The Race to Implement Artificial Intelligence

Changing practices in order to catch up with our adversaries

by LtCol Andrew J. Konicki

The DOD is at a crossroads of identity within the business side of the Department. This identity is mixed between service members who know nothing else but constant deployments and war where heavy vehicles and advancements in personal protective equipment have saved lives because of rapid acquisition. This is compared to those who continue to live the days of past where long, drawn out multi-billion dollar major defense acquisition programs continue to dominate the landscape, like the joint strike fighter. The latter, in large part, is because of a 1960's process introduced by then-Secretary of Defense Robert McNamara known as the Planning, Programming, and Budgeting System[1] combined with the Defense Acquisition System as laid out in the DOD Instruction 5000.02[2] and the Joint Capabilities Integration and Development System. These three systems make up what is known as the triad of the weapons acquisition and procurement system (See Figure 1).

>LtCol Konicki is a Ground Acquisition Professional and served as a Secretary of Defense Executive Fellow with the Microsoft Corporation.

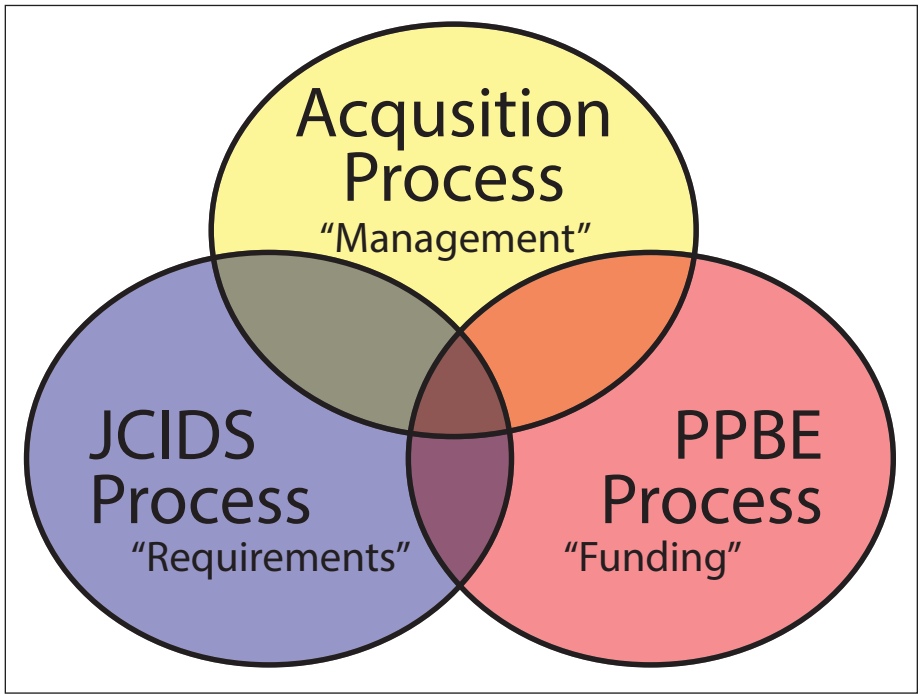

Figure 1. Defense Acquisition System Triad.[3] *(Figure by author.)*

This system may work for MDAPs; however, it hinders progress and enhancement of the DOD's ability to make decisions and field information technology (IT) equipment at the speed of relevance. Moore's Law[4] states the number of silicon transistors will double every two years.[5] In this environment of advancing technology, the DOD needs to be at the cutting edge. Experts have predicted that our near-peer adversaries will surpass the United States' technological advancements in artificial intelligence (AI) within the next one to two years.[6]

If that happens, our adversaries will have the technological advantage and a near-term capability to defeat the United States in either a kinetic or non-kinetic war. This threatens our way of life and status as a global superpower.

