quickly across the national system.[34] The MCF policy allows the central government to direct technology transfers across its national ecosystem. The only downside to this approach may be the length of time it takes China to replace foreign technology and systems with nationally designed and developed systems. China's ability to do so quickly will determine if its policy is successful. Furthermore, the CCP's policies attempt to create a robust, resilient national innovation ecosystem that requires human capital to generate the innovation has its limitations.

The CCP seems to understand its vast unskilled labor pool is not the long-term strategy to achieving its 2049 revitalization goals and has focused its efforts on establishing an innovation ecosystem that supports growing a skilled national workforce. Since the 1970s economic reforms, the CCP's policies sought to create national innovation clusters. China's recent policies incentivize higher education to provide the increased STEM graduates required by its clusters. China's policies to reform its economy, incentivize its education system for skilled STEM graduates, and establish growing innovation clusters create a foundation for the national demand conditions that helps strengthen its C4ISR diamond.

Demand Conditions

The third element of Porter's framework is demand conditions, or simply put, the ability of a country to use its domestic demand to spur international competitiveness.[35] The most significant contributors to China's C4ISR demand conditions are the CCP's drive to develop a digital economy supported by nationally produced dual-use technologies, MCF policy, and defense contractors that sell both military and civilian products. China's C4ISR demand conditions characteristics allow for the civilian and military market demand to jointly strengthen the C4ISR industry.

China's information technology market is progressing and is supported by characteristics that predict continued growth. China's large market "enables rapid, large-scale commercialization of digital business models."[36] According to Porter, the size of China's population stimulates some domestic demand; however, domestic buyers must be demanding to drive innovation from producers.[37] As China's GDP per capita rises, China's product quality should also. As incomes rise, Chinese consumers not satisfied with the domestic brands' quality will demand better product choices.[38] China's continued focus on increasing its GDP per capita could influence future domestic customer demand and stimulate producer innovation and quality over time.

China's heavy R&D investments in emerging capabilities expect to generate innovative products backed by domestic demand and exports. The establishment of domestic and global smart cities relying on China-produced technologies would create constant demand for upgrade

and sustainment of those cities, potentially creating a significant C4ISR competitive advantage through dual-use technology reliance. China's national economic structure provides it several competitive advantages in which to compete with the U.S fiercely.

Analysis of Russia's C4ISR Industry

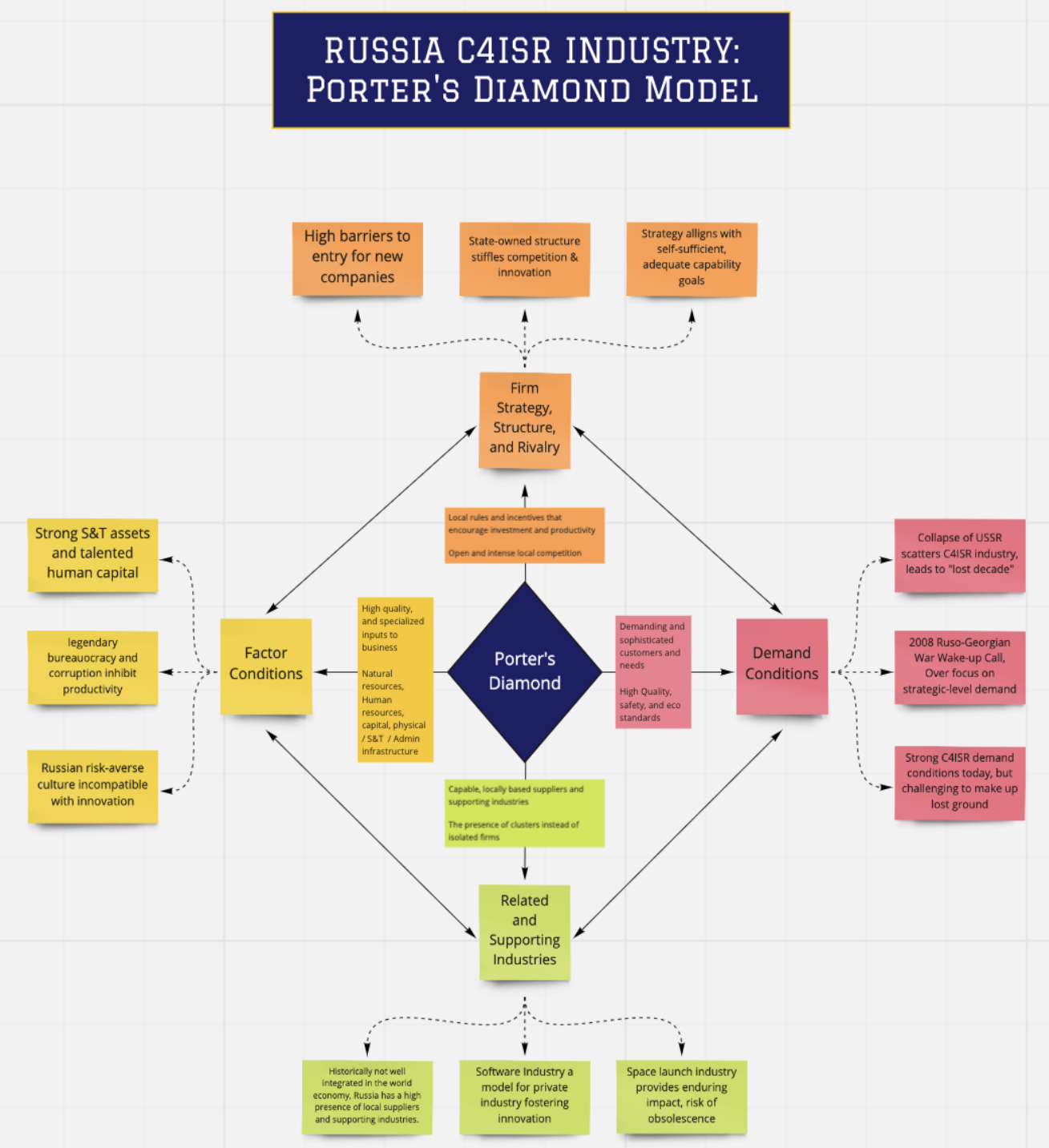


Figure 3: Porter's Diamond Analysis of Russia's C4ISR Industry

Demand Conditions

Unlike China, external events have influenced rather than shaped Russia. More than any other factor, the turbulence from the post-Cold War environment buffeted the Russian demand for C4ISR. In the late Soviet period, Marshal Nikolai Ogarkov, Chief of the Soviet General Staff, was advancing the concept of integrating precision weapons with C4ISR in "reconnaissance-strike complexes" to "wage war over much greater distances and with much greater precision, coordination, and tempo than ever before."[39] However, these innovative concepts were cut short by the fall of the Soviet Union in 1991. The collapse of the Soviet defense industry in the early 1990s disaggregated the C4ISR industrial complex; new borders confronted previously connected entities, which created hundreds of stove-piped C2 systems. It would not be until President Putin's ascension to power in the early 2000s that Russia's C4ISR industry would receive a boost. Putin leveraged the chaotic 1990s to craft a convincing narrative of restoring stability for the Russian public. Revitalizing the Russian defense industry and the central government's return of strategic direction would achieve returned stability.

Another critical moment for Russia's C4ISR industry was the 2008 Russo-Georgian War. Despite its eventual success in the campaign, the conflict served as a wake-up call for the Russian leadership. During the war, Russian forces encountered severe communication limitations and proved unable to coordinate efforts at the most fundamental levels. These failures instigated an ambitious reform program called the "New Look." The "New Look" aimed to overhaul the Russian defense sector and prioritized the development of modernized C4ISR capabilities across all echelons of command.[40] For the first time in close to two decades, Russia's C4ISR industry had a clear and broad demand signal from the government to design new products, improve productivity, and innovate. This Russian prioritization of C4ISR has endured to the present day. Given Russia's success in Ukraine, it will likely continue to abide, establishing domestic demand conditions that can aid in building a competitive advantage for its C4ISR industry to meet the demands of government buyers. Nevertheless, the rudderless post-Soviet decade and myopic strategic focus through 2008 represent a generational gap of lost ground that challenges the Russian C4ISR industry to make up.

Firm Strategy, Structure, and Rivalry

Despite its successes in revitalizing domestic demand, the competition's structures and incentives are fundamental weaknesses of the Russian C4ISR industrial complex. The state-owned structure of the Russian defense-industrial complex ultimately tempers the competitive advantage brought on by increased demand. Further, the Russian government's direct role in managing the sector limits internal competition, stifling entrepreneurship and innovation.

While Russia's mostly state-owned defense industry structure reduces its competitive advantage by limiting competition, the structure does align with Russia's overall strategy to cultivate an autonomous C4ISR industrial capability. Spurred by the 2014 international sanctions for its role in the conflict with Ukraine, Russia is eager to ensure it can domestically develop and produce critical C4ISR capabilities without having to rely on foreign suppliers or foreign financing. Russia set a goal to become even more self-reliant by creating 95 percent of hardware domestically to meet its defense requirements.[41]

It is unlikely that Russia is preparing its C4ISR industry to go toe-to-toe with U.S. capabilities. Instead, Russia seems to be aligning its industry to provide a C4ISR architecture that mitigates the risk of unforced errors like those experienced in the Russo-Georgian War while providing Russia with the freedom to exercise its strengths in areas like denial, deception, and disinformation. Doing so will align Russia's military and industry to deter American threats to Russian interests with a lower risk of escalation into outright conflict.

Factor Conditions

Factor conditions such as skilled labor, natural resources, and infrastructure are necessary to compete in the C4ISR market. However, Russia's previous strengths in these areas for C4ISR are eroding as it is unwilling to make anything more than superficial cultural and structural adjustments to foster organic growth. Russia's historic strength in this area lies in its science and technology assets and human capital resources. Despite making groundbreaking advances in electric lights, lasers, satellites, and electric digital computer technologies,[42] Russia is not currently a world leader in any of them due to a cultural environment that disincentivizes risk-taking and entrepreneurship.

Without meaningful reform in the areas of administration, corruption, and risk tolerance, the competitive advantage of one of Russia's greatest strengths, its talented human capital, will continue to erode over time. For the C4ISR industry, this erosion translates to decreased innovation, which leads to less capable solutions and the loss of technological leadership relative to its peers.

Related and Supporting Industries

For the Russian C4ISR industry, many supporting industries fall under the same state-owned umbrella organization. This organization was encouraged to ease access to standard components and promote tight-knit innovation clusters. This complementary arrangement is a historical trait of the C4ISR industry as Russia has never been well-integrated into the global marketplace, even during the Soviet era. This fact has driven Russia to develop local suppliers and domestic supporting industries over time to ensure access to critical components and services.

Two supporting industries that stand out as positive contributors to the competitive advantage of the Russian C4ISR industry are software development and space launch. Software is a crucial component of Russia's modernized C4ISR systems. Unlike the C4ISR industry, the Russian software industry is "one of Russia's most open, innovative, and successful high-technology industries."[43] In contrast to traditional Russian defense industries, Russian software is still primarily a private industry with investments from government and private sectors. Unburdened by many of the national security concerns of the traditional defense industries, Russian software is not overly regulated and does not require significant capital investments, making it an excellent candidate for internal competition.

There is perhaps no better-known C4ISR supporting industry than the vaunted Russian space industry. The Roscosmos State Corporation for Space Activities traces its lineage back to the Soviet space program and the historic days of the space race of the 1950s.[44] Despite being a government-owned and managed industry, the early achievements of Russian rocket designers

have had an enduring impact and remain world-class examples of space launch prowess. The C4ISR industry, in turn, benefits from this supporting industry by leveraging the domestic launch capability for its space-based ISR platforms, again aligning on the strategic objective of self-sufficiency. Recently, however, the lack of innovation and internal competition in the Russian space industry puts it at risk of losing its relevancy as private companies like SpaceX, Boeing, and Blue Origin, continue to evolve state of the art in space launch rapidly.

Analysis of U.S. C4ISR Industry

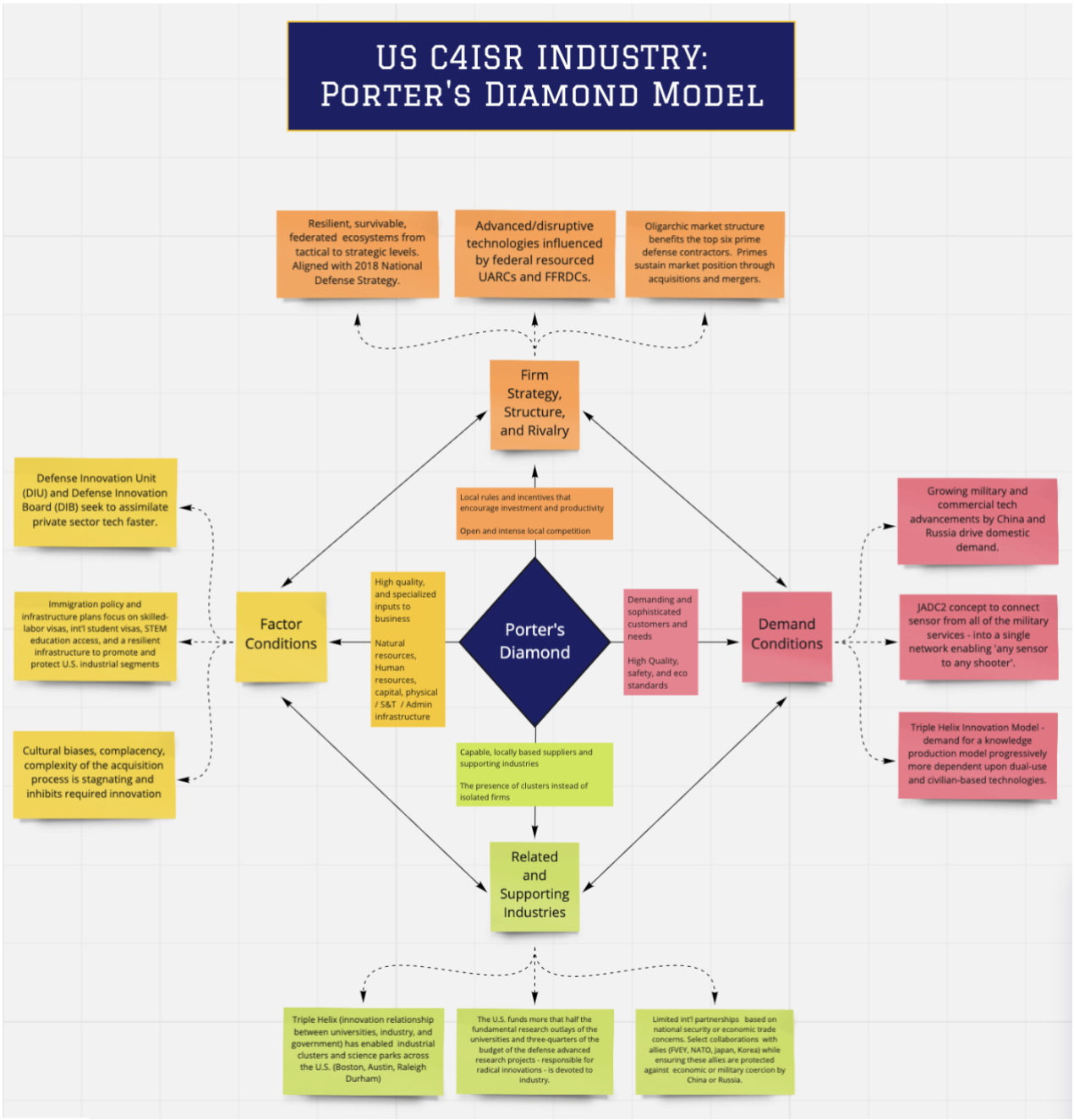


Figure 4: Porter's Diamond Analysis of U.S.' C4ISR Industry

As China and Russia innovate and field technically advanced military and C4ISR capabilities, the U.S. must focus its efforts to ensure it can maintain its place in geopolitics. As China and Russia both create instability in Europe and Asia, it is apparent that the U.S. cannot rely on the legacy weapons or battle/operational tactics of prior conflicts/wars to defend and deter against its near-peer adversaries in a GPC environment. Fortunately, as seen through the previous analysis, even though both the Chinese and Russian C4ISR industries are maturing, they still lag behind the U.S. in C4ISR technologies. However, to maintain this lead, the U.S. must continue the speed at which it develops and fields C4ISR technology and capabilities by leveraging its robust network of C4ISR partners within industry, academia, and government, known as the Triple Helix.

Firm Strategy, Structure, and Rivalry

The Triple Helix Model (THM) of Innovation is an innovation development construct consisting of the relationships between universities, industry, and government institutions.[45] These relationships have enabled the implementation of industrial clusters or science parks across the U.S. The three components of the THM are University-Industry, University - Government, and Government - Industry.[46]

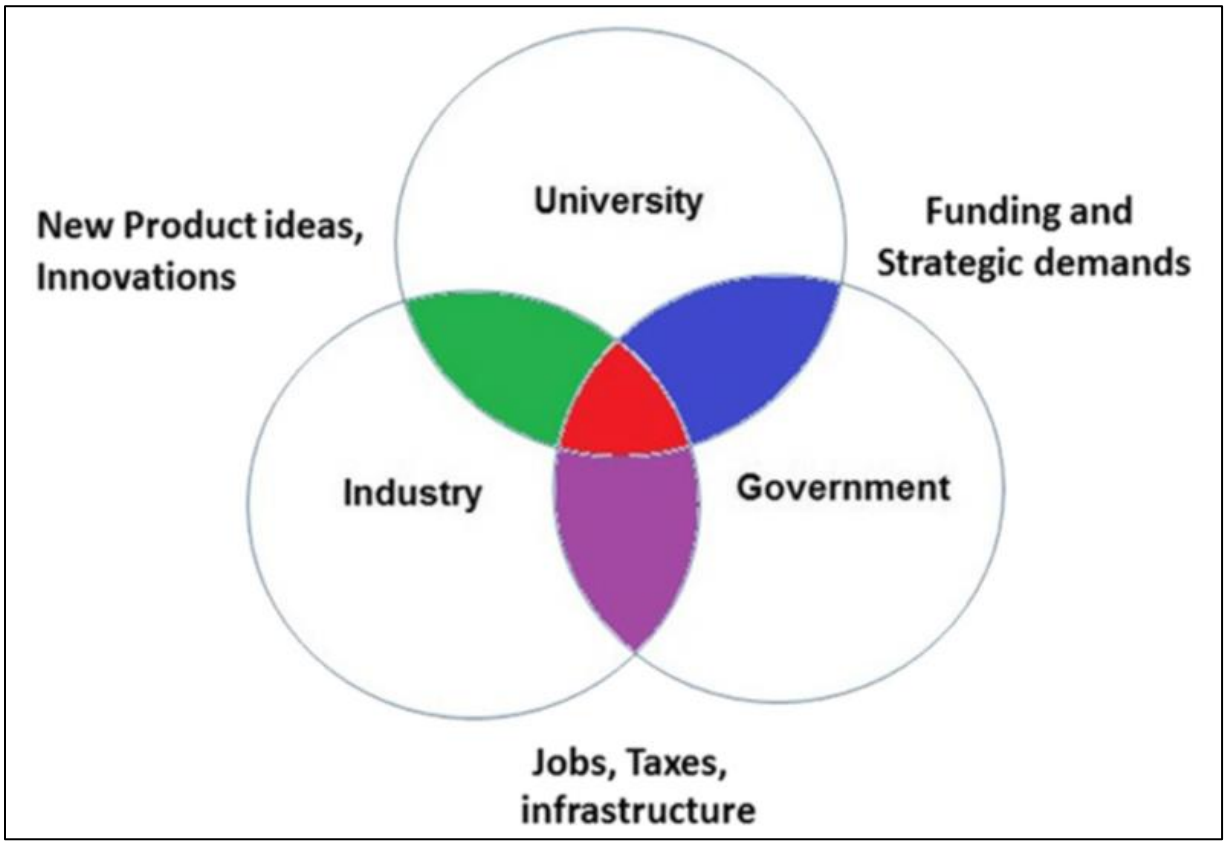


Figure 5: Triple Helix Model (THM) (Red Indicates Cluster/Science Park)
Source: Etzkowitz, H. THM: University-Industry-Government Innovation in Action, 2008

The strength of the THM is the evolving synchronization and collaboration efforts between government, universities, and industry. This "has led to a knowledge production model

progressively more dependent upon dual-use and civilian-based technologies leading to the emergence of a more open defense innovation system that includes civilian suppliers of knowledge among high technology small firms and universities."[47]

The Triple Helix is a competitive advantage within the U.S. C4ISR industry. It spurs disruptive innovation and the development of advanced technologies and capabilities. DoD and the services leverage the THM via its network of government-funded laboratories, government institutions, and commercial industry contractors.

Despite the strengths of the THM, the oligarchic structure of the C4ISR market diminishes its positive impact. Large defense primes, such as Northrup Grumman, Raytheon, and L3 Harris, dominate the industry. These primes use U.S. intellectual property protections and DoD contracting regulations to secure continued DoD reliance after selling exquisite platforms and locking out new competitors. Additional information on these C4ISR Prime Contractors can be found in Appendix A. The primes seek to continue to be the end-to-end solution provider for the C4ISR market. Rather than innovate themselves, defense primes maintain their position in the market through mergers and acquisitions of companies with niche technologies and expertise. The Defense Primes do this to obtain innovative intellectual property, but also to reduce competition by eliminating competitors before they gain size to navigate the complexities of DoD acquisition efficiently. Furthermore, security requirements, technical specifications, and long acquisition timelines associated with most C4ISR contracts create high barriers to entry for smaller companies, further limiting the pool of competitors. Fortunately, the DoD is working to correct these market trends by empowering organizations such as DoD's Defense Innovation Unit (DIU), Army Futures Command, and AFWERX. These organizations overcome the prime's dominance by teaming directly with smaller companies to bring innovative technologies into the DoD faster. These efforts create resilience in the marketplace by increasing competition and easing the "valley of death" challenge.

Demand Conditions

The need to maintain the technological and strategic edge over the U.S. GPC competitors has spurred renewed domestic demand for U.S. C4ISR technologies. While the U.S. government (USG) is a prominent buyer in the C4ISR market, it is not the sole buyer. Many C4ISR technologies are dual-use and are utilized by the commercial sector and purchased by allies and partners directly or through the DoD's Foreign Military Sales process.

A large variety of buyers and their unique sets of requirements are strengths for the U.S. C4ISR industry. Sizeable pools of buyers ensure that the industry can fund R&D necessary to advance the state of technology and continuously develop and deliver the best technologies to satisfy requirements. In addition, multiple buyers mean multiple revenue sources, so the C4ISR industry is not at the fate of unstable government budgets. DoD's 2021 budget includes $58.21 billion for C4ISR programs, an increase of $1.37 billion, or 2.4% over the 2020 request, and DoD spending for 2020-2025 was estimated to grow at a CAGR of 1.5%.[48] Furthermore, research and development test and evaluation (RDT&E) funding is projected to account for the most significant portion of the 2021 budget, totaling $24.55 billion.[49] The U.S. demand signal for C4ISR is projected to grow as the U.S. and its allies compete with Russia and China. In addition to this growth, there is a demand for accelerated delivery of these capabilities to ensure readiness

both today and in the future. Despite the demand advantages, there are also challenges. Since warfare has eliminated traditional domain boundaries, the U.S. C4ISR industry must quickly meet the new normal all-domain conflict demands. Though difficult, this trend may ultimately reinforce the industry, as it continuously adapts to new environments.

Factor Conditions

The U.S. achieved its lead in the C4ISR industry through its skilled labor force, investments in R&D, and production capabilities which enabled the U.S. to establish itself as a global technology leader for the past half-century. These conditions allowed the U.S. to produce defense technologies such as stealth, global positioning, precision weapons, and robotics. These developments, in turn, have provided the U.S. with a marked technological 'head-start' over its competitors.

Despite these initial advantages, the U.S. C4ISR market is currently struggling to compete with China's factor conditions. The U.S. STEM workforce and R&D investments gave the U.S. its lead, are no longer as dominant as they once were. Even though China is dealing with national labor force challenges on aggregate, the total number of the U.S. STEM workforce is shrinking while China's is increasing faster. Additionally, in real dollar amounts, USG R&D investment is decreasing as China's is rising.[50] If this imbalance continues, it will translate into increased Chinese capability challenging the U.S.' ability to stay ahead of the C4ISR innovation curve and maintain its competitive advantage.

Two other factor conditions, infrastructure and industrial security, are presenting new challenges within the U.S. industry. First, the DoD is saddled with substantial capital investments in technologically obsolete, legacy platforms. If these systems are not divested or modernized, the DoD's budget is insufficient to fund industrial innovation. To correct this, the DoD must reconsider its sunk-cost mindset; it cannot afford sentimentality when considering maintaining high-risk legacy platforms simply because it invested years or decades to plan for, develop, and deliver systems. Further, the DoD cannot maintain the acquisition processes that create "too big to fail" systems. Operation and Maintenance costs account for 70 percent of a typical system's total lifecycle.[51] However, this problem is compounding; as these systems age, it becomes more expensive to build backward compatibility with more advanced systems across the joint force. By keeping weapons systems in service for decades, the military also loses the benefits of frequent competition. In addition to these costs, the extensive and arguably, valid measures to counter theft of U.S. intellectual property and protect against cyberattacks create barriers to entry within the industry.

