Spring 2020

Industry Study

Final Report

United States Nuclear Command, Control, and Communications "NC3"

The Dwight D. Eisenhower School for National Security and Resource Strategy

National Defense University

Fort McNair, Washington, DC 20319-5062

Disclaimer: The views expressed in this paper are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the United States government.

Nuclear Command, Control and Communications (NC3)

ABSTRACT: Geopolitical changes, coupled with emerging and dangerous adversarial technologies, drive an urgent need to modernize the old and antiquated US NC3 system. Despite this strong impetus, modernization is only progressing slowly. The US government is not yet structured for the challenges of NC3 modernization, nor has it motivated the defense industrial base (DIB) and innovation base to support the effort. To better facilitate NC3 modernization, the government must define the desired architecture, communicate a clear demand signal, incentivize the DIB and innovation base, create effective governance and agile acquisition processes, and mitigate security clearance and facility challenges.

NC3 Industry Study Members

Students	
Lt Col David Abel	United States Air Force
Ms. Liliana Alvarado-Ortiz	Defense Contract Management Agency
CDR Edward Barry	United States Navy
Ms. Holly Carey	Department of Homeland Security
Mr. William Czajkowski	National Nuclear Security Administration
LTC Tod Marchand	United States Army
Mr. Robert McMurry	Department of State
Ms. Wendy Rhodes	Defense Department
CDR Adrienne Rosseti	United States Navy
Lt Col Justin Secrest	United States Air Force
LTC Tissa Strouse	United States Army
LtCol Christopher Tolliver	United States Marine Corps
Mr. David Tomlinson	Defense Intelligence Agency
Lt Col Kevin Walsh	United States Air Force
Faculty	
Colonel Elvert L. Gartner	United States Air Force/Faculty Lead
Ms. Cynthia Lersten	National Nuclear Security Administration

Industry Studies Outreach and Field Studies

On-Campus Presenters

National Nuclear Security Administration NC3 Enterprise Center (NEC)
The Joint Staff, Washington D.C.

- J-36, Strategic Operations Division
- Strategic Deterrence and Nuclear Policy Division Defense Logistics Agency

Office of the Secretary of Defense

- Office of the Under Secretary of Defense for Acquisition and Sustainment, Technical Director

Headquarters, United States Air Force, Washington D.C.

- AF/A10, Strategic Deterrence and Nuclear Integration, Policy and Planning Division Defense Threat Reduction Agency
- Nuclear Enterprise Directorate
- Nuclear Strategy Division
    - NATO NC3 Systems Requirements

Virtual Presenters (Post COVID-19 Limitations)

Northrup Grumman: Firm Background, NC3 Support Capabilities and Implications
Lockheed Martin: Firm Background, NC3 Support Capabilities and Implications
L3Harris: Firm Background, NC3 Support Capabilities and Implications
Collins Aerospace: Firm Background NC3 Programs and NC3 Modernization Implications

Field Studies

National Military Command Center (NMCC), Washington D.C.
Johns Hopkins, Applied Physics Laboratory, Laurel, MD
Carnegie Mellon, Software Engineering Institute (SEI), Arlington, VA
NC3 Program Executive Office (PEO), Hanscom, AFB, Bedford, MA
Raytheon—Integrated Communications Systems Office, Waltham, MA
MIT Lincoln Laboratories, Lexington, MA
MITRE Corp, National Security Engineering Center, Lexington MA
General Dynamics—Mission Systems, Dedham, MA

Executive Summary

Geopolitical changes, coupled with emerging and dangerous adversarial technologies, drive an urgent need to modernize the old and antiquated US Nuclear Command, Control, and Communications (NC3) system. Despite this strong impetus, modernization is only progressing slowly. The US government is not yet structured for the challenges of NC3 modernization, nor has it motivated the Defense Industrial Base (DIB) and innovation base to support the effort. To better facilitate NC3 modernization, the government must, define the desired architecture, communicate a clear demand signal, incentivize the DIB and innovation base, create effective governance and agile acquisition processes, and mitigate security clearance and facility challenges.

The NC3 Industry Study analyzed US government actions to implement NC3 modernization and the DIB and innovation base's readiness to support the effort. This report provides strategic context, and describes relevant industry, innovation, and market structure. It also analyzes key areas including governance, acquisitions, the supply chain, industrial security, and human capital. The analysis delivers useful insights for stakeholders involved in NC3 modernization.

Collective analysis findings are addressed with the following five NC3 Modernization recommendation areas:

1. **Define the Desired Architecture**
    - Collaborate with Government Funded Agencies
    - Create a High-Level Roadmap and Digital Engineering Platform
    - Incorporate Modularity
    - Solicit Threat-Based Research
    - Form a Threat Monitoring Advisory Committee
2. **Communicate a Clear Demand Signal**
    - Articulate the Modernization Plan
    - Provide Appropriate NEC Manpower
    - Begin Execution Short of the 100% Solution
    - Identify and Exploit Disruptive Technologies
3. **Incentivize the Industrial and Innovation Base**
    - Increase annual Science Technology and Education (STE) allocations at FFRDCs.
    - Create and Subsidize Secure Small Business Centers
    - Leverage Mutually Beneficial Relationships
    - Create Interoperability Within Programs

4. **Create Effective Governance and Acquisition Agility**
    - Designate a JADC2 Enterprise Lead and Integrate with NC3
    - Integrate NC3 Acquisition Under One PEO for Each Service
    - Establish Component Acquisition Executive (CAE) Responsibilities within USSTRATCOM Staff
    - Adopt Agile and DevSecOps Methodologies
5. **Mitigate Industry Security Clearance/Facility Challenges**
    - Expedite Security Clearances for Personnel Supporting NC3
    - Adjust Classification Status to the Lowest Level of Acceptable Risk
    - Develop a Cloud-based Classified Network

Table of Contents

"WHILE ONCE STATE-OF-THE-ART, THE NC3 SYSTEM IS NOW SUBJECT TO CHALLENGES FROM BOTH AGING SYSTEM COMPONENTS AND NEW, GROWING 21ST CENTURY THREATS."[1]

– 2018 NUCLEAR POSTURE REVIEW

I. Introduction

For nearly 75 years, nuclear weapons have served as a bedrock to US national security.[2] However, a shift in focus away from nuclear weapons capability during the post-cold-war years contributed to their modernization and sustainment neglect. Now, due to *great power competition* and emerging and dangerous adversary technologies, it is clear the US needs to revitalize its' nuclear capability. However, the negative impact of three decades of neglect to the nuclear enterprise is also clear. NC3 is the principal victim of this neglect. The 2018 Nuclear Posture Review (NPR) clearly calls for NC3 modernization and leaders at all levels have reemphasized this need. So, why does a modernization solution still seem so far off and what can be done about it? Moreover, is the DIB and innovation base prepared to help? To meet the NC3 modernization demand, the US government must define its' desired architecture, communicate a clear demand signal, incentivize the industrial and innovation bases, create flexible acquisition processes, and mitigate security clearance and facility challenges.

Purpose: This report analyzes US government efforts to modernize NC3 and assesses the DIB and innovation base's ability to support them. It also provides recommendations to improve modernization efforts. To begin, it offers context for NC3 modernization by detailing the security environment, modernization drivers and challenges, and the overall defense industrial base status. It then describes the structure of the DIB and innovation base and relevant market conditions. Next, it analyzes key areas with modernization implications including: (1) governance, (2) acquisition with emerging technology and software considerations, (3) the supply chain, (4) industrial security, and (5) human capital. Finally, this report provides actionable recommendations.

Methodology: The information used in this analysis was obtained through extensive literature reviews and direct engagements with government agencies, university laboratories and defense industry firms during site visits and interactive online meetings. The site visits and interactive meetings allowed students to identify facts and context surrounding NC3 modernization and facilitated candid discussions with NC3 experts. This, in turn, led to a rich analysis and actionable recommendations.

"NC3 Modernization" Definition: The term 'NC3 modernization' has various connotations that can confuse its' analysis. Throughout this paper, the term *modernization* assumes a combination of upgrading current systems and developing new architecture. When the terms "Next Generation," "NextGen," or "NC3 Next"

appear, they specifically reference a new architecture to replace the NC3 legacy architecture.

NC2 Definition: Nuclear Command and Control (NC2) is, "The exercise of authority and direction, through established command lines, over nuclear weapon operations by the President as the chief executive head of state."[3]

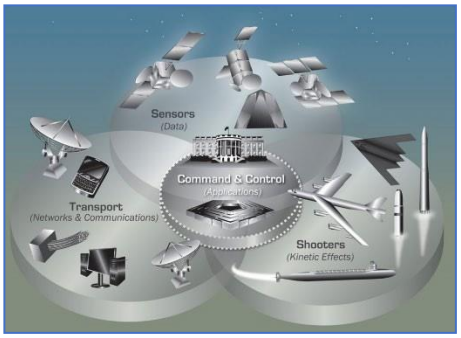


Figure 1 NC3 Components[5]

NC3 Definition: NC3 is a complex "network of communications and warning systems that ensure dedicated connectivity" to enable NC2.[4] NC3 is a system of systems consisting of early warning satellites and ground sensors, ground and airborne platforms, and data and voice delivery capabilities. (figure 1)[5] NC3 accomplishes five mission essential functions: (1) detection, warning, and attack characterization, (2) nuclear planning, (3) decision-making conferencing, (4) receiving presidential orders, and (5) enabling management and direction of forces.[6]

NC3 Industry Definition: The NC3 industry consists of firms skilled in cyber and electronic warfare technologies, space systems, software development, system integration, and aircraft manufacturing and sustainment. Firms involved in these areas support NC3 in its current legacy form and will likely support NC3 modernization. Ideally, the DIB will expand with new firms being encouraged to support modernization efforts. Firms with advanced software development and system integration capability will be key contributors. Due to the technologies involved, firms in the NC3 industry require highly skilled human capital and must be capable of working with classified information. Typically, large firms with necessary internal research and development resources take the lead, while smaller, more innovative firms, provide enhanced technical capability.

II. NC3 Modernization Strategic Context

Security Environment

China and Russia's current nuclear modernization, coupled with their aggressive advancements in hypersonic, nuclear-propulsion, cyber-security, and electromagnetic (EM) spectrum technologies, pose a grave threat to the US NC3 system's ability to detect, track, and classify adversary attacks in a timely and accurate manner. The current US NC3 and Integrated Tactical Warning/Attack Assessment (ITW/AA) systems were designed for conventional nuclear delivery systems (i.e., Inter-Continental Ballistic Missiles and strategic bombers); not disruptive technologies capable of evading the global network of sensors and corrupting the system's software and hardware.

Chinese nuclear capability and modernization has been a source of concern for the US since the nation became a nuclear power on 16 October 1964.[7] Following China's first nuclear weapon detonation, it has maintained a "no first use" nuclear policy and, instead, focuses on assured second-strike capabilities.[8] With an estimated stockpile of 280 warheads in 2018[9], China has developed a credible land and sea-based nuclear force consisting of medium-range, long-range, and intercontinental ballistic missiles.[10] In 2019, China also tested two different models of hypersonic surface-to-surface missiles.[11] Capable of traveling up to Mach 8, hypersonic missiles travel faster than ballistic missiles and along non-ballistic trajectories. This complicates detection and tracking, reduces assessment and decision-making time, and introduces a greater chance of mischaracterization and inadvertent escalation.[12] It is also believed that China could field the strategic bomber leg of its nuclear triad within the next decade.[13] Even if China chooses to focus on further global economic expansion rather than make frequent changes to its nuclear strategy, the capabilities it already has and is developing represent risk to the US.

In 2011, the Russia Federation implemented its 10-year State Armament Program (GPV – *Gosudarstvennyi Programme Vooruzheniya*) meant to modernize 70% of its military inventory by 2020[14]; with strategic forces receiving the highest priority.[15] Any expectation that this commitment is merely the natural and timely modernization of aging equipment necessary to maintain nuclear equilibrium is blind to Russia's real strategic intentions. Russia is attempting to upend the half-century old nuclear "strategic gameboard" by changing how, where, and when it competes. Rather than continuing to play the "same [historic] game" of maintaining comparative nuclear parity, Russia has chosen a strategy of "selective new game" by creating and pursuing "unique advantage[s]" through the rapid development of inspirational – possibly unviable – strategic delivery systems such as hypersonic and nuclear-propulsion technologies that exploit believed vulnerabilities in the ITW/AA system's family of sensors.[16] In fact, two *Avangard* Hypersonic Glide Vehicle systems were scheduled to deploy in 2019 with a total of 12 by 2027.[18]

In addition to advanced delivery systems capable of exploiting NC3 and ITW/AA system vulnerabilities, China and Russia continue to advance offensive cyberspace and EM spectrum capabilities. NC3 is reliant on cyberspace and the EM spectrum to enable the vast array of sensors and communications systems necessary to guarantee the transmission of information and orders, so successful attacks in these domains can prove devastating. Despite immense efforts to "harden" cybersecurity, no enterprise so dependent on electronic systems can be invulnerable to cyber-attacks. It is assumed that adversarial cyber forces are constantly probing for weaknesses in NC3, and Chinese and Russian cyber weapons and tactics (i.e. malware, insiders, social engineering) will be used throughout any nuclear escalation to achieve their strategic goals.[19] Chinese and Russian advanced

electronic warfare capabilities will also play a predominant role in any confrontation as they attempt to degrade the NC3 system, prevent national-level decision-making, and slow a US response.[20] Developing these advanced technologies while continuing to innovate to compete with the US requires China and Russia to sustain a strong DIB.

Although less robust than that of the US, the Chinese and Russian DIBs have proven capable of maintaining strong nuclear weapons programs and fielding disruptive technologies that are now complicating US NC3 modernization efforts. Despite enduring challenges, Russia's innovation and DIB is shedding some of its post-Soviet Union afflictions and receiving renewed attention to achieve President Vladimir Putin's vision of Russia's place on the global stage. In 2011, and for the first time in the post-Soviet era, Russia infused significant capital into its DIB; R20.7 trillion (approximately $700B) towards military modernization with R19 trillion directed towards weapons procurement and R1.7 trillion towards modernizing the DIB.[21] This attracted younger, more-qualified workers into the defense industry and inspired the "serial production of equipment."[22] Russia's DIB, however, continues to have challenges. Replacing aging submarines with an improved Borei-B design was cancelled due to cost inefficiencies. The Tu- 95MS *Bear* and Tu-160Ms *Blackjack* are also nearing mandatory retirement while the *PAK-DA* stealth bomber replacement is still in the planning phase.[23] [24] Finally, the two leading units of Russia's space agency – *Energiya* and the *Khrunichev Center* – are in financial trouble and the expiration of US contracts make them more dependent on state funding.[25]

Chinese nuclear weapons being classified as low quality and low inventory is a potential result of Beijing's long-term policy of "no first use."[26] However, in the last three years, China has produced an estimated ten warheads and continues to make improvements in its' conventional and nuclear arsenal. Comprised of over 200 enterprises and institutions with advanced technology and equipment and an overabundance of human capital with heavy Science, Technology, Engineering and Mathematics (STEM) backgrounds, China's DIB is making significant gains in both conventional and nuclear weaponry, and non-kinetic means.[27] Threats stemming from great power competition are one of many factors driving the need for NC3 modernization.

Additional Modernization Drivers

The 2018 NPR identified the nuclear triad as the most cost-effective and strategically sound means to ensure nuclear deterrence, and called for the modernization of aging NC3 infrastructure due to growing 21st century threats.[28] General Paul Selva, Former Vice Chairman of the Joint Chiefs of Staff, stated:

> Our nuclear deterrent is nearing a crossroads. To date, we have preserved this

> deterrent by extending the lifespan of legacy nuclear forces and infrastructure in many cases for decades beyond what was originally intended. We are now at a point where we must concurrently modernize the entire nuclear triad and the [NC3] infrastructure that enables its effectiveness.[29]

While the current US NC3 system is functioning, portions of the system are long past their service life. Moreover, manufacturers for some parts and capabilities in the NC3 system no longer exist.[30] The current architecture is complex with system modifications spanning decades.[31]

In addition to the obsolescence of supplies, the current architecture's complexity increases sustainment difficulties. Currently, NC3 consists of 204 different systems with no common standards or operating system.[32] Over the last 40 years, these disparate systems were cobbled together to create the NC3 enterprise. Since these systems have differing standards, are not compatible, and often do not communicate with each other, system operational status and failures across the enterprise are difficult to ascertain. Differing equipment standards across air, sea, land, and space-based systems increase the complexity of long-term maintenance and sustainability due to each system's unique and specialized suppliers. The opportunity and need to develop a new system with greater integration of maintenance and sustainability is another driver for modernization. However, changes in the strategic and adversarial technology environment and the "entanglement" these factors create may be the greatest driver for modernization.

The interaction between nuclear and non-nuclear domains, also called "entanglement," requires a new way of doing NC3.[33] In the cold war era, the boundaries between nuclear and non-nuclear capabilities were distinctly drawn by technology limits—ballistic missiles meant nuclear strike, satellites were immune from attack, and cyber-attacks did not exist. Under these circumstances, maintaining a distinct conventional/nuclear line was not only possible, it was desirable. Now, due to emerging technologies such as hypersonic weapons, anti-satellite capabilities, cyber weapons, and high precision/long range conventional munitions, C3 systems are facing added risk regardless of the mission they support (conventional or nuclear). For NC3 to prevent strategic miscalculation, it must see, understand, and communicate in all domains. All-domain C2 is emerging as a high priority requirement, and modernization driver as it requires nuclear incorporation.

Modernization Challenges

Despite the many good reasons to modernize NC3, progress has been slow. This is due in large part to several challenges and impediments that are hindering progress. Two of the biggest challenges are complexity and culture.

NC3 is complex in size and scope. This is problematic for sustainment and, therefore, serves as a driver for modernization; however, it also serves as an impediment. The vast array of technologies currently integrated into the NC3 system have emerged over decades. Understanding how to move forward, given this context and the contemporary threat environment, to create a new NC3 architecture is complicated. Moreover, the vast array of systems is not governed by an single organization but is rather portioned between the 10 separate Program Executive Offices (PEOs) to include eight Air Force, and two Navy.[35, 36] This creates a lack of unity and a consequential lack of unified governance. These two sub-factors of complexity coalesce to further impede modernization overall and make answering essential questions exceedingly difficult.

As leaders at US Strategic Command (USSTRATCOM) contemplate the complexity and try to develop the NC3 architecture of the future, they are suffering from "analysis paralysis" which, as the term implies, paralyzes movement. Even if there were unity of effort, the balance of the necessary questions requires detailed analysis, and consequently, time. How exactly should modernization move forward? What are the risks of different options? What is possible? These difficult questions, and the analysis each requires, contribute to the pedestrian modernization pace. In addition to complexity, differing cultures within the organizations supporting NC3 are at odds.

Culture clashes between NC3 stakeholder agencies also impede NC3 modernization. Seasoned NC3 leaders and advisors are resistant to deviate from the current legacy architecture while newcomers, academia, and industry are advocates for a clean slate, evolutionary NC3 architecture. The perceived safety and reliability of the legacy architecture is appealing to an NC3 community inculcated with a need for perfection and years of trust in the legacy way of providing NC3. There are strengths and weaknesses in each approach, and moving forward will require government, academia, and industry to work together.

The US Defense Industrial Base

The US DIB supports economic prosperity and global competitiveness and arms the military with capabilities to defend the nation. According to the Cybersecurity and Infrastructure Security Agency (CISA):

> The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet US military requirements. The Defense Industrial Base Sector provides products and services that are essential to mobilize, deploy, and sustain military operations.[40]

On July 21, 2017, President Donald J. Trump signed Executive Order (E.O.) 13806 on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States. Per the report, the industrial base faces a unique set of challenges including sequestration and uncertainty of government spending, the decline of critical markets and suppliers, unintended consequences of US Government acquisition behavior, aggressive industrial policies of competitor nations, and the loss of vital skills in the domestic workforce.[41] There are a limited number of firms within the DIB dedicated to the modernization and development of the US nuclear arsenal and NC3. These firms include Boeing, Northrop Grumman, General Dynamics, Lockheed Martin, Raytheon, L3Harris, and United Technologies.

Each firm has delivered quality products for years and shows the following strengths:

(1) Continued revenue growth increasing its ability to allocate funds for future growth initiatives
(2) Strong order backlog indicating significant demand for the firm's products and services
(3) Strong focus on research and development that enables product innovation
(4) A focus on innovative technologies such as big data, cloud computing, cybersecurity, distributed systems, immersive learning, networking, communications, and quantum physics
(5) Geographic diversification

These firms also display weaknesses in the following areas:

(1) Significant dependence on subcontractors and suppliers
(2) Decline in liquidity position which limits the ability to fund future growth opportunities
(3) Cost overruns due to unresolved problems in product delivery
(4) Significant pension benefit obligations
(5) Susceptibility to economic and political environments due to overreliance on a single geographic region for revenue

NC3 Industry Study students conducted research and detailed analysis of four of these firms: General Dynamics, L3Harris, Raytheon, and United Technologies. (Appendixes B-E) This analysis revealed that NC3 industry solvency is dependent on the government and, more specifically, the DoD. This led to a conclusion that, in the era of great power competition, the government must do what it can to support the DIB's efforts to build a skilled workforce and infrastructure, and obtain a stable funding stream. Government support to the DIB is essential to all

NC3 modernization efforts.