Since the end of World War II, the United States has enjoyed a competitive advantage over state rivals. Yet this advantage has decreased over the past several years because of the advancements in and democratization of AI technology. U.S. competitors such as China and Russia continue to embrace AI and have further encouraged the development through state investment. Russian President Vladimir Putin stated:

> Artificial Intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities,

> but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world.[7]

The Chairman of the Joint Chiefs of Staff, Gen Joseph Dunford, takes it further, stating:

> I am confident in saying we can defend the homeland and our way of life, we can meet our alliance commitments today, and we have an aggregate competitive advantage over any potential adversary. I am equally confident in saying that if we don't change the trajectory we are on … whoever is sitting in my seat five or seven years from now will not be as confident as I am.[8]

Clearly, the United States is in an AI arms race with China and Russia that according to a petition from Elon Musk and 116 other technology leaders to the United Nations,

> The introduction of autonomous [AI] technology would be tantamount to a 'third revolution in warfare,' following the development of gunpowder and nuclear weapons.[9]

To ensure the United States remains ahead of its competitors and to win the race of AI, the DOD needs to change its current acquisition business practices by doing three things: accept risk, empower and trust our uniformed and civil servants below the General Officer/Flag/SES level, and work with industry as a partner to understand the latest technology advancements.

Information Technology Risk Acceptance

It is often said the DOD is too risk averse. This statement is contrary to the very nature of military members risking their lives in a foreign land in service of their country. DOD is very risk accepting within an operational context, but tends to be more risk averse when developing and acquiring new equipment for use. This action trickles down to the service members where they are forced to use obsolete equipment unless there is some compelling reason such as the need for heavily armored vehicles or improvements to personal protective equipment to prevent injury and death at large scale. Events like these experienced during Operations IRAQI FREEDOM (OIF) and ENDURING FREEDOM (OEF) allowed for the use of a rapid procurement process, but this was an exception to the norm. Today, the United States is at war, although not a kinetic war where roadside bombs and ambushes are the actions taking place, but a non-kinetic war where cyber warfare is the primary instrument of barrage.

As indicated in the investigations following the 2016 presidential election, the Russians have already impacted our democratic electoral process through cyber.[10] This ever-evolving war of cyber with nation-states, such as China and Russia, and the democratization of cyberwarfare used by non-state actors will continue into the foreseeable future:

> Every day, the Defense Department thwarts 36 million emails full of malware, viruses and phishing schemes from hackers, terrorists and foreign adversaries trying to gain unauthorized access to military systems.[11]

Such a figure becomes even more daunting when we note that this does not account for those attacks that occur outside of email, or even those that are successful.

Daniel Coats, Director of National Intelligence, addressed this in his February 2018 statements to the Senate Select Committee on Intelligence. He stated:

> The risk of interstate conflict is higher than any time since the end of the Cold War. Our adversaries, as well as the other malign actors, are using cyber and other instruments of power to shape societies and markets, international rules and institutions, and international hotspots to their advantage. [They] seek to sow division in the United States and weaken U.S. leadership.[12]

To thwart such attacks, the business side of DOD needs to modify their approach of acquisition risk acceptance similar to how a commander accepts risk in a kinetic wartime environment.

The DOD is very familiar with operational risk. Commanders risk people and equipment every day in training and on the battlefield. They put those they are responsible for in danger and understand those dangers by weighing the likelihood of occurrence against the consequence and mitigate those things they can by reducing the chance of occurrence. The commander knows he may lose people and equipment in pursuit of an important military objective. Accepting this risk, even while actively seeking to mitigate it, is part of the training of a military professional.

However, the business side of the military is vastly different. Within the business side, risk is measured subjectively by making a best guess at the likelihood of occurrence. Then, objective terms are used to describe the consequence aspect as it relates to the equipment DOD is developing and then fielding associated to cost, schedule, and performance (C/S/P). Risks are viewed from a technical (performance) and non-technical lens (cost and schedule) based upon the maturity of the technology, staffing, funding, and manufacturing capability.

Typically, performance risk is one that is heavily looked upon as it impacts a multitude of aspects to include cost and schedule. For instance, if the maturity of a specific technology is not at the level as it should be based upon the agreed upon schedule, then there is a strong likelihood the schedule will slip while costing the government additional funds to continue the project. The program office will then look at ways to mature the technology faster to get back on schedule, but this usually adds to the cost because the contractor needs to add more people or work longer hours to advance the performance attribute.