While to date, these U.S. C4ISR industry factor conditions have not severely impacted the ability to maintain its competitive edge, but China will challenge the U.S.'s lead if steps are not taken. To ensure this does not occur soon, the U.S. must: bolster its STEM workforce pipeline, from education to recruitment to retention; maximize R&D investments in innovation and emerging technologies; make wise investments, balance divestiture of legacy systems with the need to maintain readiness and implement procedures to maximize security without inhibiting innovation and technology development.

Related and Supporting Industries

The most significant strength and competitive advantage within the U.S. C4ISR industry lies in its commercial sector developing dual-use technologies/products. The knowledge and capabilities within "Big Tech" companies, such as Amazon Web Services, Microsoft, and Google; trendsetting tech startups such as Anduril and Palantir; and commercial space launch companies such as SpaceX play a critical role in the advancement of U.S. C4ISR technology. These companies are developing cutting-edge C4ISR technology in data processing, network sensors, autonomous platforms, space launch, and satellites at the speed of technology. For example, on 9 May 2021, SpaceX launched 60 Starlink internet satellites with a reusable booster rocket, marking the company's 14th launch of the year.[52]

U.S. companies, both large and small, prove that emerging tech can be successfully implemented and continuously updated in real-time with minimal risk. By using DevSecOps processes, they are helping to break through the U.S.'s risk-averse acquisition culture. Consistently demonstrating the successful application of emerging technologies in the public and private sector is building the confidence of risk-averse C4ISR buyers, specifically DoD and the services, and increasing the rate of new tech adoption. Furthermore, the dual-use application of these technologies ensures the financial health and sustainability of these supporting industries and creates a move resilient supply chain.

To ensure small and startup companies within the supporting industry have access to opportunities to support the U.S. C4ISR Industry and innovative tech does not die crossing the "valley of death," the USG has established the Small Business Innovation Research and Small Business Technology Transfer programs.[53] These programs help small businesses and startups bridge the gap between technology development and the market through federal R&D, increasing competition, and encouraging innovation.

The U.S. C4ISR Industry also benefits from strong international partnerships with countries that have robust innovation ecosystems and ISR expertise. The ability to collaborate with foreign partners to develop ISR components or leverage their suppliers is another advantage the U.S. has against its competitors. Thales Group is one example of a foreign partner company that supports the U.S. C4ISR Industry. Additional details, including the Thales corporation and its contribution to the C4ISR/JADC2 market, can be found in Appendix A.

C4ISR Strengths, Weaknesses, Opportunities, and Threats Analysis

While the U.S. still outclasses its great power competitors in almost all sub-segments of the C4ISR market, both China and Russia are advancing core technology areas that offer opportunities to counter U.S. advantages asymmetrically. China's C4ISR diamond is strong in many areas, despite some significant weaknesses that will take time to overcome. CCP policies drive its rising economy, innovation clusters, and low R&D barriers between civilian and military producers. China's supporting industries are internationally competitive, and its near-global monopoly in C4ISR natural resources and high capital R&D investments strengthen China's factor conditions. Nevertheless, labor pool problems present a threat and a weakness as it could take decades to modernize and provide strength to the Chinese C4ISR diamond. Finally, China's demand conditions rely upon its large population to create continued demand for lower-

end dual-use technologies. Still, they do not yet demand innovation from producers or create a competitive advantage. This demand innovation is an opportunity China could leverage to strengthen its diamond. Suppose China realizes its vision of developing smart cities around the globe that rely on Chinese dual-use technologies. In that case, that success could translate into a substantial competitive advantage in its C4ISR industry, potentially rivaling that of the U.S.

For Russia, the story is more complex; its C4ISR industry has more weaknesses and threats than strengths and opportunities. As demonstrated, a competition-limiting firm structure and an innovation-stifling cultural environment weakens the Russian market. Demand conditions from the Russian government, while currently strong, are still at least a decade behind in contributing to the competitive advantage of the Russian C4ISR market, again weakening its position. However, strong supporting industries such as software, space launch, and a talented workforce present opportunity and offset some of these weaknesses. Overall, Russia exhibits a weak competitive advantage in its C4ISR industry, making it structurally incapable of the consistent innovation required to achieve peer-competitor parity. Nevertheless, Russia's C4ISR industry strategy remains aligned with its limited objectives of delivering adequate, self-sufficient capabilities to avoid repeating past failures.

The strength of the U.S. C4ISR industry is in the innovative culture of American technology companies and their R&D investments. These opportunities drive quick iterative development cycles to bring emerging technologies to market at scale, strengthening its diamond. Through collaboration with the commercial sector, DoD and services can leverage the development of dual-use technologies to bear in GPC, strengthening its position in the C4ISR market. However, the U.S. C4ISR industry is not flawless. The strength of its competitive advantage is weakened and threatened by a diminishing STEM labor force which creates resourcing shortfalls in critical C4ISR technology and the hesitancy to share information with partners and allies creating a culturally challenged future environment. Furthermore, in the growing C4ISR industry and its supporting industries, the DoD finds itself no longer the sole buyer but one of many threatening its position as a dominant influence. This new position presents an opportunity for the DoD to reassess its burdensome acquisition processes to be more responsive to a faster, more competitive buying environment. While the U.S. C4ISR industry is significantly ahead of its competitors, it still has areas that need improvement to maintain its lead. In response, industry and the DoD actively seek to mitigate these risks by looking at opportunities to increase investment in STEM education and recruitment, reduce purchasing barriers for U.S. partners and allies, streamline DoD acquisition processes for quicker development and deployment cycles, and divest antiquated legacy programs.

Looking forward, Russia's C4ISR industry will struggle to match U.S. investment and innovation in the types of novel technologies that will enable advanced warfighting concepts like JADC2. The more apparent threat to U.S. competitive advantage resides within China, which presents a plausible pathway to parity in the future if it can overcome current threats and weaknesses and harness its opportunities. When it comes to the C4ISR industrial complex, the U.S. cannot ignore Russia, but the clearer threat to the U.S.' competitive advantage lies with China. The American C4ISR market's competitive advantage is the leverage needed to create the future leading all-domain command and control concept.

Evolution of JADC2

Origin of JADC2

JADC2's historical roots took growth in the latter half of the 20th Century, but one can find traces of its fundamental principles much earlier. John Boyd's infamous Observe, Orient, Decide, Act (OODA) Loop is part of the DNA of JADC2. The OODA Loop's core takes ancient warfighting dogmas and imbues them with a present-early information era theory of waging war: operate at a quicker tempo than the adversary to disorient and ultimately defeat them.[54] Sun Tzu heavily influenced this theory, who taught that one might win a war without fighting by demonstrating superior speed, surprise, and agility of action. Boyd took Sun Tzu's teachings and concluded that numerically inferior forces could achieve victory, incorporating Tzu's tenants in his OODA Loop theory.[55]

During the 1970s and 80s, the North Atlantic Treaty Organization's (NATO's) Fulda Gap challenge presented by the Russian army provided one of the first tests of Boyd's assertion that his OODA Loop theory could help numerically inferior forces. Fresh out of the Vietnam War, the U.S. sought to rebuild its hollowed-out armed forces to deter Soviet aggression. The Defense Advanced Research Projects Agency's Assault Breaker program was an important initiative that involved coupling state-of-the-art Intelligence, Surveillance, and Reconnaissance (ISR) platforms with newly designed evolving precision-guided munitions to blunt the Soviet's numerical tank and infantry advantage. Assault Breaker's successes led the U.S. to an overwhelming victory in Desert Storm.[56]

When reviewing the success of the U.S. in the Gulf, Andrew Marshall, the notable Director of the Pentagon's Office of Net Assessment during the late Cold War, predicted the next likely technological revolution. He realized that the Soviets were anticipating the rise of an "automated reconnaissance-and-strike complex" that they believed would lead to the next revolution in military affairs (RMA). Conventional wisdom holds that the technology-driven kill chain demonstrated by the U.S. in Desert Storm was the first tangible manifestation of an "automated reconnaissance-and-strike complex," and many scholars often refer to it as the 2nd Offset. Then, by the mid-90s, the internet began connecting things. The ensuing information technology (IT) revolution took the world by storm, networking people and machines worldwide. Marshall concluded that the next RMA, or 3rd Offset, would likely combine many reconnaissance-strike systems through IT network linkages, forming a "system of systems."[57] One of the offset's most adamant supporters was Vice-Chairman Admiral William Owens who labeled his version of the 3rd Offset, Dominant Battlefield Awareness. In 1996, ADM Williams codified his vision into the concept titled Joint Vision 2010.[58] It promoted networked sensors and modern C4ISR technology to provide a better common operating picture to aid in faster battle decisions.[59]

It was not until 1998 that two gentlemen, Admiral Arthur Cebrowski and John Garstka, coined the first name that initially stuck to describe Marshall's "system of systems." They co-authored a document that described a future where commanders would seek information superiority through timely-delivered data whose speed derived from networks of automated C2 platforms. They argued that the key ingredient was the ability to make strategic choices appropriate to an ever-changing operational environment faster than your opponent. They duly

credited Boyd's OODA Loop as an inspiration and called their vision of the 3rd Offset, Network-Centric Warfare.[60]

Network Centric Warfare did not die during the Global War on Terrorism (GWOT), but neither did it thrive despite promotion efforts. In 2003, the DoD attempted to revamp its IT architecture to take advantage of network-centered warfare. It created the Global Information Grid (GIG) centered mostly around IT interoperability between services architectures. However, the GIG could not link multiple Reconnaissance-Strike Complexes together and eventually died off as the GWOT's long-term realities retook center stage during the 2007 Iraq surge.

In 2014, the idea of great power competition resurged in the U.S. after Russia invaded Ukraine and China exceeded their sovereignty rights by building islands in the South China Sea. The notion of NCW returned in 2015 repackaged and sold as the Joint Aerial Layer Network (JALN).[61] JALN offered a slight twist to the 2nd Offset by making the C2 of low-demand, high-density air assets more joint, but it did not provide a concept for fighting using Marshall's vision of a "system of systems."

The 2018 NDS officially refocused the DoD to GPC. China's intent had become increasingly apparent, as did how they intended to achieve their strategy A2/AD. Their increasingly sophisticated and integrated A2/AD systems started resembling their version of a Reconnaissance-Strike Complex. In response, the DoD is updating its NCW concept within its JADC2 efforts. The DoD, through the Joint Staff J6 and a specially formed cross-functional team (CFT), are leading the effort.[62] The CFT's Operation View-1 (OV-1) JADC2 image looks familiar to the visual concepts depicted in Joint Vision 2010.

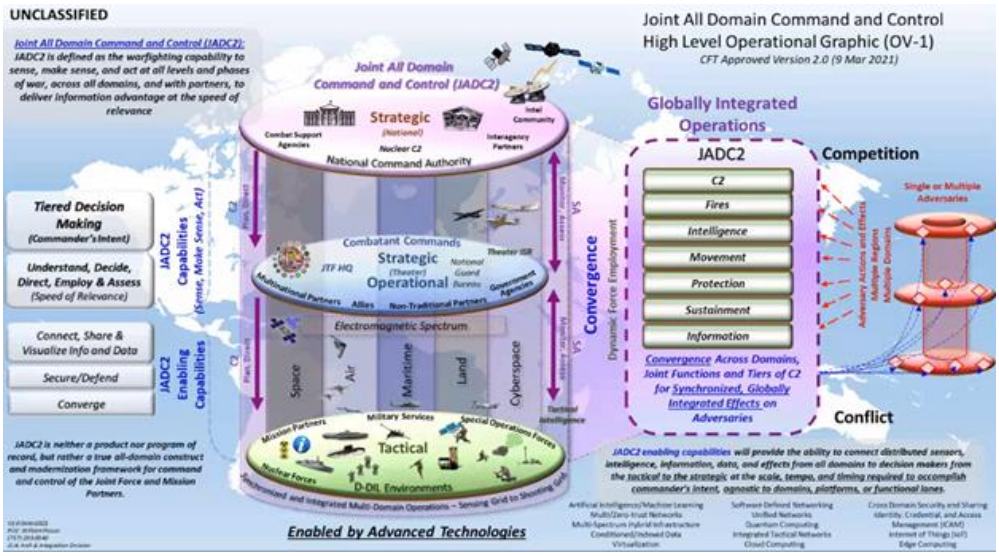


Figure 6: Joint All-Domain Command and Control (OV-1)
Source: OV-1 distributed by the JS J6, CFT

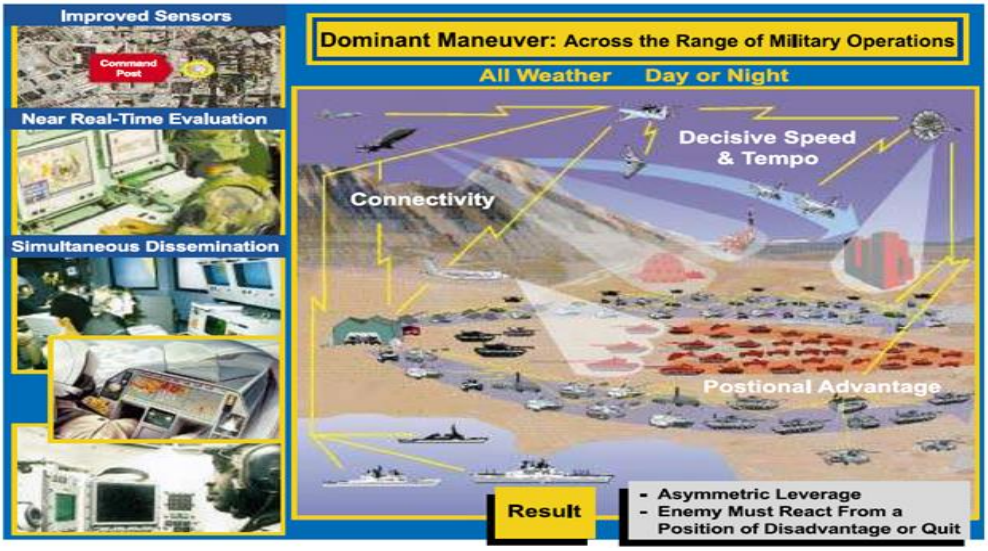


Figure 7: Joint Vision 2010
Source: "Joint Vision 2010" published July 1996

Defining JADC2

A quick survey of the literature surrounding JADC2 and multiple interviews with prominent Pentagon insiders reveals that the term "JADC2" means something different to everyone. Many proponents compare it to modern apps like Lyft and Uber to define JADC2 as "a thousand kill chains in your pocket" or the "kill web."[63] News agencies have quoted Defense/Pentagon officials who describe JADC2 as linking "any sensor, any shooter," or simply "sense, act" for the minimalist.[64] Further, the Joint Staff J6 representatives define JADC2 simply as "sense-make sense-act," indicating it could be a modernized variant of John Boyd's OODA Loop.[65] Reference Appendix B for the CFT's full OV-1/JADC2 concept. Unfortunately, one definition of JADC2 will undoubtedly fail to capture the many nuanced variables at play, and as critiques of definitions and theories have noted, it will lead to oversimplification. People oversimplify arguably they must; to make the complex simple to understand.[66]

The ambiguity surrounding if JADC2 intends to deliver a capability, concept, or strategy further exacerbates its complexity. The Pentagon's J6 lead, Lt Gen Dennis Crall, insists that JADC2 is a strategy for decision making that "is separate from - but inexorably linked to - the Joint Warfighting Concept," which is the Secretary of Defense's (SECDEF's) initiative to outline how the U.S. will fight in the 21st Century.[67] Even though DoD has yet to codify JADC2 requirements, the services, allies, and industry are already advancing developing independent C2 capabilities to prepare for and deter near-peer competitors from pursuing great power conflict. At the same time, these stakeholders may have differing ideas of the JADC2 end state, their role and responsibilities within the JADC2 construct, and how their capabilities will integrate. They all agree that JADC2 and its integrated capabilities will ensure the U.S. and its allies have the competitive advantage in GPC or conflict. The following sections describe the variety of paths and capabilities stakeholders are pursuing; highlights the complexity of the JADC2 effort and the systems requiring interoperability; and addresses the cultural, policy, and process challenges potentially hindering successful implementation of JADC2.

JADC2 Lines of Effort: Service Capabilities and Cultures

Through many interviews with DoD officials and a cursory study of defense news and interviews with DoD officials, it is apparent that each military department is pursuing different lines of effort to implement JADC2 within their cognizant domains. The scope is astounding; various combinations of departments and services are undertaking numerous experiments to test ways to modernize C2 concepts and capabilities in support of the SECDEF's Joint Warfighting Concept. The different lines of effort are focused on identifying technologies to design and build systems that will rapidly plan and execute operations in cognizant domains with the help of capabilities from all domains in a synchronized, cooperative, and efficient manner. The Academic Year 21 ES C4ISR study analyzed these individual initiatives, alongside allied and partner efforts, to understand their aims and recommend ways to improve their ultimate integration into JADC2. While the individual lines of effort are vital for meeting inter-and intra-domain operations, the eventual success of JADC2 rests upon the DoD's ability to integrate them into a user-focused final product.

USAF Advanced Battle Management System (ABMS)

The United States Air Force's (USAF) contribution to JADC2 is ABMS. ABMS was an idea born to recapitalize the E-8 Joint Surveillance Target Attack and Radar System (JSTARS) and revolutionize multi-domain operations and C2 by accelerating the OODA loop. ABMS is undoubtedly the most advanced of all service JADC2 ventures, and it has shown promising results in a series of "on-ramp" experiments. Despite some successes, ABMS faces numerous challenges. The Air Force has not effectively communicated what it is, an end state, or how it fits with other service programs, leading to a near 50% funding reduction in FY21[68] from skeptics in Congress.

The plan to replace the E-8 JSTARS is revolutionary for the DoD. The intention to move away from platform-centric capabilities and move towards software-based solutions for battle management and command and control is innovative. Speed of decision is the key ABMS buzzword and accelerating that process may be the critical capability in 21st-century warfare. According to a Rand analysis, the new method, now "supported by the U.S. Army and the U.S. Air Force, is known as multi-domain operations and looks to build nonlinear kill webs by rapidly bringing together sensors and shooters across service, domain, and functional stovepipes."[69] The real questions for the DoD are if this vision is possible and if it can connect all services across all domains. Many different cultures will need to solve the complex environment of DoD acquisition and policy before the private industry can address the technical solution.

All grand visions have a visionary leader behind them. Former Assistant Secretary of the Air Force Dr. Will Roper led the charge for ABMS and many other revolutionary ideas. A thorough review by Air Force magazine into the services innovation system pointed out that "Roper pressed to replace the E-8 JSTARS aircraft, not with another airplane but with a system-of-systems concept intended to link up everything in the battlespace. He calls the evolving network the "Internet of Military Things," a system that aims to enable almost anyone in the chain of command to access, in real-time, a complete battlefield operational picture, including threats, assets, and recommended courses of action generated through artificial intelligence."[70]

Innovation Culture

Dr. Roper is also instrumental in building an entire innovation ecosystem to develop programs like ABMS. While many in the defense industrial base continue to push for large, exquisite platforms, Roper sought cheaper, smaller, faster ways to solve military problems. He championed and bolstered organizations like AFWERX. The DoD is beginning to realize that small businesses can help solve problems that the traditional big primes may not tackle, at least not cheaply or quickly. Everstine highlights that "one of Roper's gambles has been to apply a Silicon Valley-style approach to defense technology. AFWERX is essentially a tech "startup" aimed at spurring development and connecting companies with military customers. AFVentures operates similarly to venture capitalists and secures seed funding for new businesses developing military-relevant tools.[71] These government-sponsored innovation organizations have helped connect non-traditional but innovative companies to the ABMS program.

ABMS is a complex cloud-based system with a series of enabling applications to achieve "effects integration."[72] It demonstrates that platforms are no longer the future and that software-based applications are. Several "on-ramp" experiments for ABMS have proven that the technology exists to achieve this objective. According to Roper, the purpose of the tests is to demonstrate that the concept is possible. He noted that "In September 2020, the second on-ramp experiment connected dozens of aircraft across the country, plus ground and sea-based sensors, and culminated with a remote command to down a cruise missile threat with non-typical shooters, including a "smart bullet" fired from a howitzer and a ground-based AIM-9X."[73]

Unfortunately, due to its complexity, ABMS faces an uphill battle, the path to success is not clear, and the challenges may outweigh successes. The primary issue is an inability to communicate effectively how this cloud-based approach fits into the more extensive JADC2 architecture or clearly define its attributes and value to JADC2. Many within the Air Force view ABMS as a concept, while others view it as a system and even senior leaders within the department of the Air Force have differing viewpoints.

Despite its flaws, ABMS has demonstrated a foundational JADC2 architecture that all services could leverage despite command and controls difference. However, the program's success depends on a clear definition of ABMS's intention to achieve and how, continued funding, senior leader support, and cross-service integration. ABMS may be the key to developing JADC2 and creating an asymmetric advantage or offset that will provide the edge in GPC with Russia and China.

Army Project Convergence

Project Convergence is the Army's modernization effort developing the network of systems capable of achieving joint service interoperability in JADC2. In 2020, Secretary of the Army Ryan McCarthy and Army Chief of Staff General James McConville signed the Project Convergence narrative proclaiming that "PC is the Army's new campaign of learning, designed to aggressively advance and integrate our Army's contributions to the Joint Force. It ensures that the Army, as part of the Joint fight, can rapidly and continuously integrate or "converge" effects across all domains – air, land, sea, and cyberspace – to overmatch our adversaries in competition and conflict."[74] General John Murray, Commander of Army Futures Command, said of PC in September 2020 that "this may not only be the most important thing Army Futures Command is

working on, it may be the most important thing the Army is doing today."[75] PC centers on five core elements: people, weapon systems, command and control, information, and terrain that supports JADC2.

Project Convergence 2020 (PC 20) served as the most basic exercise to link Army systems to Army systems "by integrating new enabling technologies at the lowest operational level so that the tactical networks could facilitate faster decisions."[76] Seen as a huge success, PC 20 included more than 750 Soldiers and scientists across three different installations, more than 1000 miles apart. The exercise demonstrated Artificial Intelligence (AI)-aided Threat Detection and Recognition, extended divisional battlespace, and decreased sensor-to-shooter processing time.[77]

To further support JADC2, General McConville will create five Multi-Domain Task Forces (MDTF) able to respond to regional conflict. The MDTF will serve as the Army's "organizational effort" in synchronizing "new operational concepts, technologies, weapons, and units."[78] The MDTF serves three purposes, to "gain and maintain contact with our adversaries to support the rapid transition to crisis or conflict," "to deter adversaries and shape the environment by providing flexible response options to the combatant commander," and "to neutralize adversary A2/AD networks to enable joint freedom of action."[79] MDTF-1 will participate in the PC21 exercise to process sensor to shooter systems directly linking U.S. Army capabilities with those from the Air Force, Navy, Marine Corps, and Space Force. The U.S. Army and Air Force signed a two-year agreement in 2020 to develop the Joint All-Domain concept for JADC2. The two services agreed to develop mutually supporting data sharing and services by 2022.[80]

For PC to be successful, the Army will have to create a network compatible with itself and the other services, accelerate innovation, work with the industrial base to develop new emerging technologies, and overcome cultural differences. Shifting the mindset away from sustaining legacy networks to leveraging emerging technologies for advanced data and communications capabilities is critical to successfully integrating complex systems across the Joint Force.

Navy Project Overmatch

In the maritime domain, China is making significant investments in advanced platforms and technologies. The goal of its naval buildup is to prevent the U.S. Navy from winning in a conflict. China's investments range from ships teeming with advanced weapons systems to long-range surveillance infrastructure designed to increase the speed of decision. The growing threat from China coupled with the significant development in technology presents the U.S. an opportunity to enhance its current C4ISR and C2 concepts and capabilities.

> The Navy's C2 is built around the concept of Distributed Maritime Operations (DMO). According to Vice Admiral Phil Sawyer, "DMO is geographically distributed naval forces integrated to synchronize operations across all domains. DMO is a combination of distributed forces, integration of effects, and maneuver. It will enhance battlespace awareness and influence; generate opportunities for naval forces to achieve surprise, neutralize threats and overwhelm the adversary; and impose operational dilemmas on the adversary."[81]

Knowing the limitations of its legacy systems, the Navy is leveraging emerging technologies such as AI and machine learning (ML) to enhance the effectiveness of USV (unmanned surface vehicles) and UUV (unmanned underwater vehicle) capabilities, and Navy leadership has started to explore the art of possible with C2 through its JADC2 effort known as Project Overmatch. The DMO concept and Project Overmatch are examples of how the services respond to and develop JADC2 capabilities to counter growing GPC threats.

The need for Project Overmatch has never been more critical. The Navy has the difficult task of growing its fleet to meet the essential attributes of DMO. Modern naval ships, submarines, and airborne platforms are becoming increasingly expensive, complex and require significant lead times to produce. In response, the Navy has decided to pursue unmanned autonomous and semi-autonomous platforms to maintain its edge in the maritime domain. The Navy's recently released Unmanned Campaign Plan states: "autonomous systems provide additional warfighting capability and capacity to augment our traditional combatant force, allowing the option to take on greater operational risk while maintaining a tactical and strategic advantage."[82] To successfully develop and integrate these platforms, the Navy will have to evolve its C2 and operational concepts while maximizing the impact of unmanned autonomous systems, highlighting the criticality of Project Overmatch.