III. NC3 Innovation & Industry Structural Analysis

NC3 Innovation Ecosystem

NC3 innovation exists within a *triple helix* where the government, industry, and academia interact to promote and sustain creative thinking in an innovation ecosystem. Dr. Henry Etzkowitz, Professor at University of London, Birkbeck School of Management and creator of the "Triple Helix Theory," explains how relationships in industry, government, and academia interact to drive innovation across societies, and how societal norms determine which strand of the helix has primacy over the other in driving innovation.[42] Since NC3 is a niche system, within a monopsony market, the government plays the leading role in innovation. Government drives demand and resources innovation within the Federally Funded Research and Development Centers (FFRDC), University Aligned Research Centers (UARCS), and industry. However, the risk-averse culture within the NC3 community negatively affects interactions within the NC3 *triple helix* and continues to present innovation barriers.

Innovation Barriers

Cultural differences within the NC3 innovation ecosystem present barriers to communication, understanding, and innovation. They subsequently prevent the ability of the NC3 innovation *success triangle* to reach full potential. Resistance to cultural change within NC3 governance structures creates organizational friction that negatively affects its relationship with industry. For example, the NC3 community does not agree about what the next generation NC3 architecture should look like. The more seasoned personnel within the community are resistant to deviating from the current "Thin and Thick Line" (survivable and day-to-day communications) (Appendix A) construct. Newcomers to the community advocate for a *clean-slate* concept, as does academia and industry. Until an agreement is achieved, and a requirement is sent to industry, NC3 innovation will remain stagnant.

Additionally, perceived competition between industry, FFRDCs, and UARCs serves as an innovation barrier that is hindering collaboration. Industry leaders indicate concern with FFRDCs and UARCs providing innovative ideas and intellectual property rights to the government. This practice restricts private industry profit because government may own intellectual property rights to technology that private industry sought to develop. Moreover, FFRDCs and UARCs compete for research and development dollars and therefore do not always collaborate on innovative ideas. Only one prominent FFRDC visited during this study acknowledged collaboration with a UARC on NC3 innovation. Regardless, the competition, or perceived competition for government research dollars, can be a barrier to collaboration within the NC3 innovation ecosystem.

NC3 Market: Now and Next

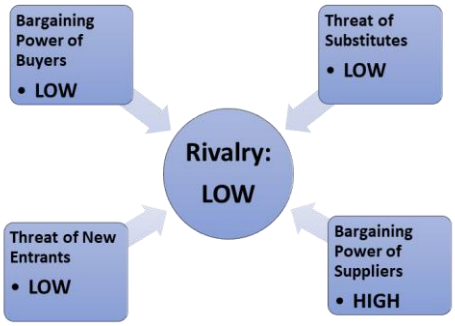


Figure 2: Porter's Five Forces and the NC3 Market

NC3 modernization is required before the system reaches end of life.[43] However, as a result of continued reliance on existing capabilities, the old system cannot simply be "turned off" while it is either upgraded or entirely replaced. This creates the challenge of upgrading the existing architecture while designing, funding, and fielding the next generation of NC3. This dual effort, maintaining the current system and designing a future system, places NC3 within two market structures; one mature and one maturing. Understanding the current market system will better enable the US to mold the future marketplace to maximize innovation and competition. Michael Porter's Five Forces will be used as a tool to analyze these markets.[44] (Figure 2)

Now

As the principle buyer of NC3 technologies and the system of systems the government controls significant portions of market demand for NC3 technologies and ideas. As most NC3 technology is not dual use, meaning it serves limited marketability outside of its primary function, the government controls a monopsony of buying power. In theory this strengthens the government's buying position,[45] but closer examination shows the government's purchasing power is dominated by other factors.

The government has relatively low bargaining power over existing equipment suppliers. Because NC3 systems must always function, the government is reliant on suppliers who provide the niche systems—suppliers are thus advantaged. For example, General Dynamics supplies the "Direct System" incorporated into the current NC3 architecture and the system distributes, receives, and authenticates Emergency Action Messages (EAMs). This capability is not easily replaced without disruption or wholesale architecture changes. Therefore, the government's demand is inelastic and General Dynamics has a pricing power advantage and, in this context, little motivation to innovate on the existing system.

The buying power of the government is further reduced because of high barriers of entry and limited product substitutions. Top Secret and Special Access Program classification levels are expensive to obtain and long lead times for certification limits most businesses from entering the market. Additionally, expenses for personnel with security clearances, facility clearances, and secure computer network access limits all but the largest defense contractors from entering the market.

No substitute exists for the NC3 system. The government must have a reliable and

credible NC3 system and sending EAMs to the warfighter cannot be substituted as long as the US needs a nuclear deterrent. At the system level, threat of substitutes is also low because most NC3 systems are uniquely designed and customized for the legacy architecture. This combined effect of high barriers to entry and limited substitutions reduces most advantages of the government's monopsony.[46]

The bargaining power of suppliers is largely defined by the limited number of major defense firms operating in the NC3 market. This oligopoly of contractors operates more as "compet-a- mates" than competitors. As each company carves out their own specialization "niche," the effective number of companies competing on any program is further reduced to one or two bidders. As an example, General Dynamics, L3Harris, and soon-to-be Raytheon Technologies comprise the majority of the NC3 Market. L3Harris has specialized communications and crypto systems, General Dynamics has the Direct System, and Raytheon Technologies has transmission and receiver equipment. The incumbent corporations operate as an oligopoly operates -- in a protected market where they have virtual monopolies on their NC3 niche system. Because the incumbents face little threat from competition, large defense contractors have significant supplier power. With few competitors, the supplier power exceeds buyer power significantly. This analysis bares out when looking at the NC3 system today. An aged, expensive system, with few replacement parts, and long-term contracts that are not to the government's advantage.

Next

What does the future market look like and what can the government do to better position itself? Because the next NC3 architecture is not yet defined, it is difficult to apply Porter's Five Forces. Today, as the government seeks inputs for the new NC3 architecture, barriers to entry are low as the NC3 Enterprise Center (NEC) seeks concepts of operations and potential current technologies which will enable future advantages. This enables new entities to enter the market and reduces the differentiation of products currently provided by traditional defense industries.[47] To maximize innovation, the government has taken some action to reduce barriers to entry and enable non-traditional defense companies and federally funded research and development centers to join traditional defense corporations. As an example, the government consulted with multiple non-traditional industries[48] to explore technologies which enable real time system updates, data collection and unauthorized access recognition software which may play critical roles in maintaining the health and security of NC3 systems.[49]

As the number of entrants in the NC3 NextGen market increases, the ability for the government to shift between suppliers improves. With growing market diversity and competition, the government will not be reliant on a small number of suppliers to generate new ideas and advance NC3 NextGen frameworks. Low barriers to entry, increased number of suppliers, and similarity of products (at this stage, "clean sheet" ideas) at the initial stages of NC3 NextGen may shift suppliers from an oligopoly toward perfect competition.[50] This near perfect competition may degrade again over

time as NC3 NextGen matures and classification requirements force non-traditional and smaller defense contractors out of the market.

IV. Analysis: Key Modernization Areas

Governance Implications

The current governance structure of US NC3 capabilities appears clean on paper, but when examined at the Combatant Command (CCMD) and service levels it becomes increasingly chaotic, fragmented, and entangled with other command, control, and communication (C3) concerns. This section examines authorities and governance structures relevant to the US NC3 enterprise and how those will affect acquisition activities while transitioning to the next generation NC3 architecture. It examines recent guidance from the Deputy Secretary of Defense, service NC3 governance, and concludes with considerations for the NC3 connection with National Leadership Command Capability (NLCC). The analysis presented here does not include NATO NC3 considerations other than to note that open architecture designs can best enable future US/NATO inoperability. The section concludes with recognition of the entangled nature of NC2, Joint All-Domain Command and Control (JADC2), and NLCC.

Deputy Secretary of Defense Directive Type Memorandum on DOD NC3 Governance.

On 17 April 2019 the Deputy Secretary of Defense (DEPSECDEF) appointed the Commander of United States Strategic Command (CDRUSSTRATCOM) as the NC3 enterprise lead via a directive type memorandum (DTM) entitled "Nuclear Command, Control, and Communication Enterprise Guidance."[53] The directive establishes NC3 enterprise policy and assigns responsibilities in support of the USSTRATCOM NC3 Governance Improvement Implementation Plan. The authorities and requirements explicit in the memo empower CDRUSSTRATCOM to sign and distribute annual NC3 capability planning guidance; organize, resource, and operate an NEC; and, accept transfer of the Joint Systems Engineering and Integration Office (JSEIO) from the Defense Information Systems Agency (DISA). The JSEIO is central to the developing NEC, which will coordinate the architecture roadmaps and technical standards of the next generation NC3 capability.

Other DoD key leader taskings of interest to this paper include:

- Appointment of Undersecretary of Defense for Acquisition and Sustainment was appointed the NC3 Capability Portfolio Manager for the DoD, a responsibility which requires "maximizing accomplishment of desired outcomes within constraints."[54]
- The DoD component heads must "operate, maintain, and change the operational configuration of NC3 systems as directed by CDRUSSTRATCOM," and "Coordinate with CDRUSSTRATCOM to ensure NC3 modernization programs comply with architecture roadmaps

and technical standards."[55]

- The Chairman of the Joint Chiefs of Staff (CJCS) has approval authority for any CDRUSSTRATCOM recommended changes to NC3 systems that affect the operational configuration of the National Military Command System (NMCS).[56]

This last delegation clearly contains a responsibility for both the CJCS and CDRUSSTRATCOM to have a common understanding on how the next generation NC3 system will interface with the existing NMCS systems as well as to anticipate future NMCS system integration or ensure open architectures compatible with future systems. The Joint Staff is currently working on concepts to define JADC2 which will enable integration of all sensors and weapon platforms (air, land, sea, space, and cyber) on the battlefield. Currently, the JADC2 effort lags the NC3 effort, with no clear governance structure, architecture, or requirements, while the services are proceeding to execute acquisition without a common vision of the joint result.[57] If JADC2 and NC3 are not integrated to some degree, the concept that *all* sensors and weapons (including nuclear) are integrated will not be achieved.

Service Execution of NC3 Acquisition

As mentioned above, the NC3 DTM also requires that the service components modernize the NC3 system in accordance with USSTRATCOM architecture and technology standards. While phrased so concisely that it may seem like an easy task, each of the nuclear services has its own unique nuclear governance structures which interact with the rest of the joint force in complex ways. The US Air Force (USAF), which holds responsibility for approximately 75% of NC3 assets, owns a variety of platforms, sensors, and communication equipment fulfilling nuclear missions. The USAF does not consolidate the equipment, and the organizations which procure it, under one structure. The complexity of the USAF system requires a great deal of communication and coordination to even approximate an integrated effort. Conversely, the US Navy (USN), with only one nuclear platform and one submarine launched missile system, has a significantly less complex NC3 environment. The following paragraphs examine the USAF and USN governance structures.

USAF NC3 Governance

The USAF manages an NC3 Weapon System, the AN/USQ-225, which is composed of 43 operational and 7 developmental systems managed by 8 PEOs. Many of these components are additionally elements of the National Leadership Command Capability (NLCC), a few are general, dual-purpose use, and a small number have no identified PEO sustainment assignment.[58] In order to clarify governance and management responsibilities the Air Force publishes Air Force Instruction (AFI) 13-550, *Nuclear, Space, Missile, Command and Control AIR FORCE NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS (NC3)*. The following are some key responsibilities from the AFI:

- The Assistant Secretary of the Air Force for Acquisition, Technology and Logistics (SAF/AQ) is responsible for acquisition and sustainment of AF NC3 systems.[59]
- Air Force Global Strike Command (AFGSC) is responsible for "…strategic vision and roadmap and identify requirements…," and serves as the lead command for NC3 and the AN/USQ-255.[60]

AFGSC executes much of this function through the Air Force NC3 Center (AFNC3C) which is the AFGSC lead to organize, train, and equip for the AN/USQ-255. These responsibilities include requirements, system architecture, and life-cycle assessment activities.[61]

The Air Force Nuclear Weapons Center (AFNWC) NC3 Integration Director (AFNWC/NC) is the "Principle Integrator for AN/USQ-255 materiel management and sustainment activities," is one of the 8 AF PEOs, and is given "authority and responsibility for weapon system architecture…,"[62] a delegation which appears to overlap with the AFNC3C's responsibilities.

The governance portion of the AFI establishes a structure intended to engage with that of the Office of the Secretary of Defense for NC3 and NLCC. It establishes a three-level system composed of a NLCC/NC3 Council at the 4-star level, chaired by AFGSC, to "exercise authority, responsibility, and establish priorities for AF NLCC/NC3." The next layer down is the AF NLCC/NC3 Board, chaired by the AFGSC Deputy Commander and the Deputy Chief of Staff for Strategic Deterrence and Nuclear Integration (AF/A10), with the role to "provide senior-level Air Force oversight and strategic direction to resolve key NLCC/NC3 issues affecting the Air Force Nuclear Mission."[63] The final layer is the AF NLCC/NC3 Group which is chaired by the AFNC3C Commander, AFNWC/NC, and AF/A10 Nuclear, and acts as "action arm" for the Board and Council. The governance bodies address requirements, architecture, resourcing, fielding, and sustainment, among other things. This structure brings together the AF NC3 stakeholders in a well-defined hierarchy; however, it entangles the NLCC and NC3 functions. The close coupling between NLCC and NC3, which are overlapping but distinct functions, and materiel, complicates NC3 management. This appears to be a systemic DoD issue.

USN NC3 Governance

The Navy's nuclear mission is focused on its Ohio class submarine fleet (soon to be replaced by the Columbia class modernization program) which carries the Trident II/D5 nuclear tipped, submarine launched ballistic missile. In support of the submarines is the E-6B Mercury aircraft which carries NC3 equipment.[64] The Navy manages the acquisition and sustainment of NC3 systems which support their nuclear mission via one senior level Executive Steering Committee (ESC). The ESC has multiple subordinate parts which represent key Navy organizations and involves two acquisition PEOs.

OPNAV Instruction F5420.116A, *Navy Nuclear Command, Control, and*

Communications Executive Steering Committee, directs the Commander, US Fleet Forces Command, to chair the Navy NC3 Executive Steering Committee, a body composed of 12 voting members.[65] While the current 5420.116 contains controlled information on the purpose of the ESC the previous version states that "The ESC will function as a senior level decision body to review and adjudicate Navy- wide NC3 operations, policy, training, materiel, and other readiness issues..," and "…oversee overall operation, sustainment, and requirements implementation of the Navy NC3 architecture."[66] Although the Navy governance and acquisition responsibilities very much parallel the Air Force's, it is simpler, likely due to the smaller footprint, and cleanly separates NC3 from NLCC.

NLCC, JADC2, and NC3

While the existing NC3 governance information covered above provides insight primarily into the current situation, the future of national command capability and networks remains largely undetermined. Title 10, § 171a., of US Code provides for a Council on Oversight of the National Leadership Command, Control, and Communications System within the DoD. It is composed of the Undersecretaries for Policy, and Acquisition and Sustainment, Vice Chairman of the Joint Chiefs, (the last two as co-chairs), CDRUSSTRATCOM, the Director of the National Security Agency, the DOD Chief Information Officer, and others as designated by the Secretary of Defense. It does not include representatives from the newly created Space Force and Cyber Command which will control key assets supporting NLCC,[67] and be heavily engaged in ensuring that those assets are adequately protected from cyber vulnerabilities and attacks.[68] The statute assigns the Council responsibility for assessment, architecture development, and resource prioritization, among other things. It also entangles NLCC with NC3 and does not require a long-term *plan* but year to year assessment and reporting mechanisms and a "description" of activities within the Future Years Defense Program.[69]

Given budgetary constraints, it is doubtful that the US can afford for nuclear command and control, NLCC, and JADC2 communication assets to exist independently of each other. Such a solution can be expected to result in wastefully redundant capability versus operationally desirable redundancies which anticipate failure mechanisms and allow for greater mission assurance instead of only greater cost.

Acquisitions Implications

The current DoD acquisitions process is neither designed nor optimized for a wholesale NC3 modernization effort. Moreover, the large number of stakeholders, whether they be designers, or customers and/or suppliers of NC3 capabilities, has created a confusing environment where centralized control and sufficient funding have proven elusive. Despite the innovative idea behind the NEC's inception, it still falls short in providing an expedient solution to the NC3 modernization problem.

This is because the NEC is tasked with creating the blueprint but does not have acquisition authority. That fact is a fundamental flaw in the current construct and one that defeats the proposed benefits of a singular leadership authority within USSTRATCOM.

Two overarching concepts are recommended to resolve these issues. They include consolidating agencies into a single governing body with the authority to make decisions, direct government, and commercial organizations, as well as provide funding. Categorizing NC3 as a single weapons system to aid in stable and flexible funding that matches existing and emerging requirements is an additional recommendation. The current DoD acquisition process is not designed or optimized for such an undertaking. A key improvement would be the designation of NC3 as its own weapons system. One could argue that this has already occurred. In 2016 the Air Force encompassed NC3 within the label AN/USQ-225. While this meets the definition of a "weapons system," it means nothing in terms of acquisitions.[70] For example, the F-35 is a designated "weapons system." Allotted funds for the F-35 program can be spent on nearly any aspect of the aircraft and its support systems at the discretion of the Joint Program Office. This is not true of the AN/USQ-225. Congressional funding is not assigned to the USQ weapons system where the services determine wherein the money goes. Instead, it is assigned to one of the 100 plus programs encompassed within the USQ designation. This inefficiency will exacerbate integration efforts and elongate the modernization timeline as it may force programs to develop in series rather than parallel.

Emerging Technology

The DoD has been carefully considering an array of architectures and emerging technologies that can be combined to provide secure, survivable, and resilient communications in the face of modern, multi-domain threats. It is time for the DoD, and specifically STRATCOM, to choose an NC3 architecture that incorporates the right emerging technologies. The top three recommended focus areas are hypersonic weapons, cyber security, and electromagnetic spectrum dominance. With proper signaling and incentives the defense industrial base is poised to research, develop, and produce capabilities within these key technology areas. Many emerging technology areas are relevant to NC3 and prioritizing these areas is important to modernization efforts. 5G technology could enhance resiliency and flexibility. Artificial Intelligence/Machine Learning (AI/ML) has the potential to accelerate and improve the quality of decision making. Quantum encryption and blockchain could strengthen security. Laser communications can resist jamming. These technologies, and many others, will contribute to NC3 NextGen; however, this Industry Study identified three emerging technology areas that should receive priority in the effort.

Hypersonic weapons. On 24 Dec 19, Vladimir Putin lauded that Russia had deployed the first nuclear-capable hypersonic missile system: "No other country possesses hypersonic weapons, let alone continental-range hypersonic weapons."[71] In 2019, China tested two different models of hypersonic surface-to-

surface missiles.[72] According to a report from the National Academies of Sciences, hypersonic missiles can travel at a speed of Mach 8, faster and lower than ballistic missiles.[73] Hypersonics are difficult to detect and track and are of importance to the NC2 process. Hypersonic speeds shrink the timelines for all phases of a response and, because conventional and nuclear hypersonic missiles are being developed in parallel, they also introduce the potential for inadvertent escalation. Failure to discriminate between conventional and nuclear attacks may result in a nuclear response to a conventional attack.[74] NC3 Next must be able to detect, track, and analyze hypersonic weapons (i.e. determine target, attribution, etc.) and then provide decision support and the means to direct a timely response. This threat redefines requirements for NC3.

Cyber security. Every nuclear force is made up of weapons systems, detection systems, and C2 nodes connected by a global network of communications and data-processing systems, all reliant on cyberspace, and all vulnerable to cyber-attacks. The threat of a cyber -attack on NC3 should provoke great concern, and illicit the question, "What emerging cyber technologies (i.e. block chain encryption, cloud security) and processes (i.e. DevSecOps, Cybersecurity Maturity Model Certification) can prevent an adversary from using a cyber-attack to trigger or disrupt nuclear capabilities?"[75] Despite immense efforts to "harden" cybersecurity, no enterprise so dependent on electronic systems can be invulnerable to cyber - attacks. It can be assumed that adversarial cyber forces are probing for weaknesses in NC3, and developing cyber weapons and tactics (i.e. malware, insiders, social engineering) to achieve strategic gains.[76] For NC3 Next, cybersecurity should be baked in from the beginning, included in defense in depth, backup systems, and be monitored and aggressively defended throughout the system's lifecycle. To be survivable in the face of relentless cyber- attacks, NC3 requires multiple, independent communications paths with no single points of failure.

