

Department of Defense Industry Perspective: A Primer Exploration

Max North, James “Wes” Rhea, Armon Ansari*, and Zachary Sellers*

*Information Systems Department
Coles College of Business
Kennesaw State University, Kennesaw, GA, U.S.A.*

Cyril Okhio and Lance Crimm

*Department of Electrical & Computer Engineering
Southern Polytechnic College of Engineering & Engineering Technology
Kennesaw State University, Kennesaw, GA, U.S.A.*

Sarah M. North

*Computer Science Department
College of Computing and Software Engineering
Kennesaw State University, Kennesaw, GA, U.S.A.*

[Abstract] This article presents a primer exploration of the Department of Defense (DoD) industry, along with details concerning the chain of commands within the DoD and its business processes. It briefly provides an overview on Information Systems/Technology and how it is structured and implemented in the DoD. Furthermore, companies that have succeeded and have not completely succeeded in implementing information systems to their companies are included to assist in formulating a conclusion. After examining the DoD’s competitive advantages, studying the importance of the value chain, and applying Porter’s Five Forces, this article concludes that, while the DoD has its flaws, it is able to uphold its competitive strategy and be successful in part due to their utilization of a separate agency for information systems and technology.

[Keywords] department of defense, DoD, Industry, information systems, engineering technology

Introduction

The Department of Defense (DoD) exists as part of the executive branch of the United States’ government that was established in September of 1947. The Department of Defense is responsible for managing all national security agencies and military departments such as the Army, Navy, Air Force, National Security Agency, National Reconnaissance Office, Defense Information Systems Agency, and others. The DoD is directed by the Secretary of Defense alongside the President of the United States. The DoD is headquartered in the Pentagon in Arlington, Virginia. Currently, the DoD employs almost three million people. The United States DoD is the largest country defense organization in the world. According to the DoD’s website, their mission is to “...provide the military forces needed to deter war and to protect the security of our country”. One of the DoD agencies is the Defense Information Systems Agency, also known as the DISA. The availability of the DISA enables military personnel, leaders, and other Defense Agencies to communicate with ease. The DISA is responsible for supporting, operating, and providing information systems/technology and infrastructure for the DoD.

Description of the DoD Industry Structure

The DoD is one of the oldest government agencies where it was evolved and now employs three million people. The Department of Defense is the only one of its kind in the industry. By analyzing through the Porter’s five forces model, the department of defense focuses on a particular industry segment. The department is run by the Secretary of Defense. It has numerous different departments within itself such as the Department of the Army, the Department of the Navy, the Department of the Air Force, the Office of

the Secretary of Defense, and the offices of the Joint Chiefs of Staffs. Its headquarters is at the Pentagon, the world's largest office building (About the Department of Defense, n.d.). Each department has a secretary, staff, and an office. This includes the Army, Navy, and Marine Corps within each department. The department of defense has twenty defense agencies, eight DoD field activities, and nine combat commands. Overall, the department of defense focuses on a strategy on one segment to provide safety for its citizens from harm; it is a profitable industry due to it being the only one of its kind in the industry in the United States, and the DoD focuses on what leads into the competitive strategy used (About the Department of Defense, n.d.).

The Dominant Competitive Strategy within the DoD Industry

The competitive strategy for the Department of Defense is simple and dominant. Here, in the United States, it is to remain the greatest and strongest military force in the world. As for the competitive strategy, it is important that the Department of Defense stay innovative with technology and nuclear force as the rise of sophisticated rivals are trying to become better trained and equipped. There has been a new competitive strategy that the DoD has launched. This being to preserve the ability to project power across transoceanic distances into any theater. According to the DoD, there are three emerging operational challenges that will be faced with this competitive advantage. For instance, the Department of Defense states, "Unlike during the Cold War, the U.S. does not maintain large combat formations in the theaters in which they are expected to fight; most U.S. combat power now resides in the continental U.S. and external states and territories. As a result, a state competitor bent on power projection in its near abroad or along its periphery will likely enjoy a time-space and force correlation advantage early in any crisis" (Defense Department Seeks Ideas for Preserving U.S. Competitive Advantage, n.d.).

For fifteen years, the competitive strategy for the Department of Defense has always been combat operations that were focused on warfare and counterterrorism. From the quote stated above from the Department of Defense, it is clear that the US military is trying to move away from constant on-ground warfare. In other words, with their new competitive strategy, they are trying to push for technology to project power without having to risk the lives of our troops.

For example, in an activity in Syria, the Department of Defense launched a missile from a US Navy warship. This is a clear example of pushing power across transoceanic distance into any threat in the world, but it does not stop here. The DoD still has many other strategies to remain the most feared military in the world (Defense Department Seeks Ideas for Preserving U.S. Competitive Advantage, n.d.).