The technical aspects are governed by the Joint Capabilities Integration and Development System requirement document which identifies threshold and objective values, such that the threshold is the absolute minimum requirement and objective is the desired level. Traditionally, performance attributes have to reach a threshold value and be validated in an operational environment through testing before the government fields the product. This type of model works well if the program is a MDAP such as the joint strike fighter or an aircraft carrier, but when it comes to IT, this model falls short. The Software Acquisition and Practices

report recently released by the Defense Innovation Board:[13]

> Hardware can be developed, procured, and maintained in a linear fashion. Software is an enduring capability that must be supported and continuously improved throughout its life cycle. DoD must streamline its acquisition process and transform its culture to enable effective delivery and oversight of multiple types of software-enabled systems, at scale, and at the speed of relevance.[14]

Performance of IT is different from a major platform such as an aircraft carrier for several reasons but predominately because it is based upon software derived code (i.e., 1s and 0s). The beautiful thing with software is that if it does not work when deployed, the organization can roll back to a previous version while working out the bugs. Even then, the deployed software platform does not have to meet 100 percent of the threshold requirements if the code is not ready. The organization may accept some risk and deploy what is available while working to improve the platform on an iterative basis.

The corporate IT world uses secure development operations (SecDevOps) as this iterative process. SecDevOps is based on an agile philosophy which stresses short development cycles with smaller goals per cycle showing demonstrable progress with each sprint. This introduces the concept of failing fast but failing small as opposed to failing big and slowing the entire process to a crawl. This practice is used throughout the life of the application. Figure 2 (on next page) displays this model.[15]

To expound further upon this thought and referring to the Defense Innovation Board's Software Acquisition and Practices report:

> Speed and cycle time are the most important metrics for managing software. To maintain advantage, DoD needs to procure, deploy, and update software that works for its users at the speed of mission need, executing more quickly than our adversaries. Statutes, regulations, and cultural norms that get in the way of deploying software to the field quickly weaken our national security and expose our nation to risk.[16]

Currently, the DOD uses the Defense Acquisition University wall chart (see Figure 3 on next page) as the process to execute defense programs from "cradle to grave," to include software programs.[17] To those who simply follow a process, this chart is very complicated and time consuming as it relates to developing, testing, procuring, fielding, and sustaining equipment for military use.

This chart is meant to serve as a framework so that as a program is moving through the appropriate gates, the events can be tailored sufficiently to mitigate risk while meeting the C/S/P parameters. However, too many of those in the acquisition workforce see this chart as *the* means to delivering a product rather than as a framework. This is meant to only serve as a guide to move a program through the various phases and is not a roadmap or blueprint to success. This requires a keen understanding of the program and where it resides regarding technological maturity. To quote Frank Kendall, former Undersecretary of Defense for Acquisition, Technology, and Logistics, "Process is the refuge of the mediocre." Those who are slaves to the process will not achieve anything beyond mediocrity because they do not think through the problem.

During the early stages of OIF and OEF, DOD exercised risk acceptance by using a rapid procurement process outside of the framework shown in Figure 3 to procure and field heavy armored vehicles and personal protective equipment. This process was authorized because thousands of service members were getting injured or dying because of roadside bombs while conducting military operations. To save lives, DOD accepted risk and shortened the acquisition timeline to months vice years.

Today, the United States remains at war, and DOD needs to treat the development and use of software, specifically AI, like the heavily armored vehicles and personal protective equipment used during OIF and OEF. DOD must act with the same sense of purpose and speed as it did following the terrorist attacks on 11 September 2001, where acquisition risk was seen as an operational risk such that human lives were on the line.