Electromagnetic spectrum dominance capabilities. The electromagnetic (EM) spectrum is the primary medium for communicating across all domains (land, sea, air, space and cyber), and is essential to NC3. In addition to the political and economic forces that restrict access, the battle for the electromagnetic spectrum is also waged by militaries through electronic and spectrum warfare.[77] Both the Chinese and Russians have developed advanced electronic warfare capabilities to confront US forces.[78] To provide assured radio and satellite communications for NC3, the DoD must invest in emerging technologies that are resistant to, or provide countermeasures for, jammers, directed energy, electromagnetic, microwave and other electronic weapons that adversaries will employ to disrupt NC3 links. Advancements in electronic countermeasures, High Frequency (HF) / Very Low Frequency (VLF) / Advanced Extremely High Frequency (AEHF) systems, as well as laser communications are examples of new capabilities appropriate for NC3 Next.

Agile / DevSecOps

NC3 Next will be a software-intensive system designed to continuously address threat-based requirements. It must be able to incorporate and exploit emerging capabilities while utilizing a trusted software backbone as its foundation. However, DoD's most commonly used legacy *waterfall* software method will not provide the agility to develop and deploy software- intensive systems at the speed of mission needs.[79] The adoption of Agile and DevSecOps methodologies and techniques could be especially useful in the rapid delivery of capabilities and the development of software architectures capable of withstanding evolving requirements and emerging threats. These techniques insert an iterative process with a user integrated approach that races to produce minimally viable products early in the development phase, resulting in the delivery of flexible, resilient, and capable open mission standard architectures.[80] Notwithstanding, while an NC3 Next system could greatly benefit from this novel software development approach, the acquisition ecosystem comprised of policy, culture, organizational structures, and resources, requires substantial improvement.

While Agile and DevSecOps methods may not conform to all developmental software activities, some DoD programs such as the Air Force's Kessel Run, F-22 TACLInk, TACMAN,[81] and the Protected Tactical Enterprise Services (PTES),[82] all suggest today's software development approaches should shift away from the legacy waterfall process towards agile and DevSecOps techniques. These techniques deliver increased success rates in software development, improved quality, and 'speed-to-market' of software products[83] delivering focused solutions and faster innovation.[84] The NC3 enterprise could leverage at-scale Agile processes to develop many of its software-defined infrastructures such as radios, receivers, conference networks, and terminals, where requirements are often independent and managed in a decentralized manner. This would enable iterative and periodic software updates necessary to maintain and refresh capabilities to deliver a competitive advantage over threats and adversaries. The DevSecOps environment broadens the Agile concept by breaking through industry and some of the weapon systems' owners, acquisition, testing, and sustainment silos that have historically divided the people who make the software, from those who test, run, secure and maintain it.[85]

Scrum creators and Agile research authorities have validated that Agile and DevSecOps approaches are more effective and smoother under five distinct conditions: (1) the problem to be solved is complex, (2) solutions are initially unknown, (3) product requirements will most likely change, (4) the work can be modularized, and (5) close collaboration and rapid feedback from the user is possible. These five conditions are commonly found in the software needs for innovative solutions. The NC3 modernization initiative, its future NC3 Next End-to-End system of systems, and the recent stand up of the NEC structure are all clear mandates to innovate. As such, its' system's vital parts and provisions are ripe for an Agile developmental approach. The NC3 Next unstable market environment, its

future solutions' requirements volatility, and the potential for work modularity and partitioning across subsystems, constitute favorable conditions for Agile and DevSecOps methodologies.

An Agile NC3 Next is heavily dependent on an acquisition framework with effective and flexible decision structures and guidance. Currently, the NC3 enterprise organizational structure, and the application of rigid acquisition frameworks within it, are at odds with the need for flexible acquisition governance, and organizational and process agility. In comparison, the new DoD Adaptive Acquisition Framework (AAF) and its associated Software Acquisition pathway, provide greater flexibility to use Agile, and DevSecOps approaches effectively. Through contracts with targeted and tailored Agile provisions, software development increases the responsiveness towards required multi-level interface standards that enable a rapid integration of functions across domains and other acquisition programs.

Supply Chain Implications

Individually maintaining a myriad of unique systems is enormously expensive and complicated as sources evaporate, and technologies become obsolete. With renewed focus by the National Defense Strategy (NDS), the NC3 enterprise has an opportunity to fix its' deteriorating systems and supply chains.

In the next generation of NC3, new architecture and policies must be created to optimize the long-term sustainability of the supply chain. More suppliers must be encouraged to compete in the NC3 market through better government policies aimed at overcoming the barriers and costs associated with classified work. Additionally, NC3 modernization success and avoiding problems like those faced now, will require standardization of an upgradable architecture and expansion of the supplier base through focused government policies.

It wasn't until 2019 that 8-inch floppy disks at the Air Force's ICBM sites were finally upgraded to a solid state device.[86] Companies stopped manufacturing 8 inch floppy disks in the 1980s.[87] Many of the computers involved in powering the current NC3 system similarly originate from the 1970s and 1980s. In another example, Boeing no longer produces the E-4B communications platform (747 Airframe) that started flying in the 1970s. Most of the current system remains analog while the world completely transitioned to digital more than a decade ago. As sources and supplies dry up, NC3 barely survives on life support.

The NC3 enterprise heavily depends on a few major defense contractors who maintain a near monopoly in their niche. Raytheon controls almost all AEHF transmission technology, and Rockwell Collins has no competition on VLF transmissions. General Dynamics cornered the market on the hardware command and control functions of NC3. With the merger of Raytheon and United Technologies, most of the hardware (transmitters, antennae, receivers, etc.) will be produced by only one company. This lack of diversity makes the NC3 supply chain vulnerable to a major disruption. If United Technologies divests its NC3 mission or

experiences a major disruption (financial, natural disaster, cyber breach), then the mission risks failure with the loss of the supply of equipment and support for a significant portion of NC3. The supplier base needs to expand to ensure resiliency of the supply chain.

Industrial Security Implications

Government policies and regulations that drive NC3 industrial security can have a negative impact on operating costs and innovation in the NC3 industry. Additionally, the current NC3 industrial security environment is one with high threats and high vulnerability, but without sound risk mitigation and countermeasures. The result is a fragmented security apparatus, incongruous defensive systems, and ill-suited means to correct them both.

To sustain the foundation of deterrence, the US cannot allow any compromise of its NC3 architecture. Given the criticality of preventing compromise, the US government has promulgated industrial security policy and regulations to protect the enterprise. Policy dictates DoD components and the Defense Counterintelligence and Security Agency (DCSA) will provide counter intelligence (CI) and security support to the NC3 enterprise.[90] These entities will assign CI and security support to NC3 systems based on component "ownership" (e.g., the Air Force Office of Special Investigations {AFOSI} will provide support for Air Force systems.[91]) To amplify these protective actions, the government requires industrial partners comply with security regulations by way of specific contractual terms.[92]

While policy and regulation seek to protect a critical government interest, they have a negative impact on industry. To comply, industry partners must hire additional personnel and implement costly security measures such as construction of Sensitive Compartmented Information Facilities (SCIFs). Increased costs and corporate expertise gained through experience dealing with burdensome security regulations serve as barriers to market entry and firms outside the market face significant capital investment requirements to compete for NC3 contracts, particularly due to meeting security requirements for SCIF space and classified information technology systems. As a result, prospective entrants will choose not to enter the market, which will in turn reduce the potential for both innovation and place upward pressure on overall market prices.

Though multiple models exist to characterize industrial security, they all converge to focus on the threat itself, vulnerabilities (i.e., susceptibility to attack), and risk management and countermeasure capacity.[93] America's adversaries make the NC3 enterprise a top priority, so the threat against it is high. Foreign intelligence entities (FIEs) seek to both penetrate NC3 systems and to understand American plans and intentions.[94] Another adversary objective is to obtain US NC3 vulnerability and counter-vulnerability data to "leap-frog" ahead of US defensive measures.[95] By achieving these objectives, US adversaries can cast doubt in the minds of American decision-makers about the credibility and assurance of US NC3 systems and, in the

extreme, prevent the US from achieving its goals in a nuclear conflict.

Compounding the priority problem are robust adversary capabilities to attack the US NC3 enterprise. US adversaries possess incredibly sophisticated open source intelligence collection capabilities that thoroughly exploit America's democratic openness. They collect and analyze in detail openly available information such as documents and postings about congressional defense authorizations and appropriations, US military and intelligence world-views and capabilities, research and development plans for US weapon systems, and DIB patents and programs.[96] With library-like indexing, retrieval, and automated search capabilities, adversary intelligence analysts are capable of strategic, comprehensive research.[97] US adversary cyber collection operations significantly supplement open source collection operations. The goal of these operations is to steal trade secrets, intellectual property, new technology, and defense contractors and government agencies are prime targets.[98] Top US adversaries, particularly Russia and China, also have robust human intelligence operation capabilities, both overt and clandestine. Given the high priority adversaries place on the US NC3 enterprise, and their robust capabilities to attack it, the threat is critically high.

The NC3 enterprise is vulnerable to this critically high threat because a protective, holistic view of the enterprise does not exist as responsible security organizations are stove-piped, defensive systems are incongruous, and synergistic enterprise capabilities to defeat the threat are poor. There is no enterprise-level apparatus with a holistic view of potential threats to or actual attacks against the US NC3 enterprise because they are all stove-piped within themselves. The same is true for cyber defense and insider threat systems as US NC3 partners use their own individual systems. These systems do not connect to each other and do not incorporate specific adversary intentions or tactics. Without an understanding of adversary targets, methods, and priorities, one can best characterize these systems as perimeter defense.[99]

Completing the industrial security model is risk management and countermeasure capabilities. Across research engagements, US NC3 partners vocalized a lack of CI support. With one exception, entities did not receive tailored training or threat advisements. They did not have cyber-specific CI analysis. They did not have incident reporting systems that could trigger CI investigations. The capacity to conduct CI investigations with a US NC3 enterprise-wide view does not exist, nor does the ability to conduct offensive CI operations. On balance, large seams exist across the US NC3 enterprise in terms of detecting, responding to, and neutralizing adversary threats to industrial security. This is particularly noteworthy given that the beginning point of an NC3, 50-plus year modernization program is the perfect time for adversaries to exploit these seams. To remedy this poorly equipped industrial security apparatus, the United States should create a subsidy-based solution and a dedicated CI and security capability to protect the NC3 enterprise in its entirety.

Human Capital Implications

People are the government's most significant asset, which is emphasized in the strategic goals of the President's Management Agenda (PMA), NDS, and National Security Strategy (NSS). The DoD needs to attract and retain top technical talent to support modernization and the next generation of the NC3. DoD competes against industry for highly sought-after disciplines to include engineering, computer science, data analytics, and emerging technologies. As such, DoD needs innovative recruitment and retention programs.

The civilian workforce supporting NC3 is aging, and a new generation needs significant training to replace retirees. In 2018, only 6% of the civilian workforce was in its 20s compared to 21% in the private sector.[102] The NC3 field consists of a limited number of experts, and most are considered "gray beards" who have already retired or will do so in the imminent future. There is a recognized talent shortfall for STEM labor across the nation and an overall shortage of human capital in the federal government. Most graduate students are foreign nationals who cannot work in NC3 programs, while US citizens typically do not pursue graduate degrees due to lucrative salary offers from industry.[103] This issue is compounded further by increasing globalization and a diminishing domestic manufacturing sector, which significantly limits US capabilities and expertise.[104] "The Contest for Innovation: Strengthening America's National Security Innovation Base in an Era of Strategic Competition," generated by the Ronald Reagan Institute concludes that an insufficient supply of STEM skills creates inherent risk, from a decline in production capacity to decreased innovation.[105] The severity of the issue has been recognized by the President and Congress and resulted in creation of a 2019 strategic plan for STEM education released by the White House titled, "Charting a Course for Success: America's Strategy for Stem Education."[106] Other policy responses include an Executive Order on "America's Cybersecurity Workforce" being issued in May 2019 and the House Committee on Oversight and Reform conducting a Hearing entitled "NextGen Feds: Recruiting the Next Generation of Public Servants" in September 2019.

The defense ecosystem is reliant on STEM knowledge and core trade skills to ensure a comprehensive approach to nuclear deterrence. Even individuals with these qualifications will need a Top- Secret clearance, possibly with Special Access Program caveats, and either have NC3 experience or receive training in this niche discipline. To ensure this no-fail mission succeeds, the government will need to develop private and public partnerships and collaborate with industry and academia, to include FFRDCs and UARCs to develop robust solutions to protect the American people at home and abroad.

The Civil Service System has not been updated since it was established approximately 40 years ago, resulting in obsolete policies and job classifications that

focus on compliance and transaction management rather than results and customer service.[107] According to OPM, it takes an average of 98 days to hire someone without a security clearance.[108] Although the backlog of security investigations has declined since the standup of the Defense Counterintelligence and Security Agency, and initial Top-Secret clearances for the DoD industry averaged 289 days during the fourth quarter of FY 19,[109] there is still plenty of room for improvement. Job seekers are not willing to wait 10-months to begin work when there are plenty of private-sector positions that can bring them on board within days. In addition, the federal government typically lags 31% behind the private sector concerning pay, and there are more significant discrepancies for high demand markets such as cybersecurity.[110] The human capital market is highly competitive, and the government must take advantage of lessons learned and best industry practices to attract the best and brightest. The government already acknowledges that its employees are its greatest asset, so it must introduce new approaches to attract, hire, develop, and retain employees. Human capital must be a key part of agency strategic plans to ensure that the DoD identifies the appropriate talent needs of the future and has mechanisms in place to attain those skills.

The ability to attract, develop and retain top technical talent is imperative to successfully transition NC3 to the next generation. DoD will need a diverse workforce that has an inclusive culture to generate innovative enterprise solutions. The government will be competing against other industries to attract talent that is in short supply to include cybersecurity, quantum computing, microelectronics, and hypersonics. To win its share of this competition, the DoD must distinguish itself and the opportunity it provides by marketing its unique mission and US national security contribution.

V. Recommendations

1. Define the Desired Architecture

In order to maintain current technological advantages, and move beyond the current NC3 system, USSTRATCOM must define the desired NC3 Next Gen architecture, and identify which existing systems can be modernized in order to prioritize rapid development and fielding.

A. Collaborate with Government-Funded Agencies

DoD and industry partners must collaborate with UARCs and FFRDCs to prioritize efforts that focus on the most important technology areas for NC3. The NC3 system is uniquely dependent on these organizations due to security classification requirements and niche technologies that do not have significant commercial applications (i.e., nuclear weapons, AEHF comms). Many of the FFRDCs and UARCs are well connected with industry and ease successful transitions from R&D to production of military capabilities.

B. Create a High-Level Roadmap and Digital Engineering Platform

The NC3 system would benefit from an End-to-End Digital Engineering Platform (NC3 High-Level Roadmap). This platform should be obtained and developed through risk reduction efforts leading up to the manufacturing and development phase(s) of smaller projects or platforms. The NEC could compete an Advanced Concept Technology Demonstration (ACTD) contract for industry to develop a Model-Based Systems Engineering (MBSE) and Digital Engineering Platform (DEP) for NC3 Next Gen. This DEP would serve as a digital ecosystem for the NC3 enterprise that could be used to prototype and validate concepts prior to development. Utilizing the roadmap and DEP concepts enables a strategic outlook on the NC3 enterprise, clarifies the business environment, and ensures new projects are relevant and effective prior to production.

C. Incorporate Modularity

The NEC must incorporate modularity into original design concepts so the next generation of NC3 is adaptable to the changing threat environment and emerging technologies. It is reasonable to assume that the next generation architecture will be expected to endure for at least thirty years. Long lifespans will require modular components that can be easily replaced as newer technologies emerge. Additionally, greater modularity will improve interoperability between systems per 2018 NDS priorities. The concept is also woven into the recently released Adaptive Acquisition Framework (AAF) process that emphasized the need for speed of delivery, continuous adaptation, and frequent modular upgrades.

D. Solicit Threat-Based Research

USSTRATCOM should update and re-release its' Nov 2018 *Next Generation NC3 Enterprise Challenge* to solicit white papers from industry partners and academia that focus on the evolution of Russia and China's future strategic positioning and specifically address unconventional threats and how to counter them.[111] At a minimum, white-paper inputs should address three subjects:

- Theorize Russia and China's "strategic game board" in the 2040-2080 timeframe. How do Russia and China expect to maintain an asymmetric advantage and exploit the NC3 weapons system?
- Hypothesize Russian and Chinese technological developments, doctrinal changes, and political commitments necessary for Russia and China to retain their strategic advantage.

- Provide technological, doctrinal, and/or policy recommendations necessary to evolve the next generation NC3 enterprise to disrupt Russian and Chinese innovation.

E. Form a Threat Monitoring Advisory Committee

Form an advisory committee comprised of organizations that provide the most comprehensive threat analysis. This committee would serve as a bridge between USSTRATCOM, FFRDCs, UARCs, and industry. It will also provide an impetus for firms to continue investing Independent Research and Development funds into their internal NC3 business segments; a process in danger of disappearing without a clear long-term DoD plan. This solicitation, and USSTRATCOM's commitment to taking results-based action, will reinvigorate leaders within NC3 business segments and provide a much-needed intellectual catalyst for addressing future threats.

2. Communicate a Clear Demand Signal

There is a clear need for both modernization and new development in the NC3 system of systems. Defining what that is and communicating that to the DIB, has been an obstacle in implementing the 2017 NSS and the 2018 NDS.

A. Articulate the Modernization Plan

Throughout multiple discussions with defense companies and government agencies, there was one consistent message: DoD must inform the DIB of its plan for modernizing the existing system as well as illustrate its concept for NC3 Next Gen. The lack of clear requirements has caused industry paralysis with respect to action, innovation, and R&D. In addition, current mechanisms do not exist which enable the NEC to actively solicit inputs from industry unless existing points of contact are known, contracts are already in place, or traditional contracting announcement processes are continuously monitored by companies.[112] This lack of communication creates an "apparent lack of demand" and must be rectified.

B. Provide Appropriate NEC Manpower

If the DoD is serious about NC3 modernization then it needs to start treating the NEC as its' charter states, "to design the next-generation NC3 architecture."[113] This begins with appropriately manning the NEC with high quality expertise of all ages. Through in-field and in-class interactions with government and industry stakeholders, it was apparent they are not fully aware of what the NC3 modernization need is or what their role might be in meeting it. Providing this human capital will give the NEC the expertise needed to get traction and structure development, project planning, and manning requirements. It also allows for time to

outline a plan and determine the manpower needs to fully staff the NEC for long term success.

C. Begin Execution Short of the 100% Solution

Critical to the success of communicating a demand signal is accepting that the 100% solution may not be attainable, affordable, or complete within a reasonable timeline. The NEC must consider that a less perfect solution, which *is* attainable, affordable and within a reasonable timeline, is likely better than the status quo. The NEC has been working on developing a plan for NC3 Next Gen while concurrently trying to modernize the current architecture. Despite modest gains, progress is insufficient to the task. With experts throughout government working together on a single executable solution, ideas can be shared, resources pooled, duplication of efforts eliminated, risks of cutting off good ideas can be mitigated, and a quicker path to an acceptable solution can be achieved.

D. Identify and Exploit Disruptive Technologies

A critical advantage of the NEC is the ability to identify the best of "mature" and "longshot" emerging technologies. Furthermore, it is important to determine how to apply them across the enterprise. Doing this over the life of the system requires a process and an organization to support it. Deloitte consultants, Krawiec and Holden, have a process for identifying new disrupting technologies and applying them to an organization's mission. Their process has seven key steps: (1) horizon scanning, (2) use case identification, (3) selection of technology, (4) scenario planning, (5) business case development, (6) use case selection, and (7) deployment.[114] There are emerging technology areas where the government has no choice but to be a first mover (i.e. hypersonic weapons, electromagnetic spectrum dominance), but there are also dual use technologies (i.e. cyber security, blockchain) that present opportunities to act as a fast follower and reduce R&D expenses. In either case, selecting and deploying emerging technology requires leadership, organizational support, DIB partnerships, and an effective process to make it happen.

3. Incentivize the Industrial and Innovation Bases

An ecosystem exists to support the NC3 innovation and industrial bases however, the government does not fully exploit the potential within them due to policy constraints. These barriers must be removed to reach full market and innovative capacity.