Although the competitive strategy has been mostly against the Soviet Union focusing on strictly military, there has been a competitive strategy within the DoD that is focusing on political, economic, technological, and ideological dimensions of national power. There is a huge factor that goes in the methodology behind the competitive strategy of the DoD. They are constantly comparing their department to other departments across the world. Not only do we look at other countries' strengths and weaknesses, but also we try to discover what our main strength and weakness is in order to successfully execute a competitive strategy to remain a superpower. As of right now, the main focus of the DoD is policies and plans, force employment, tactics, forces and organization concepts, training, and technology (Defense Department Seeks Ideas for Preserving U.S. Competitive Advantage, n.d.).

While comparing the Department of Defense's competitive strategy to the competitive strategies of other nations is a great way of measuring the effectiveness of the United States of America's DoD, the United States can compare the effectiveness of the DoD in all of the branches of the military. This is a competitive advantage for the United States because they are able to use information systems to communicate between all of the channels each branch supplies. Another advantage that the United States has is that it has a large budget to spend on the country's defense. Because this budget is much larger than other countries, the U. S. military is able to become the top of its industry, thus having a better a better competitive strategy through the use of information systems.

To conclude on the competitive strategy of the DoD, it is hard to really know what the main strategy is. The reason being, we do not want our enemy or rivals to always know what we are planning to further stay advanced in technology. One thing that can be concluded, is that the Department of Defense is

constantly working to stay on top of the competition within the world. President Trump has increased the spending within our military in order to further do research and grow the military that was shrinking for the past few years. It is important to remember that the competitive strategy changes significantly roughly every couple of years, as driven by world events. As for now, the DoD is leading with their competitive strategy and will continue to stay innovative in information systems and technology (Defense Department Seeks Ideas for Preserving U.S. Competitive Advantage, n.d.).

The Value Chains of the DoD Industry

The value chain of a business is another great system that Michael Porter came up with to ensure that companies will provide a great product to the customer that will not only leave the customer happy, but also make the company money. Within the value chain of a company, Porter stated that the value chain is the network of value-creating activities (Kroenke & Boyle, 2019). What this means is that the value chain of a business is everything that a company will do to retrieve new products and then create those products into a finished product and eventually sell to the customer. Porter suggests that each value chain will be equipped with five primary actions and four support actions.

According to Kroenke and Boyle (2019), “A value chain is a network of value-creating activities. That generic chain consists of five primary activities and four support activities.” Because the Department of Defense is a government organization whose purpose is national security, the general public does not know as much about the inner workings of the of the organization as we may about other organization, so it is hard to talk specifically about the value chain of the DoD. To reiterate, the Department of Defense is made up of the military, the National Command Authority, Chairman of the Joint Chiefs of Staff and the unified commands (DoD 101: Overview of the Department of Defense, n.d.).

Within the Department of Defense, the value chain will be a little different from a typical business. The DoD is the Government agency that is in charge of running the United States military services by providing security to the nation and deterring the United States from war. However, the DoD does have a way of providing a value chain. They do this by implementing Porter's five primary activities for a successful value chain. Instead of receiving a certain product or equipment, the DoD hires and selects people for services. The inbound logistics or first step of the value chain is to hire and receive the necessary men and women for the job that they are looking to fulfill. The Department of Defense prides itself on hiring only the best, and this is a crucial part of the value chain in that these people will be their final product.

Obviously, one of the Department of Defense's biggest sectors is the military. The military is made up of the Army, Navy, Air Force, Marine Corps, Coast Guard, and National Guard and Reserve. Each sector has their own purpose and value chain as individual departments, but as one entity, that is the military, their purpose is to “train and equip their personnel to perform warfighting, peacekeeping and humanitarian/disaster assistance tasks.” The military provides security to not only the United States but also globally to work towards peace between countries. Their intense training of the personnel of the military is an important part of their value chain. The military puts in a lot of effort to train their staff properly as to be sure they are at their best to protect the United States of America and the world (DoD 101: Overview of the Department of Defense, n.d.).

The next sector is the National Command Authority, which used to describe the joint team of the President and the Secretary of Defense. Their main purpose is to “plan, advise, and carry out the nation's security policies.” They control the overall logistics of the DoD. Without this sector the whole department would have no organization. The Chairman of the Joint Chiefs of Staff is the President's main military advisor. Depending on the background of the President, if they don't have very much military background this position is vital to the Department of Defense as a whole. The unified commanders “are the direct link from the military forces to the President and the Secretary of Defense.” In conjunction with the Chairman, JCS [Joint Chiefs of Staff] the unified commanders determine how to deploy troops. Because the unified commanders each have different responsibilities, either geographical or global, it helps the National Command Authority and the Chairman, JCS to compartmentalize different projects to make them easier to organize, thusly improving the military's effectiveness. Each of these sectors of the Department of Defense plays an important role in the value chain the overall organization, to help them to achieve their mission,

“to provide the military forces needed to deter war and to protect the security of our country” (Deputy Chief Management Officer, n.d.)