Empowerment and Trust in Warfighting and Acquisitions

At the rank of lieutenant colonel, a battalion commander is empowered and trusted to lead over a thousand plus service members into harm's way. These leaders shoulder the magnitude of successfully conducting a mission where the potential cost is human lives. Although human lives are not at risk, a lieutenant colonel program manager (PM) is charged with delivering a capability to the warfighter within C/S/P parameters. However, the same type of empowerment and trust as provided to their battalion commander counterparts is not provided to a PM where the cost is dollars, not lives. This type of juxtaposition results in stagnation and paralysis when developing and fielding future capabilities. Through empowerment and trust from seniors to juniors as dictated in military doctrinal publications and practiced throughout industry, the business arm of DOD can improve their ability to develop, procure, and implement AI capabilities that will enable the United States to remain ahead of its global competitors.

Marine Corps Doctrinal Publication 1: Warfighting (MCDP 1) captures this realization when it states, "Leaders must have a strong sense of great responsibility of their office; the resources they expend in war are human lives."[18] The gravity of the potential cost weighs heavy on commanders, yet they are entrusted to carry out their mission despite the cost as a result of training, thoroughness, and the fact that these individuals were selected by personnel of senior rank whom held similar positions. Those on the selection committees understand what it takes to command and use a rigorous process to choose those best suited.

Although PMs are selected using a similar process as commanders, the same empowerment and trust is not provided on the business side of DOD. A PM whose sole responsibility is to execute a program in accordance with the established C/S/P parameters should have the trust and confidence of those senior to obligate funds and field equipment as a result of acquisition training, education, experience, and best judgment: all similar traits as

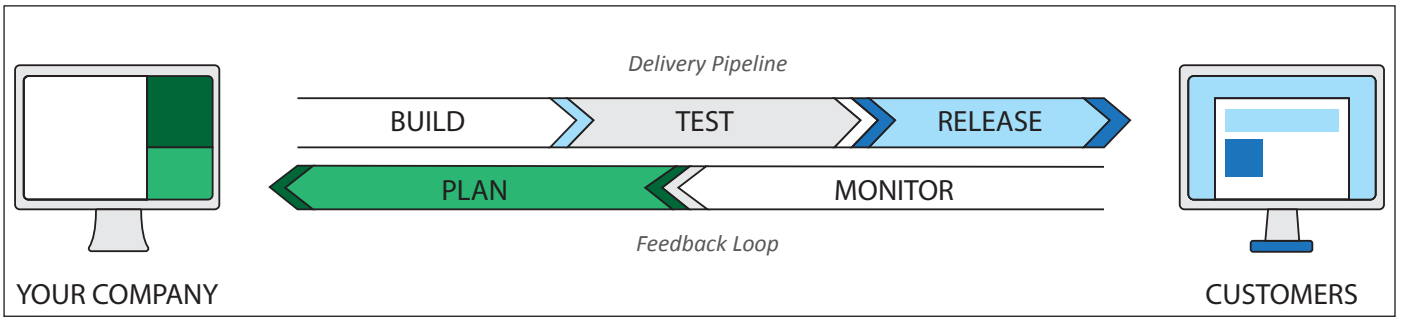

Figure 2. SecDevOps model. *(Figure by author.)*

their peers in the operational context. Why is the mindset so different from the operational environment compared to the acquisition environment? The answer is because there is a monetary value associated to that PM's decision that may cost the government millions of dollars. Which bodes the question, what is more valuable: human lives or money? Without adjustment, we have what we have today, a slow, hindering process that frequently delivers technology bordering on obsolescence.

However, there is opportunity for change. DOD can adopt something similar to the "Basic Rules of Management" according to former CEO of 3M, William McKnight:

> As our business grows, it becomes increasingly necessary to delegate responsibility and to encourage men and women to exercise their initiative. This requires considerable tolerance. Those men and women, to whom we delegate authority and responsibility, if they are good people, are going to want to do their jobs in their own way.

Mistakes will be made. But if a person is essentially right, the mistakes he or she makes are not as serious in the long run as the mistakes management will make if it undertakes to tell those in authority exactly how they must do their jobs.