A. Increase annual Science Technology and Education (STE) allocations at FFRDCs.

Congress restricts the number of STE allocations to FFRDCs which has resulted in them routinely turning away quality applicants and impactful work. However, UARCs are not bound to the same constraint. Creating consistency between the two federally funded agencies by removing this congressional restriction would allow the organizations to continue to bring in new talent to support the NC3 enterprise. Some private vendors, as well as their government representatives, may feel that FFRDCs are competitors. However, using them for more basic and applied research, while prioritizing development for vendors, may alleviate this concern.

B. Create and Subsidize Secure Small Business Centers

Most small businesses do not have the resources or expertise to attain facility clearances to perform classified work. One industry partner this industry study met with estimated that upgrading office space to comply with Special Access Program (SAP) requirements costs approximately $5 million.[115] Smaller suppliers and contractors cannot afford meeting facility security requirements and have little financial incentive for such an investment. A solution to promote small sized supplier and contractor participation in NC3 is to create DoD-owned secure facilities designated for small businesses supporting critical work. Constructing facilities around existing NC3 and communication equipment clusters (such as near Boston, MA), would enable more companies to compete and contribute and provide a larger human capital pool for all agencies involved. Establishing these small-business-focused secure work centers will require additional funding and infrastructure; therefore, the DoD must prioritize congressional advocacy for the effort.

C. Leverage Mutually Beneficial Relationships

The DoD needs innovative technology to bolster NC3, and industry needs to raise capital to develop emerging technology. Both can use each other's needs and comparative advantages for mutual gain. The DoD can initiate this partnership by: (1) offering non-dilutive financial support that does not require taking an equity stake in the company, (2) sharing resources such as classified facilities, test ranges, and datasets, (3) accelerating the 3-5 year patent application process to less than a year by labeling the application a "national security priority," and (4) serving as an early adopter for a product, providing a "government seal of approval," and giving businesses a "leg up" on the commercial market.[116]

D. Create Interoperability Within Programs

Leverage dual use functions to expand the supplier base. DoD designed the current NC3 architecture as largely segregated from all other

communication systems due to the need for hardened thin line communications and its special mission. If a new NC3 architecture incorporates dual use functions such as Joint All Domain Command and Control (JADC2) into the design, the sustainability of the supply chain would significantly increase. The NC3 enterprise would benefit from a diversification of suppliers, economies of scale, and the ability to leverage multiple systems to send Emergency Action Messages. Pursuing dual-use technologies lessens the likelihood that any single supplier failure would lead to NC3 mission failure. As dual use technologies and platforms evolve, linked NC3 systems will automatically be upgraded, possibly without the need for extra NC3-specific funding or attention.

4. Create Effective Governance and Acquisition Agility

The DoD acquisition structure supporting NC3 is complex and stove piped. Historically, NC3 has been viewed as a stand-alone capability operating on dedicated equipment. Additionally, most of the PEOs responsible for NC3 acquisitions are not focused on NC3; they are PEOs for other functions with only the JCIDS process and acquisition officials providing a clear integrating function among them. Furthermore, while the NC3 scope of this paper precludes an in-depth examination of JADC2 and the NLCC, it concludes that NC2 is a function of the NLCC, and that nuclear forces must be a component of JADC2. For the US to make the most efficient investment in these functions and networks, the DoD must consider inter-relationships between them and more clearly define and document their interfaces and dependencies.

A. Designate a JADC2 Enterprise Lead and Integrate with NC3

DoD should designate a JADC2 enterprise lead, define a clear governance structure for JADC2, as well as, between the JADC2 and NC3 sensor/communication/weapon networks. At the same time, it should develop a plan to integrate JADC2 and NC3. Given the inherent joint world-wide integrating nature of JADC2, the lead for this enterprise should be a joint leader with world-wide responsibility in all-domain operations. The Vice-CJCS may be the best candidate for this effort because of that position's joint all-domain nature and connection with NLCC governance. Finally, the governance structure should nest NC3 as a subset of JADC2.

B. Integrate NC3 Acquisition Under One PEO for Each Service

The mechanisms of NC3 acquisition used by the Air Force and Navy employ multiple PEOs and dozens of program offices without clear integrating functions. This multiplicity exacerbates the difficulty in developing, acquiring, and implementing efficient, affordable, and

seamlessly integrated NC3 capabilities and complicates NEC coordination activity with the services. As such, the Air Force and Navy should integrate NC3 acquisition under one PEO for each service. The Air Force designated the Nuclear Weapons Center NC3 Integration Director as the "principal integrator" for the Air Force's AN/USQ-255 NC3 weapon system and that office is the best candidate for a single AF NC3 PEO. The Navy's best candidate is its Strategic Systems Program (SSP) office which executes acquisition for the TRIDENT II Strategic Weapons System.

C. Establish Component Acquisition Executive (CAE) Responsibilities within USSTRATCOM Staff

While the NEC is tasked with creating the blueprint for a modernized NC3 system, it does not have acquisition authority to procure it. As a result, all purchases must be managed by the individual services and their acquisition distributed organizations. This is a fundamental flaw in the current construct and one that defeats the proposed benefits of a singular leadership authority bestowed upon the STRATCOM commander. To resolve this issue, the NEC should be given authority to direct the services what to acquire for future NC3 modernization activities. An example of this construct currently exists within Special Operations Command (SOCOM). STRATCOM staff could assume Component Acquisition Executive (CAE) responsibilities specific to NC3. This would allow the NEC direct access to the CAE thereby allowing it to negotiate memoranda of agreement with the military services to acquire equipment, material and supplies to facilitate its NC3 concept. This would solidify the NEC's ownership of NC3 and give its' parent command the authority to direct service acquisitions.

D. Adopt Agile and DevSecOps Methodologies

The adoption of Agile and DevSecOps methodologies is vital to the rapid delivery and development of adaptive NC3 software capabilities. These techniques insert an iterative process with a user integrated approach that races to produce minimally viable products for rapid integration. Given the decentralized nature of NC3 acquisition and sustainment activities, a DevSecOps Joint User Experts' Team is recommended. The NEC should resource a NC3 DevSecOps integrated product team (IPT) of Joint-User experts across the multiple NC3 platforms and commodities. These dedicated NC3 resources, while distributed across the different acquisition and sustainment organizations, would be DevSecOps trained and intricately linked to NC3 software development efforts via digital platforms and tools. Budgets for intensive and continuous Agile and DevSecOps training and expertise development must also be included.

Finally, workforce resourcing should be planned and funded by the NEC, and negotiated with the involved acquisition organizations, well in advance of any NC3 DevSecOps program initiation.

5. Mitigate Industry Security Clearance/Facility Challenges

Participation and collaboration in the NC3 enterprise is limited by the stringent security environment in terms of access to information and clearances for personnel and facilities.

A. Expedite Security Clearances for Personnel Supporting NC3

Although the backlog of security investigations has declined since the standup of the Defense Counterintelligence and Security Agency (DCSA), there is still plenty of room for improvement. For example, initial top-secret clearances for the DoD industry averaged 289 days during the fourth quarter of FY 19.[117] Many NC3 clearances require even more time. A solution could include DCSA adoption of a new policy that expedites clearances for government and industry personnel involved with NDS priorities such as NC3. Another option is to apply data analytics to determine risk factors and streamline the process accordingly. If suppliers are guaranteed timely and predictable clearance adjudications, they will be more likely to compete in the NC3 space.

B. Adjust Classification Status to Lowest Level of Acceptable Risk

The Top Secret and Special Access Program classification levels create significant barriers to entry for most firms. To widen the potential supplier base, the DoD should actively pursue acquisition of equipment and material at the lowest possible classification level. The DoD should perform risk and classification assessments of individual systems and pursue proper acquisition channels to maximize suppliers and subsequent competition. As an example, according to IBISWorld, as of 2020, there were 714 communication equipment manufacturers in the U.S.[118] If DoD designates a blanket Top Secret / Special Access Program acquisition strategy across NC3 Next Gen, then only a handful of those companies will contribute to NC3.

C. Develop a Cloud-Like Classified Network

While industrial security policies seek to protect critical government interests, they have a negative impact on industry. In order to comply with such policies, industry partners must implement costly security measures such as construction of SCIFs and classified networks. Firms outside the market face significant capital investment requirements to compete for NC3 contracts, particularly in terms of meeting security requirements for SCIF

space and classified information technology systems. As a result, prospective entrants will choose not to enter the market. To reverse these trends, the government should develop a cloud-like classified network that NC3 partners can use. In addition to increasing the potential for innovation by opening the number of partners with access to a classified network, the government would be better positioned to monitor the security of a single network as opposed to the disparate ones currently in use.

VI. Conclusion

NC3 Modernization needs a jump start. The 2018 NDS outlines modernization priorities and the nuclear triad, to include NC3, is the first area addressed under the increase lethality priority. This prioritization is heavily influenced by emerging threats posed by great power competitors, antiquation and failings of the legacy system, rising sustainment costs, and the chance to harness powerful new technologies and processes. STRATCOM has been designated the operational lead for NC3 and billions of dollars are budgeted to support NC3 modernization. Despite senior leadership support and resourcing, progress to modernize NC3 has been painfully slow. This is not without reason. STRATCOM leaders face some daunting challenges: technical complexity, culture clashes, a lean DIB and innovation base with high barriers to entry, supply chain and human capital challenges, as well as delays from acquisitions and C2 entanglement (JADC2/NLCC).

As history has proven, wicked problems like modernizing NC3 can be effectively solved when the *triple helix* is employed. *The triple helix is* where the government, industry, and academia collaborate to promote and sustain creative thinking in an innovation ecosystem. The 2020 Eisenhower School NC3 Industry Studies team concluded that significant effort should be applied to improving the triple helix for NC3 and provided five series of recommendations for doing that. To jump-start an integrated modernization process for NC3, STRATCOM NEC must define the desired architecture for the next generation NC3 system. Once defined, STRATCOM should create a strong demand signal that clearly communicates requirements for NC3 to the triple helix. That alone will drive action but incentivizing the DIB and innovation base to meet those requirements, and mitigating acquisitions and security challenges will deliver faster results.

If we expect nuclear deterrence to be a cornerstone of strategic security in the future, as it has been for most of the last 70 years, decisive action is required to modernize the nation's NC3 system.

APPENDIX A: Definitions

Governance. The process by which an organization safeguards the interests of its stakeholders. The governance process ensures accountability, fairness, and transparency and provides a system of checks and balances that is a combination of those with associated and distributed responsibility to verify its proper execution. (CJCSI 3280.01C)

Nuclear Command and Control (NC2). The exercise of authority and direction by the President, as Commander-in-Chief of the U.S. Armed Forces, through established national command authority lines over nuclear weapons, nuclear weapon systems, and nuclear weapon operations of military forces. (Source: *Presidential Policy Directive (PPD)-35*)

NC2 mission essential functions (Source: Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6811.01C, *Nuclear Command and Control System Technical Performance Criteria*):

- **Force Management**. Force Management is the set of Command, Control, and Communications (C3) activities relating to the assignment, training, deployment, maintenance, and logistic support of nuclear forces and weapons, before, during, and after any crisis.

- **Planning**. Planning is the set of C3 activities relating to the development and modification of plans for employment of nuclear weapons and other operations in support of nuclear employment

- **Situation Monitoring**. Situation Monitoring is the set of C3 activities relating to the collection, maintenance, assessment, and dissemination of information on friendly forces; adversary forces and possible targets; emerging nuclear powers; and military, political, environmental, and other events.

- **Decision Making**. Decision Making is the set of C3 activities relating to the assessment, review, and consultation regarding consideration for use or movement of nuclear weapons or the execution of other nuclear control orders.

- **Force Direction**. Force Direction is the set of C3 activities relating to the implementation (preparation, dissemination, and authentication) of decisions regarding the execution, termination, destruction, and disablement of nuclear weapons.

Nuclear Command and Control System (NCCS). The Nuclear Command and Control System is the combination of capabilities necessary to ensure the authorized employment and termination of nuclear weapon operations under all threats and scenarios; to secure against accidental, inadvertent, or unauthorized access to U.S. nuclear weapons; and to prevent loss of control, theft, or unauthorized use of U.S. nuclear weapons. Collectively, these capabilities help ensure the effectiveness of the U.S. nuclear deterrent. (Source: PPD-35)

Nuclear Command, Control, and Communications (NC3). The means through which Presidential authority is exercised and operational command and control over U.S. nuclear forces is conducted. The NC3 system is part of the larger NLCC, which encompasses the three broad mission areas of: (1) Presidential and senior leader communications; (2) NC3); and (3) continuity of operations and continuity of government communications. Facilities, equipment, communications, procedures, and personnel that enable presidential nuclear direction to be carried out. (DoDD S-5210.81)

NC3 System. The NC3 System is the means through which Presidential authority is exercised and operational command and control of nuclear operations is conducted. The NC3 System is part of the larger National Leadership Command Capability (NLCC), which encompasses the three broad mission

areas of: (1) Presidential and senior leader communications; (2) NC3; and (3) continuity of operations and continuity of government communications. (Sources: PPD-35 and DoDI S-3730.01, *Nuclear Command, Control, and Communications (NC3) System*, see sources for the full, classified definition)

NC3 Architecture

The NC3 system is a large and complex system of systems comprised of numerous terrestrial, airborne, and space-based components used to assure connectivity between the President and nuclear forces. The current NC3 architecture consists of systems that support day-to-day nuclear and conventional operations prior to a nuclear event, as well as those systems that are to provide survivable, secure, and enduring communications through all threat environments.

NC3 Enterprise Center (NEC)

Oversees and manages NC3 operations, maintaining enterprise-wide visibility, assessing comprehensive operational and technical risk, and—with NC3 stakeholders' participation—develops and advocates future capabilities, risk management options, and prioritization recommendations. The NEC acts as the heart of the NC3 enterprise, which has the primary goal of focusing on restructuring situation monitoring, decision-making, force direction, force management and planning for NC3.

National Leadership Command Capability (NLCC). A capability encompassing the entirety of the DoD command, control, communications, computer, intelligence, surveillance, and reconnaissance systems and services that provides national leadership, regardless of location and environment, with diverse and assured access to integrated, accurate, and timely data, information, intelligence, communications, services, situational awareness, and warnings and indications from which planning and decision-making activities can be initiated, executed, and monitored. This capability includes appropriate interagency contributions as agreed to. (DoDI 3710.01)

National Military Command System (NMCS). The NMCS provides senior leaders with assured access to a secure and collaborative information environment that enables situational awareness, course of action development, national-level decision-making, force execution, and monitoring across the range of military operations. CJCSI 3280.01D, *National Military Command System*, identifies the five NC2 Mission Essential Functions as five of the six Mission Essential Tasks supporting the NMCS mission essential function "continuous, survivable, and secure NC2". (Source: CJCSI 3280.01D)

Thick-Line Communications

The first layer is the day-to-day and crisis architecture, which can also be described as a "thick-line." This architecture supports current U.S. national policy in that it responds under all conditions in both peacetime and war to provide the means to exercise positive control and direction by the President, the Secretary of Defense, and Combatant Commanders; provides secure, reliable, immediate, and continuous access to the President; and provides robust command and control over nuclear and supporting government operations. (NMHB)

APPENDIX A: Definitions

Thin-Line Communications

The second layer provides the survivable, secure, and enduring architecture known as the "thin-line." The thin-line responds to policy that requires assured, unbroken, redundant, survivable, secure, and enduring connectivity to and among the President, the Secretary of Defense, the CJCS, and the designated commanders through all threat environments to perform all necessary NC2 functions. The thin-line NC3 architecture must be sustained and supported during any modernization effort to ensure presidential requirements can be met. (NMHB)

APPENDIX B: Industry Analysis Firm Briefs: GENERAL DYNAMICS

GENERAL DYNAMICS

Firm Brief

NC3 Industry Study (Seminar 14):
Eisenhower School for National Security
and Resource Strategy
17 March 2020

Firm Brief Team: Tod Marchand, Robert McMurry, Wendy Rhodes, Justin Secrest

0

GENERAL DYNAMICS

Firm Brief Overview

- Story & Profile
- Corporate and Business Strategy
- Key Indicators & Value Creation
- Market Competition
- Strategy Drivers (Porters Diamond)
- Salient Features Affecting Industry
- Human Capital Challenges
- When, Where, and Rivalry
- Supply Chain Issues
- Conclusions and Recommendations

1


General Dynamics Story
Investor Relations
$163.03
General Dynamics creates shareholder value by delivering superior products and services to military, other government and commercial customers.
Secrest
2


Key Event Timeline
ESTABLISHMENT
Incorporated in 1952—targeted aerospace and defense (Electric Boat, Canadair)
1952
Tanks, rockets missiles, submarines, warships, fighters and electronics to DoD
Early 90s
EXPANSION
Bought Gulfstream, combat-vehicle-related businesses, IT product and service companies and additional shipyards (Bath Iron Works)—acquired 19 Firms since mid 1990s
2018
GD
canadair
BIW
CSRA
?
DIVEST TO SURVIVE
Down-turn of defense—divested of everything except military-vehicle and submarine businesses
Mid 90s
Expansion/Diversification
2018: Acquired CSRA for $9.7B—largest acquisition in company history
• Corporate HQ in Reston, VA, significant presence in 14 states, employees in all 50 states, and operates in 70 countries around the world.
• 107,000 Full-time employees (90K in US and 17K abroad).
Secrest

GENERAL DYNAMICS

Strategy

Aerospace | Land Systems | Mission Systems | Marine Systems | Information Technology

Corporate

Business Unit Organization

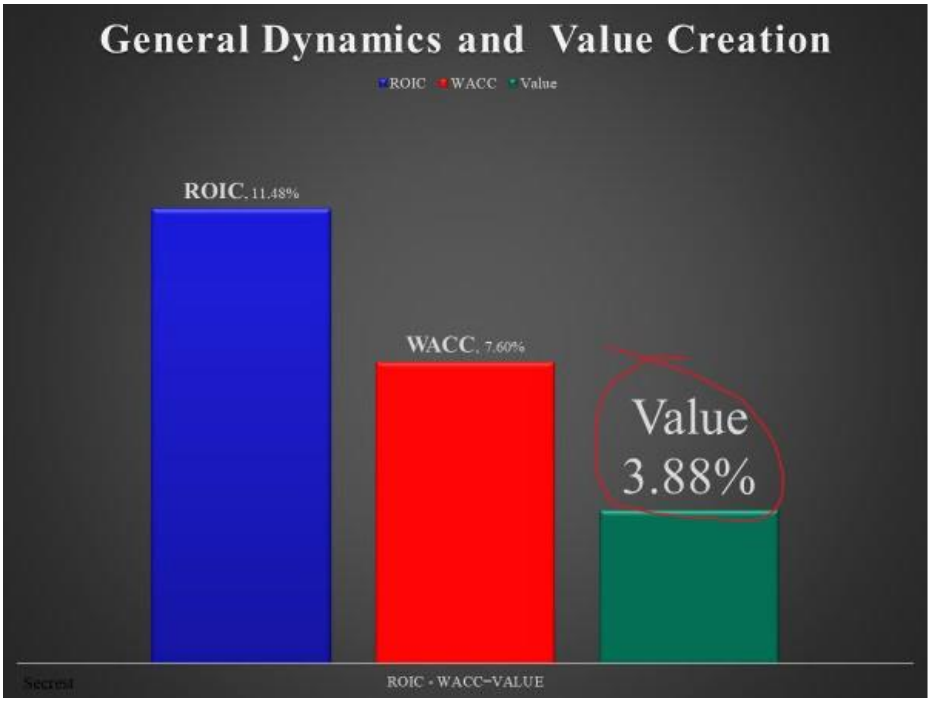
- Leverages strength in Aerospace/Marine units
- Symbiotic Effort with Business Units
- "Boosting return on invested capital and disciplined capital deployment"
  - Partner with a primes to gain value in its smaller segments. (i.e. GBSD)
  - Enduring Value versus chasing "revenue"

Business

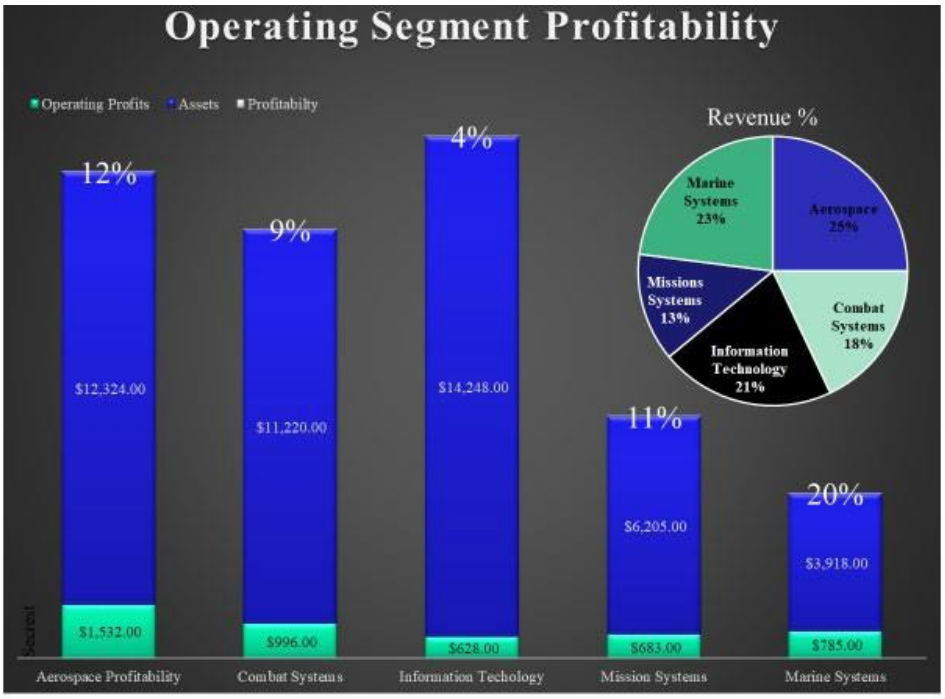
Integrate units and focus portfolios to Demand Conditions