The next step for the DoD will be the operation or manufacturing. In this, the DoD will take their newly hired men and women and shape them into the final product that they need them to be. An example of this would be Marines going off to basic training for 13 weeks in which they will train, mold, and shape each individual into the type of Marine they want them to be. Next, the DoD will continue to implement an activity called “out bounding logistics.” Outbound logistics is when the company finalizes their products and ships them to customers. For the DoD, this would be considered when the now trained soldier, guard, or simply employee is sent to their designated stations to begin active work for their department within the DoD.

After operation and manufacturing is sales and marketing. For the Department of Defense, this is a pretty simple task in that citizens want to be protected and feel safe. By supplying the best product of servicemen, it becomes easy for the buyers (citizens) to get behind the DoD and its philosophies. Finally, the last step is customer service. In our eyes, the Department of Defense uses the final step of the Value Chain very well at ensuring the customer is satisfied with the product. It is hard to complain about the DoD in that we are one of the safest countries in the world. The Department of Defense still does an excellent job of showing the citizens of the United States of America how they plan to continue keeping our country safe and protecting the security of each and every citizen in our country. The DoD uses the value chain of a business a little different than a typical industry, but they definitely still implement the value chain to ensure that they get the best product available.

The Business Process of the DoD Industry (Chain of Command)

According to appian.com, “A business process is a collection of linked tasks which find their end in the delivery of a service or product to a client. A business process has also been defined as a set of activities and tasks that, once completed, will accomplish an organizational goal.” The Department of Defense uses the End-To-End Business Process to run their organization. The Deputy Chief Management Officer heads the process. Their website states “The intent of the End-to-End (E2E) framework is to serve as the foundation for Business Process Reengineering (BPR), which drives business improvement and encourages interoperability, ensuring defense business systems support and enabling cross functional Business Mission Area processes. This framework provides a common point of reference for E2E [End-To-End] efforts throughout all levels of the DoD.” The Business Process is made up of fifteen smaller business processes, including everything from Procedure to Pay, Service to Satisfaction, and Deployment to Redeployment/Retrograde. These fifteen business processes are broken up into five levels 0-4, which break them down even further. The E2E framework also helps with financial organization. The E2E has become a vital business process for the DoD to keep it running smoothly and to highest quality level (Business Process Definition, n.d.).

As outlined in the introduction the Department of Defense, the DoD is responsible for providing the military forces needed to deter war and protect the security of the country. The elements that make up the forces are the Army, Navy, Marine Corps, and Air Force. The President is the Commander-in-Chief and resides over the Secretary of Defense, who exercises authority, direction, and control over the Department of Defense. The office of the Secretary of Defense, Chairman of the Joint Chiefs of Staff, and the Joint Staff provide staff assistance as well as command advice to the Secretary of Defense. These departments are separate from one another and are organized differently, but they function in full coordination and cooperation.

The Office of the Secretary of Defense include many different offices that deal with different entities. For example, the office includes the Director of Operational Test and Evaluation, the Inspector General, as well as the Director of Defense Research and Engineering. The heads of these offices report to the Secretary and carry out commands as they are given. Each different branch of the military is organized under its own Secretary and functions under the authority, direction, and control of the Secretary of Defense. The Secretaries of the different military departments are responsible for the operation and efficiency of his or her department. The orders that the military departments receive are issued through the secretaries of these

departments, their designees, by the Secretary of Defense, law, or under authority specifically delegated in writing by the Secretary of Defense. All of the commanders across the different military departments are responsible for accomplishing military missions assigned to them by the President and Secretary of Defense and exercising command authority over forces assigned to them (About the Department of Defense, n.d.).

Role of Information Systems in the DoD Industry

The Defense Information System Agency (DISA) conducts most of the information systems work for the US Department of Defense. DISA's service catalog lists the various services: command & control, computing, contracting, cybersecurity, enterprise services, enterprise engineering, network services, spectrum, and testing. These services include anything from basic multimedia messaging, all the way to providing systems for critical missions. DISA's contracting can include working with private companies for services such as installing and managing private high-speed network lines. DISA's spectrum services include managing services related to the electromagnetic spectrum. The electromagnetic spectrum includes frequencies below modern radio frequencies. DISA is tasked with managing the network activities of the DoD. The network activities can include private mobile and voice networks and secure voice networks for the President and other high-ranking officials' communication. Additionally, DISA provides information systems support for payroll, accounting, records keeping, and other similar standard departments (Defense Information Systems Agency, n.d.).