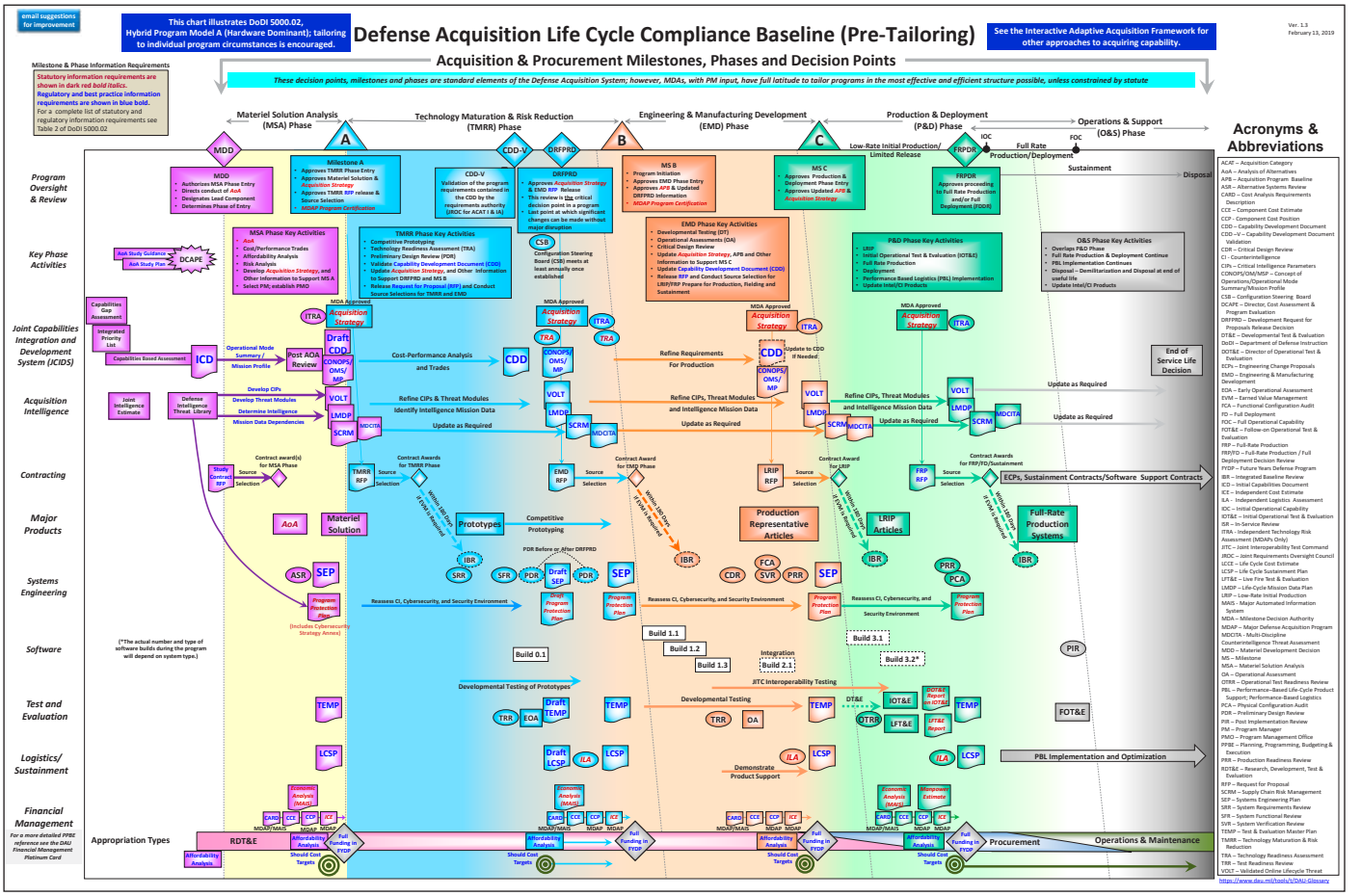

Figure 3. Defense acquisition life cycle wall chart. *(Figure provided by author.)*

Management that is destructively critical when mistakes are made kills initiative, and it is essential that we have many people with initiative if we are to continue to grow.[19]

In 1948, William McKnight instituted this approach throughout the company, and it is still applied today. DOD can learn something from 3M and institute a similar approach.