- Centralize Platforms (**Cloud/Data/AI**) while allowing Business unit flexibility
- Great Power Competition customer requirements
- GD "onesources" enables cost competitiveness using GD business units as supply chain platforms.
- Seeking "new game" in IT (CSRA acquisition)
- NextGen and focus on "completions" versus "cost-plus"

Secrest 4



5



6

GENERAL DYNAMICS

Relevant Market(s) Competition

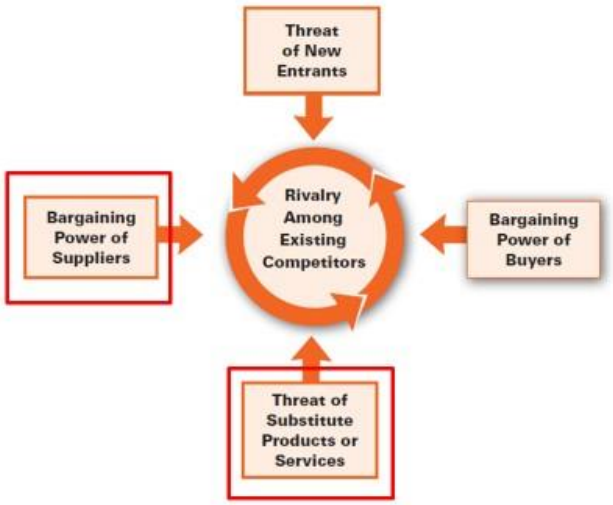
MARKET STRUCTURE				
CHARACTERISTIC	*PERFECT COMPETITION*	*MONOPOLISTIC COMPETITION*	*OLIGOPOLY*	*MONOPOLY*
Number of firms	*Many*	*Many*	*Few*	*One*
Type of product	*Identical*	*Differentiated*	*Identical or differentiated*	*Unique*
Ease of entry	*High*	*High*	*Low*	*Entry blocked*
Examples of industries	• *Wheat* • *Apples*	• *Selling DVDs* • *Restaurants*	• *Manufacturing computers* • *Manufacturing automobiles*	• *First-class mail delivery* • *Tap water*

7

Marchand

GENERAL DYNAMICS

Factors Driving Strategy



8

Marchand

GENERAL DYNAMICS

Salient Forces Affecting Industry

- **Federal Government is Primary Buyer/Revenue Source**
- **DoD Budget Uncertainty**
- **Defense Industry is regulated by the FAR/DFARS**
- **Joint Ventures/Teaming is common due to size and complexity of systems**
- **Future profitability dependent on ability to develop innovative products**
- **Cyber security target by adversaries for intellectual property**

9

Rhodes

GENERAL DYNAMICS

Salient Forces Affecting Industry

- NC3 is a niche market with limited expertise
- Technological Obsolescence/Weapons at end of service life
- Testing and certification is a lengthy process
- New Security Classification Guide

10

Rhodes

GENERAL DYNAMICS

Human Capital Challenges

- Mission Systems employs 13,000 engineering & technical professionals
- Competitive Human Capital Market
  - Aging population/Strong Economy/Low unemployment
  - Lucrative salaries offered by Google, Facebook, & Amazon for technical disciplines
  - More appealing mission such as App development
- Cleared personnel
  - Lengthy security processing
  - Proposed security classification guide increases NC3 to Top Secret/SAP

11

Rhodes

GENERAL DYNAMICS

Human Capital Challenges

- Legacy systems are operating with old software/systems which are only known to Gray Beards
- Generation Z want the ability to work in any place at any time which is not an option for classified programs
- One-fifth of GD's employees are under collective agreements with various labor unions and worker representatives
  - Agreements covering approximately 10% of total employees are due to expire in 2020
- Porter's Five Forces
  - Threat of New Entry
    - Specialized knowledge - Acquisition of companies to acquire talent in emerging technologies

12

Rhodes

GEN GENERAL DYNAMICS

NC3 "Rivalry"

General Dynamics

Raytheon

Boeing

United Technologies

L3 Harris

13

McMurry

GENERAL DYNAMICS

Conclusions

1. GD is dependent on U.S. government contracts
2. Aerospace and Marine Segments are GD's strengths; however, it needs its smaller segments to pick up in order to generate more value and to diversify
3. GD's purchase of CSRA and "new game" appears to be aimed at competing in dynamic information age—it needs it to be
4. GD is set to be a key contributor to U.S. national security needs including NC3—it needs a demand signal.

16

Team

GENERAL DYNAMICS

Recommendations

GD:

1. Provide more "top down" focus on smaller segments (Aero and Marine are dominating) and emphasize to share holders

2. Focus Info Tech on markets outside the govt by leveraging "dual use" technologies

Government:

1. Send a strong Demand Signal—put it in the budget
2. Offer fixed price "as a service" contracts versus cost-plus (stability and cost effectiveness in the eyes of GD)
3. Assist with security in the form of facilities clearances and personnel clearances - especially for small subcontractors/suppliers
4. Eliminate or reduce delays in contract award

17

Team

APPENDIX C: Industry Analysis Firm Briefs: L3HARRIS

Industry Analysis

L3HARRIS™

L3Harris Firm Brief

AY 2019-2020

LTC Tissa Strouse | CDR Adrienne Roseti | Mr. David Tomlinson

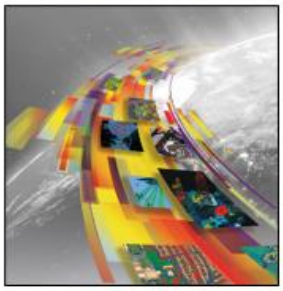
Introduction

- The Firm
- The Market
- The Strategy
- Findings and Recommendations

L3HARRIS™

The Firm: Profile

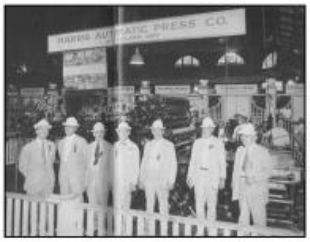
- Technology innovator
- Mission critical communications systems
- Delaware and Florida
  - Over 100 global operating locations
- 18,200 employees (8,000 engineers and scientists)
- Business segments: from 3 to 4
  - Space and Airborne Systems
  - Aviation Systems
  - Communications Systems
  - Integrated Mission Systems



Tomlinson - 2

The Firm: History

- L-3 Communications
- Harris
- Merger
  - Combined innovative capacity
  - Workforce and customers
  - Market focus
  - Challenge primes



Tomlinson - 3

The Firm: Business Values

- Ethics
  - Code of conduct
  - ACT decision-making framework
  - Customer loyalty

Tomlinson - 4

The Firm: Supply & Human Capital

- Supply chain vulnerabilities
  - Industry-wide
  - Tariffs and global economic weaknesses
  - Vertical integration
- Human capital
  - Market sectors
  - Salaries
  - Invention incentive
  - Pension

Tomlinson - 5

The Firm: Financials

Overview	
Total Liabilities:	$6.8B
Current:	$2.3B
Long-Term:	$4.5B
Assets:	$2.6B

Key Ratios	
Debit-Equity Ratio:	2.01
Current Ratio:	1.14
Long-Term Debt/Equity:	0.673

Profit & Cash Flow			
	2019	2018	2017
Profit:	$444M	$808M	$710M
Cash Flow:	$1185M	$751M	$569M

ROIC v. WACC			
	2019	2018	2017
ROIC:	4.12%	12.35%	8.46%
WACC:	6.30%	7.30%	7.90%

Business Segments			
		2019	2018
Communication Systems:	Profit	$499M	$432M
	ROIC	31.90%	27.60%
Electronic Systems:	Profit	$654M	$566M
	ROIC	15.10%	13.60%
Space and Intelligence Systems:	Profit	$359M	$331M
	ROIC	16.30%	15.60%

Tomlinson - 6

The Firm: Financials (Continued)

Key Ratios – L3Harris	
Debit-Equity Ratio:	2.01
Current Ratio:	1.14
Long-Term Debt/Equity:	0.673

Key Ratios – Motorola	
Debit-Equity Ratio:	-8.30
Current Ratio:	3.03
Long-Term Debt/Equity:	-4.14

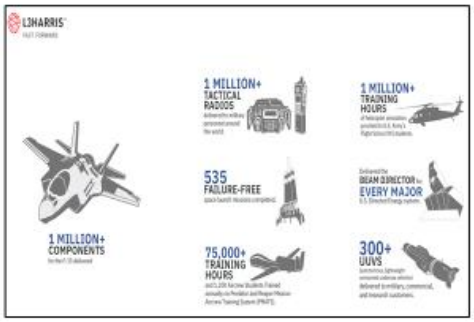
ROIC v. WACC			
	2019	2018	2017
ROIC:	4.12%	12.35%	8.46%
WACC:	6.30%	7.30%	7.90%

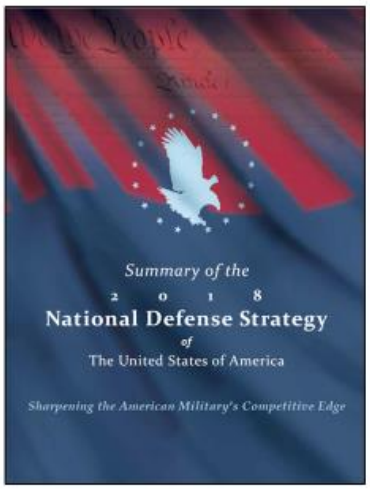
Creating value at an acceptable level of risk

Tomlinson - 7

The Firm: Defense Readiness

- Communications
- C4ISR
- Merger
- Financial position





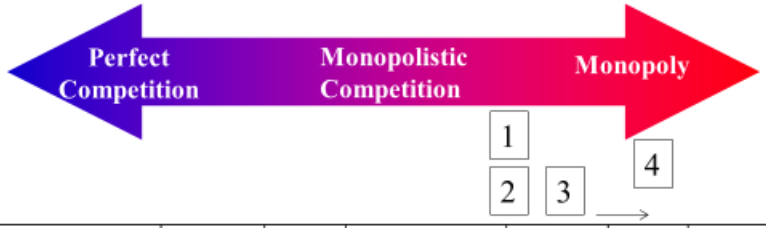
Tomlinson - 8

The Market: Structure

Market	# of Firms	Product	Ease of Entry	Market Structure
Tactical HF/UHF Communications	Few	Differentiated	Low	Oligopoly
Broadband Satellite Communications	Few	Differentiated	Low	Oligopoly
Type 1 Crypto Processors	Few…but Better	Differentiated… but Better	Low	Oligopoly…but Monopoly
Advanced Wave Form Antennas	One	Unique	Blocked	Monopoly

Roseti - 9

The Market: Competitive Spectrum



(1) Tactical HF/UHF Communications	B: Few S: Many	Perfect	Similar but differentiated	Small but Real	↘	Less
(2) Broadband Satellite Communications	B: Many S: Many	Perfect	Similar but differentiated	Small but Real	↘	Efficient
(3) Type 1 Crypto Processors	B: Few S: Few	Perfect	Similar but differentiated	Small but Real	↘	Less
(4) Advanced Wave Form Antennas	B: One S: One	Perfect	Unique	High	↘	Less

Roseti - 10

Industry: Communications

- Favorable: supply-side, switching costs, capital, incumbency, distribution, government policy
- Risk: demand-side

- High competition from new entrants and other defense contractors w/ new tech
- High exit barriers
- Slow industry growth
- Limited product differentiation / high expense for product development
- Lots of rivals from other contractors

- Limited sourcing options
- Technical labor force
- Limited substitutions

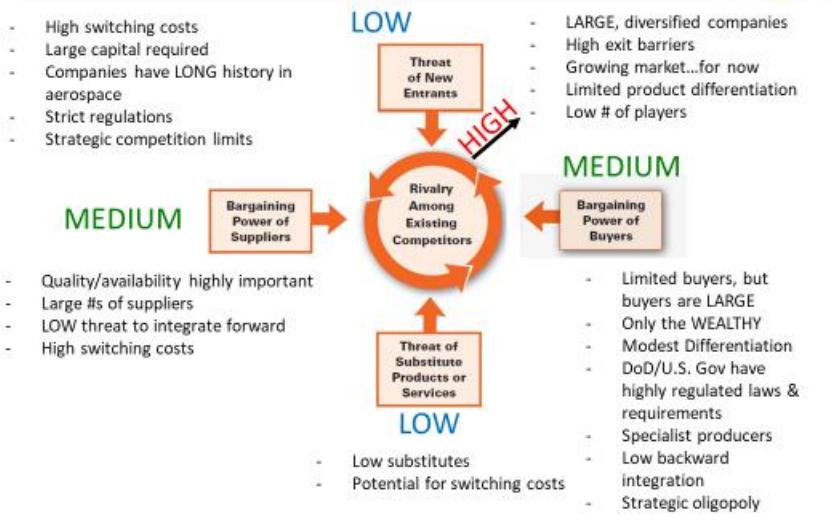
- Intl Sales
- Discounted sales / no price control

- Buyers mostly military
- Required to have competitive bidding processes
- Low threat of integrating backwards
- High price sensitivity
- DoD/U.S. Gov have highly regulated laws & requirements (inspections, security clearances)

- Low substitutes
- Potential for switching costs

Roseti - 11

Industry: Aerospace & Defense



- High switching costs
- Large capital required
- Companies have LONG history in aerospace
- Strict regulations
- Strategic competition limits

- LARGE, diversified companies
- High exit barriers
- Growing market...for now
- Limited product differentiation
- Low # of players

- Quality/availability highly important
- Large #s of suppliers
- LOW threat to integrate forward
- High switching costs

- Limited buyers, but buyers are LARGE
- Only the WEALTHY
- Modest Differentiation
- DoD/U.S. Gov have highly regulated laws & requirements
- Specialist producers
- Low backward integration
- Strategic oligopoly

- Low substitutes
- Potential for switching costs

Roseti - 12

Strategy: Strategic Game Board

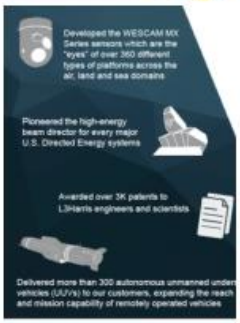
- First Mover – Innovation and Speed
  - "Fast and Forward"
- Differentiation
  - Communications
  - Technologies
  - Organizational Culture
- Competing through Technology and Quality

Strouse - 13

Strategy in Action

- Divesting in Business Segments
  - Airport security
  - 8-10% more
- Research and Development
  - 5% of revenue
- Organizational Culture
- Community Outreach
  - STEM programs K-12
  - $22 million donated

"High-margin, high-growth, technology-differentiated businesses where we can win and generate attractive returns." – L3Harris CEO Brown, Defense News



Strouse - 14

Findings and Recommendations

- L3Harris: successful and creating value in communications
  - As integrator/prime, too soon to tell (positive trend)
- L3Harris well positioned to meet U.S. national security needs
- Capitalize on innovative capability (shift risk of innovation cost from L3Harris to government)
  - Cost-plus contracts
  - Design/development/prototype contracts
- Foreign military sales support
  - Increase demand-side (to drive innovation)
  - "Valley of Death" pass through

Strouse/Roseti/Tomlinson - 15

APPENDIX D: Industry Analysis Firm Briefs: RAYTHEON


FIRM OVERVIEW
INDUSTRY
DEFENSE (69%)
INTERNATIONAL (29%)
BUSINESS SEGMENTS
INTEGRATED DEFENSE
INTELLIGENCE, INFORMATION, SERVICES
MISSILE SYSTEMS
SPACE & AIRBORNE SYSTEMS
FORCEPOINT
Image Source: Raytheon.com
MS. Holly Carey


FIRM OVERVIEW
WHERE WE STARTED
WALTHAM, MA (HQ)
7 ADDITIONAL CONUS
76 TOTAL WORLDWIDE
70,000 EMPLOYEES
RAYTHEON'S CORPORATE CULTURE IS GROUNDED IN ITS COMPANY VALUES:
TRUST, RESPECT, COLLABORATION, INNOVATION AND ACCOUNTABILITY.
Raytheon International, Inc. business development offices
Raytheon International, Inc. business development headquarters
Raytheon Systems Limited
Raytheon Australia Pty. Ltd.
Raytheon Canada Ltd.
Thales Raytheon Systems
Image Source: Raytheon.com
MS. Holly Carey

STRATEGY

- **Broad mix of technologies, domain expertise and key capabilities position Raytheon favorably to grow**
- **Merger with UTC complements Raytheon strategy**

RAYTHEON'S GROWTH STRATEGY

1. **BUILD** ON **AREAS OF STRENGTH** WITHIN OUR KEY MISSION AREAS
2. **FOCUS** ADDITIONAL RESOURCES ON **EMERGING OPPORTUNITIES** WITHIN THE DoD MARKET
3. **EXTEND** RAYTHEON **CYBER SOLUTIONS** TO GOVERNMENT AND COMMERCIAL MARKETS
4. **ENGAGE KEY COUNTRIES** AS INDIVIDUAL MARKETS WITH MULTIPLE CUSTOMERS

NATIONAL DEFENSE STRATEGY INVESTMENT PRIORITIES

- ☑ NUCLEAR FORCES
- ☑ SPACE AND CYBERSPACE AS WARFIGHTING DOMAINS
- ☑ C4ISR
- ☑ MISSILE DEFENSE
- ☑ JOINT LETHALITY IN CONTESTED ENVIRONMENTS
- ☑ FORWARD FORCE MANEUVER AND POSTURE RESILIENCE
- ☑ ADVANCED AUTONOMOUS SYSTEMS
- ☐ RESILIENT AND AGILE LOGISTICS

FUTURE DoD BUDGETS ALIGNED WITH NDS PRIORITIES

DoD BASE BUDGET MODERNIZATION AND RDT&E GROWTH

	FY17	FY18	FY19	FY20
Modernization				
	$1870	$2220	$2290	$2350
% growth	3%	19%	3%	3%
RDT&E				
	$738	$888	$948	$1048
% growth	6%	21%	7%	10%

Image Source: Raytheon.com

MS. Holly Carey

FINANCIAL ANALYSIS

Raytheon	2017	2018	2019
Sales	$25,348M	$27,058M	$29,176M
Operating Expenses	$21,117M	$22,520M	$24,402M
Profit	$4,231M	$4,538M	$4,774M
Share Price	$186.28	$153.35	$219.84
Intelligence, Information and Services ROIC	7%	8%	15%
Missile Systems ROIC	13%	12%	11%
Integrated Defense ROIC	16%	17%	22%
Space and Airborne Systems	19%	13%	13%
Sales	$7,427M	$6,748M	$6,430M
Profit	$991M	$884M	$862M
Raytheon ROIC	14%	14%	14%
WACC	7.1%	9.2%	7.6%
Debt to Equity Ratio	210%	178%	183%
Current Ratio	154%	146%	134%
Long Term Debt to Equity Ratio	136%	106%	103%

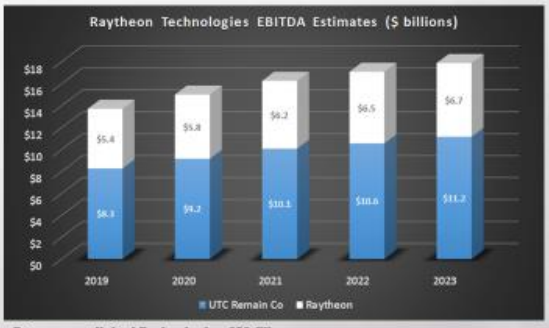
- **THE FIRM IS CREATING VALUE AT AN ACCEPTABLE LEVEL OF FINANCIAL RISK.**
- **THE RELEVANT BUSINESS UNITS ARE CREATING VALUE AT AN ACCEPTABLE LEVEL OF FINANCIAL RISK.**