These new classes of unmanned platforms offer a rare opportunity to start with a virtual blank slate of systems and employment concepts. USV/UUV are cutting-edge technologies and, when coupled with AI/ML technologies, also offer opportunities for smaller companies to work on JADC2 projects outside the defense primes. Now, the Navy's focus must be on working with industry, both small companies, and large primes, to improve its current C2 capabilities and prepare for future JADC2 integration through open architectures and contractor agnostic systems. Furthermore, like the Army, the Navy must ensure that Project Overmatch's contributions to JADC2 are defined and communicated. The path towards incremental implementation and integration is aligned with JADC2 stakeholders and partners.

Perhaps the best opportunity to link the Navy's effort to enhance its C2 capability to JADC2 is in the unmanned air portfolio. A problem the Navy must handle is that the sheer size of the Pacific theater requires a large fleet of airborne ISR assets to collect intelligence. The Triton UAS (unmanned aircraft system) is an extremely capable platform, but limited numbers and high cost per unit have impacted the ability to field it in significant numbers. Navy leaders have recognized the need to look outside of the sea service for ways to increase airborne ISR and flip the script on the historic use of the MQ-9B. They have begun the process of "pairing an MQ-9B Sea Guardian drone with a guided-missile cruiser capable of firing anti-air, anti-surface, and anti-submarine missiles as a hunter-killer team in an unprecedented exercise testing new unmanned systems."[83] This pairing could be the Navy's first step in showing JADC2's potential. Changing the Navy culture will take time, and a steady plan to incorporate innovative technologies, updated C2 concepts, and integration of threat information into DMO will be required for a successful on-ramp into JADC2.

Project Overmatch incorporates these new unmanned platforms with the existing capability to increase speed, opportunity, and lethality against peer threats. As the Navy works through its DMO and Overmatch concept development and experimentation, it expects to see

incremental changes in new capability integration to keep ahead of its competitors. However, like the Army, Navy C2 efforts have areas of improvement. Specifically, the Navy must collaborate with industry, be threat informed, acknowledge inter/intra-service cultural barriers, and incorporate innovative concepts and technologies.

Space Force

In GPC, C4ISR from space will be essential to maintaining an up-to-date intelligence picture at the strategic, operational, and tactical levels of conflict or war. Space-based ISR capabilities provide the persistent global monitoring capabilities unhindered by flyover restrictions required to deliver JADC2. America's space capabilities must continue to operate and counter those near-peer competitors China and Russia, who are developing capabilities to disrupt, degrade, and destroy U.S. satellites.

Great Power Competition in Space

Anti-satellite missiles, lasers, co-orbital satellites, and jamming technology have proliferated and are now in the hands of other space-faring nations. U.S. space ISR platforms have been targeted as an effective way to blind and deafen the U.S. in times of escalating tension. A2/AD space threats are proliferating and endanger the advantages that enable the U.S. military in war or conflict. "Russia and China are building capabilities to challenge us in space because if they can challenge us in space, they understand as dependent as we are in space capabilities that they can challenge us as a nation," said General John E. Hyten, Vice-Chairman of the Joint Chiefs of Staff.[84] Therefore, like the branches of the military dedicated to protecting and securing the air, land, and sea, the U.S. recognizes the importance of safeguarding space.

Allies and international partners are an integral part of the future of U.S. space C4ISR capabilities. Many allies and partners have integrated their space capabilities with the U.S. Space Force (USSF), making their contribution integral to collective security. The DoD and USSF promote burden-sharing with our allies and partners, developing and leveraging cooperative opportunities in policy, strategy, capabilities, and operational realms. Additionally, to enable JADC2, information-sharing relationships with capable allies and partners should be expanded and incorporated as a priority requirement in JADC2 contracts.

Space-based ISR is a recognized and acknowledged enabler of America's instruments of power and a vital element to U.S. national power. On the modern battlefield, space capabilities have become a prerequisite for global deterrence and power projection. However, the USG and industry with partners and allies must reform security classification and information protection processes to maximize data sharing. Special Access Programs (SAPs) and restricted information boundaries have resulted in government organizations and industries developing multiple classified systems. Additionally, DoD has nurtured a culture of over-classification that discourages information sharing, especially with allies and partners. The USG "NOFORN," Not Releasable to Foreign Nationals designation, is a hindrance that dissuades allies and partners from committing to help the U.S. meet its JADC2 and future C4ISR vision. Allies and partners will be essential in GPC by strengthening and globalizing C4ISR capabilities.

Allies and Partners – Working to Develop a Culture of Proactive Inclusion

> "The strength of the United States is our network of allies and partners that we have…That's why the U.S. can deal with any of the challenges we have in the world. I am very confident of our ability to deal with the challenges because of our network of allies and partners."[85]
>
> - Chairman of the Joint Chiefs of Staff, General Joseph Dunford
>
> -

In his opening days as Chairman of the Joint Chiefs of Staff, General Dunford opined on the priorities listed in the 2018 National Defense Strategy and noted the importance of America's strong collection of partners and allies. In an interview with Defense News, he stated that partners and allies provided the U.S. an asymmetric advantage against its Great Power Competitors.[86]

The U.S.' traditional answer for ensuring communication interoperability is through sales of new and excess defense articles to foreign militaries.[87] By selling the same platforms used by the U.S. services, the DoD can dictate a minimum level of interoperability with foreign services. However, multiple trends, including the modernization of allied and partner industrial bases and the JADC2 concept's transition away from hardware-based solutions to software-based interoperability, threaten to impact U.S. interoperability with partners and allies.

The need to connect across new and legacy systems has created a complex ecosystem of experimentation, programs, and contracting solutions. The USAF, alone, had 28 vendors for its JADC2 line of effort, titled ABMS.[88] Ultimately, the entry of new participants into the defense industrial base should result in greater competition and resilience in developing the JADC2 concept. While the U.S. has been the world leader in exporting military hardware, including C4ISR systems, the overwhelming competitiveness of the U.S. C4ISR industry has pushed many countries to prioritize defense spending on domestically produced products to support indigenous industrial bases and boost gross domestic product.

Including Partners and Allies to Spur Healthy Competition and Innovation

Due to the inherent military application of C4ISR industries, the market is dependent on government purchasers. But the government intervention does not stop there; the USG maintains an elaborate system of laws, policies, and procedures that creates a high barrier to entry for new applicants, both foreign and domestic.

The first series of governmental interventions fall under the umbrella of the Arms Export Control Act (AECA) and International Traffic in Arms (ITAR) regulations. These laws, enshrined in the U.S. legal code, govern the import and export of defense articles and services.[89] While these laws were not designed specifically to protect U.S. companies from foreign competition, it is a latent effect. The AECA and ITAR have spawned further export restriction regimes, like the Missile Technology Control Regime (MTCR) and Anti-Tamper (AT) reviews that create more barriers to entry for new entrants, especially from our partners and allies.

Additionally, the USG has also created security policies that set additional conditions for developing, protecting, transport, and handling C4ISR equipment. Policies like the Committee for National Security Systems Publications 8 and 14 (CNSSP-8/14) require U.S. classified systems to implement nationally approved encryption devices and algorithms to protect the

classified information inherent in their architecture.[90,91] As with the AECA, while these policies were not designed to promote traditional DoD contractors, they create an advantage for U.S. defense companies in this segment.

While the goal of JADC2 is to link the Joint Force and its allies and partners in a manner never seen before, it will likely take time to achieve. The current state of Joint C2 is a hodgepodge of precariously linked information systems developed in service stovepipes and executed in a manner that follows service-specific warfare concepts. These service-specific C2 concepts and systems for high-end conflict were developed for the Cold War and largely languished due to demands generated by the Global War on Terror. Legacy systems supported by obsolete technology coupled with cultural barriers and outdated policies and processes further complicate JADC2 efforts. However, since JADC2 is in its early stages of development, overcoming these barriers is possible. Continuing to modernize legacy systems and develop capabilities that align with the current JADC2 construct and are designed with partner and ally interoperability will help mitigate these risks. JADC2 cannot be built in a vacuum with partner input and capability bolted on after it is finalized, or it will fail to meet the intent of JADC2 to be the connective force. The Army and Air Force initiative to share common data by 2022 is an effective first step toward jointness. The services are solving complex command and control for their specific domains, and meshing these concepts together will create a true Joint All-Domain network of sensors to include American partners and allies.

Challenges and Recommendations for DoD Stakeholders Building JADC2 Culture

Challenges Integrating JADC2 into U.S. Laws, Policies, and Procedures

The complexity of JADC2 is not only in the technology but also in the approaches and mindsets of its stakeholders. For JADC2 to become a reality, Congress, the services, allies, partners, and industry must recognize and mitigate the challenges and leverage the opportunities present in service cultures, acquisition processes, legacy systems, and security requirements. Overcoming the challenges and leveraging the opportunities in these areas will build the foundation on which JADC2 requires to evolve and adapt to meet the emerging threats of GPC and conflict.

Maximizing Acquisition Models for Agile Development Programs

The combined force will need more than new technology to become more responsive, capable, and maneuverable. New technologies require new acquisition practices and business models to harness the best of what the commercial industry and innovation have to offer. Today's U.S. military force design results from several incremental law and policy reform efforts in the past 50 years that relied on an industrial age view of weapons systems. The current acquisition process is a formidable waterfall requirements machine that uses stage-gate processes to develop and approve detailed operational and technical requirements documents used to oversee a weapon system acquisition program. Functional requirements and "capabilities" are broad to maintain trade space for analysis of alternatives. Teams may spend three years or more to agree on a description of the requirement before obligating the first dollar on a solution. These

requirements are also projected far into the future based on an assumed "service life" to predict what will be needed against future adversaries and update the plan to deliver it. In theory, this system can provide thoroughly engineered systems accountable to widely approved performance objectives. In practice, the waterfall process drives numerous unintended behaviors and impedes rather than improves performance and schedule. The result is a system that attempts many things but excels at none.

Following the requirements process, a similar waterfall development model attempts to deliver the requested product but usually falls short. Most importantly, adversaries and technology react to our decisions more quickly than we can implement them, and operational requirements outdated before system development even begins. This pattern is increasingly prevalent in digital systems, where software evolves a new generation before the stakeholders can convene their next conference meeting. As the acquisition program proceeds, a significant sunk cost bias emerges. Bureaucrats are rewarded for focusing on finishing a previously agreed plan rather than changing that plan to meet new realities and deliver success.

Today's military redesigns the largest weapons systems and programs every 20 years. The future digital force must keep pace with technological change by redesigning and refactoring their systems multiple times per year, drawing from the best that industry offers continuously.

As the military migrates from defense-unique products (tanks and ships) to leverage more commercial products and services (drones and cybersecurity), the DoD should embrace private capital innovation and commercial investment to complement military development programs. Groups like the Defense Innovation Unit in Silicon Valley, Dcode, Hacking for Defense, and the National Security Innovation Network began educating the military in commercial business in 2015. Relative to the vast size of defense spending, this innovation is very small:[92] DoD and the tech industry must collaborate on a greater scale to deliver JADC2 solutions on a meaningful timeline.

The military’s sophistication as a customer dominates how industry specializes in meeting its needs. Two factors drive today’s low sophistication. First, the military prefers long-lived weapon systems, often operating the largest combat platforms like aircraft, ships and satellites well beyond their original design service lives. This service life extension drives operating costs up and discourages investment in emerging technologies by favoring incremental upgrades to outdated proprietary designs.[93] By limiting design life and focusing on delivery to schedule over perfecting performance, the government can remove industry’s incentive to make closed, expensive systems that lock in decades of sustainment revenue.[94] This commitment to revalidation of requirements will ensure the DoD stays nimble in its tech acquisition and can maintain its JADC2/C4ISR competitive advantage.

Second, DoD's ability to understand rapidly changing technology has atrophied; the engineering, contracting, and operations expertise built with the rare new combat platform competition is quickly lost. DoD must invest in a culture and skillset that champions frequent competition and renewed demand for the best in industry.

DoD preference for complex monoliths creates high barriers to market entry. Up to 90% of defense contracts face no competition, so defense firms have little incentive to be more

innovative or cost-conscious.[95] Limited competition opportunities also reduce the return on investment for companies that could introduce innovative products for reuse across several military customers. More frequent acquisition cycles will help competition between defense contractors.

To shift demand conditions and incentivize companies to pursue innovation rather than sustainment, each service should design a rapid and iterative competition program to introduce new companies and ideas to solve a core problem. By starting with small-scale pilots rather than large combat platforms, defense employees will learn with industry how to lower the barriers for new entrants, award concise and practical contracts, and measure performance continuously.

Classification and Program Security Challenges for JADC2 Integration

The U.S. industrial security apparatus is a foundational set of programs and responsibilities throughout DoD, the interagency, industry, and allies; it protects the critical information that maintains our warfighting advantage and leverage in the GPC. The National Industrial Security Program Operations Manual (NISPOM) is the governing document for the National Industrial Security Program (NISP). It exists as the guiding document for how the USG handles and secures its secrets, at nearly all levels and almost all locations, both in the government and industry (Appendix C). It has accomplished this task by creating program-specific silos and stovepipes associated with platforms, subcomponents, and capabilities. While some programs are bucketed and briefed together, relatively few operators or managers are briefed into adjacent programs, thereby erecting "firewalls" for information protection. This model has effectively protected our secrets, reflecting how we traditionally fought our wars – in service isolated silos and stovepipes. Unfortunately, while our warfighting CONOPS are evolving, the industrial security architecture governing its existing systems and protecting its programs has not. As it stands, current US industrial security programs and processes are significant impediments to creating a networked JADC2 warfighting enterprise.

Today's security policies are challenged by the daunting task of securing a flexible network of sensors and shooters spanning the joint force and leveraging capabilities across all domains. These new non-linear kill chains demand flexibility among previously disconnected platforms and rapid communication with our international security partners. Today's systems do not support this. As currently written and executed, the Cold War's industrial security policies and stovepipe security cultures make a JADC2 model unachievable. This antiquated security policy creates a chicken and the egg scenario for JADC2 proponents. What should come first? Industry waits for a clear set of requirements from the government, while the government has resolved to hold off on requirements until understanding what industry can provide. Despite this stand-off, all parties agree that current information security requirements are limiting our ability to communicate what capabilities the joint force currently has, develop new systems to integrate existing sensors or shooters, or even deeply discuss binding the hundreds of SAP protected platforms and capabilities to scope the effort. Some of the problem stems from the byzantine security process for SAPs; precious few are cleared to know about a single program, much less have access to enough to have a clear picture of the joint forces' current capabilities. SAP awareness is not comprehensively implemented across the Government and industry to properly understand and develop JADC2 requirements and solutions. As a result, services have "bought-in" at different levels, each with its concept envisioned to snap into the overarching JADC2

architecture. The DIB has also made halfhearted attempts to demonstrate new sensor/shooter combinations within their proprietary offerings. Unfortunately, the security barriers between programs hobble any meaningful conversations inside government or industry. There is no critical mass of knowledge across the SAP secured programs to develop required solutions.

Furthermore, tensions between interoperability and cybersecurity hamper DoD CIO and DISA efforts to advance JADC2 principles. The same agencies responsible for supporting and accelerating joint interoperability are also responsible for ensuring the security of DoD's networks. Cybersecurity is not a new problem but rather a blind spot that has only more recently become glaringly and embarrassingly apparent. GAO conducted a cybersecurity study of weapons systems in 2018. They found "mission-critical cyber vulnerabilities in nearly all weapons system development."[96] DoD CIO and DISA must address evolving cybersecurity challenges as DoD procures increasingly interconnected weapon systems.

The DoD CIO and DISA's answer to cybersecurity are currently Joint Regional Security Stacks (JRSS). The DoD Department of Defense Information Network (DODIN) director and DoD CIO JRSS lead both call JRSS "the most critical near-term element of DoD's Joint Information Environment."[97] The DISA-managed JRSS technology represents a protect-the-castle cultural mindset prevalent in DoD. Initiated in 2010, it consists of a series of switches, routers, and firewalls at the edges of the DODIN that work to secure all data inside its walls and repel cybersecurity invaders.[98] JRSS is not yet a failed joint program, but it is getting close. In 2019 the DoD Inspector General audited the program and found that JRSS was not meeting security objectives and was likely to hinder the security of the Joint Information Environment (JIE). In agreement with DoD I.G.'s findings, Congress has already noted that the Senate Armed Services Committee questioned whether JRSS is obsolete and cut funding for the SIPR JRSS implementation in the final 2021 National Defense Authorization Act.[99] To hedge against the possibility of losing JRSS, DISA is pursuing zero-trust technology, a change in architecture that obviate the need for JRSS. Zero-trust architectures place the burden of cybersecurity on network endpoints. To implement JADC2, both DoD CIO and DISA need to reconsider how they are implementing cybersecurity. Zero-trust might be a step in the right direction.

The Complexity of Designing *Truly* Joint Programs and Concepts

In addition to the previously mentioned complexities, JADC2 is forced to confront an ugly reality: joint programs have a long history in the DoD and a bad reputation. Historically they experience higher failure rates than their single-service counterparts.[100] Interservice interoperability concerns are frequently at the heart of joint program failure.[101] The purpose of JADC2 is interoperability itself, which means that it is an inherently complex problem. As the JADC2 CFT develops the new warfighting concept requirements, it should start with lessons learned from previous failures and successes of joint programs.

In theory, joint programs should be easy. If two organizations have similar requirements, they can create efficiencies by sharing the resource burden. Congress, responsible for efficiently spending taxpayers' dollars, should be interested in saving money by reducing redundancies within the DoD. Policy organizations like DoD CIO should like this plan too; they would not have to write joint doctrine or policy vice interservice. Unfortunately, the reality of joint

programs is not that simple, and what appears at first to be an easy solution can end in utter failure.

Despite the history of failures, Congress continues to push DoD to pursue joint programs. Since Congress ultimately holds the purse strings, they are nearly always interested in improving efficient resourcing. On the other hand, when Congress is unhappy with the direction of a program or needs to prioritize one program over another, it will cut that program's resources. Highlighting where equipment is manufactured is a common strategy to defend programs in Congress. Congress clearly and repeatedly sends signals that it is interested in greater efficiency and increased jointness. Is it easier to find thousands of different motivations to appeal to each member and staff member of Congress, or would it be more effective to do what Congress keeps asking DoD to improve joint capabilities? In addition to Congress's power to end joint programs, services also can sabotage joint programs due to the services' inability to agree on a shared joint vision. If the services cannot move beyond cultural divisions, a complex program like JADC2 will not succeed.

The Complexity of Integrating with Allies and Partners

The DoD cannot neglect its partners and allies in developing JADC2 and expect to maintain its asymmetric advantage in an era of GPC. As the INDOPACOM J6 noted: "if we build a network…[it's] not releasable to our mission partners, we're going to lose."[102] Fortunately, the DoD already has the tools to ensure that it can work around these hurdles; it needs to implement these tools to ensure success.

First, the DoD must acknowledge the role of partners and allies and bring them into the planning process. By bringing them into the planning process while the DoD is developing its strategy, it can strengthen its future warfighting concepts through the diversity of thought and identify potential roadblocks posed by competitive international defense markets.

Secondly, the DoD should stand up a JADC2 International Cooperative Program. Acting through the Undersecretary of Defense for Acquisitions and Sustainment, International Cooperation (OUSD A&S IC), the DoD can initiate international agreements with partners and allies to research, develop and field JADC2 systems. By starting an international cooperative development program, the DoD can ensure interoperability through collaborative development of shared equipment. Additionally, it can reduce the acquisition costs of JADC2 technologies through cooperative funds and advanced foreign sales. Finally, the DoD can use a cooperative program to build partner and allied trust by sharing equipment production across multiple industrial bases.

Despite the U.S.' dominance of the global C4ISR markets, continued success is not a given. Rising economic competition with partners and allies dampens the advantages U.S. companies enjoy. Additionally, protectionism distorts the marketplace, impairing sales and cooperation while stifling innovation. To keep pace with the changing character of war, the DoD should update its policies, advocate for changes to the AECA, bring partners and allies into its JADC2 planning processes, and finally initiate a JADC2 cooperative program with interested partners. Without making these changes, the DoD risks losing its asymmetric advantage and will find itself deterring its Great Power Competitors alone.

Conclusion

Winning the current era of GPC is not only a challenge facing the U.S. but one posed to nations that support rules-based world order. Adversaries, specifically China and Russia, seek to undermine the trust and confidence in the world order to advance their economic, political, and military interests. China and Russia's gray zone activities walk a fine line between competition and conflict, and the threat of escalation is looming. Therefore, the U.S. and its allies must not delay taking action to deter and defend world order, peace, and democracy. To counter the evolving GPC threat, the U.S. is pursuing a JADC2 concept. The DoD defines JADC2 as a "concept to connect sensors from all of the military services - Air Force, Army, Marine Corps, Navy, and Space Force - into a single network."[103]

JADC2 is an inherently revolutionary and complex concept. The complexity is not due to a lack of funding, innovation, or technologies. Instead, as the initial planning demonstrates, the complexity lies in its implementation. Implementing JADC2 will require revolutionary changes in U.S. service cultures, partnerships and agreements with our partners and allies, DoD's acquisition policies and processes, and how DoD, services, partners and allies, and industry approach interoperability. Change can be unsettling and difficult to accept and implement, but revolutionary change is disruptive and harder to accept and implement as it is riskier. However, not implementing change because it is risky or disruptive will only exacerbate the current GPC challenges and hasten a potentially more undesirable outcome. The uncertainty and risk of change are yet another piece of the JADC2 complexity puzzle facing the U.S. and its allies and partners. It moves towards establishing capabilities, structures, and operations for a fully integrated and interoperable Joint Force.

Recommendations

To ensure the successful implementation of JADC2, the authors propose the following four recommendations: 1) Joint Staff undertakes an evaluation of the market strengths and weakness of its great power competitor, 2) implement reforms to the DoD's acquisition policies and processes that encourage competition in the C4ISR market, 3) develop a trust-based culture for joint and coalition warfighting, and 4) continuously evaluate security/classification requirements to remove hurdles that prevent effective interoperability and delegate an authorized board of senior stakeholders that can adjudicate hurdles beyond the scope of individual services.

While the U.S. outmatches both great power competitors in almost all areas of the C4ISR industry, the U.S. must consider the strengths of China and Russia while building JADC2 capabilities. However, based on Porter's Diamond analysis China is the clear threat catalyst for JADC2. China's whole-of-nation approach and Military-Civil Fusion (MCF) strategy present a plausible pathway to parity with the U.S. C4ISR market and JADC2 capabilities in the future. China's approach allows technology and concepts to be quickly shared and transferred between military and civilian sectors and shortens its acquisition and development timeline significantly compared to the U.S./DoD. However, the American innovation culture and the tech community's constant pursuit of improving and advancing technology fosters healthy competition and creates a comparative advantage.

To ensure the federal acquisition system keeps pace with advancements in industry and technology, the government, DoD, and the services are taking steps to modernize it. However, the underlying policies and processes on which the system was built need to evolve faster. The current acquisition process promotes long-term lifecycle sustainment rather than innovation and development. Today's defense contractors seldom compete, are rewarded with "winner takes all" contracts, and have no incentive to replace legacy systems with new technology or platforms. This type of demand signal impedes the DoD and the services' ability to harness new technologies and reduces competition within the defense industry because it inhibits the frequent rebidding and updating of contract requirements. The current acquisition model needs to pursue an intelligent divestiture of legacy programs and systems to develop cost-efficient innovative technologies and capabilities that pressure and deter adversaries. Modernizing the acquisition model cannot be done in a vacuum; it must also include acquisition culture reform. A program's perspective on risk must change. Programs must take risks and not fear failing to bridge the "valley of death" gap. In the GPC environment, low risk/low reward programs and systems will not create or maintain the advantage needed; future initiatives need to be balanced with high risk /high reward activities to keep pace with technology.

Creating an authentic joint service culture for JADC2 is essential as All-Domain Command and Control is an inherently joint way of fighting. The services each have an initiative designed to support JADC2 development; Air Force: ABMS; Army: PC and Project Overmatch for the Navy. Each of these service-specific efforts demonstrate the ability to execute multi-domain operations, but on a limited scale. Sharing essential sensor data and being resilient in conflict will enable whatever competitor can dominate this space.

The integration and interoperability of these systems and the collaboration across the services are the next steps in bringing JADC2 to fruition. However, each service has a unique culture and operating structure that must be deconflicted and aligned. Overcoming cultural differences and biases takes time, but the DoD and the services are making progress through joint exercises and testing JADC2 capabilities and agreements to develop interservice data sharing by 2022 between the Army and Air Force.

The risks associated with the U.S. taking unilateral action against a GPC competitor are unacceptable. Therefore, integration and interoperability with U.S. partners and allies cannot be an afterthought and must be done in parallel. Ensuring interoperability with U.S.'s international partners is foundational in the development and successful operation of JADC2. Even though incorporating partners and allies into JADC2 presents risks regarding data collection/sharing and system/platform connections, the U.S. does not have the geopolitical power, the resources, or bandwidth to win the competition/fight alone.