As McKnight says, "Mistakes will be made," but how the organization reacts to the mistakes dictates future behavior. Commonly, DOD punishes the many for the mistakes of the few. Knee jerk reactions associated with poor judgment or misguided individuals are common place. As a result, the acquisition decision making authority is pulled up to the highest levels within the Services such that the cycle-time of the observe–orient–decide–act (OODA) loop is dramatically increased to the point of causing near paralysis. This type of approach is not conducive to instilling initiative within a military force, particularly within an acquisition workforce focused on delivering a capability like AI.

MCDP 1 discusses how Marines on the battlefield need to display "a penchant for boldness and initiative down to the lowest levels."[20] This same mentality should carry over to the business workforce of DOD. Initiative and boldness will carry the Department forward as it transforms its digital presence; however, senior leaders must have a moderate appetite to allow for failure.

As McKnight states, "Management that is destructively critical when mistakes are made kills initiative." *MCDP 1* echoes this sentiment,

> junior leaders stemming from overboldness are a necessary part of learning. We should deal with such errors leniently; there must be no 'zero defects' mentality.[21]

However, removing a zero defects mentality does not remove criticism or accountability. In fact, criticism and accountability are crucial as it leads to learning; otherwise, individuals act reckless and without consequence while never learning from their mistakes.

Corporate America refers to this as "failing fast." This allows for a quicker cycle time of figuring out what does not work, and then making adjustments to figure out what does work. Not only is this cycle time faster, but the expense on resources, such as time and funding, is minimized to the greatest extent possible. DOD can take this as a lesson learned and reduce the amount of funding chasing failing technology and invest in technologies that are proving out. The Defense Innovation Board concurs as representative in their Software Acquisition and Practices study. An idea for change regarding software development is to "encourage projects and pilot efforts that serve to reduce risk and complexity—fail fast."[22]

Industry as a Partner

A strong, mutually beneficial partnership between DOD and the IT industry is required to maintain U.S. global superiority. Senior DOD officials like to refer to industry as "partners," but the relationship is not a true partnership where both entities have shared interests and a common purpose or goal. Often government and military personnel view industry through the lens of orthogonally aligned incentives and value models. This misperception creates a relationship of mistrust and hidden agendas which is not conducive to a successful partnership. Additionally, DOD believes certain companies would not exist without their funds. Although this may be the case for a very select few, most large, successful technology companies do not need to work with DOD in order to maintain their bottom line.

As an example, Microsoft Corporation has worked with DOD for over twenty years, and earns roughly one percent of their annual revenue from DOD business. [23] Microsoft chooses to work with DOD because they understand that although they are a global company, supporting the DOD allows Microsoft to continue to operate as a U.S.-based company.

Recently, in response to employee backlash, Satya Nadella defended Microsoft's position on an Army contract for augmented reality when he stated,

> We made a principled decision that we're not going to withhold technology from institutions that we have elected in democracies to protect the freedoms we enjoy.[24]

Not only does this company and many like it, want to work with DOD, they understand the importance as it relates to national security.

Ultimately, DOD is highly dependent upon outside contractors to deliver goods and services to enable the warfighter. Contrary to that position, very few companies rely upon DOD as a contracting source to generate large revenue streams. Those companies that are leading the way in cloud computing, AI, and software development do not need DOD to please their shareholders or improve the bottom line on their income statement. These companies want to work with DOD as a means to share technology and allow for its use to ensure that the United States remains a step or two ahead of its global competitors.

A contributing factor to the adversarial positioning previously mentioned is the way DOD acquisition professionals view profit. As good stewards of the taxpayers' dollar, the business side of DOD aims to get value out of every dollar spent. This is very noble and is an excellent practice. However, the partnership crumbles when DOD tries to squeeze every bit of profit out of the vendor to the point where the vendor is basically giving the product away at cost. This type of practice does not foster a good relationship for either party. In fact, this type of practice incites bad practices such as cost and schedule overruns in non-firm fixed price contracts, hidden costs for increased capability, and "balloon payments" when exercising option years on a contract. These types of behavior have an end result where the government is forced to pay more than they bargained for because the vendor has to show a profit margin.