Mr. Bill Czajkowski

MERGER WITH UTC

United Technologies | Raytheon

- UTC PRAT & WHITNEY AND COLLINS AEROSPACE WILL MERGE WITH RAYTHEON
  - RAYTHEON BECOMES A WHOLLY OWNED SUBSIDIARY OF UTC NOW CALLED RAYTHEON TECHNOLOGIES
  - FOR 2018, THE COMMERCIAL AND MILITARY AEROSPACE SALES FOR UTC WERE 39% AND 14% OF CONSOLIDATED SALES.
- BENEFITS
- RISKS



Data source: United Technologies SEC filings

MS. Holly Carey

PORTER'S FIVE FORCES

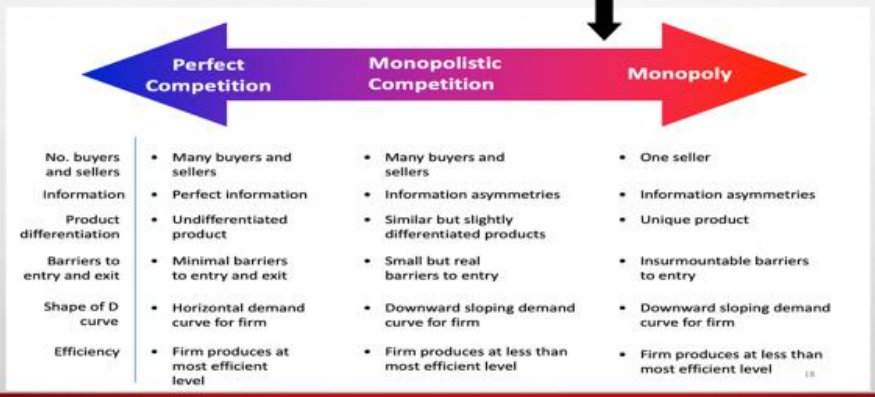
MS. Holly Carey

SPACE AND AIRBORNE SYSTEMS (SAS)

- WHAT DOES THIS HAVE TO DO WITH NC3?
  - EO/IR SENSORS, PRECISION GUIDANCE SYSTEMS, TACTICAL / STRATEGIC COMMUNICATIONS, SPACE QUALIFIED SYSTEMS
- PRINCIPLE PRODUCT LINE
  - INTEGRATED COMMUNICATIONS SYSTEMS (ICS)
    - ADVANCED TACTICAL AND PROTECTED NETWORKING, PROTECTED SITCOM: AEHF, FAB-T, GLOBAL AIRCREW STRATEGIC NETWORK TERMINAL (ASNT)

LT COL Kevin Walsh

BEFORE WE GET CRAZY



	Perfect Competition	Monopolistic Competition	Monopoly
No. buyers and sellers	Many buyers and sellers	Many buyers and sellers	One seller
Information	Perfect information	Information asymmetries	Information asymmetries
Product differentiation	Undifferentiated product	Similar but slightly differentiated products	Unique product
Barriers to entry and exit	Minimal barriers to entry and exit	Small but real barriers to entry	Insurmountable barriers to entry
Shape of D curve	Horizontal demand curve for firm	Downward sloping demand curve for firm	Downward sloping demand curve for firm
Efficiency	Firm produces at most efficient level	Firm produces at less than most efficient level	Firm produces at less than most efficient level

LT. COL Kevin Walsh

BOARD GAMES ARE THE COOLEST

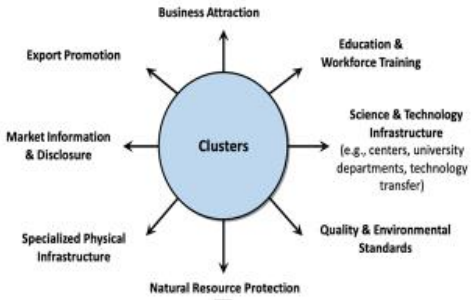
- WHERE / HOW IS RAYTHEON COMPETING WITHIN THE SPACE AND AIRBORNE SYSTEMS MARKET?
  - WHERE:
    - WHEREVER IT WANTS…
    - IN SERVICES WHERE IT HAS A HISTORY OF SUCCESSFUL PRODUCTS
    - WHERE IT RARELY OVERLAPS WITH "COMPETITORS"
  - WHEN:
    - WHEN COMPETING FIRMS FAIL (FAB-T)
    - WHEN A PRODUCT WILL HAVE FOLLOW-ON OPPORTUNITIES
    - WHEN THE R & D WILL BENEFIT OTHER PRODUCTS / IDEAS
- WHERE / HOW IS RAYTHEON COMPETING WITHIN THE SPACE AND AIRBORNE SYSTEMS MARKET?
  - HOW
    - VIA TRADITIONAL RULES – THAT'S WHY RAYTHEON IS RAYTHEON
    - IN RESPONSE TO DOD REQUIREMENTS / REQUESTS
    - PRICE VS. DIFFERENTIATION

Lt COL Kevin Walsh

CLUSTERS

- HQ'D IN MCKINNEY, TX
- 130,000 AEROSPACE WORKERS AT 1,300 ESTABLISHMENTS
- 15 ACTIVE MILITARY BASES
- JOHNSON SPACE CENTER
- TEXAS ENTERPRISE FUND / SPACE X
- BOEING, LM, L-3
- EDUCATED WORKFORCE

Public Policy around Clusters



Clusters provide a framework for organizing the implementation of many public policies and public investments directed at economic development to make them more effective

Business in Texas.com

Lt. COL Kevin Walsh

CLUSTERS

- NEW ENGLAND
- 218,000 JOBS, $17.0 BILLION PAYROLL
- 4,600 FIRMS TIED TO DOD AND DHS

Raytheon

SPACE AND AIRBORNE SYSTEMS

INTEGRATED SENSOR, ELECTRONIC WARFARE AND COMMUNICATION SYSTEMS FOR MILITARY AND CIVIL CUSTOMERS WORLDWIDE

- Applied signal technology
- Electronic warfare systems
- Integrated communication systems
- Intelligence, surveillance and reconnaissance (ISR) systems
- Secure sensor solutions
- Space solutions

RICHARD R. YUSE
President
HQ: McKinney, Texas

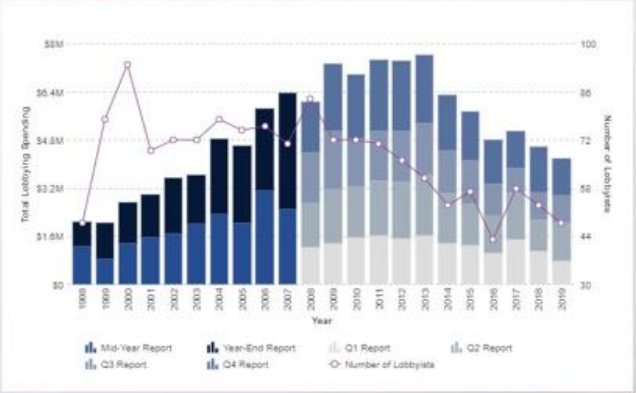
16

UMASS Donahue Institute

Lt. COL Kevin Walsh

SAS COMPETITIVE ADVANTAGE

- LOBBYING
- SAS ACTIVITIES THAT ALIGN WITH RAYTHEON STRATEGY
- INNOVATION
- APPROACH TO CHANGE



Lt. COL Kevin Walsh


PORTER'S DIAMOND
FACEOFF!
RAYTHEON VS LOCKHEED MARTIN
Government
Firm Strategy, Structure, and Rivalry
Factor Conditions
Demand Conditions
Related and Supporting Industries
Chance
Lt. COL Kevin Walsh


SUPPLY CHAIN SECURITY
CMMC, NIST, & DFARS CYBERSECURITY CLAUSE -BASELINE FOR SECURING SUPPLY CHAIN
ANNUAL SUPPLIER CYBER CERTIFICATION
COUNTERFEIT MATERIALS, PARTICULARLY ELECTRONICS, NOT VISUALLY OBVIOUS, TESTING
SUPPLY CHAIN IS VULNERABLE TO CYBER ATTACK AND CYBER DEFENSES ARE ONLY AS STRONG AS THE DEFENSES OF EVERYONE CONNECTED TO IT
SECURITY ASSESSMENTS – ORGANIC AND THOSE OF SUPPLIERS
EDUCATION AND TRAINING - WORKFORCE AWARENESS THROUGH TRAINING AND CULTURAL EMPHASIS ON STRONG "CYBER HYGIENE"
BREACHES WILL HAPPEN - INCIDENT RESPONSE AND REPORTING PROCEDURES ARE IMPORTANT
INVESTING – SMALL COMPANIES CAN'T AFFORD IT, INVESTING IN THESE SUPPLIERS IS AN INVESTMENT IN ORGANIC SECURITY
AN ORGANIZATION IS ONLY AS SECURE AS THE ENTIRE SUPPLIER BASE.
Mr. Bill Czajkowski


Image credit: https://www.geojobe.org/Radios/MyRadios/Ray/TTP/Ray/TTP.html
SUPPLY CHAIN MANAGEMENT
MAJOR FOCUS IS MAXIMIZING VALUE
BIG DATA-DRIVEN SUPPLY CHAIN DECISION MAKING
TRACK SUPPLIERS' FINANCIAL STABILITY AND PERFORMANCE
INFORMATION TOOLS, BUSINESS INTELLIGENCE, SUPPLIER PORTAL ACCESSED COMMUNICATIONS AND PROCESS AUTOMATION
OUTSOURCING NON-CORE ACTIVITIES ENABLES RAYTHEON TO FOCUS RESOURCES ON DRIVING THE VARIOUS STRATEGIES
CONFLICT MINERALS
DODD-FRANK ACT, SECTION 1502, CONFLICT MINERALS RULE, DRC, 3TG (W, TA, SN, AU)
2021, EUROPEAN UNION (EU) CONFLICT MINERALS REGULATION, APPLIES TO IMPORTERS OF MINERALS ORIGINATING FROM ANY CONFLICT ZONE OR HIGH-RISK AREA
DFARS, SPECIALTY METALS SHALL BE MELTED/PRODUCED IN THE US, OUTLYING AREAS, QUALIFYING COUNTRY, SOME STEELS, TITANIUM, ZIRCONIUM AND SOME OF THEIR ALLOYS
Mr. Bill Czajkowski
Image credit: https://www.supplychaindigital.com/supply-chain-management/can-blockchain-bring-supply-chain-21st-century


HUMAN CAPITAL CHALLENGES
Image credit: Wordpress
SKILLS
PEOPLE
HUMAN CAPITAL
ROLES
PUBLICLY TRADED COMPANIES HAVE A ONE-IN-THREE CHANCE OF FAILING IN THE NEXT FIVE YEARS
BACKGROUNDS, EXPERIENCES AND SKILLS NECESSARY TO SUPPORT THE COMPANY'S SUCCESS
NATIONWIDE SHORTAGE OF SKILLS IN STEM AND TECHNOLOGY FUNDAMENTALS
SHORTAGE OF "SOFT" SKILLS SUCH AS PROBLEM-SOLVING, CRITICAL THINKING, LITERACY, COMMUNICATION AND COLLABORATION
COMPANIES MUST INNOVATE AND ADAPT THEIR BUSINESS AND OPERATING MODELS TO SURVIVE
DELIVER LEARNING IN WAYS THAT ENABLE THEM TO RESPOND TO RAPID CHANGE
COMMITMENT TO DIVERSITY AND INCLUSION
SHIFTING ATTITUDES AMONG YOUNG PROFESSIONALS ABOUT JOB SATISFACTION
" ...the industry faces impending retirements and a shortage of trained technical graduates while work and skills requirements become increasingly advanced... " - AEROSPACE INDUSTRIES ASSOCIATION
Mr. Bill Czajkowski

Appendix E: Industry Analysis Firm Briefs: *UNITED TECHNOLOGIES*

United Technologies

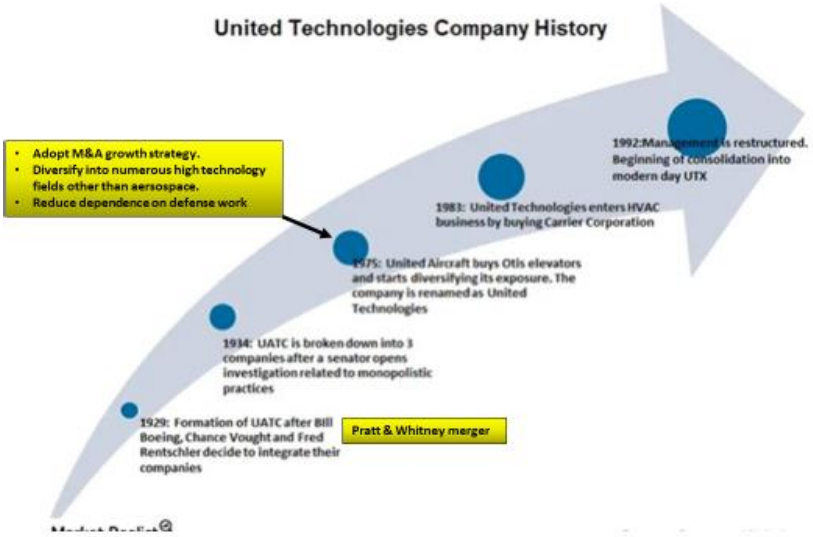
United Technologies

TOLLIVER

History

United Technologies

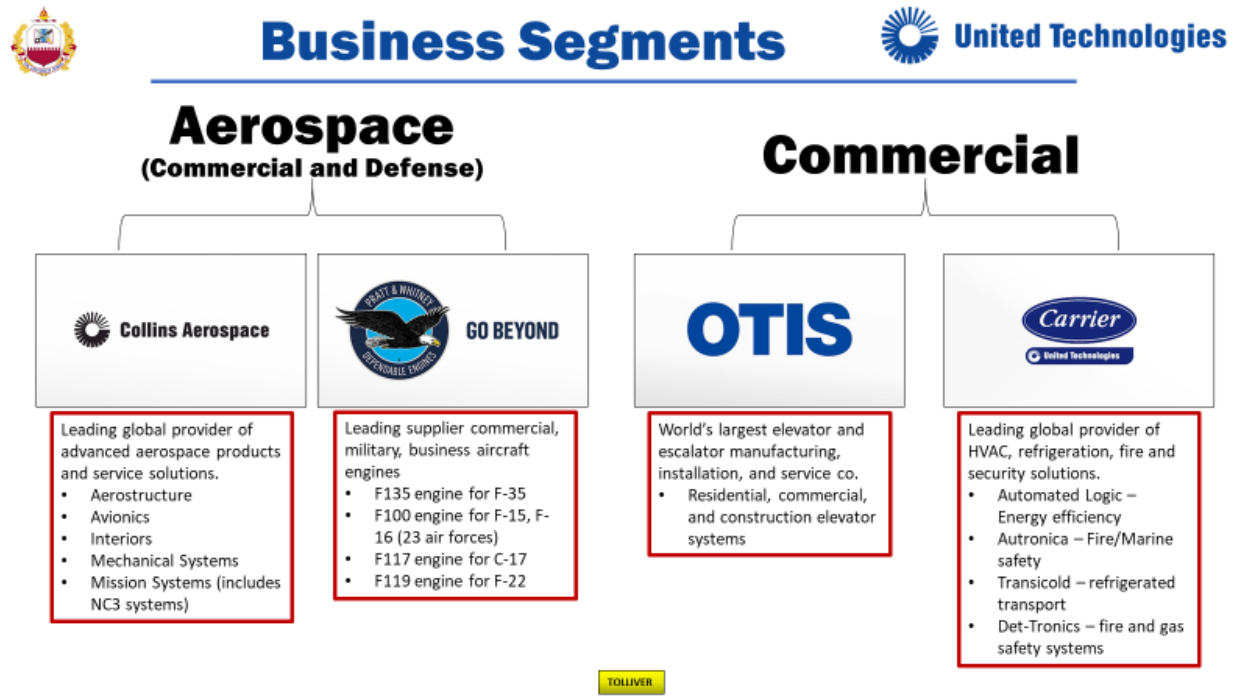
United Technologies Company History

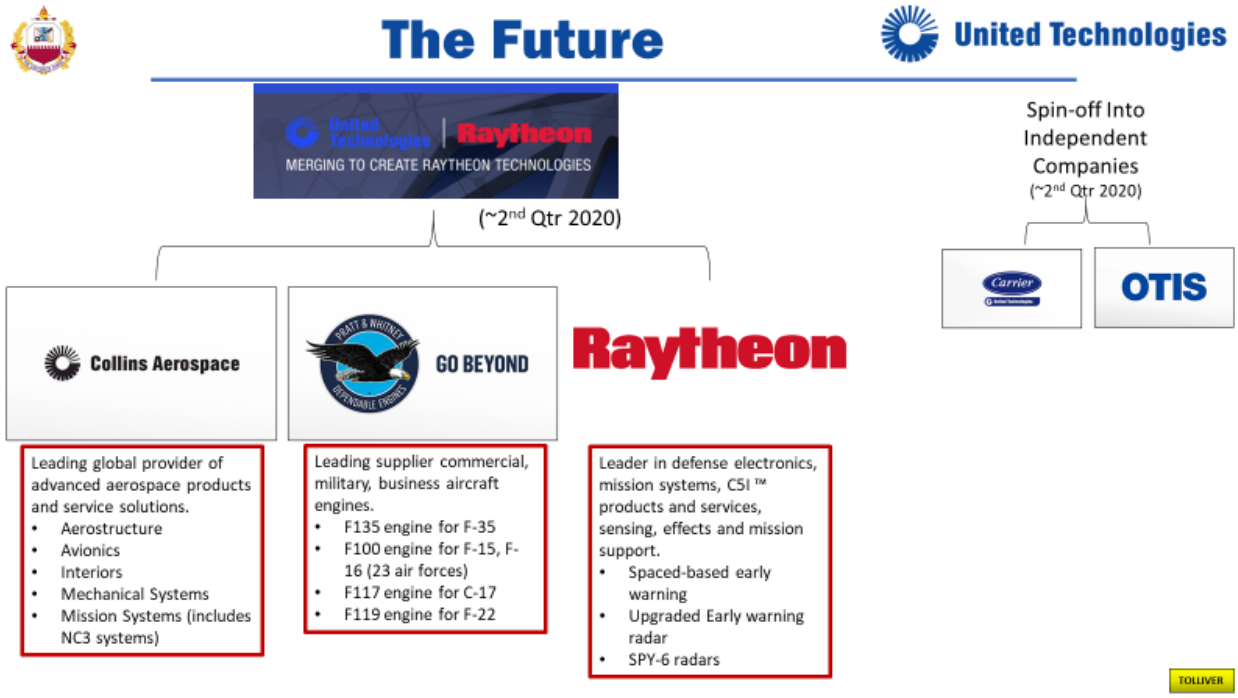


Additional Growth

- **Chubb Security** (2003) – Fire and security
- **Kidde** (2005) – Fire and security
- **NORESCO** (Mar 2008) – Energy services
- **49.5% of Clipper Windpower** (Dec 2009) – Wind turbine manufacturing
- **UT Research Centre Ireland** (Apr 2010) – Research in energy/security systems
- **Complete Clipper Acquisition** (Oct 2010)
- **GE's Security Equipment** (2010) – Bolster UTC's Fire & Security unit
- **Goodrich Corp** (July 2012)
  - Aircraft components
  - $18.4 bn; $1.9 bn in GC debt
  - Merged with Hamilton Sundstrand to create UTC Aerospace Systems
- **Rockwell Collins** (Nov 2018) – merged with UTC Aerospace Systems to form Collins Aerospace

TOLLIVER


Business Segments
United Technologies
Aerospace
(Commercial and Defense)
Commercial
Collins Aerospace
GO BEYOND
OTIS
Carrier
Leading global provider of advanced aerospace products and service solutions.
• Aerostructure
• Avionics
• Interiors
• Mechanical Systems
• Mission Systems (includes NC3 systems)
Leading supplier commercial, military, business aircraft engines
• F135 engine for F-35
• F100 engine for F-15, F-16 (23 air forces)
• F117 engine for C-17
• F119 engine for F-22
World's largest elevator and escalator manufacturing, installation, and service co.
• Residential, commercial, and construction elevator systems
Leading global provider of HVAC, refrigeration, fire and security solutions.
• Automated Logic – Energy efficiency
• Autronica – Fire/Marine safety
• Transicold – refrigerated transport
• Det-Tronics – fire and gas safety systems
TOLLIVER


The Future
United Technologies
United Technologies | Raytheon
MERGING TO CREATE RAYTHEON TECHNOLOGIES
(~2nd Qtr 2020)
Spin-off Into Independent Companies
(~2nd Qtr 2020)
Collins Aerospace
GO BEYOND
Raytheon
Carrier
OTIS
Leading global provider of advanced aerospace products and service solutions.
• Aerostructure
• Avionics
• Interiors
• Mechanical Systems
• Mission Systems (includes NC3 systems)
Leading supplier commercial, military, business aircraft engines.
• F135 engine for F-35
• F100 engine for F-15, F-16 (23 air forces)
• F117 engine for C-17
• F119 engine for F-22
Leader in defense electronics, mission systems, C5I ™ products and services, sensing, effects and mission support.
• Spaced-based early warning
• Upgraded Early warning radar
• SPY-6 radars
TOLLIVER

The Strategy

United Technologies

The Conglomerate Discount

- Tendency of markets to place greater value in a conglomerate's parts than its sum
  - Conglomerate – one company holding a controlling stake in a number of smaller companies that operate independently of other business divisions.
- Problems with conglomerates
  - Diversification can be difficult to manage effectively
  - Adds layers of management that can create substantial overhead expenses
  - Reduces transparency
  - Prevents corporate-level focus and prioritization
- Discourages investors. Investors more interested in focused companies, driving conglomerates to spin-off or divest subsidiary holdings.