The biggest benefit of the Department of Defense's information systems is how connected the government is or can be in temporary situations. DISA has made it fairly easy and secure for the Department of Defense, the President, and others to communicate around the world. Another benefit is the fact that all of the work is done in-house. This can help eliminate hiring a private company that could release sensitive information. Personnel can still leak information, but at least an entire company does not have access to all of the sensitive information. However, the biggest drawback for the age of technology that is utilized by the DoD. Many of the systems are close to 50 years old. The Department of Defense's nuclear messaging system backup uses 8 inch floppy disks. Although, the Department of Defense's chief information officer states that the system is closed that makes it secure and the system is still reliable. This may be true, but because the system is so obsolete, parts are hard to find. The ethics of the Department of Defense's information systems can vary on how people view the DoD. Some U.S. citizens would believe that the information systems are tools for war, especially today with drone strikes. Yet, others might believe that the systems help keep the US safe. It can be hard to define ethical behavior, and the ethics of the Department of Defense's information systems can be hard to evaluate. As with most government agencies, the DoD has had its fair share of bribes, misuse of money, credit card abuse, and more. Simply put, the information systems utilized by the Department of Defense can in a way be considered weapons based on the way the world fights its wars in the modern era. Whether or not the war itself is ethical or justified is up to the individual (Trujillo, 2016; Defense Information Systems Agency, n.d.).

There are many very important roles of information systems within the Department of Defense. The main focuses are in enterprise resources, asset management and protection, and processes. These areas are necessary in accomplishing an information benefit and distributing information throughout the Department of Defense as well as other critical partners. The Department plays a major role in managing the life cycle as it relates to information and data. The processes utilized by the Department of Defense to accomplish their purposes and missions include a focus on information risk management. Also, as it relates to protecting and guarding the information enterprise, the Department incorporates undertakings associated with designing, constructing, populating, obtaining, managing and operating the information and data life cycle. The Department has oversight on interrelated assets such as personnel, finances, general equipment, national security information systems and information technology. By being a part of the information life cycle, the Department can play a major role in ensuring management and protection of resources (Chief Information Officer, U.S. Department of Defense, 2012).

The Chief Information Officer (CIO) for the Department of Defense enabled Defense Information Enterprises to facilitate a new and fresh approach of working. Basically, the information builds it. In addition, it establishes standards, services and processes that allow information across the board to users

that are verified and authorized to access the information. The Defense Information Enterprises is as defined package of services and instruments that provide information and competencies that allow end-users to be more efficient and hopefully more successful in supporting the mission operations. Last but not least, the Defense Information Enterprises includes the information security standards for protecting the information as well as the oversight of the networks (Chief Information Officer, U.S. Department of Defense, 2012).

To assist in accomplishing their missions, groups that work with the Department of Defense and have an information interest must choose the information specific to meet their needs. Therefore, each group needs to define, design, and implement resolutions centered on the business processes and engineering solutions that can take advantage of resources across the enterprise to accomplish the needs of the mission (Chief Information Officer, U.S. Department of Defense).

Dana Deasy, Department of Defense's Chief Information Officer, spoke at the Armed Forces Communications and Electronics Association's Defensive Cyber Operations Symposium in Baltimore on May 17, 2018. He talked to the members of the Department of Defense's technology group about how critical it is to be focused on the mission as well as being flexible enough to be innovative and ground-breaking in the areas of information and information protection. Prior to joining the Department of Defense, Deasy's technology experience was in the private sector. Deasy understands how important it is to communicate the Department of Defense's mission to his stakeholders. During the Armed Forces Communications and Electronics Association's Defense Cyber Operations Symposium, Deasy stated, "When you ask 10 different people in the private sector 'Why are we here?' you might get 10 different answers. But here (DoD), everyone talks about the mission and how it aligns to the National Defense Strategy." "Everybody is crystal clear on the focus of the mission."

Deasy specifically envisions information systems being innovative in cyber for the following disciplines:

- Data integration
- Big data
- Machine learning
- Artificial intelligence
- Cloud

Concerning the cloud, Deasy stated, "It's really important to understand this is not a case where you're trying to lift out of your old world and you're suddenly trying to drop into your new world. But this is the most phenomenal opportunity I think we've ever experienced as technical folks ... to be able to look at your legacy estate and say, 'This is a brilliant opportunity to reengineer.'" "Cloud allows you to do amazing things that you simply haven't been able to do historically. It gives us as IT professionals a whole new way to operate our estate and to build the future of how we want IT to run." (Costello and Information Technology Initiatives Must Be Tied to DOD's Mission, Official Says, 2018).

Drawbacks: Drawbacks can be drawn from the content presented. For example, implementing IT systems into any environment warrants properly securing these environments (Kroenke & Boyle, 2019). Large amounts of IT infrastructure require large amounts of security infrastructure, especially concerning the level of clearance required to work within the United States government. Cost can also be a drawback given the size of government infrastructure and upkeep required to run such a large-scale government IT environment.