Ultimately, the vendor is held accountable by its board of directors and their shareholders. If the business is not turning a profit, then they simply will not do business with DOD. Additionally, a fair "profit margin is required for companies to remain in business and

for competition to exist, which is also necessary to maintain a robust military industrial base."[25]

As a means to better partner with industry, DOD should periodically meet with industry technology leaders to understand the latest advancements. This will help generate new applications for the use of the technology and foster a warfighter need. Additionally, DOD should take greater advantage of releasing draft requests for proposals to gain industry's perspective on the requirements. There are times when industry will come back and say something is not technologically achievable, or more likely that technology has advanced beyond what DOD is asking for, and that they should modify the request for proposal to make it more reflective of current technology. Either way, positive two-way communication is essential to a strong partnership.

A strong partnership between DOD and industry is crucial to success. By ensuring a mutually beneficial relationship, DOD and the technology industry will better enhance the warfighters' capabilities while securing the freedom of the United States, to include those companies headquartered here.

Conclusion

As DOD continues to prepare for future conflicts orchestrating around a visible enemy, they are missing the fight that is already occurring: the cyberwar and AI arms race. Within a few years, global competitors such as China and Russia will surpass the United States' technological advantage which will cripple U.S. global superiority. DOD must take action in this realm with the help and partnership of the IT business community coupled with some uncomfortable cultural changes/business practices. Practices such as failing fast, use of SecDevOps, and empowerment and trust are all needed to remain ahead of the adversaries' OODA loop. DOD must engage faster in its digital transformation or fall to the point of irrelevancy against its global challengers.

Background

For the past nine months, I have had the fortunate opportunity to serve as a Secretary of Defense Executive Fellow (SDEF) with the Microsoft Corporation. As a Fellow with Microsoft, I have seen first-hand the culture of a company that drives an average $95 billion in annual revenue over the past 5 years.

As a member of the SDEF program, I am part of a small group of military lieutenant colonel/colonel level personnel selected to earn senior service college credit outside the traditional war college path by training with corporate America. Annually, each Service chooses roughly three to four service members. Those chosen "have earned a reputation for insightful long-range planning, organizational and management innovation, and implementation of new information and other technologies."[26]

Prior to arriving to corporate assignments, Fellows receive a month of strategic familiarization training associated to the current geopolitical environment and issues facing DOD. This includes lectures by subject matter experts on current political/military issues and leading-edge technologies; meetings with senior DOD officials; business executives; Members of Congress; the press; and former SDEF officers and sponsors. Additionally, Fellows receive executive-level graduate business instruction from professors at the Darden School of Business located at the University of Virginia. Throughout our assignment, Fellows visit other companies participating in the program where they hear from and engage with corporate leaders. Each one of these visits, commonly referred to as "Company Days," lasts for one to two days and each Fellow will attend at least six Company Days throughout the program.

This year, Fellows had assignments to Microsoft, SAP, Raytheon, McAfee, Textron Systems, Johnson & Johnson, 3M, Google, Deutsche Bank, Pratty & Whitney, SpaceX, Cisco Systems, Accenture, Merck & Company, Autodesk, Union Pacific Railroad, McKinsey & Company, VMware, Boeing, and Amazon.

Notes

1. Department of Defense, *DoDI 5000.02: Operation of the Defense Acquisition System,* (Washington, DC: August 2017). In 2003, DOD renamed PPBS to the Planning, Programming, Budgeting, and Execution process "to emphasize the need to better manage the execution of budget authority provided by Congress." Although the name changed, the overall function of the process remained the same.

2. Ibid. *DoDI 5000.02* provides the detailed procedures that guide the operation of the system.

3. Berton Manning, "Acquisition Topics: JCIDS Process," *AcqNotes*, (November 2018), available at http://acqnotes.com.

4. Moore originally made his prediction in 1965, but his prediction was pessimistic as the amount of transistors doubled approximately every 18 months for the next 50 years. This growth is because of the shrinking size of the transistors. In the late 1940s, the transistor was measured in millimeters; in 2010, the size was measured in tens of nanometers which is one-billionth of a meter. This is a reduction factor of over 100,000.