Source: Investopedia https://www.investopedia.com/terms/c/conglomeratediscount.asp

TOLLIVER

The Strategy

United Technologies

Why Divest

- UTC has a lopsided split between commercial and defense.
- Carrier and Otis almost solely commercial and can stand on their own. They don't want defense business.

2019 Segment Sales by Product Type (2018 in parentheses) *Dollars in millions*

	Otis	Carrier	Pratt & Whitney	Collins Aerospace
Commercial and Industrial (non-aerospace)	13,113 (12,904)	18,608 (18,922)	102 (55)	51 (60)
Commercial Aerospace	-	-	14,516 (14,027)	19,005 (12,564)
Military Aerospace	-	-	6,274 (5,315)	6,972 (4,010)
Total Segment	**13,113 (12,904)**	**18,608 (18,922)**	**20,892 (19,397)**	**26,028 (16,634)**

- Otis and Carrier have their own, strong value streams. Allows them to more easily pursue innovation and mergers and acquisitions.
- Allow them to focus on core competency and attract greater investment
- Collins Aerospace did not depend on Otis/Carrier for revenue sharing
- UTC is historically an airplane company and is doubling down on core competency – Aerospace and Defense

TOLLIVER

The Strategy

United Technologies

Why Acquire

- L3/Harris merger was a threat. Saw it as a consolidation of the communications market.
  - UTC-Rockwell Collins merger wasn't enough
- Remaining Raytheon business segments are highly complementary to remaining UTC business segments.
  - Complementary skills set between companies
  - Create synergies by growing while shedding weight
- Does not intend to compete with major primes – Lockheed, Boeing
- Want to become industry leading Aerospace and Defense provider (including commercial)
  - The Prime for some systems (e.g. Ballistic Missile Defense, sensors) and the Go-To Sub for others (e.g., aircraft)
  - Acquisition makes them a "Tier One" supplier.
- Long term vision is to be THE "Tier One Integrator".
  - Vertical integration of commercial and defense aerospace systems – Everything but the airframe
  - Collins Aerospace becomes the business integrator

TOLLIVER

The Strategy

United Technologies

What Does it Mean for DoD

- Regulators prevented monopoly
  - Required Raytheon to spin-off airborne communications business sector because Collins Aerospace already had large portion of that market
  - Required Collins Aerospace to spin off GPS sector because their current near market monopoly would have been even further tightened with acquisition.
- Acquisition of Rockwell Collins (2018) and Raytheon creates ***Bilateral Monopoly*** Raytheon Technologies aerospace defense business segment
  - DoD (and some foreign militaries) is a **Monopsony Buyer** – the sole buyer of aerospace defense technology
  - Raytheon Technologies seeks to become a **Monopoly Producer** – one or very few sellers in a market

TOLLIVER

Industry Structure

United Technologies

United Technologies

WACC (<8%)

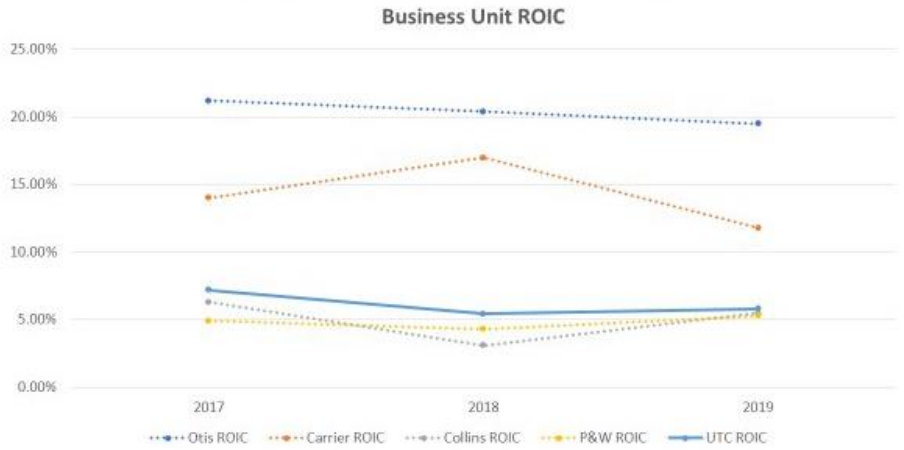
Current Operating Profit: $269.7 Million ↓ ROIC: 11.8% ↓	Current Operating Profit: $166.8 Million ↑ ROIC: 5.3% ↑	Current Operating Profit: $410.0 Million ↑ ROIC: 5.5% ↑	Current Operating Profit: $194.8 Million ↑ ROIC: 19.5% ↓
• HVAC business • Commercial	• Aerospace Business • Aircraft engines • Commercial & Defense	• Aerospace Business • Avionics • Technology • Commercial & Defense	• Elevator Business • Commercial

ABEL

Industry Structure

United Technologies

United Technologies



ABEL

Industry Structure

United Technologies

United Technologies

- Profitable
- Raytheon Merger
- Conglomerate Discount

ABEL

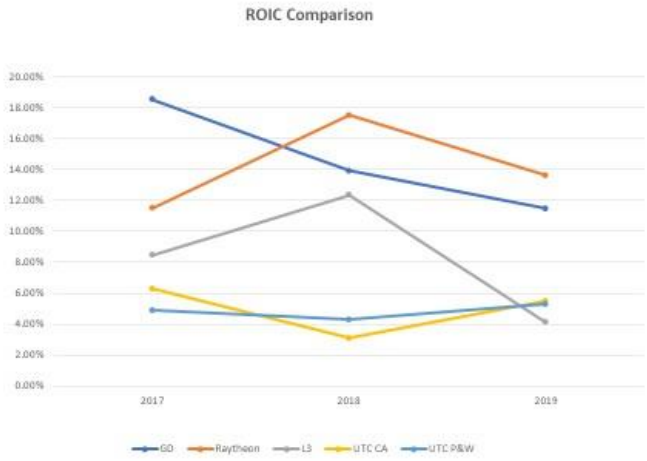
Peer Competitors

United Technologies

L3HARRIS™

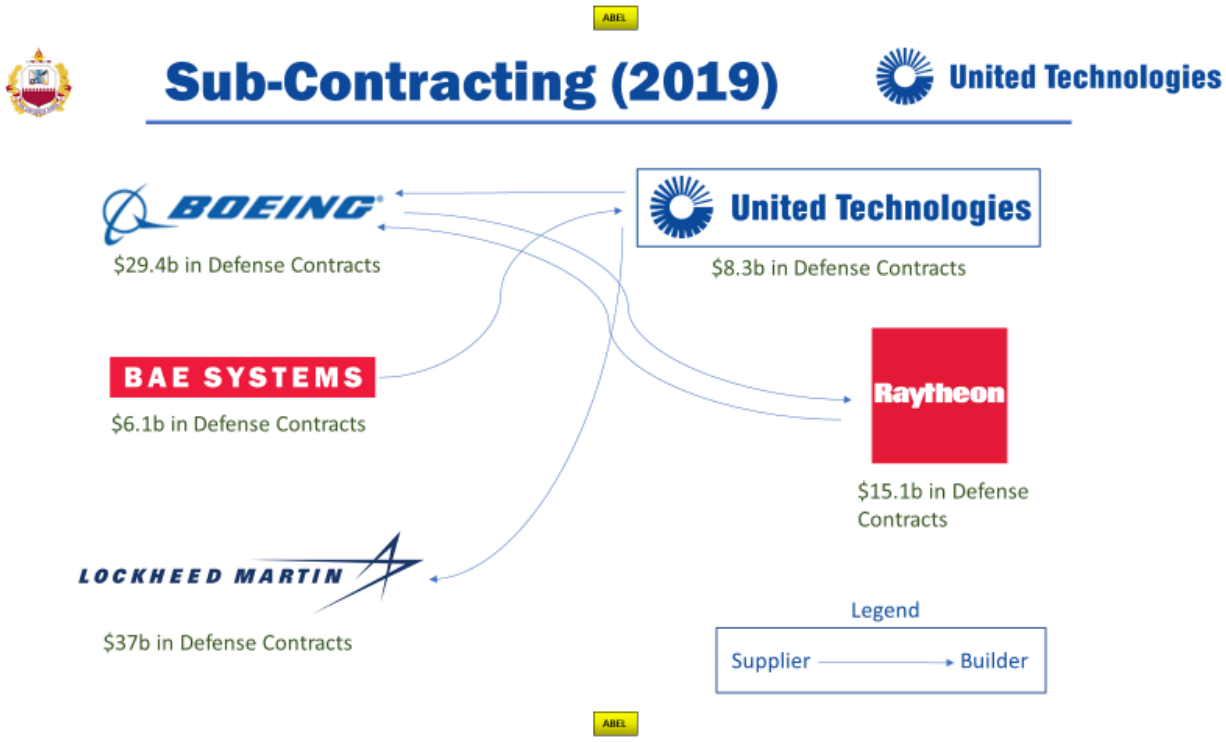
Raytheon

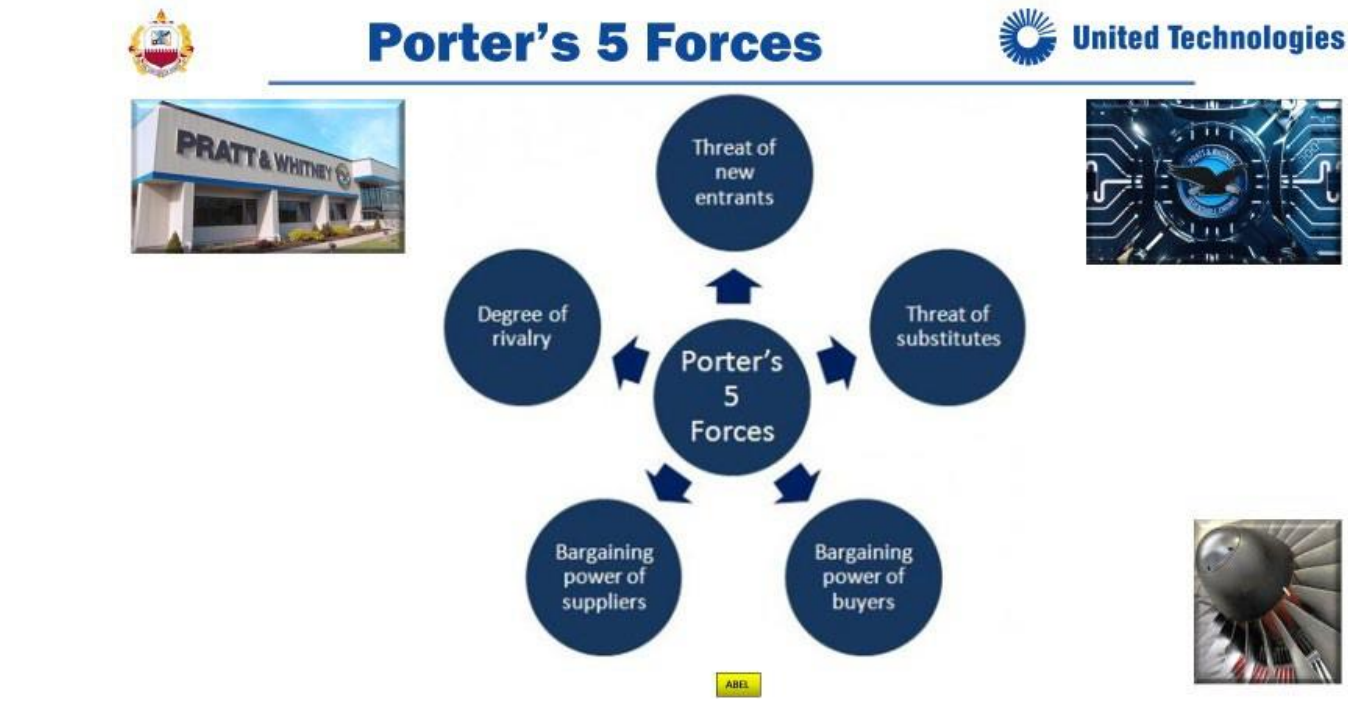
GENERAL DYNAMICS

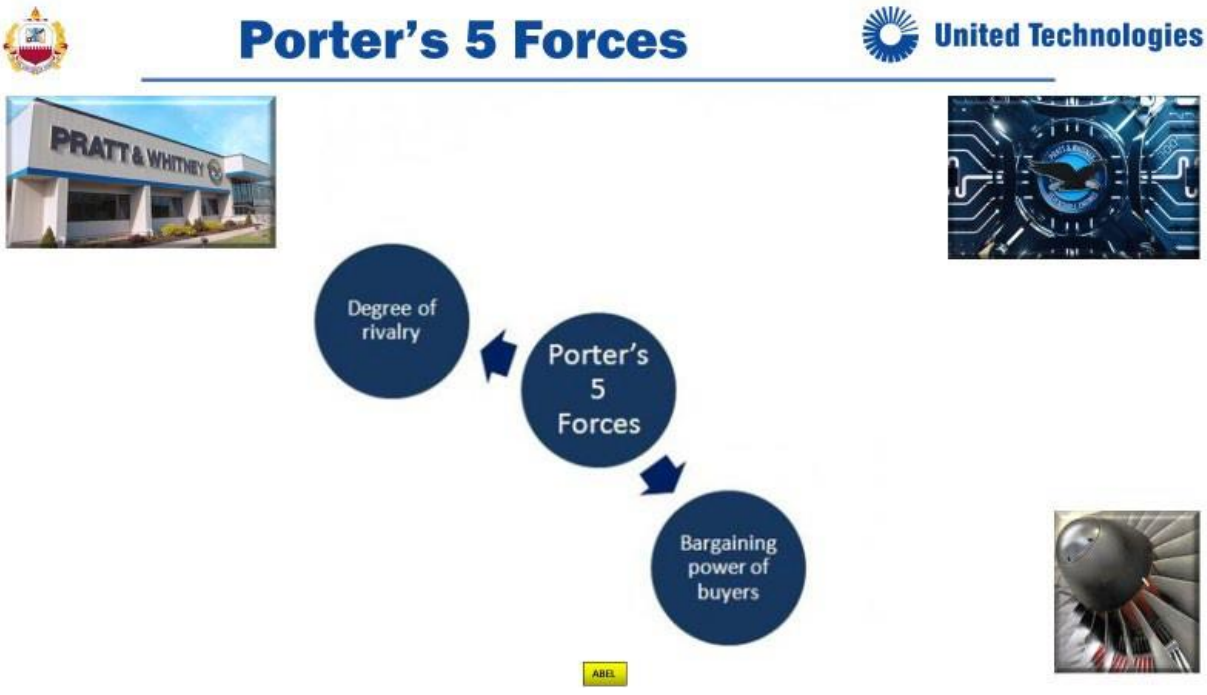


ABEL


Industry Partners
United Technologies
BOEING
NORTHROP GRUMMAN
Raytheon
BAE SYSTEMS
AIRBUS
GENERAL DYNAMICS
LOCKHEED MARTIN


ABEL
Sub-Contracting (2019)
United Technologies
BOEING
$29.4b in Defense Contracts
United Technologies
$8.3b in Defense Contracts
BAE SYSTEMS
$6.1b in Defense Contracts
Raytheon
$15.1b in Defense Contracts
LOCKHEED MARTIN
$37b in Defense Contracts
Legend
Supplier
Builder
ABEL


Porter's 5 Forces
United Technologies
PRATT & WHITNEY
Threat of new entrants
Degree of rivalry
Threat of substitutes
Porter's 5 Forces
Bargaining power of suppliers
Bargaining power of buyers
ABEL


Porter's 5 Forces
United Technologies
PRATT & WHITNEY
Degree of rivalry
Porter's 5 Forces
Bargaining power of buyers
ABEL

Strategic Game Board

United Technologies

DIMENSION I: *Where* to Compete
- Aircraft engines

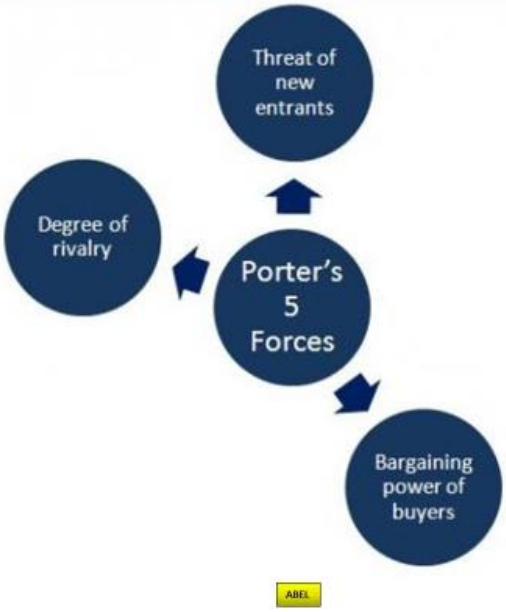
DIMENSION II: *How* to Compete
- Differentiation
- Same game

DIMENSION III: *When* to Compete
- First mover
- Buyer-focused investment

ABEL

Porter's 5 Forces

United Technologies



ABEL

Strategic Game Board

United Technologies

DIMENSION I: *Where* to Compete
- Avionics
- NC3 comms

DIMENSION II: *How* to Compete
- Differentiation
- Same game

DIMENSION III: *When* to Compete
- Follower (in most cases)
- Buyer-focused investment

ABEL

United Technologies

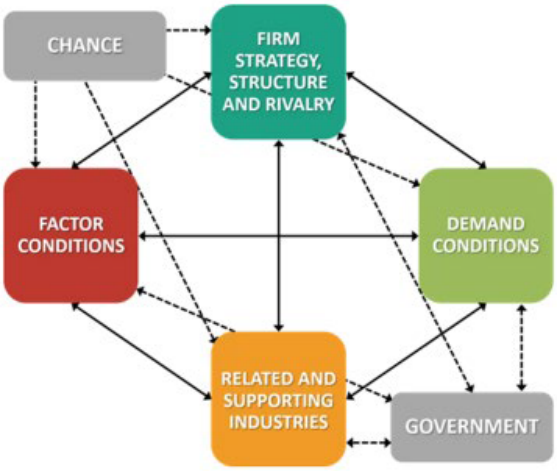
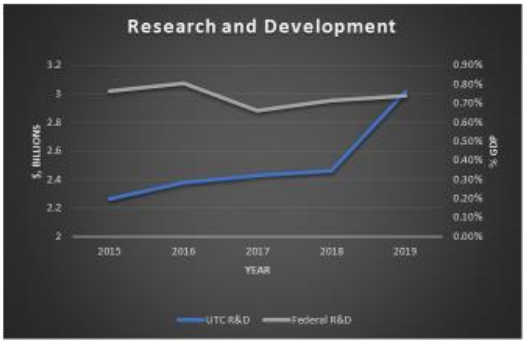


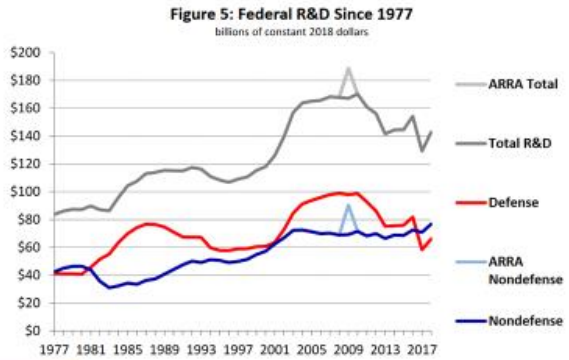
Figure 1: Porter's Diamond Model of National Competitive Advantage

BARRY

Research and Development $$

United Technologies

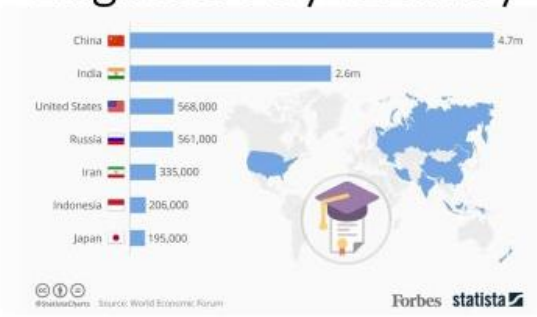




BARRY

United Technologies

Engineers by Country



BARRY

United Technologies

Does Porter's Diamond lead us to any conclusions on whether UTC made the right decision to consolidate and focus on avionics?