Laws and Ethics: One of the major Laws found concerning DoD IT systems is the Privacy act. This law guarantees three primary rights:

- The right to see records about oneself, subject to the Privacy Act's exemptions;
- The right to amend a nonexempt record if it is inaccurate, irrelevant, untimely, or incomplete; and
- The right to sue the government for violations of the statute, such as permitting unauthorized individuals to read your records.

This law raises an eyebrow to ethical collection of potential sensitive data. Is the DoD collecting information the individual or group without their knowledge? Do the American people truly depend on this form of covert data collection to maintain security?

Role of Engineering and Engineering Technology in the DoD

The United States has complex challenges from adversaries worldwide and within. Both conventional and non-conventional weapons represent some of the arsenal that are assessable to these adversaries some of which can be very destructive (Defense Business Board, Implications of Technology on the Future Workforce..., n.d.).

The literature on this subject suggests that government agencies need early assessment of the threats to identify the associated issues that can help the protect our societies. Whether a funded research will raise important legal, ethical, and societal concerns should be given the serious considerations that they deserve.

Experience shows that superiority in Engineering & Technological military capability represents the best way for US preparedness and making sure that National Security is assured. So, Engineering and Technological Superiority is very important (The Defense Science Board, 1999). Modern developments are making it possible for the Military to function in an argyle and better-prepared ways than ever before. Command & Control, Surveillance and reconnaissance, intelligence are all now readily available for decision-making, when and where they are needed – All the above justifies the continued development and sustenance of a sophisticated Engineering & Technology infrastructure. Those who want to hurt America seek technologically aided capabilities too, which they can often acquire even from the USA. The devil in the detail is that it is not inconceivable that once these adversaries are able to acquire such capabilities, these might/could end up being used against the United States. Fundamental science that often produce developments that help the military, and vice-versa, often generate or produce spin-offs that have enormous benefits for civilian use and should continue to be encouraged. These investments need to be continued and encouraged (National Research Council, on Being a Scientist, 1995).

Companies within the DoD Industry with Successful Implementation and use of Information Systems

In the defense industry, three companies that have successfully implemented information systems are Lockheed Martin (United States of America), Boeing (United States of America), and Northrop Grumman (United Kingdom). These three companies are some of the largest in the defense industry. They all provide different services for the defense industry. Lockheed Martin mainly sells weapons, Boeing sells aeronautics, and Northrop Grumman sells cyber technology to the Department of Defense. In order to get to where they are today, their use of information systems has been a major reason why they are the leaders in their respective industry (The 25 Biggest Defense Companies in America, 2012)

Lockheed Martin is one company in the defense industry that has successfully implemented information systems. As a company, Lockheed Martin has grown into the one of the largest defense companies in the United States in terms of revenue with \$50 billion earned in recent years. Of this revenue, 71 percent of it was earned through government contracts, with most of the revenue coming from the DoD. Lockheed Martin has a division for their Information Systems team. In the business, it says that the information systems division's main function is "supports customers in data analytics, cyber security, air traffic management and energy demand management. It also provides network-enabled situational awareness, delivers communications and command and control capability through complex mission solutions for defense applications, and integrates complex global systems to help customers gather, analyze and securely distribute critical intelligence data." (Department of Defense Strategy for Operating in Cyberspace, 2011).

The information systems division had made approximately \$700 million in profit in recent years. In 2016, Lockheed Martin combined its information systems with Leidos. The goal of this transaction was "to add large, complex IT system implementation and operation experience, and additional federal and international IT solutions and services work to the Leidos portfolio, providing more venues to sell value

added services such as cybersecurity and analytics.” This transaction was completed and integrated in late 2016 (Lockheed Martin Corporation, 2019; Lockheed Martin Information Systems & Global Solutions, n.d.; Holdings, 2016).

Boeing is another company in the defense industry. As a company, they design, manufacture, and sell airplanes, rockets, and satellites all around the world. In their 2016 annual report, they had over \$100 billion in revenues with 64 percent of that revenue being earned from the DoD. With Boeing, they have a *Terms of Use page* that describes what their information systems main responsibilities are. In the page, it talks about the access right that a buyer has. The buyer is allowed to have access to Boeing’s information system during the length of their contract. Also, Boeing has security assessments for buyers. The buyers have to complete a questionnaire in order to have the right to view information that Boeing provides in their information system. Boeing has rules where their information cannot be transferred to an external system and it does not let buyers have information that is not needed for the use of a contract. (Boeing Company, 2019 Annual Report, 2019; Terms of Use Boeing Information and Electronic Systems, 2016)

Northrop Grumman has been a major company in the defense industry. Their main job activities have been cyber security, where they sell to governments and others for commercial use. Additionally, they are developing autonomous machines. They had over \$24 billion dollars in revenue with a “significant portion” of that coming from the Department of Defense. In their annual report, Northrop Grumman says their information system “provides full life cycle information systems modernization and sustainment, primarily in support of civil government agencies. Key capabilities reside in areas of analytics, mission information processing, cyber and secure networking, and software development” (Northrop Grumman, 2019). Their information system is highly extensive since their main product is an information system, which also has a highly effective fraud detection service. Overall, Northrop Grumman has the best use of information systems in the defense industry because they have been able to make billions of dollars by perfecting and selling it (Northrop Grumman, 2019).