A large portion of the data involved in building a comprehensive all-domain network is classified as "Special Access" and cannot be utilized by U.S. partners and allies. This constraint severely limits data sharing and does not meet the intent of JADC2. Without equal information sharing, JADC2 will not effectively bring together multi-service/agency capabilities and data to quickly assess and respond to threats in the GPC environment. Another risk of integrating with partners and allies is allowing their indigenously developed and produced systems and sensors to connect to U.S. systems and networks. Not only does it introduce supply chain risk, but network access points that are outside the cybersecurity purview of the U.S. Furthermore, it presents an

economic dilemma as it brings the relationships between the DoD/Congress/Industry into conflict over profits and jobs created by developing and implementing portions of JADC2 in the U.S. or in our partners and allies. Ultimately, the risks associated with data classification and sharing data and component manufacturing locations is a cultural challenge more than a technical challenge.

Overall, JADC2 faces many complex challenges before it can be a joint concept. The U.S. greatest competitors, China & Russia, are the critical motivation needed to overcome these challenges and accelerate the development and delivery of JADC2. China and Russia have capability gaps in their all-domain capabilities, and now is the time for the U.S. and its partners and allies to act to ensure they do not fill those gaps and gain an advantage in GPC.

The U.S. has shown the services' ability to implement JADC2 in limited scope while including partners. The synchronization of innovation and integration of disruptive technologies will provide the U.S. with an accelerated vehicle to complete JADC2. GPC is not a challenge the U.S. or its allies and partners can win alone. The best defense is a joint defense that leverages the culture-shifting ideas and technological innovations across the Triple Helix and the U.S.'s allies and partners.

APPENDIX A: U.S. C4ISR Prime Contractor Firm Briefs

Northrup Grumman Firm Brief

NORTHROP GRUMMAN

Agenda

- Company Profile
- Business Segments
- Acquisitions and Divestitures
- Strategy and Competing Markets
- Supply Chain Vulnerabilities
- Human Capital Challenges
- C4ISR UAS Market
- UAS Market Characteristics
- Firm Structure (Porter's Five Forces)
- C4ISR Satellite Market
- Satellite Market Characteristics
- Strategy Pursuit (Strategic Gameboard)
- Innovation & Approach to a Changing Industry
- Financial Market
- National Security Recommendations

2

NORTHROP GRUMMAN

Understanding the Firm

- What is Northrop Grumman's Profile?
- Where are they located?
- What is their Evolution?
- What are their four operating business segments?
- What was their most recent acquisition?
- What was their most recent divestiture?
- What is their global strategy and corporate strategy?
- What are Northrop Grumman's supply chain vulnerabilities?
- What are Northrop Grumman's human capital challenges?

NORTHROP GRUMMAN

Firm Profile

- Headquarters: Falls Church, VA
- CEO: Kathy J. Warden
- Currently #4 of U.S. defense firms
- Ranked #368 on Global 500; #144 on S&P
- Employees: 97,000 (2020); 90K (2019); 85K (2018)
- Revenue: $37B (2020); $34B (2019); $30B (2018)
- Backlog: $81B (2020); $65B (from 2019); $54B (2018)
- Pension: $1B (2020); $1.8B (2019); $655M (2018)
- Contractual Obligations: $45B through 2026 and beyond
- 51M square feet of floor space in 530 locations

NORTHROP GRUMMAN

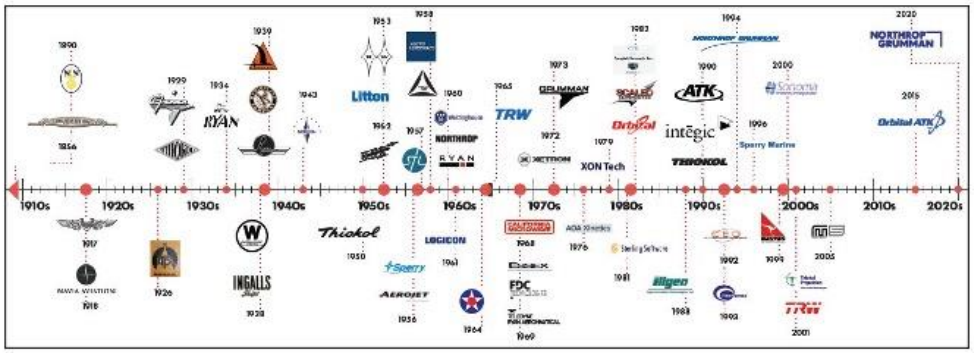
Global Presence

- Australia
- Europe
- Japan
- Middle East
- Poland
- South Korea
- United States

5

NORTHROP GRUMMAN

NG Evolution



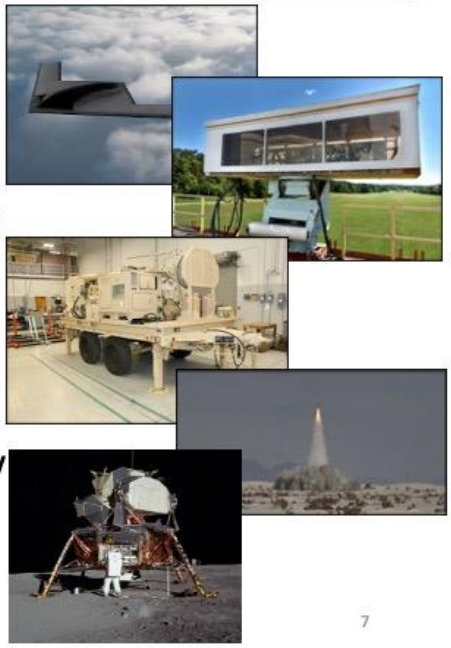
- **Founded: 1939, Hawthorne, CA – Northrop Aircraft Incorporated**
- **Reincorporated: 1985 – Northrop Corporation**
- **Reincorporated: 1994 – Northrop Grumman Corporation (Merger with Grumman Corp.**
- **Founders: Jack Northrop and Leroy Grumman**

6

NORTHROP GRUMMAN

Business Segments

- **Aeronautics Systems – Palmdale, CA**
  - **Autonomous Systems**
  - **Manned Aircraft**
- **Defense Systems – McLean, VA**
  - **Battle Management & Missile Systems**
  - **Mission Readiness**
- **Mission Systems – Linthicum, MD**
  - **Airborne Sensors & Networks**
  - **Cyber & Intelligence Mission Solutions**
  - **Maritime/Land Systems & Sensors**
  - **Navigation, Targeting, and Survivability**
- **Space Systems – Dulles, VA**
  - **Launch & Strategic Missiles**
  - **Space**



7

NORTHROP GRUMMAN

Recent Divestiture

- 2020 – Federal IT and Mission Support Systems to Peraton, affiliate of Veritas Capital for $3.4B, cash
- Veritas is a global leader in data protection; recently named as a 2021 Gartner Peer Insights Customers' Choice in Enterprise Information Archiving
- Peraton provides mission critical technology solutions to government customers
- Expected to generate $2.3B in revenue for Northrop Grumman
- Sale proceeds will go to share repurchases, to offset dilution from the transaction, and for debt retirement

VERITAS

Peraton

9

NORTHROP GRUMMAN

Global Strategy

- Northrop Grumman is a leading global aerospace and defense company
- Operates in a highly competitive market, including U.S. defense firms, foreign and multinational firms, and new entrants
- Considers sales outside the U.S. to be an important aspect of their global strategy
- NG maintains a global presence in 25 countries
- $5.8B of all revenue comes from foreign sales; $31B from the U.S.
  - $31.6B - America
  - $2.1B -- Europe
  - $2.0B – Asia Pacific
  - $1.7B -- Other

10

NORTHROP GRUMMAN

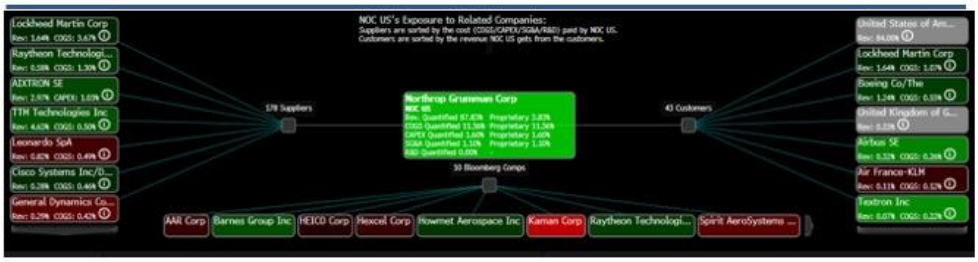
Strategy

- NG strategy begins with its customer, and operates in a highly competitive security market
- Dependence is largely centered on the U.S. government
- Focused on using their broad portfolio of capabilities and technologies
- Their strategy is accomplished through four operating business sectors

11

NORTHROP GRUMMAN

Supply Chain Vulnerabilities



- Over $11 billion spent in 2019 on domestic sub-contractor support
- 178 Suppliers
- Requires a broad base of suppliers to provide:
  - Raw material, chemicals, components and subsystems
  - Develop SW and IP; produce hardware elements and sub-assemblies
- Requires global suppliers/partnerships
- Need to increase supplier diversity
- Suppliers must act ethically, use environmentally best practices
- Cybersecurity risks to supply chain

12

NORTHROP GRUMMAN

Human Capital Challenges

- Total Workforce: 97,000
  - New hires in 2020 – 13,000
  - 4,000 employees covered by 17 collective agreements which 6 were renegotiated in 2020; 5 will be renegotiated in 2021
  - Need to retain personnel with local qualifications and experiences outside U.S.
- Facing competition for talent both from defense and commercial companies
- Requires highly technical cleared individuals
- High Pension/Post-retirement benefit costs

13

NORTHROP GRUMMAN

UAS Market Transition

- What is the scope of the Unmanned Aircraft Systems (UAS) market?
- What are the market's key characteristics?
- Where does the UAS Market fall along the competitive spectrum?
- How does NG's UAS Product Line compete?
- How does NG fit into the market?

14

NORTHROP GRUMMAN

Unmanned Aircraft Systems

"UAS are air vehicles and associated equipment that do not carry a human operator, but instead are remotely piloted or fly autonomously. UAS commonly are referred to as Unmanned Aerial Systems (UAS), Unmanned Aerial Vehicles (UAV), Remotely Piloted Aircraft Systems (RPAS) and drones. A UAS generally consists of 1) an aircraft with no pilot on board, 2) a remote pilot station, 3) a command-and-control link, and 4) a payload specific to the intended application/operation, which often includes specialized cameras or other sensors that collect data for near term analysis."

15

NORTHROP GRUMMAN

UAS Market Characteristics

- Global Market Size:
  - UAS (Military) - $7.94 billion 2020
  - UAV - $19.3 billion in 2019 → $45.8 billion by 2025
- Growth:
  - Global defense spending highest in last 10 years
    - $1.92 billion (2019), 3.6% higher 2018 & 7.2% higher 2010
    - Largest spenders: U.S, China, India, Russia, & Saudi Arabia (62% of total)
  - Highest growth in Military/Defense markets: Enhance combat capabilities; ISR segment
  - Highest growth in commercial sector: construction (surveying & design mapping), product delivery, monitoring
  - Remotely operated UAVs continue to lead the market – wider range of capabilities

16

NORTHROP GRUMMAN

UAS Market Characteristics

- Trends:
  - Technology advancements:
    - Integration of AI & ML software to enhance data collection and information analysis
    - Advance features to increase precision, accuracy, reliability, and speed
    - Improved efficiency in intelligence, surveillance, and reconnaissance (ISR)
  - Expansion into commercial, scientific, recreational and civil services (i.e., disaster relief, forest monitoring, cinematography, agriculture)

17

NORTHROP GRUMMAN

UAS Market Characteristics

- Geographic:
  - North America, Europe, Asia Pacific, Middle East, Latin America, Africa
  - Military/Defense market growth highest in U.S., China, India, Russia, Saudi Arabia
  - U.S – top global exporter (ISR UAVs)
  - China – top exporter of multi-role strike capable UAVs
- Opportunities
  - Dual use
  - Collaboration – Large and Small businesses; emerging technologies

18

NORTHROP GRUMMAN

UAS Market Structure

- Many buyers: Domestic & Foreign
- Many sellers: Domestic & Foreign
- Low/Medium Barriers to Entry: Domestic vs. Foreign
- Differentiation: Customization
- Production: Under capacity with all emerging customers

19

NORTHROP GRUMMAN

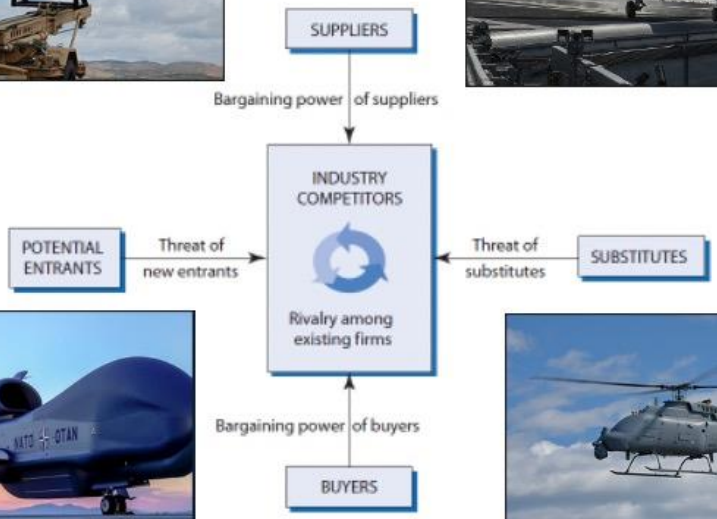
NG's UAS

- High-Altitude Long-Endurance (HALE)
  - RQ-4 Global Hawk (U.S. Air Force)
  - MQ-4C Triton (U.S. Navy)
  - Alliance Ground Surveillance (AGS) (NATO)
  - X-47B UCAS (U.S. Navy)
- Medium-Altitude Long-Endurance (MALE)
  - MQ-8B/C Fire Scout (U.S. Navy)
  - Firebird (multiple customers)
  - Bat
- Both HALE and MALE UAS reuire runways and clear line-of-sight communications connected to ground stations for take-off and landing
- In flight large UAS operation using beyond line of sight (BLOS) communication links

20

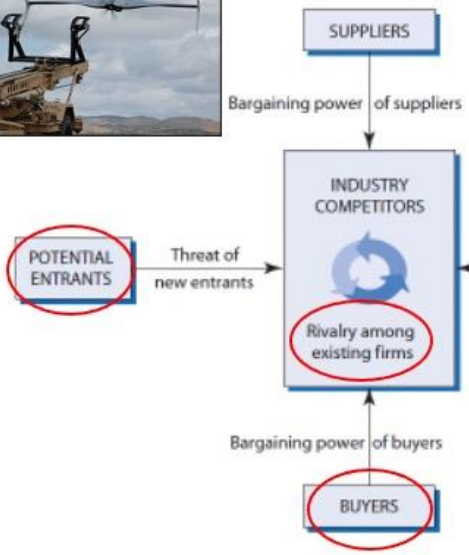
NORTHROP GRUMMAN

UAS Porter's Five Forces



NORTHROP GRUMMAN

NG Most Important Forces



NORTHROP GRUMMAN

NG Most Important Forces

Google

AeroVironment™

GENERAL ATOMICS AERONAUTICAL

Raytheon

dji

BOEING

Parrot

amazon

LOCKHEED MARTIN

Aurora FLIGHT SCIENCES A Boeing Company

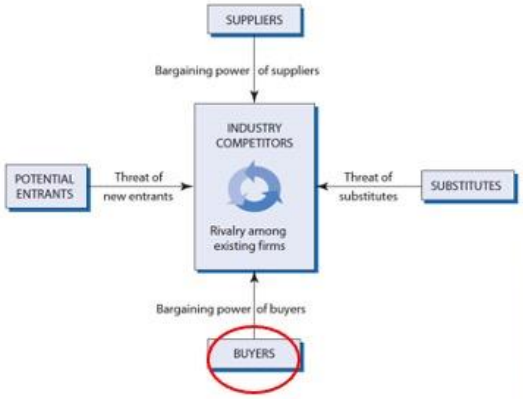
IAI

CASC

中国航天

NORTHROP GRUMMAN

NG Most Important Forces



- Shift in customer preferences
  - Quantity vs. Quality
  - Price sensitivity
  - Emerging Technologies
- High risks?
  - Global Hawk
  - Triton

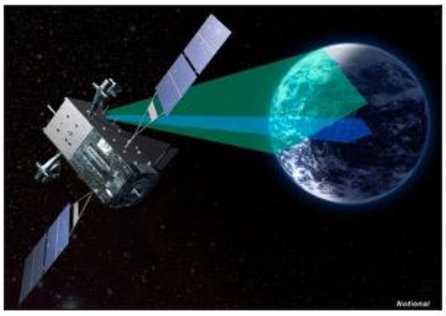
NORTHROP GRUMMAN

Satellite Market Transition

NORTHROP GRUMMAN

C4ISR Satellite Market

- Competitive market necessary for National Security
- C4 – communications satellites
  - E.G. – Milstar , AEHF, Enhanced Polar System, and Enhanced Polar System Recapitalization, Evolved Strategic SATCOM
  - ISR– IMINT (EO, IR, SAR), SIGINT
  - E.G. – SBIRS, Next Generation OPIR
- Related Functions – commercial satellites, propulsion, lift vehicles, space vehicles, logistics support
  - E.G. – GeoStar, Cygnus Spacecraft, Mission Extension Vehicle



26

NORTHROP GRUMMAN

C4ISR Satellite Market

- Military Satellite Market
  - 2020 – $387 Billion cumulative revenues
  - 2020-2028 Compounded Annual Growth Rate – 76.6%, $195.1 Billion
  - Largest growth forecast in Asia
  - Small/nano satellite largest emerging market
- NOC Space Systems 2020
  - $8.7B Sales – $1.3B/18.1% increase

27

NORTHROP GRUMMAN

Nature of Firms Competing

- Overall satellite market relatively broad, C4ISR satellite market very narrow
  - Barriers to entry – high
  - Rivalry – medium
- Boeing, Lockheed, Raytheon, Northrop Grumman
  - Produce limited numbers, high price point
  - Government forces integration
  - Often prime / sub-prime for each other
- Oligopoly – small number of firms, produce similar products, profitability relies on interactions with other firms

28

NORTHROP GRUMMAN

Market Strategy

- Key to pursuing strategy – maintain long-standing business relationships, pursue relatively low risk ventures to maximize shareholder profits
  - Grow core businesses that focus on technology and innovation
  - "Reliability, speed and affordability" for customer
  - Expand business on international market
- Competitive advantage – leverage history and experience in payload design and implementation
- Independent Research and Development
  - 2020 - $1.1 billion, 2.9% total sales
  - 2019 - $953 million, 2.8% total sales
  - 2018 - $764 million, 2.5% total sales
- Risks
  - Spacecraft loss on launch or flight
  - Program cancelations or contract adjustments
  - Contract type affects profitability
  - Flat/declining DoD budgets

29

NORTHROP GRUMMAN

Strategic Gameboard

- Same Game / Across-the-board Strategy
- Defines the market and functional approach
- Where to Compete
  - Specific market segment
  - Defend market space
- How to Compete
  - Better execution and price
- When to Compete
  - C4ISR satellite market demand increasing
  - Continued incremental improveme
- Recommendations
  - Seek innovation within segment
  - Find niche supporting markets

30

NORTHROP GRUMMAN

Innovation

- Payload sensor packages
- Mission Extension Vehicle-1
  - Identified new market
  - Rendezvous, correct and maintain orbit of Intelsat 901
  - Multi-mission technology
- James Webb Space Telescope
  - Successor to Hubble telescope and 100 time more powerful
  - Numerous spin-off technologies
- Advanced manufacturing practices
  - Dockable Gantry System – combination Automated Fiber Placement and Automated Tape Laying
- "JADC2 the company"

Evolutionary or Revolutionary Approach to Innovation?

31

NORTHROP GRUMMAN Approach to Industry Change

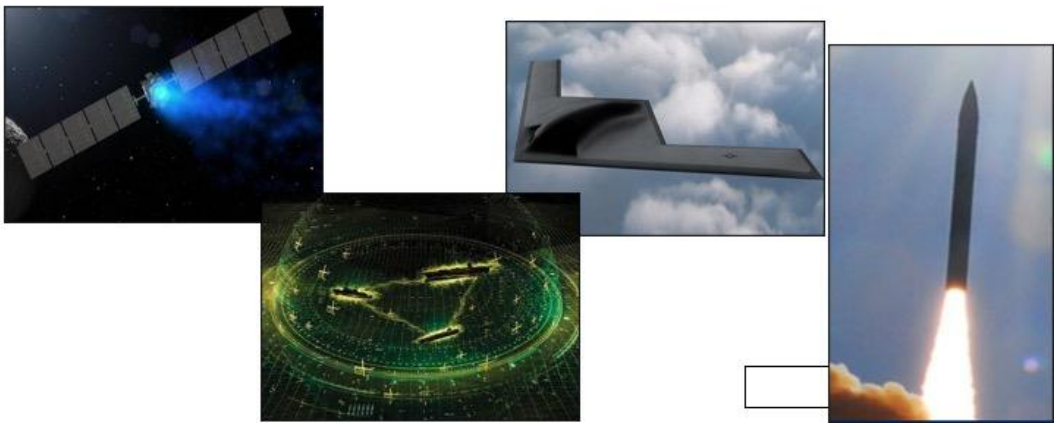
- Threats to large/exquisite satellite market
- Current small satellite provider
- At risk of missing Cube/Nano satellite market
  - Provides lift/ride share
- Competition with Space X model
- Increase commercial space investment and dual use technology

I won't support the development any further of large, big, fat, juicy targets. – Gen John Hyten

32

NORTHROP GRUMMAN NG Financials Transition

- How does the DoD value Northrup Grumman?
- How does Northrup Grumman create value?
- How does Aeronautics and Space Sector relate to NG overall?
- How do stockholders (owners) value Northrup Grumman?