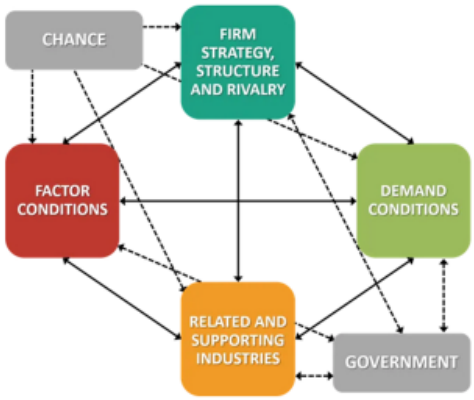


Figure 1: Porter's Diamond Model of National Competitive Advantage

BARRY

UTC Firm Risks

- Cyber Security
- Raw Material Availability/Prices
- Classification limitations

- Credit Market
- Economic Activity
- Currency Exchange Rates
- Debt Levels
- Contracting Strategy

- Supplier financing
- Raw Material Availability
- International Operations
- Cyber Security
- IP

- Globalization
- Spin offs and Acquisition
- Competition
- Human Capital

Alvarado

NC3 Industry Gaps

United Technologies

- **Supply System**
  - Limited Revenue
  - Bounded Innovation
  - Human Capital Challenges
  - Constrained Infrastructure
  - Restricted Supply Chain
- **Demand System**
  - Inconsistent and Limited Gov't Demand
  - Narrow Commercial Applications/ITAR
  - Restricting IP requirements
- **Financing System**
  - Competing/Diminishing R&D $$'s
  - Limited VC market

Industry Objective: $\frac{\text{REV} - \text{COST}}{\text{INVESTMENT}} > \text{WACC}$

Alvarado

Policy Recommendations

United Technologies

Research	Diffuse	Develop
• Expand R&D $$'s • IP regulations • Restructure clearance process	• Decrease Anti-Trust Laws • Trade policies/ITAR • Gov't and VC share cost of R&D • Industry/Academia Partnership Frameworks	• Subsidize Cleared Facilities • Consistent DoD budgets • Clear demand signal

Policies supporting a Defense Market Innovation that can be translated into Revenue and Expanded Markets

Alvarado

Thank you! Questions?

United Technologies

Chris, Dave, Ed, Lili

End Notes

[1] Nuclear Posture Review of the United States of America, The Department of Defense, February 2018, page XIII, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

[2] "The US Nuclear Deterrent: Past, Present, and Future," Nuclear Matters Handbook 2020", accessed March 2020, page 1, https://www.acq.osd.mil/ncbdp/nm/nmhb/chapters/chapter1.htm.

[3] Ibid, 22.

[4] Ibid, 22.

[5] Ibid, 26.

[6] Ibid, 22.

[7] Nicola Horsburgh, "*Change and Innovation in Chinese Nuclear Weapons Strategy*," *China Information* 26, no. 2 (July 2012): 186, https://doi.org/10.1177/0920203X12439973.

[8] Ibid, 187.

[9] "Time to Address China's Expanding Nuclear Weapons Program | Arms Control Association," 4, accessed February 3, 2020, https://www.armscontrol.org/blog/2018-08-22/time-address-chinas- expanding-nuclear-weapons-program.

[10] Heginbotham et al., "*China's Evolving Nuclear Deterrent: Major Drivers and Issues for the United States*," 37.

[11] David Axe, 'Wait, China Has TWO Hypersonic Missiles?', Text, *The National Interest* (The Center for the National Interest, 3 December 2019), accessed 13 April 2020 https://nationalinterest.org/blog/buzz/wait-china-has-two-hypersonic-missiles-101422.

[12] Richard Seebass, *Read 'Review and Evaluation of the Air Force Hypersonic Technology Program' at NAP.Edu* (National Academy Press, 1998), accessed 13 April 2020 doi:10.17226/6195.

[13] "Time to Address China's Expanding Nuclear Weapons Program | Arms Control Association," 5.

[14] Guy Anderson, *Russian Federation – Market Report; Navigating Emerging Markets*, Janes, updated January 22, 2020, accessed February 3, 2020, https://janes-ihs-com.nduezproxy.idm.oclc.org/Janes/Display/JIQ0090-JIQ.

[15] Pavel Baev, "Russian Nuclear Modernization and Putin's Wonder-Missile: Real Issues and False Posturing," Notes de l'Ifri, Russie.Nei.Visions 115, Russia/NIS Center, August 2019, accessed March 22, 2020,

[16] Roberto Buaron, "New-game strategies," *McKinsey Quarterly*, no. 1 (Spring 1981): 26, accessed

April 13, 2020, https://nduezproxy.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&Auth Type=ip,url,uid&db=buh&AN=6989238&site=eds-live&scope=site.

[18] Ibid, 14.

[19]Michael Klare, 'Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation', *Arms Control Association*, November 2019, accessed 13 April 2020 https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new- pathways-escalation.

[20] J.R. Wilson. *Today's Battle for the Electromagnetic Spectrum*.

[21] Richard Connolly and Mathieu Boulegue, *Russia's New State Armament Programme: Implications for the Russian Armed Forces and Military Capabilities to 2027* (Chatham House, The Royal Institute of International Affairs: Russia and Eurasia Programme, May 2018), 5.

[22] Ibid, 2.

[23] Pavel Baev, *Russian Nuclear Modernization and Putin's Wonder-Missiles: Real Issues and False Posturing* (Russia/NIS Center, Notes de l'Ifri, Russie.Nei.Visions 115, August 2019), pg 15.

[24] Congressional Research Service, *Russia's Nuclear Weapons: Doctrine, Forces, and Modernization*, by Amy F. Woolf, January 2, 2020, p. 16, accessed February 3, 2020, https://fas.org/sgp/crs/nuke/R45861.pdf.

[25] Pavel Baev, *Russian Nuclear Modernization and Putin's Wonder-Missiles: Real Issues and False Posturing* (Russia/NIS Center, Notes de l'Ifri, Russie.Nei.Visions 115, August 2019), pg 16.

[26] Ibid, 123

[27] "China National Nuclear Corporation - China Nuclear Forces," accessed February 3, 2020, https://www.globalsecurity.org/wmd/world/china/cnnc.htm.

[28] Nuclear Posture Review of the United States of America, The Department of Defense, February 2018, page II, https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

[29] "The US Nuclear Deterrent: Past, Present, and Future," Nuclear Matters Handbook 2020", accessed March 2020 https://www.acq.osd.mil/ncbdp/nm/nmhb/chapters/chapter1.htm.

[30] Anonymous. Non-attributional information received from officials during class visits to Government and Industry sites. Academic Year 2019-2020.

[31] Anonymous. Non-attributional information received from officials during class visits to Government and Industry sites. Academic Year 2019-2020.

[32] Lockheed Martin NC3 Program (Remote Presentation, Blackboard Virtual Environment, April 3, 2020)

[33] James Acton, *For Better or for Worse: The Future of C3I Entanglement*, Nautilus Institute for Security and Sustainability Special Report, Berkeley, California: NAPSNet Special Reports, 21 November 2019. Accessed March 14, 2020. https://nautilus.org/napsnet/napsnet-special- reports/for-better-or-for-worse-the-future-of-c3i-entanglement/.

[35] Air Force Nuclear Weapons Center NC3 Integration Directorate, Air Force Nuclear Command, Control, & Communications (NC3) Weapon System AN/USQ-

255: Constituent Systems and External Dependencies Handbook 1.0, (Kirtland AFB, NM: US Department of the Air Force, 2017), 4-64.

36 "E-6B Mercury," Naval Air Systems Command, accessed March 22, 2020, https://www.navair.navy.mil/product/E-6B-Mercury.

40 "Defense Industrial Base Sector," Department of Homeland Security – Cybersecurity Infrastructure Security Agency, accessed March 2020, https://www.cisa.gov/defense-industrial-base-sector.

41 "Report in Fulfillment of Executive Order 13806, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," The Department of Defense, September 2018, page 2, https://media.defense.gov/2018/Oct/05/2002048904/-1/- 1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE-AND-SUPPLY-CHAIN-RESILIENCY.PDF

42 Etzkowitz, Henry, *The Triple Helix University- Industry-Government Innovation in Action*

(Routledge, 2008), 8–9.

43 Congressional Budget Office, *Projected Costs of U.S. Nuclear Forces, 2017 to 2026* (Washington, D.C., GPO February 2017), 1.

44 Robert Grant, *Contemporary Strategy Analysis, Ninth Edition*, West Sussex, United Kingdom: John Wiley & Sons Ltd, 2013, pp 68-76.

45 Porter Michael, "Five Competitive Forces that shape Strategy," *Harvard Business Review* 86 (January 2008): 83.

46 Ibid, 83-84.

47 Ibid, 78-93.

48 Specific industries are not identified to prevent association with NC3 modernization efforts.

49 Anonymous. Non-attributional information received from officials during class visits to Government and Industry sites. Academic Year 2019-2020.

[50] Porter Michael, "Five Competitive Forces that shape Strategy," *Harvard Business Review* 86 (January 2008): 83.

[53] David Norquist, *(U)Nuclear Command, Control, and Communication Enterprise Guidance,*

(Washington, DC: DOD, April 17, 2019, Effective though April 16, 2020), 1.

[54] Ibid., 2.

[55] Ibid., 3.

[56] Ibid., 3.

[57] Theresa Hitchens, "OSD & Joint Staff Grapple with Joint All-Domain Command," *Breaking Defense*, November 14, 2019, accessed March 23, 2020, https://breakingdefense.com/2019/11/osd- joint-staff-grapple-with-joint-all-domain-command/.

[58] Air Force Nuclear Weapons Center NC3 Integration Directorate, *Air Force Nuclear Command, Control, & Communications (NC3) Weapon System AN/USQ-255: Constituent Systems and External Dependencies Handbook 1.0*, (Kirtland AFB, NM: US Department of the Air Force, 2017), 4-64.

[59] Ibid., 8.

[60] Ibid., 8-9.

[61] Ibid., 9.

[62] Ibid., 9.

[63] Department of the Air Force, Nuclear, Space, Missile, Command and Control, Air Force Nuclear Command, Control, and Communications (NC3), Air Force Instruction 13-550, (Washington, DC: Secretary of the Air Force, April 16, 2019)

[64] "E-6B Mercury," Naval Air Systems Command, accessed March 22, 2020, https://www.navair.navy.mil/product/E-6B-Mercury.

[65] Matthew J. Kohler, *Navy Nuclear Command, Control, and Communications Executive Steering Committee*, OPNAV Instruction F5420.116A, (Washington, DC: Department of the Navy, November 5, 2019), 1-5.

[66] Ted N. Branch, *Navy Nuclear Command, Control, and Communications Executive Steering Committee*, OPNAV Instruction 5420.116, (Washington, DC: Department of the Navy, December 15, 2015), 2.

[67] "Commander's Narrative," United States Space Command, accessed April 7, 2020, https://www.spacecom.mil/Portals/32/Documents/USSPACECOM%20Commanders%20Narrative- v10.pdf, 2.

[68] "Achieve and Maintain Cyberspace Superiority, Command Vision for US Cyber Command," US Cyber Command, accessed April 7, 2020, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pd f?ver=2018-06-14-152556-010, 1.

[69] Title 10 USC, § 171a.

[70] "Joint Operations," Joint Publication 3-0, 17 January 2017.

[71] Andrew Reddie, 'Hypersonic Missiles: Why the New "Arms Race" Is Going Nowhere Fast', Bulletin of the Atomic Scientists, *Bulletin of the Atomic Scientists*, (13 January 2020), accessed 13 April 2020 https://thebulletin.org/2020/01/hypersonic-missiles-new-arms-race-going-nowhere-fast/.

[72] David Axe, 'Wait, China Has TWO Hypersonic Missiles?', Text, *The National Interest* (The Center for the National Interest, 3 December 2019), accessed 13 April 2020 https://nationalinterest.org/blog/buzz/wait-china-has-two-hypersonic-missiles-101422.

[73] Richard Seebass, *Read 'Review and Evaluation of the Air Force Hypersonic Technology Program' at NAP.Edu* (National Academy Press, 1998), accessed 13 April 2020 doi:10.17226/6195.

[74] Reddie, 'Hypersonic Missiles'.

[75] Dorit Dor, 'These Are the Top Cybersecurity Trends to Watch out for in 2020', *World Economic Forum*, 7 January 2020, accessed 13 April 2020 https://www.weforum.org/agenda/2020/01/these- will-be-the-main-cybersecurity-trends-in-2020/.

[76]Michael Klare, *Cyber Battles, Nuclear Outcomes? Dangerous New Pathways to Escalation, Arms Control Association*, November 2019, accessed 13 April 2020https://www.armscontrol.org/act/2019-11/features/cyber-battles-nuclear-outcomes-dangerous-new- pathways-escalation.

[77] J.R. Wilson, 'Today's Battle for the Electromagnetic Spectrum', *Military Aerospace Electronics*, 1 August 2016, accessed 13 April 2020 https://www.militaryaerospace.com/communications/article/16709112/todays-battle-for-the- electromagnetic-spectrum.

[78] J.R. Wilson. *Today's Battle for the Electromagnetic Spectrum.*

[79] J. Michael McQuade et al., "Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage" (Defense Innovation Board, May 2019), p.i, https://innovation.defense.gov/software/.

[80] Thomas Lam and Nicolas Chaillan, "DoD Enterprise DevSecOps Reference Design" (Department of Defense (DoD) Chief Information Officer, 2019), p.27. https://dodcio.defense.gov/Portals/0/Documents/DoD%20Enterprise%20DevSecOps%20Reference% 20Design%20v1.0_Public%20Release.pdf?ver=2019-09-26-115824-583.

[81] J. Michael McQuade et al., "Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage" (Defense Innovation Board, May 2019), p.v, https://innovation.defense.gov/software/.

[82] Sandra Erwin, "Air Force to Accelerate Deployment of Anti-Jam Satellite Communications Equipment," *Space News*, December 26, 2018, https://spacenews.com/air-force-to-accelerate- deployment-of-anti-jam-satellite-communications-equipment/.

[83] Darrell K. Rigby, Jeff Sutherland, and Hirotaka Takeuchi, "Embracing Agile: How to Master the Process That's Transforming Management.," *Harvard Business Review* 94, no. 5 (2016): 41.

[84] Darrell K. Rigby, Jeff Sutherland, and Hirotaka Takeuchi, "Embracing Agile: How to Master the Process That's Transforming Management.," *Harvard Business Review* 94, no. 5 (2016): 41.

[85] Suzanne Miller and Dan Ward, "Update 2016: Considerations for Using Agile in DoD Acquisition" (Software Engineering Institute: Carnegie Mellon University, December 2016), p.9, https://resources.sei.cmu.edu/asset_files/TechnicalNote/2016_004_001_484651.pdf.

[86] Stack, Liam. 2019. "Update Complete: US Nuclear Weapons No Longer Need Floppy Disks." *The New York Times*, October 24, 2019, sec. US https://www.nytimes.com/2019/10/24/us/nuclear- weapons-floppy-disks.html.

[87] "8-Inch Floppy Disk (1971 - Early 1980s)." 2013. Museum of Obsolete Media. August 7, 2013. https://obsoletemedia.org/8-inch-floppy-disk/

[90] Department of Defense, *Critical Program Information (CPI) Identification and Protection Within Research, Development, Test, and Evaluation (RDT&E)*, DODI 5200.39 (Washington DC: US Department of Defense, October 15, 2018, Incorporating Change 2), 6-7; Department of Defense, *Counterintelligence (CI) Activities Supporting Research, Development, and Acquisition (RDA)*, DODI O-5240.24 (Washington, DC: US Department of Defense, October 15, 2013, Incorporating Change 1), 2.

[91] Department of Defense, *Counterintelligence (CI) Activities*, DODI O-5240.24, 12.

[92] Department of Defense, *Critical Program Information*, DODI 5200.39, 2.

[93] David L. Russell and Pieter C. Arlow, *Industrial Security: Managing Security in the 21st Century*

(Hoboken, New Jersey, John Wiley & Sons, Inc., 2015), 3.

[94] Interviews with USG NC3, continuity of government, and continuity of operations counterintelligence experts, January 31, 2020, and February 14, 2020. All interviews were conducted in confidentiality, and the names of the interviewees are withheld by mutual agreement.

[95] Ibid.

[96] William C. Hannas, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (New York: Routledge, 2013), 26-32.

[97] Ibid., 38.

[98] White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World* (Washington, DC: GAO Press, June 2018), 3.

[99] Chris Nissen, John Gronager, Robert Metzger, and Harvey Rishikof, *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War* (McLean, VA: The MITRE Corporation, August 2018), 11.

[100] "Gross Domestic Product, Fourth Quarter and Year 2019 (Advance Estimate) | US Bureau of Economic Analysis (BEA)," accessed March 24, 2020, https://www.bea.gov/news/2020/gross- domestic-product-fourth-quarter-and-year-2019-advance-estimate.

[101] "The Employment Situation - February 2020.Pdf," accessed March 24, 2020, https://www.bls.gov/news.release/pdf/empsit.pdf.

[102] Elijah E Cummings et al., "House Committee on Oversight and Reform: 'NEXTGEN Feds: Recruiting The Next Generation of Public Servants', H.R. Rep. No. 116–65" (2019).

[103] Yasmin Tadjdeh, "Defense Sector Straining to Attract STEM Talent," *National Defense Magazine.*, January 22, 2020, https://www.nationaldefensemagazine.org/articles/2020/1/22/defense- sector-straining-to-attract-stem-talent.

[104] Interagency Task Force in Fulfillment of Executive Order 13806, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States (September 2018),"

[105] Ronald Reagan Institute, "The Contest for Innovation: Strengthening America's National Security Innovation Base in an Era of Strategic Competition," December 2019.

[1] National Science and Technology Council. "Charting a Course for Success: America's Strategy for STEM Education." (2018).

106 National Science and Technology Council. "Charting a Course for Success: America's Strategy for STEM Education." (2018).

[107] MITRE, "Symposium for the Federal Workforce of the 21st Century," October 2018.

[108] Nicole Ogrysko, "98 Days and Counting, Will Federal Hiring Ever Get Easier?" *Federal News Network*, March 6, 2020.

[109] Nicole Ogrysko, "Progress on Security Clearance Backlog Is Real, but Federal Contractors Still Seeking End-to-End Solutions," *Federal News Network*, February 24, 2020.

[110] Eric Yoder, "Federal Employee Salaries Lag by Average of 31 Percent, Pay Group Reports," *Washington Post*, November 14, 2018.

[111] "Next Generation NC3 Enterprise Challenge," *BetaSam.gov*, originally published November 27, 2018, accessed April 16, 2020, https://beta.sam.gov/opp/39060979136484 2047d3ab34aa7d1441/view?keywords=Next%20Generati on%20NC3%20Enterprise%20Challenge&sort=-relevance&index=opp&is_active=false&page=1.

[112] Anonymous. Non-attributional information received from officials during class visits to Government and Industry sites. Academic Year 2019-2020

[113] Sandra Erwin, *STRATCOM to Design Blueprint for Nuclear Command, Control and Communications*, "SpaceNews" March 29, 2019, https://spacenews.com/stratcom-to-design- blueprint-for-nuclear-command-control-and-communications/

[114] J Krawiec and Alan Holden, 'Emerging Technologies Will Disrupt Government. Here's What to Do About It.,' *Nextgov*, 19 October 2018, accessed 13 April 2020, https://www.nextgov.com/ideas/2018/10/emerging-technologies-will-disrupt-government-heres- what-do-about-it/152045/

[115] General Dynamics Mission Systems, (Presentation, General Dynamic Offices, Dedham, MA, February 28, 2020)

[116] Jeff Decker, 'Renewing Defense Innovation: Five Incentives for Forming Pentagon-Startup Partnerships', *War on the Rocks*, 3 May 2018, accessed 13 April 2020 https://warontherocks.com/2018/05/renewing-defense-innovation-five-incentives-for-forming- pentagon-startup-partnerships/.

[117] Nicole Ogrysko, "Progress on Security Clearance Backlog Is Real, but Federal Contractors Still Seeking End-to-End Solutions," *Federal News Network*, February 24, 2020.

[118] Holcomb, Griffin. 2020 "Communication Equipment Manufacturing in the U.S." IBISWORLD. March 2020. https://my-ibisworld-com.nduezproxy.idm.oclc.org/us/en/industry/33422/industry-at-a-glance