Companies within the DoD Industry with Exceling Potential to Thrive

In the defense industry, three companies that have exceling potential to progresses are CACI International, Navistar Defense, and ManTech. These three companies supply different needs in the defense industry, but they have had some challenges in the past. CACI International provides the United States Army with an information lifeline. Navistar Defense provides ambush-protected vehicles that have a V-shaped hull to deflect IED (Improvised Explosive Devices) blasts away from the troops inside for the United States Marines and the Army. ManTech provides the United States Government's advanced technological needs, from maintaining military surveillance systems to detecting incoming attacks on bases. These three companies could be leaders in the defense industry but they have fallen short (The 25 Biggest Defense Companies in America, 2012; Ausick, 2018).

CACI International provides information solutions and services in support of national security missions and government transformation for Intelligence, Defense, and Federal Civilian clients. CACI provides solutions that enable their clients to make sense of data to make better decisions, improve operations, and gain the information advantage in every mission environment. According to the CACI International website, CACI delivers solutions that enable available data to be used more effectively to provide assessments, gain and maintain situational awareness, support decision-making, and improve operations. CACI used to be the dominant company in the defense industry but has recently taken a backseat. Over the past five years, CACI International has had some financial challenges, which has led to some organizations not putting the trust and money into CACI International. The company had too much budget uncertainty to be a successful leader in the defense industry, however, has a great potential to succeed (Decisive Expertise for Creating Actionable Intelligence, n.d.).

Another company that is not on the top 25 list in the defense industry is Navistar Defense. Navistar Defense is responsible for some of the military vehicles. Navistar offers skilled and specialized support in all of their vehicles, anywhere. This is a great feature to have so the troops do not ride alone and have the

technology to miss an ambush. The only problem is Navistar Defense had to recall over 4,000 vehicles due to an electrical issue and engines that Navistar rushed to use because the original engines did not pass EPA standards. The engine and electrical issue caused the vehicles to have sudden power loss and the engines stalled. This is a big problem because the navigation and help Navistar provides in their vehicles would not work. The only reason the military chose to use Navistar is that the company guaranteed that no troop would ever ride alone. These issues led to a financial hit. Organizations were not putting their trust in Navistar Defense anymore. Navistar could be very successful in the defense industry if their vehicles provided the technology that they have intended (Navistar Defense, n.d.).

The last company has a great potential in the defense industry is ManTech (not near top 25 biggest defense companies list. ManTech is a company that uses advanced technology to help the United States Government protect information. ManTech also supports and maintains critical systems. The company has developed an integrated system to handle the government's complex needs. ManTech International is doing many positive things. The company is cutting down costs and making them more competitive. The problem is ManTech cannot secure contracts with other companies. The reason ManTech International can secure more contracts is that their pricing is extremely high, even with lowering their prices. Additionally, their technology is not as advanced as their competitors are so the price does not work. Overall, ManTech is a great company but they are not able to compete with leaders in the defense industry (The 25 Biggest Defense Companies in America, 2012; Ausick, 2018).

DoD Industry Exploration in View of the Porter's Five Forces Model

Bargaining Power of Customers

For the aspect of bargaining power of customers, the Department of Defense works differently than most employers. There is no particular customer because the Department of Defense is the United States military service. The Department of Defense is responsible for providing security to the whole country of the United States from outside threats and war. Being the nation's largest employer by roughly having two million employees the DoD prides itself on providing the best overall product (security to the nation) to the customers (American Citizens).

As stated on the DoD official website, there truly is no buyer. The Department of Defense works in that the President of the United States is the CEO, Congress is the Board of Directors, and the U.S. citizens are their stockholders. There is no control from the buyer because the DoD works as a government-run agency. It is up to the DoD to help ensure that each part of the DoD is doing their job correctly to help guarantee safety across America. From the Military, National Guard, to thousands of civilians employed by the DoD, it is their responsibility to continue hiring the best to serve and protect this great nation (DoD Open Government, n.d.; About the Department of Defense, n.d.).