5. Staff, *Encyclopedia Britannica,* s.v., "Moore's Law: Computer Science," (March 2019), available at https://www.britannica.com.

6. Will Knight, "China May Overtake the US with the Best AI Research in Just Two Years." *MIT Technology Review.* (March 2019), available at https://www.technologyreview.com.

7. James Vincent, "Putin Says the Nation That Leads in AI 'Will Be the Ruler of the World'," *The Verge*, (September 2017), available at https://www.theverge.com.

8. Jim Garamone, "Dunford Discusses Near-Peer Competition, Keeping U.S. Military Edge," *Defense.Gov*., (December 2018,) available at https://dod.defense.gov.

9. "Putin Says the Nation That Leads in AI 'Will Be the Ruler of the World'."

10. Staff, "2016 Presidential Campaign Hacking Fast Facts," *CNN,* (October 2019), available at https://www.cnn.com.

11. Frank Konkel, "And You Thought Your Inbox was Dangerous," *Nextgov,* (January 2018), available at https://www.nextgov.com.

12. Jim Garamone, "Cyber Tops List of Threats to U.S., Director of National Intelligence Says," *Defense.Gov.,* (February 2018), available at https://dod.defense.gov.

13. The DIB provides independent advice and recommendations to the Secretary of Defense, Deputy Secretary of Defense, and other senior leaders across the Department in areas associated to people and culture, technology and capabilities, and practice and operations. Board

members are non-DOD distinguished leaders with a "track record of leading large, innovative organizations or conducting groundbreaking research in technical areas relevant to DoD," (Washington, DC: Defense Innovation Board, 2019).

14. J. Michael McQuade, "Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage," *Defense Innovation Board*, (May 2019), available at https://innovation.defense.gov.

15. Staff, "What is DevOps?" *Amazon Web Series,* available at https://aws.amazon.com.

16. "Software Is Never Done."

17. T.R. Pilling, "Updated DoD Acquisition Life Cycle Wall Chart," Defense Acquisition University, (May 2017), available at https://www.dau.mil.

18. Headquarters Marine Corps, *MCDP 1, Warfighting*, (Washington, DC: 1997).

19. Jonathan Becher, "McKnight's Management Methodolgy," *Forbes,* (February 2016), available at https://www.forbes.com.

20. *MCDP 1.*

21. Ibid.

22. "Software Is Never Done."

23. Staff, "Microsoft Annual Report 2018," Microsoft, (October 2018), available at https://www.microsoft.com.

24. Klint Finley, "Microsoft CEO Defends Army Contract for Augmented Reality," *Wired*, (February 2019), available at https://www.wired.com.

25. Steve Mills, "We Don't Dance Well: Government and Industry Defense Material Acquisition," *Defense AT&L,* (Fort Belvoir, VA: Defense Acquisition University, March-April 2010).

26. Office of the Under Secretary for Personnel and Readiness, "SECDEF Executive Fellows," *Defense.Gov*., available at https://prhome.defense.gov.

>Author's Note: Serving as a Secretary of Defense Executive Fellow during 2018-19 with Microsoft has been an amazing, educational, and eye-opening experience. I would like to thank several people for allowing me to travel on this journey the past year. First, I would like to thank my wife for being by my side, supporting me, listening to me, serving as my counsel, and putting up with my travel schedule while attending to the house and our children. Thank you! I would also like to thank Col Brock McDaniel for nominating me for this program and ensuring I had this opportunity. I am extremely grateful. Lastly, I would like to thank those at Microsoft that openly welcomed me aboard from Day One and allowed me to have an up close and personal view of their world. Thank you: Greg, Leigh, Drifter, Marc, Suj, Derek, Rob, Steve, Jim, Sean, Julie, and Pat. All of you are amazing, and I look forward to maintaining contact well into the future.