NORTHROP GRUMMAN

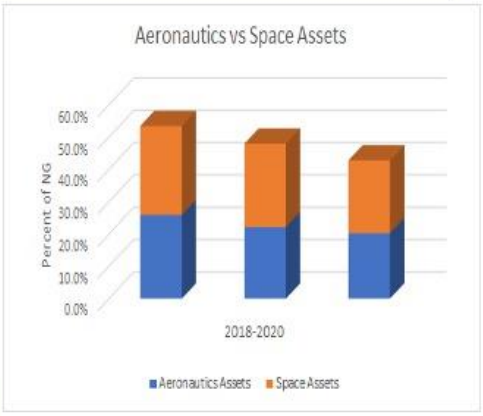
Financials Overview

- Assets
- Revenue / Revenue Growth
- Profit / Margin Growth
- Debt and Corporate Tax Rate
- ROIC / WACC
- Stock Price Causality
- Understanding Northrop Grumman…

34

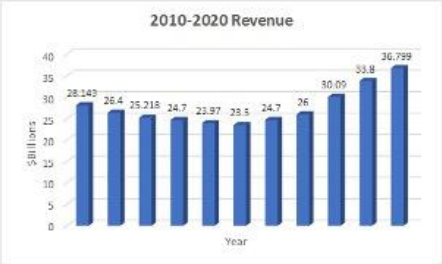
NORTHROP GRUMMAN

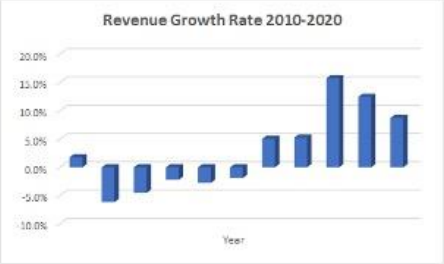
NG Assets



NORTHROP GRUMMAN

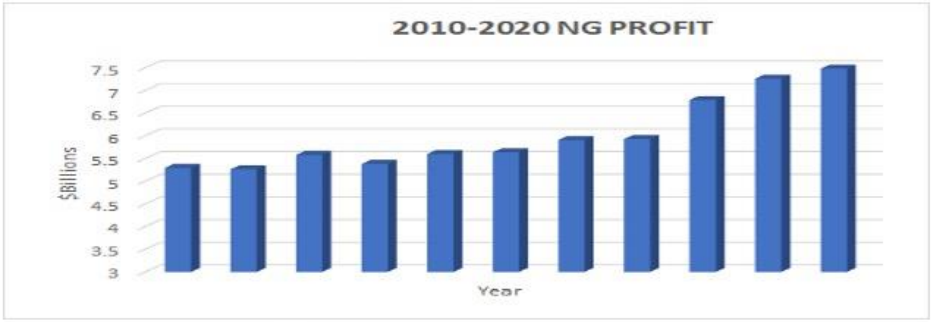
NG Revenue





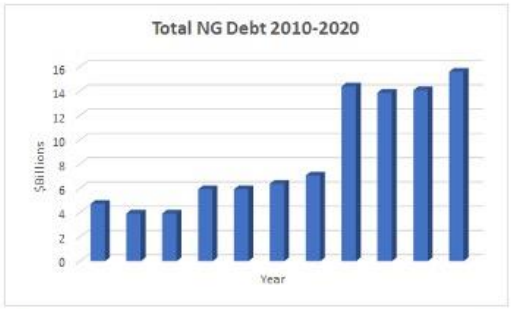
NORTHROP GRUMMAN

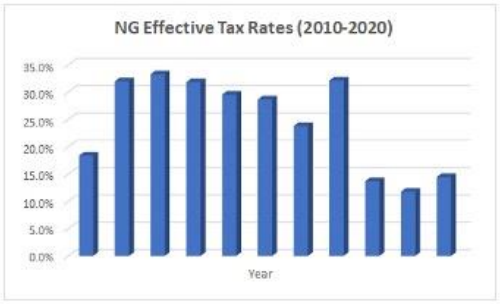
NG Profit



NORTHROP GRUMMAN

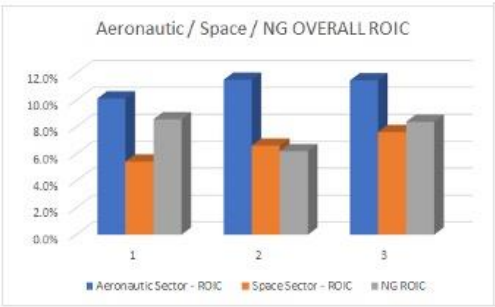
DEBT and Long-Term Tax Rates

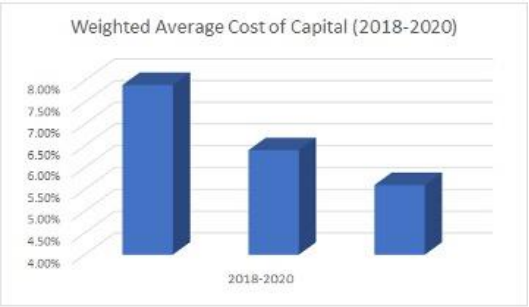


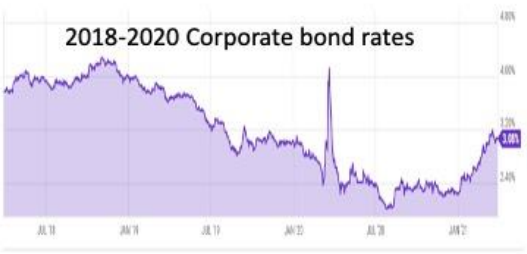


NORTHROP GRUMMAN

Return on Invested Capital (ROIC) and Weighted Average Cost of Capital (WACC)







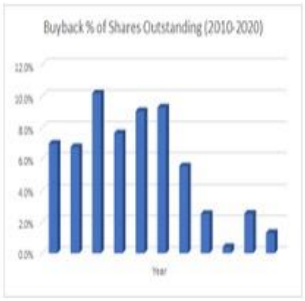
Bond Rating				
Moody's	Standard & Poor's	Fitch	Grade	Risk
Aaa	AAA	AAA	Investment	Lowest Risk
Aa	AA	AA	Investment	Low Risk
A	A	A	Investment	Low Risk
Baa	BBB	BBB	Investment	Medium Risk
Ba, B	BB, B	BB, B	Junk	High Risk
Caa/Ca	CCC/CC/C	CCC/CC/C	Junk	Highest Risk
C	D	D	Junk	In Default

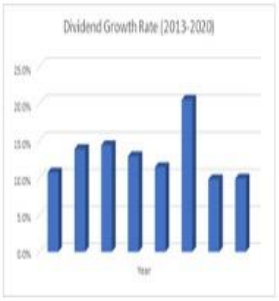
39

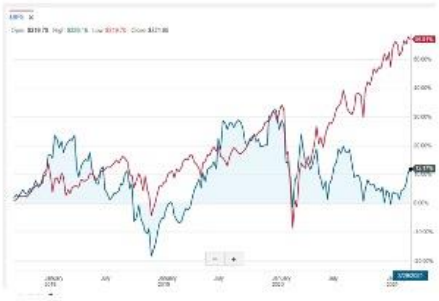
NORTHROP GRUMMAN

Current Stock Prices

- Share repurchase
- Dividend growth rate
- NOC stock – Last three years to 1 April +17% vs SP500 71%







NORTHROP GRUMMAN

NG Summary

- What does the DoD want from our primes?
- Can taxpayers have an expectation of a prime?
- What are shareholder expectations?

41

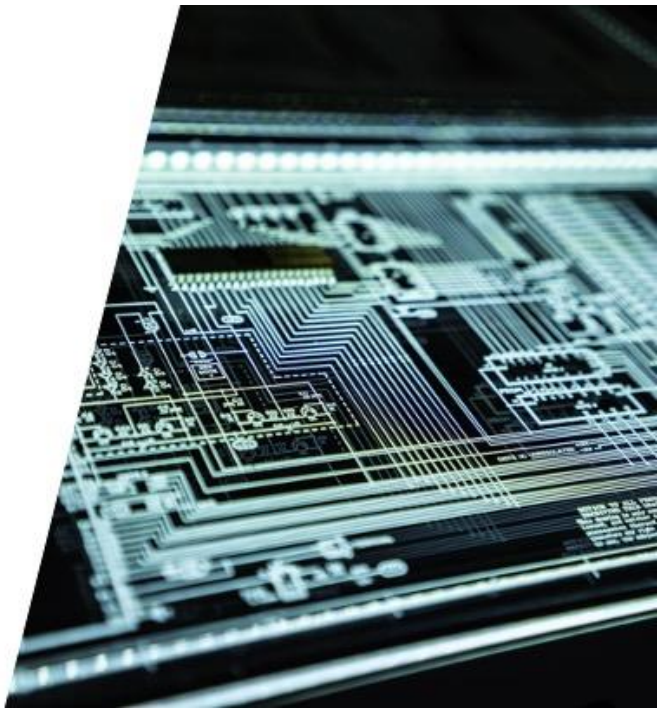
NORTHROP GRUMMAN

National Security

- **Huge defense contractors building profitable huge programs (B-21/JSF/Ford CVN/Columbia SSBN/Legacy Space Vehicles) -**
- **UAS / Satellites – Innovation / Partners and Allies**
- **U.S. Export Policies – Evaluate**
- **Increase participation in SBIR / STTR – Innovate better with Small Business**
- **S&T development with University**

42

Raytheon Firm Brief



Raytheon Technologies

Industry Analysis

Tom Potter
Aaron "Easy" Capizzi
Cliff "Diesel" Taylor
Mike Kruk

5 April 2021

1

"Combining complementary portfolios with advanced technology and R&D platforms, we are delivering transformative solutions to usher in the future of aerospace and defense."

– Gregory J. Hayes, CEO, Raytheon Technologies

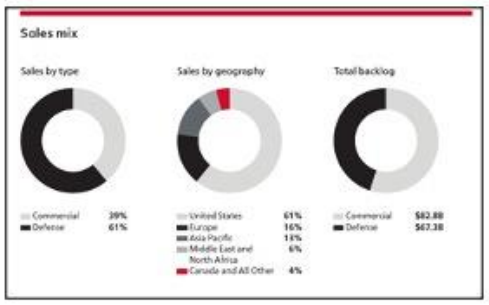
2

| Raytheon Technologies

- **Raytheon Technologies** (NYSE: RTX) is an aerospace and defense company that provides advanced systems and services for commercial, military and government customers worldwide. The company was formed in 2020 through the combination of Raytheon Company and the United Technologies Corporation aerospace businesses, and is headquartered in Waltham, Massachusetts. 2nd largest aerospace and defense company by sales behind Boeing.
- **Quick Facts:**
  - **181,000 Employees; 61,000 Engineers; 46,000 Patents; $64.6B (2020 adj revenue); 190+ Years of combined innovation (UTC)**
- **Four Highly Specialized Businesses:**
  - **Collins Aerospace:** Specializes in aerostructures, avionics, interiors, mechanical systems, mission systems, and power and control systems that serve customers across the commercial, regional, business aviation and military sectors.
  - **Pratt & Whitney:** Designs, manufactures and services the world's most advanced aircraft engines and auxiliary power systems for commercial, military and business aircraft.
  - **Raytheon Intelligence & Space:** Specializes in developing advanced sensors, training, and cyber and software solutions — delivering the disruptive technologies its customers need to succeed in any domain, against any challenge.
  - **Raytheon Missiles & Defense:** Provides the industry's most advanced end-to-end solutions to detect, track and engage threats
- **Values**: Trust, Respect, Accountability, Collaboration, Innovation
- **Social Impact**: Enabling Lifelong learning, honor those we serve and Supporting communities

| Raytheon Technologies

- **Raytheon 2020 Annual Report Highlights:**
  - On April 3, 2020, United Technologies Corporation (UTC) completed the separation of its business into three independent, publicly traded companies – UTC, Carrier Global Corporation and Otis Worldwide Corporation. Additionally, on the same day, UTC completed its all-stock merger-of-equals transaction with Raytheon Company. Upon the closing of the merger, Raytheon Company became a wholly owned subsidiary of UTC, which changed its name to Raytheon Technologies Corporation.
  - $57.1Bil adjust net sales
  - $2.73 adj earnings per share
  - $6.7Bil R&D
  - $4.3Bil cash flow from operations
  - $1.425 dividends per common share post-merger
  - 30% debt to capital ratio



4

| Raytheon Technologies 2020

- **Collins Aerospace:**
  - **Modernization of US ICBM under AF Ground Based Strategic Deterrent Program**
  - **Selected to provide Army with Mounted Assured Postilion, Navigation and Timing System (MAPS) Gen II for manned/unmanned vehicles**
  - **Army Future Vertical Lift program**
  - **Commercial Aviation: accelerated initiatives from airport curb to final destination; touch free lavatories; hand sanitizing stations; HEPA filters – cabin air purity.**

Collins Aerospace's leadership has defined clear priorities for the future. Our strategic framework encompasses several commercial and defense innovation areas, including connected digital ecosystems, aircraft electrification, autonomous operations, and the development and use of advanced materials. Despite the pandemic, we continue to advance these key technologies to ensure that when the commercial aviation industry invariably returns to normalcy, Collins Aerospace stands ready to meet the demands of the next generation of aerospace platforms.

5

| Raytheon Technologies 2020

- **Pratt & Whitney:**
  - **Geared TurboFan (GTF) Engine**: reducing fuel consumption by up to 20%, regulated emissions by 50% and noise footprint by 75% compared to other engines, while giving smaller planes the range to cross oceans.
    - Expanded GTF maintenance, repair and overhaul network
    - In 2020, Aegean Airlines, Aircalin, China Express Airlines, Middle East Airlines and Swiss International Air Lines each took delivery of their first GTF-powered A320neo family aircraft; JetBlue received its first A220 aircraft
  - **Completed planned upgrades during aviation downturn**
  - OCT2020 announced world-class turbine airfoil production facility to be built in Asheville, North Carolina ($650 mil)

In 2020, Pratt & Whitney used a sharp downturn in commercial air travel as an opportunity to accelerate planned upgrades on idled aircraft while also making significant investments in future growth. In a difficult year, the benefits of Pratt & Whitney's superior technology were never more apparent.

6

| Raytheon Technologies 2020

- **Raytheon Intelligence and Space (RI&S):**
  - **The U.S. Navy conducted its first flight test of our Next Generation Jammer Mid-Band in AUG2020**
    - The advanced electronic attack system denies, disrupts and degrades enemy communication and air defense systems. The open-system architecture allows for quick hardware and software upgrades, which are essential in defeating rapidly evolving sensing and jamming technologies.
  - **The Navy received first production unit of the Joint Precision Approach and Landing System for the F-35 Lightning II fighter**
    - Precision landing system accurately guides aircraft onto carriers and amphibious assault ships in surface conditions up to sea state 5.
  - **Air Force awarded RI&S a contract valued at up to $950 million for the Advanced Battle Management System**
  - **JUN2020 – awarded development contract for DARPA's Blackjack program**
    - **Blackjack: low-Earth orbit satellite constellation program to track multiple threats simultaneously**
  - **SEP2020 – delivered nest High-Energy Laser Weapon System to USAF**

Raytheon Intelligence & Space's investments in space, sensor and communication technologies led to a number of important milestones in 2020, while also generating new commitments from our customers.

7

| Raytheon Technologies

- **Raytheon Missiles and Defense (RM&D):**
  - Standard Missile-3, a defensive weapon built to destroy ballistic missiles, completed first intercept of a simulated intercontinental ballistic missile off the coast of Hawaii
  - U.S. Navy also completed two flight tests with RMD's newest cruise missile variant, the Tomahawk Block V
  - Delivered first AN/SPY-6(V)1 radar for Navy's Flight III guided-missile destroyer
    - The SPY-6 family of radars performs simultaneous air, missile and surface defense on seven types of Navy ships, delivering greater range, accuracy and advanced electronic protection than current deployed radars
  - Awarded a $126 million (Navy) contract to continue manufacturing Enterprise Air Surveillance Radars for its amphibious ships, carriers and frigates
  - OCT 2020 Air Force approved Storm Breaker smart weapon for use on the F-15E Strike Eagle aircraft.
    - Munition can hit moving targets in adverse weather > 40 miles away, reducing the time aircrew spend in harm's way.
  - U.S. Army needed to replace its Patriot air & msl defense system to combat new threats, including hypersonic weapons, we began developing the Lower Tier Air and Missile Defense Sensor.

Raytheon Missiles & Defense made substantial progress in 2020 in customer commitments and deliveries, as well as in product development and testing. Innovation was key to our success.

8

| Market Competition

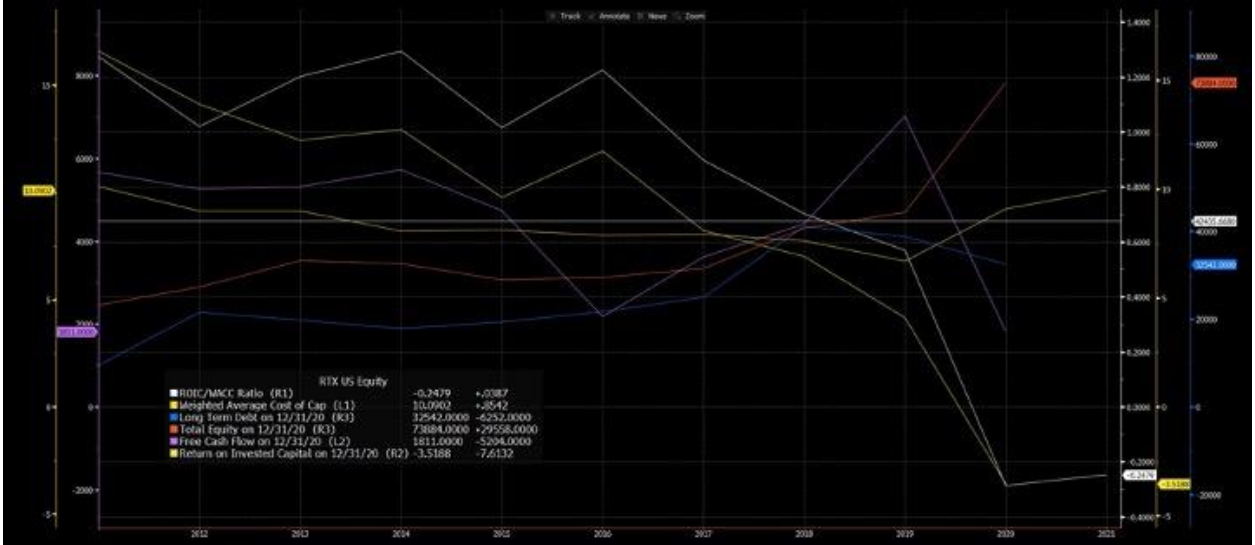
- **Raytheon: Monopolistic Competition**

- **Specialized Businesses:**
  - **Collins Aerospace:** Monopolistic Competition
  - **Pratt & Whitney:** Oligopoly
  - **Raytheon Intelligence & Space:** Monopolistic Competition
  - **Raytheon Missiles & Defense:** Monopolistic Competition

- **Industrial security, supply chain management, global trade**

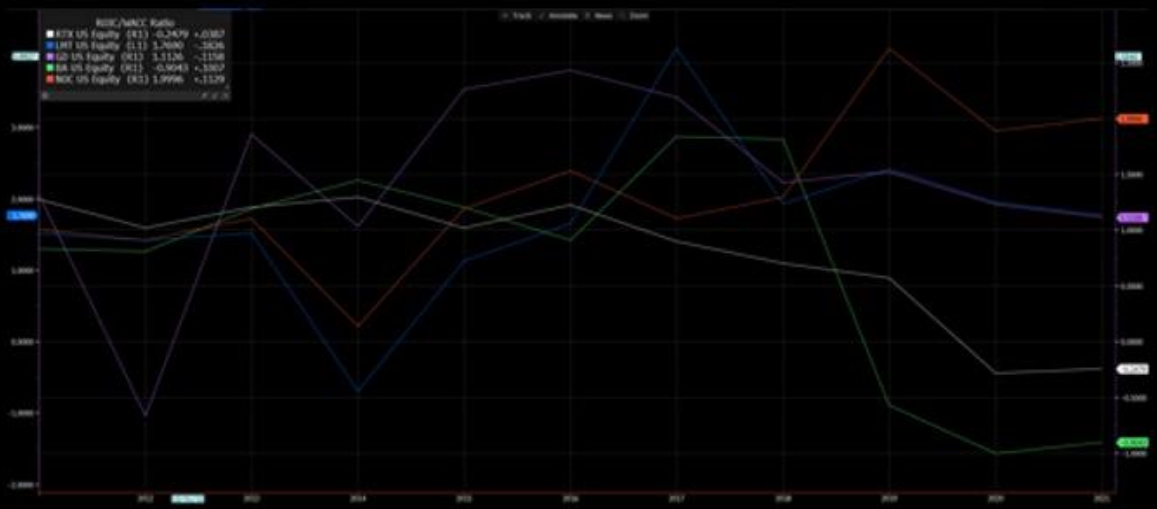
9

| RTX Financials



10

| Competition Financials



11

| Innovation Ecosystems and Disruption

Commercial Sensors

Autonomy / AI

Modular systems

Commercial Space

Cybersecurity

Networked Sensing

12

| C4ISR Market: Radars

- Niche, high-end electronics market
- Sophisticated ceramics, rare earth elements
- Analog-digital signal processing

Raytheon Technologies

Air Combat
- APG-63 (F-15C)
- APG-79 (EA/F-18)
- APG-82 (F-15E)
- APQ-181 (B-2)
- Raytheon Adv Combat Radar
- Adv Airborne Sensor (P-8)

Missile/Air Defense
- AN/TPY-2
- LTAMDS
- AN/MPQ-64 Sentinel

Maritime:
- SPY-6
- Sea Based X-band

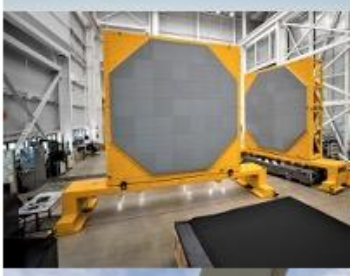
NORTHROP GRUMMAN
- APG-83 (F-16)
- APG-81 (F-35)
- APG-77 (F-22)
- APY-9 (E-2D)
- MESA (E-7)
- ASQ-236 Pod
- ZPY series for drones

LOCKHEED MARTIN
- AEGIS (SPY-1, SPY-7)
- TPY-X Air Surveillance
- APY- Early warning
- Long Range Discrimination (BMD)

L3HARRIS
TASR, SPS-48, APY-11

THALES
RBE2 (Rafale), Air Traffic Control

BAE SYSTEMS
Signal Processing



13

| Market Strategy: Radars

Suppliers
Niche electronics
Rare earths

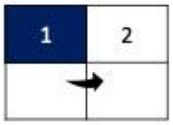
New Entrants
RF Design
Manufacturing
Digital Backend*

Rivalry

Substitutes
Networked sensing
Multi-spectral
Smaller / drones

Buyers
Platform dependencies
"Open" architectures
Modularity (RF/Digital)

Strategic Gameboard



- Currently market leader – continue same-game approach
- Compete on performance, cost
- Moderate investment in decoupling / modularity / open systems
- Prepare for hyper-networked sensors
- Ignores* smaller / mass / drone markets and nascent metamaterials radar tech

14

| C4ISR Market: Command and Control

- Almost entirely software-focused and communications-enabled
- Unique to military structure, systems and culture of decision making

Raytheon Technologies

Air Traffic Control
- STARS
- MARS
- Remote Virtual Tower
- AirMap strategic partnership

Ground Stations
- Distributed Common Ground System
- GPS OCX
- FORGE (Open Arch SBIRS, NextGen OPIR)
- Joint Polar Satellite System

Battle Management
- EW Planning & Management
- Air Operations Center Modernization
- Trailbazer -> Army Command Post Compute Environment

NORTHROP GRUMMAN
- Forward Area Air Defense C2 (C-sUAS)
- Integrated Battle Command Sys
- Joint BM Sys (RAAF)
- Distributed Autonomy / Responsive Control

LOCKHEED MARTIN
- C2BMC (MDA)
- Theater BM Core System
- MD Synch Effects Tool
- Universal GCS
- GPS Ground Control
- iSpace

L3HARRIS
- InControl
- Mobile TOC
- NOAA Space Weather C2

THALES
- ThalesRaytheonSystems joint venture for NATO Collective Defense BMD

BAE SYSTEMS

15

| Market Strategy: Command and Control

Suppliers
Competition for talent

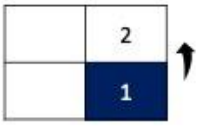
New Entrants
Commercial Tech
Autonomy / AI

Rivalry

Substitutes
Enterprise GCS
Microservices

Buyers
"Open" architectures
Enterprise services
Security / data standards

Strategic Gameboard



- Exploit head-start in software competencies, OCX lessons learned to become DEVSECOPS vendor of choice
- Materiel-independent architecture and systems engineering
- Build software and compliance workforce
- Build open platforms (FORGE, AOC) that drive support/integration dependencies

16

| Raytheon Technologies Strategy

The marriage of Raytheon and UT was one of equals in every way, but it demands alignment of over 100 years of fundamentally different strategies.

17

| Raytheon M&A Strategy

- Raytheon est. 1922
  - Started the company with battery elimination via AC conversion.
  - Never a "platform" centric company

Raytheon's strategy was growth through M&A focused on defense related electronics.