Threat of Substitutions

At this time, the Department of Defense can have a few or no competitors because it is the only one in its industry at this moment. However, the DoD can have substitutions that are being created due to its many conflicts with its current suppliers and contractors. Fortunately, during that time, contracts can take a really long time to change or make; since contracts take a while to finish or make on short notice, the DoD does not have many substitutions in its products and services they run. However, the DoD would need to further improve on its standards if it is willing to work with its current providers. The Department of Defense is trying to maintain the control of its current production because some of its providers like its suppliers and contractors are not able to meet the current demands of the DoD; this will allow other substitutions and firms to increase, making the DoD improve its current requirements for its local suppliers and contractors. To its advantage, the DoD can receive foreign products and services as a second source, but it can quickly become a national threat towards the DoD because foreign products and services are unfamiliar to the United States (Kroenke & Boyle, 2019).

Bargaining Power of Suppliers

The Department of Defense has a vast number of contractors that supply them. The companies that supply to the DoD range from weapons and vehicle manufacturing companies to companies that offer training and relocation services. The number of companies that supply to the DoD is so vast and provide many different types of services that it is almost impossible for most of the companies to hold any sort of advantage when it comes to prices. There are at least 55,000 companies that supply to the DoD. There are few companies that can control the price to a certain extent. Companies like Lockheed Martin and Northrop Grumman provide the government with airplanes can control the price because there are so few competitors in the industry. It is easy to switch contractors; once the contract is expired, the contract is rebid.

Threat of New Entry

The Department of Defense is a United States government agency that is part of the executive branch (The Executive Branch, 2015). Due to the fact that the DoD is run as a government entity, it is deemed a nonprofit organization or NPO (Freeman, 2011). Due to the extensive changes in government structure required to create a new DoD like entity, the threat of new entrants is incredibly low to nonexistent. Therefore, this section of Porter's Five Forces is difficult to apply unless you look at the companies contracted out by the DoD.

At first glance, one might think business with the U.S. Department of Defense is relatively possible for any size business. The DoD even provides step by step documents on their website for small businesses to enter into the realm of defense contracts. A recent movie titled "War Dogs", based on a true story, depicts working for the pentagon and how this process is possible. Taking a closer look into the level of business required to earn DoD contracts proves that the experience depicted in "War Dogs" is more of an outlier. Looking at contract data from recent years, "the top 10 defense contractors received {approximately over} \$200 billion dollars in recent years" (Ausick, 2018). This makes up 41 percent of the spending budgeted for the year 2014 (just list an example).

Rivalry (Competitive)

Within the defense industry, companies compete for government contracts for services as well as weaponry and combat gear; these different companies become rivals through tough price competition. The rivalries in the defense industry arise from companies bidding on projects and contracts for weapons because in this industry, the lowest price usually wins. There are not as many competitors in this industry as others because it is such a specialized area, and in most cases, the rivals are of similar size. With this being true, companies have to be aware of their rivals' reverse engineering products. Reverse engineering is taking apart a product in order to mimic the makeup of that specific product. To combat the possibility of a rival reverse engineering a product, companies will only sell certain products to the military in order for other companies to refrain from obtaining valuable trade secrets (Department of Defense 1994, n.d).

Direct rivals to the DoD would basically include all enemies domestic and abroad, because the DoD is the department that defends this country from potential danger (anyone or any group that poses a threat is a rival). Rivals of the DoD also include people in the country that may cause unrest or chaos; this is evident when military forces are sent to areas in the midst of turmoil to suppress the situation (Department of Defense 1994, n.d).

Concise Conclusions and Recommendations

The Department of Defense's use of a separate agency just for information systems and technology is why the Department of Defense succeeds with its information systems. The Department of Defense is able to uphold its competitive strategy of remaining the strongest military force in the world through its use and implementation of information systems and technology. The Department of Defense does have its flaws when it comes to technology; however, they do know how to manage their technology in an effective manner.

The department of defense should elect a chief officer who can help and work with the department to create more innovations. It should also establish a computer innovation like a "human cloud" where it can

become a resource on software and establish programs to solve software problems in a quick manner. Overall, there should be more emphasis on properly training decision makers of the military and the DoD in the art of business management, logistics, and finance. This will create greater accountability to the American people and help cut such large random surplus of materials or assets.

Acknowledgment

The content of this descriptive article does not reflect the position or policy of the Department of Defense and all affiliated entities; and no official endorsement should be inferred. Armon Ansari and Zachary Sellers are Information Systems undergraduate students who diligently conducted the initial research for this article. Authors are merely reporting a collection of publicly available information about the Department of Defense. Furthermore, authors are not implicitly or explicitly expressing any opinions in this article.