- 1928 – QRS Company (Electron Tubes)
- 1933 – Acme-Delta (Transformers)
- 1959 – Apelco Electronics (Nav/Radio)
- 1967 – Amana (Microwave) Div 1996
- 1985 – Beech Aircraft (Platforms) Div 2006
- 1995 – E-Systems (Electronics)
- 1997 – Chrysler Defense, TX Instruments Defense, Def. Systems & Electronics Grp., Hughes Electronics, Delco Electronics, Magnavox Electronics
- 2007 – Sarcos (Robotics R&D)
- 2009 – BBN (Advanced R&D)
- 2010 – Applied Signal (ISR Systems)
- 2015 – Websense (Cyber security) Div 2020

18

| United Technologies M&A Strategy

- United Technologies est. 1934
  - Merger of Boeing and PW to consolidate aviation companies for civil & mil business
  - Always platform centric when in the defense market with PW, Sikorsky, Vought, Hamilton Propeller

UT's strategy was growth through M&A and stability through diversification

- 1975 – Pivot to diversified hostile M&A
- 1976 – Otis (Elevator)
- 1979 – Carrier (Refrigeration)
- 1999 – Sundstrand Corp (aero electrical)
- 2003 – Chubb Security (Detect/ Alarms)
- 2004 – Schweizer Aircraft (Fixed & Rotary)
- 2005 – Kidde (Detect/Alarms)
- 2008 – NORESCO (Energy Company)
- 2009 – Clipper Windpower (Turbines)
- 2013 – Divested PW/Rocketdyne (rockets)
- 2015 – Divested Sikorsky (Helicopters)
- 2018 – Rockwell Collins (A&D Electronics)

19

| Raytheon Technologies Blended Strategy

- How are they different?
  - Raytheon is deeply focused while UT is highly diversified
  - Raytheon is platform light while UT is platform heavy
  - Raytheon nearly all DOD/allied sales, UT exploits commercial markets in non-allied nations
- What do they have in common?
  - Each understands M&A and exploiting synergies through acquisition
  - Advanced R&D as a core competency
  - Both have deep experience in DOD and international defense sales
  - Each fill gaps in other's portfolio (systems v platforms)

20

| Blended Strategy

- What did they do?
  - Adopt & Sharpen the Raytheon focus
    - Prioritize US DOD/USG over all else
    - Divested UT's diversified holdings (Carrier, Otis)
    - Divested Raytheon's non-core BUs (Forcepoint)
    - Exit non-allied commercial markets (China)
    - Remain "platform" agnostic
  - Capitalize UT's complimentary holdings
    - Establish a deep and broad capability in A&D
    - Take over controlling position in exquisite geared turbofan propulsion
    - Significant aviation R&D expansion

21

| Blended Strategy

- What are they now?
  - RTX represents one of the largest A&D engineer consolidation in the world
    - 60,000 engineers
  - Postured as one-stop-shop for multi-platform sensors and final engagement
    - Radars & Missiles
  - Non-electronic technologies are still core exquisite A&D engineering
    - Pratt and Whitney
  - Focused & aligned to satisfy integrated DOD & allied defense needs
    - JADC2!
  - EXPLOIT SNYERGIES of merger - drive down costs and return to profitability
    - Eliminate fat, non-core, or duplicative

22

| Strategy In Execution

- BL – Integrated JADC2 sensor and engagement solution
  - Seamless fusion of platform agnostic tipping/cueing (Radars & C2)
  - Unified tip/cue/engage solution tied to RTX missile technology
  - Fund the JADC2 R&D w/cost synergies of merger balanced w/increased R&D from combined company w/shareholder returns
    - 2B in cost savings since RTX merger
    - 600M in additional synergies from Rockwell Collins
  - Float RTX on strong PW engine sales
    - Forecast US DOD and allied purchase of revolutionary geared turbofan is high
    - Commercial Boeing forecast recovery EOY 2021

23

| Ethics

- Internal Policies
  - "Open Door Policy"
  - Accounting and Controls Hotline
  - Contact the Board of Directors
- External Policies
  - Antitrust
  - Corruption
  - Data Privacy & Security
  - Government Contracts
  - Global Trade Compliance

24

| Raytheon Ethics in Practice

POGO — PROJECT ON GOVERNMENT OVERSIGHT — ABOUT POGO — OUR WORK — TAKE ACTION

33 Instances of Misconduct since 1995

2 additional instances of misconduct pending resolution

Date	Instance	Penalty
5/1/2004	Raytheon Securities Litigation	$410,000,000
2/12/2021	Cruz v. Raytheon (ERISA Violation)	$59,170,000
2/27/2003	Improper Communications Equipment Export	$26,000,000
6/26/2006	Violations of SEC Rules	$14,774,840
2/8/2000	Ysleva v. Hughes Aircraft (Drinking Water Contamination)	$13,000,000
4/30/2013	AECA and ITAR Violations	$8,000,000
9/10/1996	Electronic Equipment Testing False Claims Act Violations	$4,050,000
6/26/2008	TCE Contamination at Kansas Airport	$3,195,633
4/9/1996	Improper Classification of Costs	$2,700,000
3/1/2000	F-14 and F-15 Aircraft Contract False Claims Act Violations	$2,113,000
11/30/1997	Defective Pricing	$2,099,042
3/6/2009	Miller v. Raytheon (Age Discrimination)	$1,492,795

25

POGO — PROJECT ON GOVERNMENT OVERSIGHT — ABOUT POGO — OUR WORK — TAKE ACTION

Date	Instance	Penalty
11/21/2019	Casias v. Raytheon (Whistleblower Retaliation)	$1,043,000
7/2/2015	Al-habash v. Raytheon (Discrimination)	$821,525
10/28/1999	Improper Export of Defense Articles and Technical Data	$550,000
5/14/1997	United States v. Hughes Aircraft (Department of Defense Contract False Claims Act Violations)	$500,000
1/8/1999	Aircraft Maintenance Overcharge	$400,000
8/13/2014	Ineligible Meal Expenses	$360,000
8/25/2009	Missile Component Testing Dispute	$212,915
9/29/2008	High Resolution Optics Patent Infringement	$191,125
11/5/2004	EEOC v. Raytheon Technical Services (Racial Discrimination)	$165,000
6/30/1996	Contractor Kickbacks	$115,310
8/31/1995	Substitution/Nonconforming Product (1995)	$95,000
2/13/1996	Substitution/Nonconforming Product (1996)	$82,000
1/7/2019	Wetlands Violations in Andover, MA	$45,750

| UT Ethics In Practice

POGO — PROJECT ON GOVERNMENT OVERSIGHT — ABOUT POGO — OUR WORK — TAKE ACTION

25 Instances of Misconduct since 1995

4 additional instances of misconduct pending resolution

Date	Instance	Penalty
2/21/2007	Price Fixing	$295,000,000
6/5/2006	Noncompliance With Cost Accounting Standards	$283,000,000
6/26/2012	Illegal Export of Military Software to China	$75,700,000
8/1/2008	Defective F-15 and F-16 Engine Turbine Blade Replacements	$50,326,000
5/20/1997	United States v. United Technologies (Preparing False Purchase Orders and Submitting False Invoices)	$14,800,000
9/12/2018	Illicit Payments in Asia	$13,986,534
2/6/2007	Clean Water Act Violations (2007)	$12,000,000
6/22/2016	Submitting False Invoices on Jet Engine Contract	$11,050,790
3/31/2014	Charging Inflated Prices for Blackhawk Spare Parts	$3,500,000
12/11/2009	CERCLA Cleanup of Memphis Site	$3,207,936
6/10/2010	NASA Contract False Claims	$2,988,819
3/25/2009	Black Hawk False Claims Settlement	$2,941,000

26

POGO — PROJECT ON GOVERNMENT OVERSIGHT — ABOUT POGO — OUR WORK — TAKE ACTION

Date	Instance	Penalty
12/19/2017	Counterfeit Helicopter Engine Microprocessors	$1,060,000
9/9/2011	Blackhawk Spare Parts Overcharging	$1,000,000
6/7/1999	Navy SH-3 Sea King Helicopter Defective Pricing	$304,729
6/27/2006	Federal Air Pollution Standards Violations	$176,000
10/27/1999	Violations of Workplace Injury & Illness Recordkeeping Requirements	$155,000
11/18/1997	Cost and Labor Mischarge	$150,000
6/1/2015	Spokane Air Emission Release	$75,878
1/21/2014	U.S. v. Khazaee (Exporting F-35 Documents to Iran)	$60,000
12/2/2002	Air Emissions Violations	$17,700
9/7/2004	Violations of Underground Tank Systems Standards	$10,000
7/7/2005	Brainard v. Pratt & Whitney (Uniformed Services Employment and Reemployment Rights Act Violation)	$0
3/12/2012	Haney v. Boeing, et al. (Wrongful Death)	$0
11/7/2014	U.S. v. Long (Attempting to Transport Sensitive Documents to China)	$0

| Industry Ethics Survey

- RTX – 58 Violations (410M)
- NG – 50 violations (325M)
- L3 Harris – 26 Violations (140M)
- Thales - ?
- LMCO – 91 Violations (300M)

27

| Innovation

"Combining complementary portfolios with advanced technology and R&D platforms, we are delivering transformative solutions to usher in the future of aerospace and defense."

- Gregory J. Hayes, CEO, Raytheon Technologies, 2020

- Innovation and Development
  - **"Innovative Solutions"**
  - **"Innovation Incubator"**
  - **"Innovative Features" that differentiate themselves from competitors**
- Innovation Areas:
  - Artificial Intelligence
  - Advanced Propulsion
  - Cybersecurity
  - Advanced materials & manufacturing
  - Power & thermal management
- Radars and C2 Software
  - Lower Tier Air and Missile Defense Sensor (LTAMDS) Radar designed to detect hypersonic threats
  - Advanced Battle Management System (ABMS) is the Air Force's technology approach for Joint All-Domain Command and Control

28

| Approach to Industry Change

"There was no playbook on how to deal with COVID-19. There was no playbook for the majority of a workforce unable to work in an office environment. There was no playbook on how to deal with a 90% decline in air traffic. And there was no playbook for forging the culture of a new company remotely amid a global shutdown. As we did in both companies for decades, we relied on the experience and pioneering spirit of our team."

- Gregory J. Hayes, CEO, Raytheon Technologies

2020 Letter to Shareholders, "A New Playbook"

- **Diversity**
  - Land, Sea, Air, Space, and Cyberspace
  - Focus on demand markets.
- **Adaption**
  - Assess how the geopolitical climate and technological environments are affecting industry and create solutions.
  - Rapidly evolve to the needs of customers globally.
- **Interconnectivity**
  - Radar and C2 software

29

| Supply Chain Vulnerabilities

"We are dependent upon the availability of materials and major components and the performance of our suppliers and subcontractors. Some products require relatively scarce raw materials and parts."

- Raytheon Technologies SEC Form 10K

- Raytheon has not experienced significant difficulties in procuring the necessary raw materials, components and other suppliers for production
- **Consolidations and business closures among suppliers may affect supply chains**
- **Monitor geopolitical and international trade developments for material or parts shortages**
- **Scarce raw material required for some products are controlled by a single country**, sourcing those materials is dependent on U.S. relations with that country
- **Must comply with specific procurement requirements** which limit the suppliers and subcontractors utilized
  - In some instances, Raytheon depends on sole-source suppliers
- Dependent on genuine original manufacturer equipment and parts
  - Robust standard of policies to detect counterfeit material, especially electronic components
- **Mitigation strategy is to enter long-term or volume purchases agreements to ensure availability.**
- **Strategic Sourcing**

30

| Human Capital Challenges

"We depend on the recruitment and retention of qualified personnel, and our failure to attract, train and retain such personnel to maintain our corporate culture and high ethical standards could seriously harm our business."

- Raytheon Technologies SEC Form 10K

- Requires key technical personnel and executive officers.
  - Company growth increases the need for qualified personnel.
- Competition for personnel is intense and Raytheon might be unable to attract the necessary qualified personnel
- **A significant percentage of Raytheon's current workforce is nearing or eligible for retirement.**
  - **Possible loss of critical knowledge if not transferred to new employees**
- **"New qualified personnel have different expectations from our current workforce, resulting in difficulties attracting and retaining new employees."**
- **Raytheon believes that a critical component of their ability to successfully attract, train, and retain qualified personnel is their corporate culture**
  - Fostering innovation, collaboration and a focus on execution, and an environment of high ethical standards

31

| Great Power Competition

"Our defense technologies, used for missile warnings, surveillance, air dominance, fighter jet platforms, hypersonics, cyber security, and beyond, are essential for global security."

- Raytheon Technologies SEC Form 10K

- Raytheon is very careful not to mention "Great Power Competition" but their support is evident:
  - Air Dominance
    - Air warfare
  - Integrated Defense
    - Counter-UAS
    - Hypersonics
    - Missile Defense
      - Sensors
      - Interceptors
    - Cybersecurity
    - Naval warfare
    - Land warfare
  - Intelligent Operations
    - Decision superiority
    - Targeting and C2
    - Communications and Navigation
    - Space solutions
  - Mission Support
    - Avionics
    - Displays and Controls
    - NORAD Operations and Sustainment
    - Readiness
  - Simulation and Training
    - Training systems
    - Test and training instrumentation
    - Synthetic Training Environment
    - Persistent Cyber Training Environment

32

| Summary

- Raytheon Technologies well poised to meet Combat Radar needs through investments in engineering expertise and acquisition of specialized electronics companies
- DoD adoption and requirement for open system architectures, modularity, and reuse across platform stovepipes is largest hurdle for improving delivery outcomes
- Raytheon Technologies building expertise in modern Command and Control software through government development contracts, struggling to compete for high end talent with commercial tech firms
- Poor definition of JADC2 policy and implications for system design and acquisition strategy/data rights is both an impediment to meet demand, and an opportunity to shape the market favorably

33

L3Harris Firm Brief

FIRM PROFILE

- 2019 "Merger of Equals"- L3 Technologies & Harris Corporation
- Headquarters – Melbourne, FL
  - 340 Locations in U.S., Europe, Canada, Australia, Asia, Middle East and South America
- 48,000 Employees
  - including approx. 19,000 engineers and scientists

3

BUSINESS SEGMENTS

- All segments relevant to C4ISR
- Equal distribution of revenue
- Streamlining through divestitures
- Market Characteristics
  - Limited universe of sellers/buyers
  - DoD acquisition rules (ITAR)
  - Primarily defense
  - Multiple categories of goods
- Oligopolistic Competition
  - Few firms
  - Differentiated products
  - Low ease of entry

AVIATION SYSTEMS

$3.4B

Commercial and military aviation solutions, systems, networks and pilot training

Defense Aviation | Commercial Aviation | Commercial & Military Training | Mission Networks

SPACE AND AIRBORNE SYSTEMS

$4.9B

Mission solutions for space and airborne domains with defense, intelligence and commercial applications

Space | Intel and Cyber | Avionics | Electronic Warfare

INTEGRATED MISSION SYSTEMS

$5.5B

Leading technology integrator to U.S. and international militaries for complex ISR, airborne, maritime and space platforms

ISR | Maritime | Electro-Optical

COMMUNICATION SYSTEMS

$4.4B

Secure ground and airborne communications and network systems for U.S. military, international forces and commercial customers

Tactical Communications | Broadband Communications | Integrated Vision Solutions | Public Safety

4


OVERALL FIRM STRATEGY
• "Building a technology-focused operating company and becoming a full end-to-end mission solutions prime contractor to drive shareholder value"
• Innovation focus: realigned R&D towards open architecture & multi-function software-defined technologies across C4ISR portfolio
• Long-term value creation by exiting non-core businesses
• Align portfolio with national security priorities identified in NDS
• Strategic Priorities
• Grow the Top-Line
• Complete the integration
• Expand margins
• Maximize cashflow to support capital returns
William M. Brown, Chair & CEO
5


2020 FINANCIAL PERFORMANCE
• ROIC: 3.15%
• WACC: 7.20%
• Current Ratio (liquidity): 1.57
• Long-Term Debt-to-Equity (solvency): 0.33
• Debt-to-Equity: 0.77
LHX
Source: Bloomberg, L3Harris 2020 Annual Report

- L3Harris is shedding value and trending down
- Continuing operations income down 31% from 2019
  - Impairment of goodwill (-$748M) from COVID downturn in commercial aviation market
  - Divestments lowered revenues
- Recovery plan:
  - Grow revenue through R&D investments in high-growth, high margin areas where tech is a key differentiator
  - $350M in cost synergies from the merger by end of 2021
  - Maintain portfolio alignment with defense priorities
- Low levels of liquidity and solvency risk provide strategic freedom of maneuver

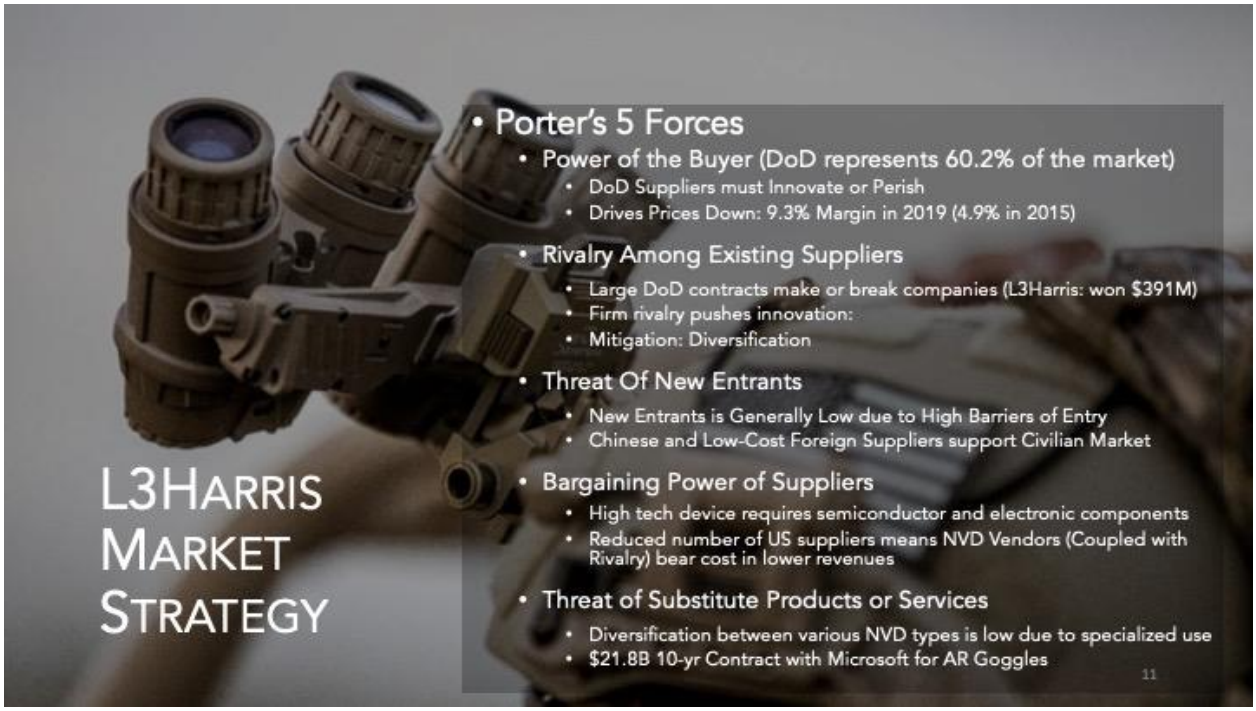
LHX

Source: Bloomberg, L3Harris 2020 Annual Report

MARKET ANALYSIS

- Total Industry Revenue for NVDs in the United States: $2.7B
  - 44.4% Thermal Systems, 37% Light Amplification/Optics
- Growing Market: Expected Growth of 2.7%/yr until 2024 ($3.1B)
- Market Share (Medium Concentration):
  - FLIR (14.1%), Raytheon (11.7%), L3Harris (3.7%), and Leonardo DRS (3.5%)
- Domestic Market:
  - Exports: 14.2% of Revenue, Imports: 13.5% of Domestic demand

10

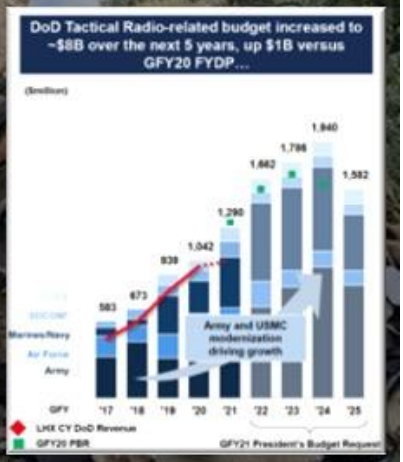

L3HARRIS MARKET STRATEGY
• Porter's 5 Forces
• Power of the Buyer (DoD represents 60.2% of the market)
• DoD Suppliers must Innovate or Perish
• Drives Prices Down: 9.3% Margin in 2019 (4.9% in 2015)
• Rivalry Among Existing Suppliers
• Large DoD contracts make or break companies (L3Harris: won $391M)
• Firm rivalry pushes innovation:
• Mitigation: Diversification
• Threat Of New Entrants
• New Entrants is Generally Low due to High Barriers of Entry
• Chinese and Low-Cost Foreign Suppliers support Civilian Market
• Bargaining Power of Suppliers
• High tech device requires semiconductor and electronic components
• Reduced number of US suppliers means NVD Vendors (Coupled with Rivalry) bear cost in lower revenues
• Threat of Substitute Products or Services
• Diversification between various NVD types is low due to specialized use
• $21.8B 10-yr Contract with Microsoft for AR Goggles
11


L3Harris Strategic Game Board
• Where to Compete:
• Focused on Market's Largest Buyer (Niche)
• How to Compete
• Same Game Vs. New Game
• Attempt to Restructure Company to focus on high end products for DoD customer
• Uses Understanding of Customer to Shape R&D
• Is this Same or New?

MARKET ANALYSIS

Porter's Five Forces

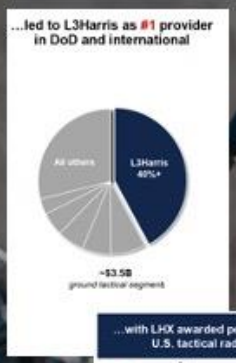
- **Power of customers:**
  - 69 % of sales to U.S. Government customers
  - 65 % derived from contracts where L3Harris was the prime contractor
- **Competition in the industry:**
  - DoD Tactical Radio-related budget increased to ~$8B over next 5 years
  - ~ 15 major suppliers who rely on cutting edge R&D / Innovation
- **Potential of new entrants into the industry:**
  - Threat of new entrants is generally low due to High Barriers of Entry
  - Mergers and acquisitions (M&A)
- **Power of suppliers:**
  - High tech device requires semiconductor and electronic components
  - Reduced US suppliers means industry bears cost in lower revenues
- **Threat of substitute products:**
  - Software defined radios versus traditional hardware defined radios
  - New wave forms: DARPA Wideband Secure and Protected Emitter and Receiver (WiSPER) project



14

L3HARRIS MARKET STRATEGY

- **Drivers supporting medium-term growth**
  - Increased focus on warfighter effectiveness and resilient comms
  - Ramping multi-billion-dollar U.S. DoD / Int'l radio and night vision modernization
  - Demand for connected air and ground information networks… leverage incumbent position to drive spectrum superiority
  - Managing budget / operational constraints in Public Safety caused by COVID-19…right sized cost for eventual recovery
- **Global leadership; driven by commercial model**
  - LHX awarded positions on all major U.S. tactical radio contracts
- **Executing on well-funded DoD modernization priority**



15

L3HARRIS MARKET STRATEGY

- **Maintaining international leadership**
  - Drive global refresh & modernization leveraging incumbency and local partnerships
  - Capture Allies / NATO modernization programs with Falcon IV next gen products
  - Penetrate new geographies and customers with unique needs to address evolving regional threats
- **Expand into near adjacencies…tactical radio segments**
  - Tactical ISR
  - Airborne
  - Network Systems

…supporting global modernization with integrated solutions in 10 focus countries

16

National Security Assessment

- Spending 4% on Research and Development
- Ability to service partners and Allies not limited by ITAR restrictions
- Shedding nonproductive defense segments to better meet GPC needs
- Looking for expansion opportunities
- Investing in next generation capabilities

- "high-margin, high-growth, technology-differentiated businesses where we can win and generate attractive returns"

Human Captial / Ethics

- 3,000 new employees
- Robust internships
- University Partnerships
- STEM investments
- Benefits
- Diversity

1	2	3	4
Be accountable for our own conduct	Comply with the policies, laws, and regulations that apply to our jobs	Seek guidance, raise concerns, and report any observed or suspected misconduct • Cooperate with investigations	Complete all required training on-time, including certification to our Code to add text

18

Firm Policy Recommendations

- Continue to build relationships with Higher Education Organizations
- Prevent IRAD investment from falling below 4%
- Look for opportunities to increase Integrated Mission Systems portfolio through acquisition
- Anticipate customer requirements
- Better integrate business segments to foster total innovation
- Grow international partnerships
- Leverage international footprint to shore up Supply Chain access and sustainability

19

National Policy Recommendations

- Reward companies who maintain higher levels of IRAD funding
- Encourage companies to expand international footprint to Include additional partner nations
- Increase SCO/DARPA/National Lab funding and tightly couple IRAD and National R&D efforts
- Conduct a War Game focused on ability for Defense Contractors to meet mobilizations demands during a Great Power Conflict


QUESTIONS
21

Thales Firm Brief

Outline

THALES

Trent (About Thales)
- Overview
- Business Segments: Aerospace, Space, Transport, Defense, Digital ID
- Mergers and Acquisitions
- Corporate Strategy
- Future Strategy

Julie (Cloud Product Market)
- Overview
- Cloud Market Analysis
- PaaS and Porter's Five Forces
- Thales' Cloud Strategy
- Cloud Market Opportunities

Dan (Tactical Radio Product Market)
- Overview
- Competition
- Strategy
- Where to Compete
- How to Compete
- Strategic Competition
- Future Opportunities

Grim (Financials and National Security Implications)
- Financial overview
- COVID Impact
- Financial Risk
- Thales R&D and Competitors
- National Security Implications
- Thales and Great Power Competition
- Policy Recommendations

2

Overview

THALES

Publicly owned company based in France

- 26% owned by France
- 25% owned by Dassault Aviation

80k+ employees operating in 68 countries

More than half of overall revenue from EU

- 53% of revenue from EU
- 14% Asia
- 11% North America
- Balanced approach (civil and military)

Business Segments

THALES

THALES

Aerospace

THALES

- Onboard connectivity and in-flight entertainment systems
- Civil and military aircraft simulators
- Onboard electronic equipment for aircraft to armed forces, airlines and aircraft manufacturers
- Satellites, systems, payloads, equipment and services
- Major customers include telecommunications operators, space agencies, armed forces, satellite operators and scientific institutions

Space

THALES

- Joint Venture between Thales (67%) and Leonardo (33%)
- Teams up with Telespazio to form the parent companies' "Space Alliance"
- Telecommunications, navigation, Earth observation, environmental management, exploration, science and orbital infrastructures
- Major customers include civil and military space organizations

Transport

THALES

- Urban transport networks (metros and trams)
- Mainline networks (conventional, high-speed and freight)
- Ticketing solutions
- Major customers include rail transport operators

Defense and Security

THALES

- Communications
- Command and control systems
- Sensors and mission systems
- Security
- Cybersecurity solutions
- Networks and infrastructure systems
- Major customers include security forces, armed forces and major corporations

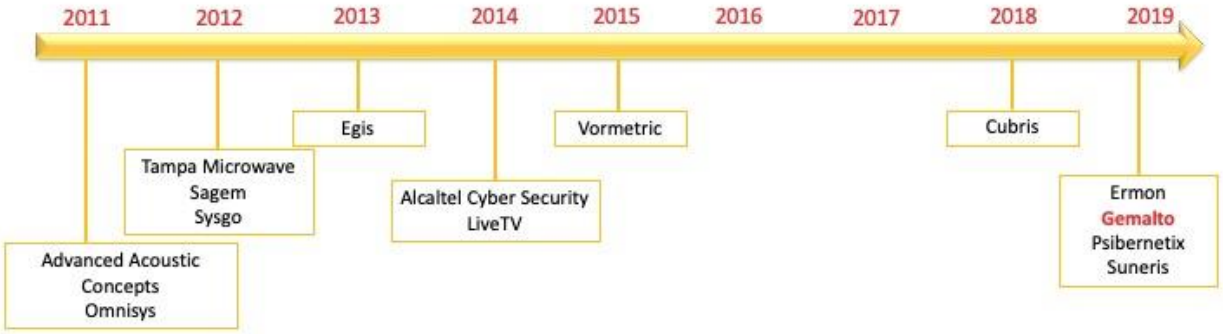
Digital ID and Security

THALES

- Digital identity and security solutions for identification of persons and things
- Analyzes data
- Encryption and authorize access to digital services
- Its major customers include private and government organizations

Mergers & Acquisitions

THALES



- Mergers and Acquisitions are an important part of Thales' business model
- Thales SA has acquired 15 companies in the last 10 years, including 5 in the last 5 years
- Thales SA has acquired in 4 different U.S. States, and 5 Countries
- The Company's most targeted sectors include Aerospace and Defense and Security

gemalto

Corporate Strategy

THALES

Thales's strategy primarily focuses on areas of growth, efficiency and portfolio. The company plans to strengthen its relationship with its customers across the world and expand its business in the emerging markets. It plans to work constantly to improve its processes and focus on developing new products to create value. It plans to ensure consistent and high-quality supply of the materials in sufficient quantities through backward integration for major raw materials.

11

Future Strategy

THALES

Thales Ambition 10 Plan

- Invest to sustain Long-Term Growth
  - *Research and Development* (R&D) is core activity in Thales
    - 2019 – 6% of revenue (€1.1 B) in self-funded R&D – increase 25% by 2023
    - 40% of workforce (30,000 people) involved
    - R&D Targeted at technologies that span across their business segments.
  - *Targeted acquisition* to consolidate technology portfolio and increase growth
  - Continuous *connection* with start-ups (1000+) and academia (supports 200+ PHD students)
- Optimizing *operational performance*
  - Since 2015, continuous decrease in administrative costs as a percentage of sales.

12

Cloud Market Overview

THALES

Exceptional R&D at the heart of a global innovation ecosystem → A unique portfolio of digital competencies → An in-depth knowledge of its markets → A global footprint

- Cloud, C4ISR and JADC2
- Diversification and Digitization
- R&D through Acquisition
- Global footprint
- 2020: Global Cloud Tipping Point, 50%+
- Increased security concerns
- Space for Thales' expansion
- Nexium Defence Cloud

NATO Selects Thales to Supply Its First Defence Cloud for the Armed Forces | Business Wire

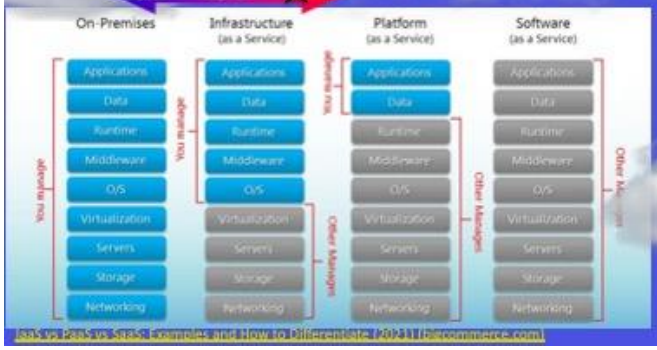
13

Cloud Market Overview

THALES

IaaS
Infrastructure as a Service
(Amazon Web Services)
Amazon (47.8%) Microsoft (15.5%)
Alibaba (7.7%)
Google (4.0%) IBM (1.8%)

SaaS
Software as a Service
(MS O365, Blackboard)
Microsoft (17%)
Salesforce (12%) Adobe (10%)
SAP (6%) Oracle (6%)



PaaS
Platform as a Service
(AWS Electric Beanstalk)
360+ vendors
90% operate within one segment
21 Market segments

14

PaaS and Porter's Five Forces

THALES

Buyer Power – Moderate
- Everyone is a buyer
- Some more equal than others
- JEDI
- Cloud – indispensable?

Rivalry – High
- 360+ vendors
- Exponential growth
- Potential consolidation and acquisition

Supplier Power – High
- Demand for highly skilled workers
- Demand for microchips and other key technology (silicon wafers, oligopoly)
- Few substitutes

New Entrants - Moderate
- Exponential growth
- Variety of products
- Brand preference
- National brand preference

Substitutes – Low
- On premise storage/computing
- Security and privacy

15

Thales Cloud Strategy

THALES

Diagnosis
- Opportunity for growth in PaaS
- Concerns about security
- Protectionism and national preference
- Digitization of defense market

Guiding Strategy
- Improve data protection capability
- Increase security offerings
- Leverage national preference
- Focus on R&D

Coherent Actions
- Acquired Gemalto
- Created Digital Identity and Security business unit
- "Complete solutions to secure entire decision-making chain"
- Nexium Defense Cloud

Securing data in the indispensable and increasingly vulnerable cloud environment through a PaaS solution

16

Cloud and Market Opportunities

THALES

- American vs. Chinese vs. European clouds
- Collaboration with Google on data security in hybrid cloud solutions
- Alibaba: China-focused vendor, great potential for growth in Chinese market
- Thales inroads into China:
  - Beijing R&D center includes cloud security (Gemalto)
  - Providing security for YunOS, Alibaba cloud/IoT Linux-based operating system

Tactical Handheld Radio (THR) Overview

THALES

4 strategic assets

- **Exceptional R&D at the heart of a global innovation ecosystem**
- **A unique portfolio of digital competencies**
- **An in-depth knowledge of its markets**
- **A global footprint**

- Market segmented by radio capability options:
  - Size, weight, power
  - Waveforms (Software Defined, Proprietary)
  - Security
  - Voice only vs. Voice/Data/Video
  - Networking
- Market segmented geographically
  - Governments can protect or open market
  - Regulations for Spectrum, Power, Security
- Nine "global" competitors

Thales has fielded more than 800,000 radios in over 50 countries

THR Market Competition

THALES

Rivalry Among Competitors: High
- Several well-established companies
- Significant R&D with patent protection
- Product differentiation
- Constant innovation pressure
- High competition without profit erosion

Threat of New Entrants: Low
- Extensive R&D & other investments
- High technical knowledge
- High on-ramp for production knowledge
- Well-known global companies
- National Champion could enter

Supplier's Bargaining Power: Medium
- Supply chain risks from China
  - Semiconductors
  - Rare Earths

Rivalry Among Existing Competitors

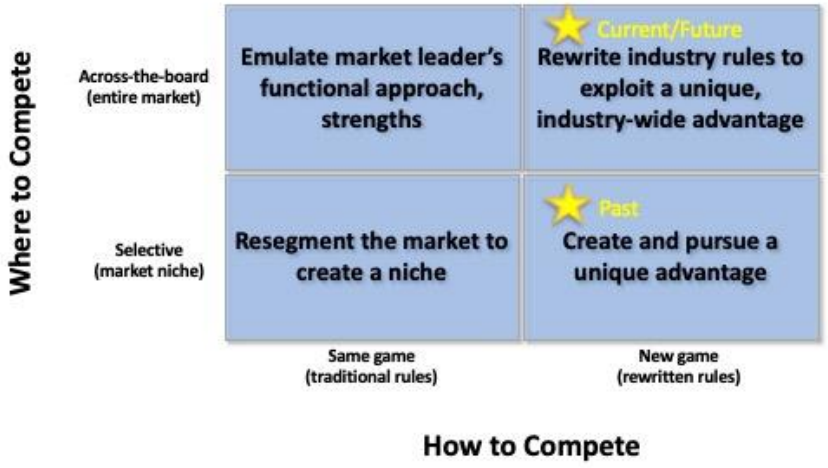
Buyer's Bargaining Power: Low-Medium
- How many producers are available?
  - Product differentiation
    - Thales selling top radio or lesser capable
  - Geographical segment
    - Thales selling in France, EU, or US

Threat of Substitutes: Medium
- High Buyer cost to switch
- Continuous innovation will eventually create substitute and new market segment (ex. wearables)

19

Thales THR Market Strategy

THALES



20

Where to Compete – THR Market Segments

THALES

Market Segment	Tactical Radio Competitors	Market Structure	Competitive Spectrum
	THALES	Monopsony / Monopoly	
	THALES, L3HARRIS, Collins Aerospace, General Dynamics, Raytheon	Oligopoly	
	THALES, LEONARDO, Rohde&Schwarz, Bittium	Oligopoly	
	THALES, LEONARDO, Bittium, Rohde&Schwarz, aselsan, Collins Aerospace, Raytheon, L3HARRIS, General Dynamics	Monopolistic Competition	

21

How to Compete - Competitive Advantage

THALES

Thales was the first company to provide a 2-channel Software Defined Radio

THR Differentiation through Corporate R&D strategy

- *Best in Data security* – (Digital Identity & Security)
- *Software Defined Waveforms* for interoperability (Aerospace / Transport)
- *Radio Spectrum Knowledge* (Aerospace / Transport / Space)
- *Extended Range* (Aerospace / Transport / Space)
- *Beyond-Line-of-Sight SATCOM Integrated Waveform* (Space / Aerospace)
- *Enhanced frequency hopping* (Digital Identity & Security / Aerospace)

22

Strategic Competition – U.S. Example

THALES

2012 → Current

SOCOM Contract
THALES
L3HARRIS

Army JTRS R/R Contract
THALES
GENERAL DYNAMICS

Thales leverages U.S. Sales in Int'l Mkt

Thales Launches Tactical Radio To Quicken Response Time in Combat
By: Pierre Tran

U.S. Soldiers Rely on Thales for Tactical Command and Control Communications

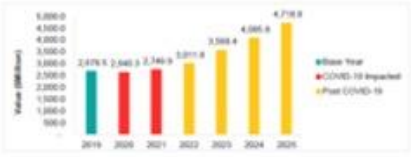
Thales Gains Back Market Share with New Radio Contract

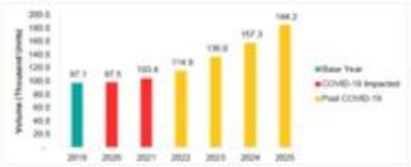
23

Future Opportunities

THALES

Global Growth Projections





Powered by Soldier Modernization

- "North America to account for the largest market for soldier modernization"
- "Asia Pacific region to be the one of the most attractive markets for soldier modernization"
- "Europe is poised to maintain a steady growth"
- "Saudi Arabia and Israel to drive investments in the Middle Eastern market"

Directed by Future Requirements

- Decrease Size, Weight
- Increase Power
- Increase interoperability / flexibility
- Increase security
- … for faster decision making

24

Financials – Overview

THALES

Is Thales creating value at an acceptable level of risk?

2019 vs. 2018 Performance:

- ROIC (11) consistently > WACC (5.75) - creating value
- Gemalto acquisition finalized in October of 2019:
  - Operating Profit: down by 9% - restructuring costs + increased R&D strategy
  - Human Capital: headcount up 20%; increased pension bill
  - Sales: increased by 16%
  - Net Profit: up 9%
  - Cash flow from Operations: up 40%

Thales' acquisition strategy: short-term pain for long-term gain

25

Financial Risks

THALES

Liquidity

- Current Ratio: changed from 1.16 in 2018 to .907 in 2019

Solvency

- Long-Term Debt to Equity Ratio: increased from 0.87 in 2018 to 1.48 in 2019
- Across Industry:
  - Raytheon: - 2018 = 1.01 - 2019 = 0.901
  - Northrup: - 2018 = 1.695 - 2019 = 1.448
  - L3/Harris: - 2018 = 1.04 - 2019 = 0.901

Thales anticipates 3 years before merger shows the impact of created value

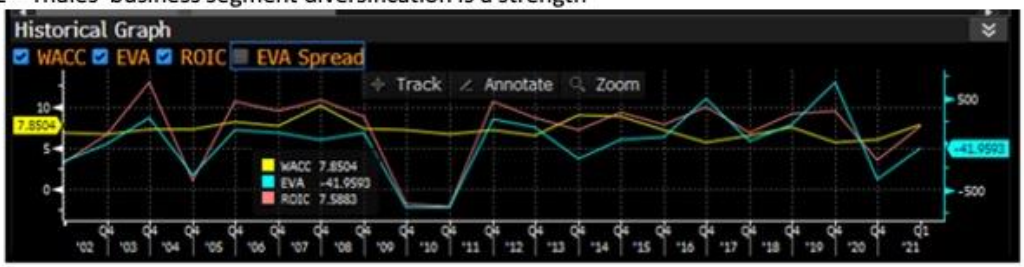
26

COVID Impact

THALES

COVID issues in 2020:

- Reduced 2020 dividend from €2.05 to €0.60 – Avoids outbound cashflow of ~ € 430M
- Biggest loser, aerospace segment followed by transportation
- Defense sector largely stagnant
- But, brilliant hedge into the digital segment (increased revenue in 2020)
- BL – Thales' business segment diversification is a strength



27

Thales' R&D vs. The Competitors

THALES

R&D Expenditures as a percent of sales (2019)

- Thales: 5.9%
- Raytheon: 2.5%
- L3Harris: 4.8%
- Northrup: 2.8%

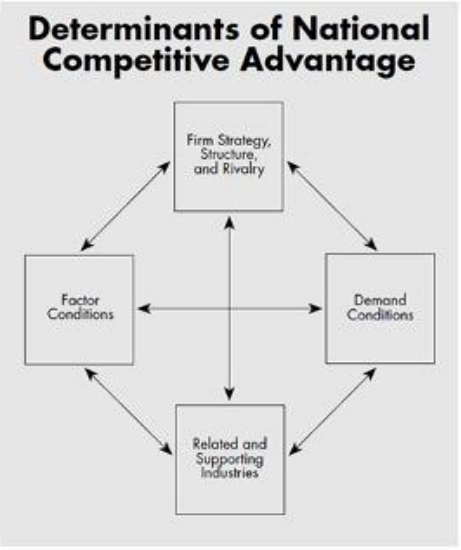
So, is Thales creating value at an acceptable level of risk for themselves? For US National Security?

28

National Security Implications

THALES

- **Storyline Themes:**
- R&D is a strength
- Geographic diversification is a strength
- Business segment diversification is a strength
- Thales as a French national champion offers both solutions and conundrums...



29

Thales and Great Power Competition

THALES

- China
  - Present in China for more than 30 years
  - Trusted partner for Chinese aviation and urban rail transportation industries
  - Selected Thales metro signaling system
  - Collaboration with Alibaba on securing cloud operating system
  - Two Chinese R&D centers: Beijing and Dalian
- Russia
  - Provides full avionics suite for Sukhoi SuperJet 100, MI38 multipurpose helicopter and VRT500 helicopter
  - Joint production of spacecraft with Gazprom Space Systems
  - Ruselectronics Holding providing switches for Thales' spacecraft
  - Did not wait for Russian waiver for Gemalto merger
- Other Markets
  - Collaborating with Turkish industry: 3D Radar Modernization, Helmet Mounted Sight Display with Aselsan, Genesis with Havelsan and Göktürk with TAI
  - Main supplier to Turkish Navy, including radars, radios and SATCOM
  - Provides Kazakh Air Force long-range air defense radar
  - South Korea and Turkey selected Thales' metro signaling system

Opportunities for growth into markets less friendly to American companies

30

Policy Recommendations

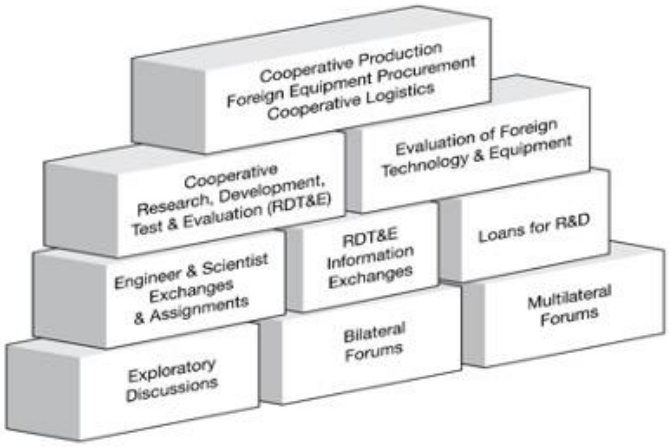
THALES

Thales Policy

1. Security/Ethics - Firewall Chinese digital venture from the rest, or reconsider
2. Supply Chain Vulnerabilities – Diversify; ID bottlenecks (I.e., semiconductors)

US Policy

1. Security/Proliferation - Strategic dialogue with French government over GPC concerns
2. Coalition Building - Seek opportunities for International Armament Cooperation (IAC) Programs
3. US Readiness/Mobilization Needs - Promote incentives to grow Thales' US based subsidiary



Defense Institute for Security Cooperation Studies, "Greenbook," 40.0, May 2020, Chapter 13, "Systems Acquisition and International Armaments Cooperation"

31

Resources (1 of 2)

THALES

- *Global Super Soldier Wearable Technology Market*, (California: BIS Research Inc., September 2020), 146, https://nduezproxy.idm.oclc.org/login?url=https://www.emis.com/php/search/docpdf?pc=YY&doc_id=693998560
- Federal Communications Commission (FCC), *Personal Radio Services*, Accessed: January 23, 2020, https://www.fcc.gov/consumers/guides/personal-radio-services-prs-keeping-touch
- Federal Communications Commission (FCC), *Radio Spectrum Allocation*, Accessed: January 23, 2020, https://w ww.fcc.gov/engineering-technology/policy-and-rules-division/general/radio-spectrum-allocation
- "Multiband Iner/Intra Team Radios," *Thales Group*, Accessed: January 22, https://www.thalesgroup.com/en/mark ets/defence-and-security/radio-communications/land-communications/tactical-radios/anprc-148-0
- "Universal Registration Document: Including the Annual Financial Report," *Thales Group*, 2019, 49, https://thale sgroup.com
- MarketLine, *"Soldier Modernization: Renewed emphasis on the infantry battalion is improving growth"*, May 2017, 2, https://advantage-marketline-com.nduezproxy.idm.oclc.org/Analysis/ViewasPDF/soldier-modernization-renewed-emphasis-on-the-infantry-battalion-is-improving-growth-48832
- Michael E. Porter, "The Five Forces that Shape Strategy," *Harvard Business Review*; Jan 2008, Vol. 86 Issue 1, p. 78-93
- Thales, "Thales Awarded $37M U.S. Army Contract for New Security Force Assistance Brigades," December 12, 2017, https://www.thalesgroup.com/en/worldwide-defence/radio-communications/news/thales-awarded-37m-us-army-contract-new-security-force
- Thales, "Thales Receives Continued Orders for the U.S. Army's Leader Radio Program," January 27, 2021, https://www.thalesgroup.com/en/group/journalist/press-release/thales-receives-continued-orders-us-armys-leader-radio-program
- Bob Brewin, "Pentagon Shutters Joint Tactical Radio System Program Office," *Nextgov*, August 1, 2012, https://www.nextgov.com/it-modernization/2012/08/pentagon-shutters-joint-tactical-radio-system-program-office/57173/
- Pierre Tran, "Thales Launches Tactical Radio to Quicken Response Time in Combat," *Defense News*, June 12, 2016, https://www.defensenews.com/digital-show-dailies/eurosatory/2016/06/12/thales-launches-tactical-radio-to-quicken-response-time-in-combat/
- Greg Giaquinto, "Thales Gains Back Market Share with New Radio Contract," *Defense & Security Monitor: Forecast International*, August 9, 2018, https://dsm.forecastinternational.com/wordpress/2018/08/09/thales-gains-back-market-share-with-new-radio-contract/
- Robert Buaron, "New-game Strategies," *McKinsey Quarterly*, June 2000
- Michael E. Porter, "The Competitive Advantage of Nations," *Harvard Business Review;* Mar/Apr 1990, Vol. 68 Issue 2
- Defense Institute for Security Cooperation Studies, "Greenbook," 40.0, May 2020, Chapter 13, "Systems Acquisition and International Armaments Cooperation"

33

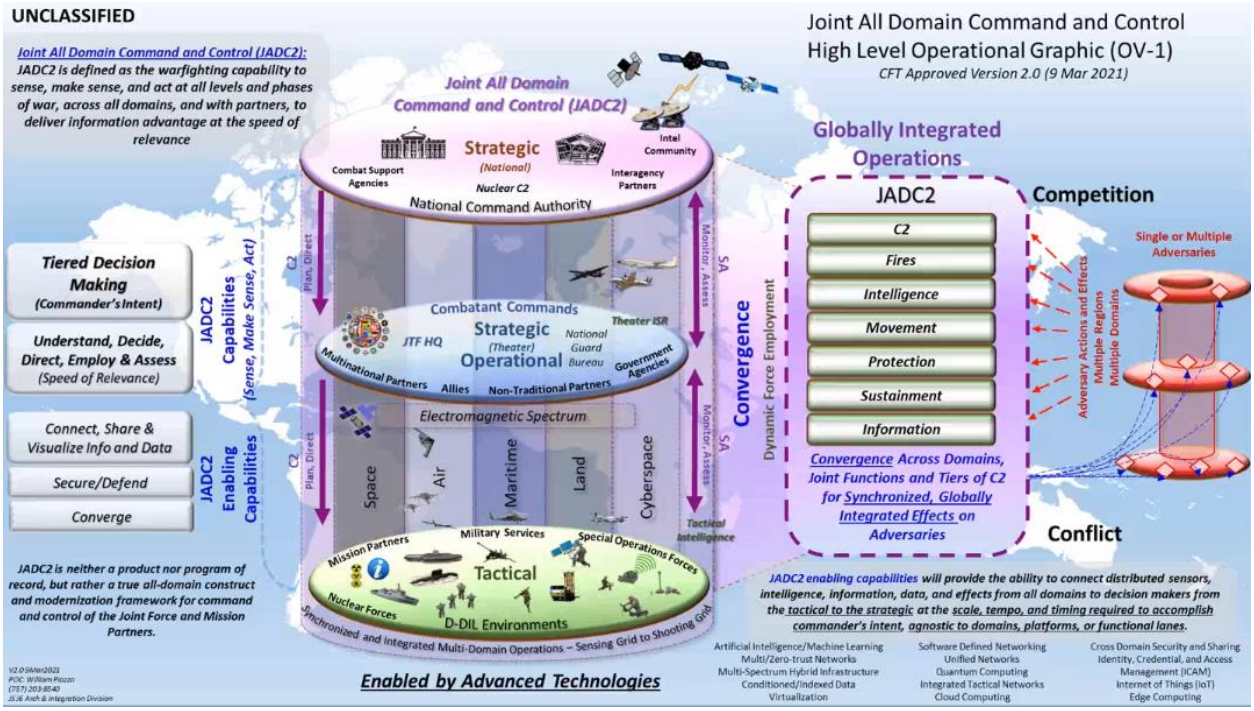
Resources (2 of 2)

THALES

- Kinsta. "Cloud Market Share – a Look at the Cloud Ecosystem in 2021," November 11, 2019. https://kinsta.com/blog/cloud-market-share/.
- Dignan, Larry. "Alibaba Cloud Nears Profitability as Customers Move from IaaS into AI, Data Analytics Workloads." ZDNet. Accessed March 26, 2021. https://www.zdnet.com/article/alibaba-cloud-nears-profitability-as-customers-move-from-iaas-into-ai-data-analytics-workloads/.
- Gartner. "Gartner Says Nearly 50 Percent of PaaS Offerings Are Now Cloud-Only." Accessed March 26, 2021. https://www.gartner.com/en/newsroom/press-releases/2019-02-27-gartner-says-nearly-50-percent-of-paas-offerings-are-.
- "Global Cloud Tipping Point: The 2020 Thales Data Threat Report-Global Edition Shows Organizations Struggle with Security Post Digital Transformation | Thales Group." Accessed March 26, 2021. https://www.thalesgroup.com/en/group/journalist/press-release/global-cloud-tipping-point-2020-thales-data-threat-report-global.
- The BigCommerce Blog. "IaaS vs PaaS vs SaaS: What You Need to Know + Examples (2018)," October 18, 2018. https://www.bigcommerce.com/blog/saas-vs-paas-vs-iaas/.
- one, d'wise. "Meet YunOS — Alibaba's OS For All Purposes." Medium, March 18, 2017. https://medium.com/chip-monks/meet-yunos-alibabas-os-for-all-purposes-146d50ca1bfe.
- "NATO Selects Thales to Supply Its First Defence Cloud for the Armed Forces | Thales Group." Accessed January 29, 2021. https://www.thalesgroup.com/en/group/journalist/press-release/nato-selects-thales-supply-its-first-defence-cloud-armed-forces.
- "Thales and Google Cloud Join Forces to Deliver Breakthrough Capability for Enterprises to Control Their Data in the Cloud | Thales Group." Accessed March 26, 2021. https://www.thalesgroup.com/en/group/journalist/press-release/thales-and-google-cloud-join-forces-deliver-breakthrough-capability
- Thales Group Overview. Accessed March 14, 2021. https://www.thalesgroup.com/sites/default/files/database/document/2021-03/Thales_Group_overview_EN-04032021.pdf

34

APPENDIX B: JADC2 Definition



Source: OV-1 distributed by the J6, CFT

Three observations of note:
-First is the CFT's definition of JADC2 in the upper left-hand corner. There is a discrepancy between OV-1 calling JADC2 a capability versus Gen Crall calling it a strategy.[104] The definition covers two JADC2 principles, *data* (information) and *speed*. It could imply *trust* with its references to partners and that activities will work across all domains (i.e., across services). However, its coverage of *C2 philosophy* is weak. It mentions the capability to work at all levels of war but does not imply that it cares about weapons' tasking and release authorities at the appropriate level of war.