References

- Boeing Company, *2019 Annual Report*. Retrieved from <http://www.annualreports.com/Company/boeing-company>
- Lockheed Martin Corporation, *2019 Annual Report*. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/eo/documents/annual-reports/lockheed_martin_annual_report_2019.pdf
- Northrop Grumman, *2019 Annual Report*. Retrieved from <https://www.northropgrumman.com/who-we-are/annual-reports/>
- Navistar Defense. n.d. Retrieved from <https://www.navistardefense.com/navistardefense/>
- About the Department of Defense. (n.d.). Retrieved from <http://www.defense.gov/About-DoD>
- Business Process Definition. Appian. n.d. Retrieved from appian.com/bpm/definition-of-a-business-process
- Decisive Expertise for Creating Actionable Intelligence. (n.d.). Retrieved from http://www.caci.com/intelligence_services/
- Department Of Defense. (n.d.). Retrieved from defense.gov/News/Article/Article/994585/defense-department-seeks-ideas-for-preserving-us-competitive-advantage/
- Defense Information Systems Agency. n.d. Retrieved from allgov.com/departments/department-of-defense/defense-information-systems-agency?agencyid=7363
- Department of Defense 1994. (n.d.). Retrieved from <http://govinfo.library.unt.edu/npr/library/status/mission/mDoD.htm>
- Products and Services End-to-End Business Process Integration Framework. n.d. Retrieved from dcmo.defense.gov/Products-and-Services/End-to-End-Business-Process-Integration-Framework/
- DoD 101: Overview of the Department of Defense. *U.S. Department Of Defense*. n.d. Retrieved from defense.gov/About/DoD-101/
- Department of Defense Strategy for Operating in Cyberspace. (2011). Retrieved from <https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf>
- DoD Open Government. (n.d.). Retrieved from <http://open.defense.gov/Transparency/Privacy-Act-and-Records/>
- Holdings, I. L. (2016). *Leidos to Combine with Lockheed Martin Information Systems & Global Solutions Business (IS&GS)*. Retrieved from <https://www.prnewswire.com/news-releases/leidos-to-combine-with-lockheed-martin-information-systems--global-solutions-business-isgs-300209692.html>
- Kroenke, D. M., Boyle, R. J., 2019. *Using MIS. Eleventh Edition*. Boston: Pearson.
- Lockheed Martin Information Systems & Global Solutions. (2015). Navistar Defense. (n.d.). Retrieved from navistar.com/navistar/globalportfolio/products/defense
- Freeman, R. J. (2011). *Governmental and nonprofit accounting: Theory and Practice*. Boston, MA:

- Pearson Education.
- Terms of Use Boeing Information and Electronic Systems. (2016). Boeing Suppliers. Retrieved from http://www.boeingsuppliers.com/terms_conditions/TermsOfUseOfBoeingInformationAndElectronicSystemsSupplement_062016.pdf
- The 25 Biggest Defense Companies in America. (2012). Retrieved from businessinsider.com/top-25-us-defense-companies-2012-2
- Ausick, p. (2018). America's 15 Biggest Defense Contractors. Retrieved from <https://247wallst.com/special-report/2018/07/02/americas-15-biggest-defense-contractors/>
- The Executive Branch. (2015). Retrieved from <https://www.whitehouse.gov/1600/executive-branch>
- Trujillo, M. (2016). *Five of the most outdated IT system in the government*. Retrieved from <https://thehill.com/policy/technology/281560-five-of-the-most-outdated-it-system-in-the-government>
- Chief Information Officer, Department of Defense. 2012. Retrieved from <https://DoDcio.defense.gov/InTheNews/DoD-Information-Enterprise-Architecture/DataandServicesDeployment-DSD/>
- Costello, Noreen. Information Technology Initiatives Must Be Tied to DoD's Mission, Official Says. May 2018. Retrieved from <https://www.defense.gov/Explore/News/Article/Article/1525373/information-technology-initiatives-must-be-tied-to-DoDs-mission-official-says/>
- Defense Business Board, Implications of Technology on the Future Workforce DBB FY17-04 Recommendations on the impact of automated technologies, (2016). Retrieved from [https://dbb.defense.gov/Portals/35/Documents/Reports/2017/DBB%20FY17-04%20Implications%20of%20Technology%20on%20the%20Future%20Workforce%20-%20Final%20\(Jun%202018\).pdf](https://dbb.defense.gov/Portals/35/Documents/Reports/2017/DBB%20FY17-04%20Implications%20of%20Technology%20on%20the%20Future%20Workforce%20-%20Final%20(Jun%202018).pdf)
- National Research Council, On Being a Scientist, *National Academy Press*, Washington, D.C. (1995). 20-21.
- Defense Science Board, *The Defense Science Board 1999 Summer Study Task Force on 21st Century Defense Technology Strategies*, Volume 1, U.S. Department of Defense, (1999). Retrieved from <http://www.dtic.mil/docs/citations/ADA433941>