-Second, the "JADC2 enabling capabilities" description correlates well to the word descriptors in the Joint Vision 2010 excerpt above.

-Third, you can visually see how complicated JADC2 has become and the number of extra "challenges" that the CFT thinks JADC2 can solve by observing how busy the OV-1 picture is versus the Joint Vision 2010's excerpt, especially under the "Globally Integrated Operations" section. This observation could lead one to conclude that the CFT is trying to solve everything for everyone at once instead of taking an incremental proof-of-concept approach to their detriment.

APPENDIX C: The National Industrial Security Manual (NISPOM)

The National Industrial Security Program Operations Manual

The National Industrial Security Program Operations Manual or NISPOM is the governing document for the National Industrial Security Program (NISP). It exists as the guiding document for how the US government handles and secures its secrets, at nearly all levels and nearly all locations, both in the government and industry. "Established in 1954, the NISPOM is the responsibility of the National Security Council (NSC), and although the SECDEF is the executive agent, he shares responsibilities for its implementation with the Secretary of Energy, Chairman of the Nuclear Regulatory Commission (NRC), and the Director of National Intelligence (DNI). The manual applies to all Executive branch Departments, and Agencies and all cleared contractor facilities within the US."[6] It's extremely rigorous in its methodology and control of classified information.

Security Implications through Porter's Five Forces[7]

The current industrial security posture affects all stakeholders throughout the value chain and has unintended implications across the DIB. While the main benefit is realized by protecting our national secrets, many costs are borne by parties throughout the system. Some are directly affected, such as producers (prime contractors), suppliers (subcontractors), and customers (the US Government). Others are indirectly affected, such as the American people, allied partners, nations, and commercial entities kept out of the marketplace by high barriers to entry.

Overall, the NISP, NISPOM, and the associated industrial security architecture have dramatic effects throughout the value chain and have unintended consequences on competition throughout the industry. It will entice some while discouraging others. It creates "fast tracks" for those with experience and impossible barriers to those without experience. Costs are increased for all parties, and risk models are higher. Any additional or associated requirements present headwinds to new entrants in the marketplace, and security is no different. Excessive security requirements eliminate new entrants. They often have neither the experience nor budget available to compete with existing firms in the DIB effectively.

Unintentionally, the industrial security framework increases the power of existing suppliers. It rewards those who have developed a system of silos and stovepipes where synergies and efficiencies can't be uncovered or exploited. Existing suppliers understand this and are not incentivized to modify the system. Their investment, both financial and operational, in satisfying the more than the intended requirement differentiates them in a field of competitors.

Burdensome industrial security masks itself as providing leverage to the customer. In short, the government can demand extensive requirements on its first-tier suppliers and throughout the supply chain. On the surface, it would appear as a unilateral lever of power to the customer. However, once beyond securing the information, any additional burden on the supplier is ultimately passed back as a higher cost to the customer. In short, the customer overpays for what they get. Moreover, the high barriers to entry unintentionally eliminate challengers, stifles competition, and eliminates valuable cost competition.

Finally, the current system creates almost unachievably high barriers to entry against smaller, potentially more agile, and innovative firms. Startups cannot effectively bear the costs of erecting, managing and maintaining the requirements set forth by the NISPOM. Thus small,

entrepreneurial firms either self-eliminate and choose not to compete, or in the best case, operate for a short period, show value to a prime as a potential acquisition, and ultimately are absorbed into the monolithically giant corporation where they eventually lose the agility that made them valuable in the first place. In summary, an overburdened industrial security apparatus not only retards the pace of existing producers but also stifles the emergence of new, lighter, and more nimble entrants into the marketplace.

APPENDIX D: Acronyms

A2/AD	Anti-Access/Area-Denial
ABMS	Advanced Battle Management System
AECA	Arms Export Control Act
AFLCMC	Air Force Lifecycle Material Command
AI	Artificial Intelligence
AO	Action Officer
AT	Anti-Tamper
BICES	Battlefield Information Collection and Exploitation Systems
BMEWS	Ballistic Missile Early Warning
C2	Command and Control
C4	Command and Control, Communications and Computer
CCBP	Cyber Capability Building Program
CCEB	Combined Communications and Electronics Board
CCMD	Combatant Command
CCP	Chinese Communist Party
CENTCOM	United States Central Command
CENTRIX	Combined Enterprise Regional Information Exchange System
CFT	Cross-Functional Team
CIO	Chief Information Officer
COMSEC	Communications Security
CONOPS	Concept of Operations
CRS	Congressional Research Service
CSIS	Center for Strategic & International Studies
DCS	Direct Commercial Sale
DISA	Defense Information Security Agency
DISN	Defense Information Systems Network
DIU	Defense Innovation Unit
DMO	Distributed Maritime Operations
DNI	Director of National Intelligence
DOD	Department of Defense
DODI	Department of Defense Instruction
DOD IG	Department of Defense Inspector General
DODIN	Department of Defense Information Network
DoS/L	Department of State Legal
DSCA	Defense Security Cooperation Agency
DTSA	Defense Technology Security Agency-led
EADGE-T	Extended Air Defense Ground Environment-Transformation
ES	Eisenhower School
EU	European Union

EUCOM	United States European Command
FFRDC	Federally Funded Research and Development Centers
FMS	Foreign Military Sales
GAO	Government Accountability Office
GDP	Gross Domestic Product
GIG	Global Information Grid
GPC	Great Power Competition
GPS	Global Positioning System
GWOT	Global War on Terrorism
IARPA	Intelligence Advanced Research Projects Agency
IC	Intelligence Community
ISR	Intelligence Surveillance and Reconnaissance
IT	Information Technology
ITAR	International Traffic in Arms Regulations
JALN	Joint Aerial Layer Network
JIE	Joint Information Environment
JRSS	Joint Regional Security Stacks
JSTARS	Joint Surveillance Target Attack and Radar System
MCF	Military Civil Fusion
MDTF	Multi Domain Task Force
MGI	McKinsey Global Institute
ML	Machine Learning
MTCR	Missile Technology Control Regime
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NCW	Network Centric Warfare
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operations Manual
NRC	Nuclear Regulatory Commission
NSC	National Security Council
NWC	National War College
OODA	Observe Orient Decide Act
OUSD A&S IC	Undersecretary of Defense for Acquisitions and Sustainment, International Cooperation
OV-1	Original Vision 1
PARTNERS AND ALLIES	Partners and Allies
PC	Project Convergence
R&D	Research and Development
RMA	Revolution in Military Affairs
SAP	Special Access Program
SBIR	Small Business Innovation Research

SBTR	Small Business Technology Transfer
SECDEF	Secretary of Defense
SIPR	Secret Internet Protocol Router
STEM	Science Technology Engineering Math
UARC	University Affiliation Research Center
UAS	Unmanned Aerial System
US	United States
USA	United States of America
USAF	United States Air Force
USG	United States Government
USSF	United States Space Force
USV	Unmanned Surface Vehicle
UUV	Unmanned Underwater Vehicle

Endnotes

1. “AY21 C4ISR Industry Study Analytic Framework,” Dwight D. Eisenhower School for National Security and Resource Strategy, 1.

2 “AY21 C4ISR Industry Study,” Dwight D. Eisenhower, 1.

3. “Joint All-Domain Command and Control (JADC2),” *Congressional Research Service*, March 18, 2021, https://www.citationmachine.net/chicago/cite-a-website/custom.

4. John R. Hoehn, ““Joint All-Domain Command and Control (JADC2),” *Congressional Research Service*, IF11495, March 18, 2021, https://crsreports.congress.gov.

5. “Assessment of the US DoD C4ISR Market, Forecast to 2025,” Frost & Sullivan, August 2020, 11.

6. “AY21 C4ISR Industry Study Analytic Framework,” Dwight D. Eisenhower School for National Security and Resource Strategy, 1.

7. Berry R. Posen, Command of the Commons: The Military Foundation of U.S. Hegemony, International Security, *MIT Press*, Vol. 28, No. 1, pp 5-46.

8. John R. Hoehn, “Joint All-Domain Command and Control (JADC2),” *Congressional Research Service*, March 18, 2021, https://crsreports.congress.gov.

9. John R. Hoehn, ““Joint All-Domain Command and Control (JADC2),” *Congressional Research Service*, IF11495, March 18, 2021, https://crsreports.congress.gov.

10. “Assessment of the US DoD C4ISR Market, Forecast to 2025,” Frost & Sullivan, August 2020, 11.

11. “Assessment of the US DoD,” Frost & Sullivan, 11.

12. John R. Hoehn, ““Joint All-Domain Command and Control (JADC2),” *Congressional Research Service*, IF11495, March 18, 2021, https://crsreports.congress.gov.

13. John R. Hoehn, ““Joint All-Domain Command and Control (JADC2),” *Congressional Research Service*, IF11495, March 18, 2021, https://crsreports.congress.gov.

14. Robert Atkinson, “Understanding the U.S. National Innovation System, 2020,” *Information Technology & Innovation Foundation*, November 2020, 4.

15. Michael Porter, “The Competitive Advantage of Nations,” *Harvard Business Review*, v.68, no.2, Mar/April 1990, 77, https://hbr.org/1990/03/the-competitive-advantage-of-nations.

16. Porter, “Competitive,” 77.

17. Porter, “Competitive,” 82.

18. “China Plans Huge Investment in Next-Generation Chips: Report.” Accessed May 17, 2021. https://www.aljazeera.com/economy/2020/9/4/china-plans-huge-investment-in-next-generation-chips-report.

19. Michael Dahm, “China’s Desert Storm Education.” Proceedings. March 2021. Vol.147/3/1,417.

20. Jeffrey Witsken, *“Network-Centric Warfare: Implications for Operational Design.”* United States Army Command and General Staff College, 2002.

21. U.S. Library of Congress, Congressional Research Service, *Semiconductors: U.S. Industry, Global Competition, and Federal Policy*, October 26, 2020, R46581, Summery, https://crsreports.congress.gov/product/details?prodcode=R46581.

22. Bonnie Glaser, “Made in China 2025 and the Future of American Industry,” Congressional Testimony, February 27, 2019, 4.

23. NPR.org. “A Cautionary Tale For China’s Ambitious Chipmakers.” Accessed May 17, 2021. https://www.npr.org/2021/03/25/980305760/a-cautionary-tale-for-chinas-ambitious-chipmakers.

24. Andrew Tate, “China now has world’s largest Navy as Beijing advances towards goal of a “world-class military by 2049, says US DoD.” Janes.com, Sep 2, 2020. https://www.janes.com/amp/china-now-has-world’s-largest-navy-as beijing/znlJK3dhvu9mz28xajRJVkc5dVi5VFp1cVMwPQ2.

25. Jamie Smyth, “Industry needs a rare earths supply chain outside China,” *Financial Times*, July 27, 2020, https://www.ft.com/content/fc368da6-1c86-454b-91ed-cb2727507661.

26. HRM Asia. “China Set to Overtake the US in STEM Talent by 2030,” October 3, 2019. https://hrmasia.com/china-will-overtake-the-us-in-stem-talent-by-2030/.

27. “China and the World: Inside the Dynamics of a Changing Relationship,” *McKinsey Global Institute*, July 2019, 58, https://www.mckinsey.com/~/media/mckinsey/featured%20insights/china/china%20and%20the%20world%20inside%20the%20dynamics%20of%20a%20changing%20relationship/mgi-china-and-the-world-full-report-june-2019-vf.ashx.

28. Ellen Nakashima and Gerry Shih, “China builds advanced weapons systems using American chip technology,” *Washington Post*, April 9, 2021, https://www.washingtonpost.com/national-security/china-hypersonic-missiles-american-technology/2021/04/07/37a6b9be-96fd-11eb-b28dbfa7bb5cb2a5_story.html.

29. China Power Team, "How Developed Is China’s Arms Industry," *Center for Strategic & International Studies*, February 18, 2021, Updated February 25, 2021, https://chinapower.csis.org/arms-companies/.

30. John Sargent Jr., "U.S. Research and Development Funding and Performance: Fact Sheet," *Congressional Research Services*, RR44307, January 24, 2020, 1. https://crsreports.congress.gov.

31. Phil Budden and Fiona Murray, *Defense Innovation Report: Applying MIT Innovation Ecosystem & Stakeholder Approach to Innovation in Defense on a Country-by-Country Basis*, May 2019, 75, https://inn ovation.mit.edu/assets/Defense-Innovation-Report.pdf.

32. “Breaking Down China’s 2020 Defense Budget.” Accessed May 17, 2021. https://www.csis.org/analysis/breaking-down-chinas-2020-defense-budget.

33 Budden and Murray, “Defense Innovation Report,” 76.

34. Ibid.

35. Porter, “Competitive,” 77.

36. “China and the World,” *MGI*, 64.

37. Porter, “Competitive,” 82.

38. China and the World,” *MGI*, 17.

39. Dima Adamsky, *The Culture Of Military Innovation* Palo Alto: Stanford Security Studies, 2010.

40. Keith Crane, Olga Oliker, Brian Nichiporuk. “Trends in Russia’s Armed Forces. An Overview of Budgets and Capabilities. The Rand Corporation. 2019. 56.

41. Igor Sheremet, "Cyber Threats To Russia Grow: The Situation In This Sphere Is Changing For The Better, Far More Slowly Than The Development Of The Geopolitical Situation Requires", *Voyenno-Promyshlennyy Kuryer*, 2014.

42. Loren Graham, *Loren Graham (MIT) - Why Does Russian Innovation Fail,* video, 2016, https://www.youtube.com/watch?v=MrWiP23Tlwk.

43. Andrew Radin et al., *"The Future Of The Russian Military,"* Santa Monica: RAND Corporation, 2019, https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3099/RAND_RR3099.pdf.

44. Elizabeth Howell. "Roscosmos: Russia's Space Agency." Space.com Last modified May 2018. https://www.space.com/amp/22724-roscosmos.html.

45. Henry Etzkowitz, *The Triple Helix: University-Industry-Government Innovation in Action*; Routledge: New York, NY, USA, 2008.

46. Henry Etzkowitz, *The Triple Helix: University-Industry-Government Innovation in Action*; Routledge: New York, NY, USA, 2008.

47. A.D. James, "Reevaluating the Role of Military Research in Innovation Systems: Introduction to the Symposium," J. Technol. Transfer. 2009, 34, 449–454.

48. "Assessment of the US DoD C4ISR Market, Forecast to 2025," Frost & Sullivan, August 2020, 11.

49. "Assessment of the US DoD C4ISR Market, Forecast to 2025," Frost & Sullivan, August 2020, 11.

50. Phil Budden and Fiona Murray, *Defense Innovation Report: Applying MIT Innovation Ecosystem & Stakeholder Approach to Innovation in Defense on a Country-by-Country Basis,* May 2019, 75, https://inn ovation.mit.edu/assets/Defense-Innovation-Report.pdf.

51. Gary Jones, Edward White, Erin Rya, and Jonathan Ritschel. "Investigation into the Ratio of Operating and Support Costs to Life-Cycle Cost for DoD Weapon Systems. *Defense Acquisition Research Journal*, January 2014, Vol. 21 No1: 444, https://apps.dtic.mil/dtic/tr/fulltext/u2/a600495.pdf.

52. Amy Thompson, "SpaceX launches 60 Starlink satellites in record 10th liftoff and landing of reused rocket," *Space.com.* Accessed 11 May 2021, Last Modified: 9 May 2021, https://www.space.com/amp/spacex-starlink-27-10th-falcon-9-rocket-launch-landing-success.

53. SBIR. STTR "America's Seed Fund" www.sbir.gov. Accessed May 02, 2021.

54. OODA stands for Observe, Orient, Decide, and Act. Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War,* 1st ed (Boston: Little, Brown, 2002), 328.

55. Coram, 331.

56. James Kitfield, *Prodigal Soldiers*, Brassey's paperback ed, An AUSA Institute of Land Warfare Book (Washington, [DC]: Brassey's, 1997), 153.

57. Andrew F. Krepinevich and Barry D. Watts, *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy*, First edition (New York: Basic Books, 2014), 195-201.

58. Krepinevich and Watts, 222.

59. John M. Shalikashvili, "Joint Vision 2010" (Joint Staff, Pentagon, Washington, D.C. 20318, July 16, 1996), https://www.airforcemag.com/PDF/DocumentFile/Documents/2005/jv_2010_071696.pdf, 17 and 23.

60. Arthur K. Vice Admiral Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future" (Proceedings, January 1998), 4-5.

61. Joint Chiefs of Staff, "Joint Concept for Command and Control of the Joint Aerial Network," March 20, 2015.

62. John R. Hoehn, "Joint All-Domain Command and Control (JADC2)" (Congressional Research Service, n.d.).

63. "Interview with Preston Dunlap, Chief Architect, US Air & Space Force," accessed April 20, 2021, https://youtu.be/PZftxqZeWE0.

64. Theresa Hitchens, "Exclusive: J6 Says JADC2 Is a Strategy; Service Posture Reviews Coming," *Breaking Defense*, accessed April 20, 2021, https://breakingdefense.com/2021/01/exclusive-j6-says-jadc2-is-a-strategy-service-posture-reviews-coming/.

65. Hitchens.

66. Winton, "An Imperfect Jewel," 856.

67. Hitchens, "Exclusive: J6 Says JADC2 Is a Strategy; Service Posture Reviews Coming."

68. Sara Sirota, "Defense spending bill slashes ABMS budget nearly in half," Inside *Defense*, December 21, 2020, https://insidedefense-com.nduezproxy.idm.oclc.org/insider/defense-spending-bill-slashes-abms-budget-nearly-half.

69. Nicholas O'Donoughue, Samantha McBirney, and Brian Persons, "Distributed Kill Chains: Drawing Insights for Mosaic Warfare from the Immune System and from the Navy, (Santa Monica: RAND Inc, 2021), xi, https://www.rand.org/pubs/research_reports/RRA573-1.html.

70. Brian W. Everstine, "The Great Experimenter", *Air Force Magazine*, January 25, 2021, 4, https://www.airforcemag.com/article/the-great-experimenter/.

71. Everstine, "Experimenter", 4.

72. Preston Dunlop, "Multi-Domain Operations, Powered by Digital Advanced Battle Management Systems", *SAF/AQ*, (2019).

73. Everstine, "Experimenter", 8.

74. Army Futures Command, *"Project Convergence Narrative,"* https://armyfuturescommand.com/wp-content/uploads/2021/01/Project-Convergence-Description.pdf, (Accessed April 10, 2021).

75. Mark Schauer, "The Most Important Thing the Army Is Doing": Project Convergence's Impact Will Resonate for Years to Come," *Army.mil*, September 28, 2020, https://www.army.mil/article/239442/the_most_important_thing_the_army_is_doing_project_convergences_impact_will_resonate_for_years_to_come.

76. Congressional Research Service, Updated October 8, 2020, *The Army's Project Convergence,"* https://fas.org/sgp/crs/weapons/IF11654.pdf, (Accessed April 21, 2020).

77. Army Futures Command, *"Army Futures Command 2020 Year in Review,"* https://armyfuturescommand.com/year-in-review/, (Accessed April 21, 2021).

78. Congressional Research Service, Updated April 13, 2021, *"The Army's Multi-Domain Task Force (MDTF),"* https://fas.org/sgp/crs/natsec/IF11797.pdf, (Accessed April 22, 2021).

79. CRS, *"The Army's MDTF."*

80 Joe Lacdan, Army News Service. "Army, Air Force form partnership, lay foundation for CJADC@ interoperability." Oct 1, 2020. www.army.mil.

81. Edward Lundquist, Special Correspondent. “DMO Is Navy's Operational Approach to Winning the High-End Fight at Sea.” *Seapower*, February 2, 2021. https://seapowermagazine.org/dmo-is-navys-operational-approach-to-winning-the-high-end-fight-at-sea/.

82. Department of the Navy, *“Unmanned Campaign Framework,”* March 16, 2021, 6, https://www.navy.mil/Portals/1/Strategic/20210315%20Unmanned%20Campaign_Final_LowRes.pdf.

83. Oriana Pawlyk, “An MQ-9 Drone Is Teaming Up with a Navy Warship to Obliterate Targets at Sea.” *Military.com*, April 22, 2021. https://www.military.com/daily-news/2021/04/22/mq-9-drone-teaming-navy-warship-obliterate-targets-sea.html.

84. David Vergun, “Space Force Exists to Deal with Threats in Space Domain, Vice Chairman Says,” *DoD News*, accessed 26 April 2021, https://www.defense.gov/Explore/News/Article/Article/2480459/space-force-exists-to-deal-with-threats-in-space-domain-vice-chairman-says/#:~:text=News%20Reform-,Space%20Force%20Exists%20to%20Deal%20With,Space%20Domain%2C%20Vice%20Chairman%20Says&text=Threats%20by%20Russia%20and%20China,the%20Joint%20Chiefs%20of%20Staff.

85. Jim Gramone, “Milley Will Use Defense Strategy to Chart Way Ahead for Joint Force.” December 2, 2019, *Defense*.gov, https://www.defense.gov/Explore/News/Article/Article/2029719/milley-will-use-defense-strategy-to-chart-way-ahead-for-joint-force/.

86. Gramone, “Milley.”

87. Robert Sprout, Interview with DSCA Action Officer. Email, January 14, 2021.

88. Adrian Rosenberg, “Air Force Announces $950M Investment for JADC2 Development*,” Potomac Officers Club*, June 3, 2020, Accessed April 29, 2021, https://potomacofficersclub.com/air-force-announces-950m-investment-for-jadc2-development/.

89. Department of State, Directorate of Defense Trade Controls, *“Arms Export Control Act (AECA),”* Accessed: April 29, 2021, https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=b9a933addb7c930044f9ff621f961932.

90. Committee for National Security Systems, “CNSSP-8: Policy Governing the Release and Transfer of and U.S. Government Cryptologic Security Material, Information, and Techniques to Foreign Governments and International Organizations.”

91. Committee for National Security Systems, "CNSSP-14: National Policy Governing the Release of Information Assurance (I.A.) Products and Services to Authorized U.S. Persons or Activities Not a Part of the Federal Government.”

92. Christopher Zember and Peter Khooshabeh, “Defense Innovation Is Falling Short,” *War on the Rocks*, September 25, 2020, https://warontherocks.com/2020/09/defense-innovation-is-falling-short/.

93. Merritt, “Weapon System Sustainment: Selected Air Force and Navy Aircraft Generally Have Not Met Availability Goals, and DoD and Navy Guidance Need to Be Clarified.”

94. Morgan Dwyer, “The Air Force Digital Century Series: Beyond the Buzzwords” (Center For Strategic and International Studies, November 8, 2019), https://www.csis.org/analysis/air-force-digital-century-series-beyond-buzzwords.

95. Eric Lofgren, “Analyzing Corporate Welfare in Defense,” *Acquisition Talk* (blog), January 30, 2019, https://acquisitiontalk.com/2019/01/analyzing-corporate-welfare-in-defense/.

96. Christina Chaplain, “Weapons Systems Cybersecurity” (United States Government Accountability Office, October 2018), https://www.gao.gov/assets/gao-19-128.pdf.

97. Tracy Sharp, “DISA Hosts Successful Workshop to Improve JRSS Capabilities,” accessed April 25, 2021, http://disa.mil/NewsandEvents/2020/workshop-improve-JRSS-capabilities; “Audit of the DoD’s Implementation of the Joint Regional Security Stacks DODIG-2019-089,” Department of Defense Office of Inspector General, accessed April 25, 2021, https://www.dodig.mil/reports.html/Article/1867983/audit-of-the-dods-implementation-of-the-joint-regional-security-stacks-dodig-20/.

98. DODIG, “Audit of the DoD’s Implementation of the Joint Regional Security Stacks DODIG-2019-089.”

99. Andrew Eversden, “The Senate Has Questions about DISA’s Network Security System,” *C4ISRNET,* June 29, 2020, https://www.c4isrnet.com/cyber/2020/06/29/the-senate-has-questions-about-disas-network-security-system/.

100. John A. Tirpak, “Out of Joint,” *Air Force Magazine* (blog), accessed April 9, 2021, https://www.airforcemag.com/article/0813joint/.

101. Tirpak, “Out of Joint.”

102. Paul McLeary, “JADC2 Faces ‘Huge Weakness’: Old Policies, Old Tech,” *Breaking Defense,* March 3, 2021, Accessed April 29, 2021. https://breakingdefense.com/2021/03/jadc2-faces-huge-weakness-old-policies-old-tech/.

103. “Joint All-Domain Command and Control (JADC2).” *Congressional Research Service*, March 18, 2021. https://www.citationmachine.net/chicago/cite-a-website/custom.

104. Hitchens, “Exclusive: J6 Says JADC2 Is a Strategy; Service Posture Reviews Coming.”