DEFENSE INNOVATION BOARD

RECOMMENDATIONS

People & Culture

Recommendation 1: Appoint a Chief Innovation Officer and Build Innovation Capacity in the Workforce. Appoint a DoD Chief Innovation Officer (CINO) to serve as an advocate for innovation; coordinate, oversee, and synchronize innovation activities across the Department; and lead capacity-building efforts to promote innovation in the workforce. Working with relevant senior officials in the Department, the CINO should (a) design a template for innovation and set of principles that can be broadly applied; (b) establish a program office to build capacity to spur workforce-driven innovation, such as innovation tournaments and educational activities; and (c) launch a Defense Innovation Network (DIN), a community of interest and internal technology platform for information-sharing. The DIN will spearhead activities to increase rapid incorporation of the best available innovations and practices, and facilitate internal crowdsourcing activities.

Recommendation 2: Embed Computer Science as a Core Competency of the Department through Recruiting and Training. Establish a career track for computer scientists in the military that is intended to provide incentives for service members to specialize in computer science and programming fields, to get the additional training and opportunities they require to advance, and protect them from pressures to rotate into unrelated roles. To attract Science, Technology, Engineering, and Math (STEM) talent to this cadre, establish new and expand existing programs that attract promising undergraduate and graduate students in computer science, engineering, and related fields to commit to military service for a period of time in exchange for scholarships or debt relief. These recruits should have recruiting standards and training that is tailored appropriately to their unique role.

Recommendation 3: Embrace a Culture of Experimentation. Encourage evidence-based, outcome-driven policies and experimentation by (a) testing multiple strategies simultaneously and using evidence to assess them; (b) testing different operational approaches in real time to accelerate learning; (c) creating opportunities to incorporate diverse viewpoints into decision-making processes; (d) offering bonuses, recognition, awards, and other incentives for managers who promote innovation and experimentation, give employees greater voice, and encourage creativity and divergent views.

Technology & Capabilities

Recommendation 4: Assess Cyber Security Vulnerabilities of Advanced Weapons. Direct U.S. Cyber Command, working in coordination with the National Security Agency, to conduct regular security reviews of embedded software and networks for weapons systems to identify vulnerabilities. Require that source code for such systems be made available on an ongoing basis for such testing, and that any detected vulnerabilities are removed. The DoD should identify new standards and practices to eliminate

system vulnerabilities, particularly those that require collaboration between DoD and the defense industry.

Recommendation 5: Catalyze Innovations in Artificial Intelligence and Machine Learning. Establish a DoD center for studying artificial intelligence and machine learning. Like the institutions established in the past to ensure DoD's technological advantage in nuclear weapons, DoD now needs a centralized, focused, well-resourced organization to propel applied research in artificial intelligence and machine learning. This center would coordinate research in these areas across the Department, and liaise with other labs in the private sector and universities, and would also conduct educational efforts to inform the Department about the implications of these advances for the Defense enterprise.

Recommendation 6: Expand Use of Available Acquisition Waivers and Exemptions. Improve the speed and timeliness of acquisition processes by increasing the use of available mechanisms for waivers and exemptions, and by offering incentives for quick resolution of concerns. Identify and broaden the use of "best practices" by specifying aspects of acquisition approaches and techniques that are effective in the Special Operations community that could be applied more generally.

Recommendation 7: Increase Investment in New Approaches to Innovation. Increase investment in and support for the Defense Advanced Research Projects Agency (DARPA), the Strategic Capabilities Office (SCO), the Defense Innovation Unit Experimental (DIUx), Defense Digital Service (DDS), rapid equipping units, and other small, agile, innovation-focused organizations within the DoD. Establish activities to improve communication and coordination between them and to educate DoD leaders and the workforce about their efforts to drive innovation as a means to enhance the Department's overall capabilities. An annual Innovation Synchronization Conference should be held semi-annually to increase information exchanges between these groups. One potential theme for this conference could be Third Offset technologies where each organization brings forward current challenges and potential technological solutions in fields that are relevant to the Third Offset.

Practices & Operations

Recommendation 8: Improve DoD Access to Code. Require that all systems purpose-built for the DoD should have their source code available to DoD. The Department should have the rights to and be able to modify the code.

Recommendation 9: Establish Software Development Teams at Each Major Command. Establish an embedded software development team of government employees -- a "human cloud" of computer programmers and software developers responsive to the commander -- who are available on-demand to swiftly solve software problems by working directly with the owner of the requirement. Small teams of these developers should be assigned to commanders to provide an organic, on-demand resource that is immediately responsive to warfighter needs without necessitating writing a requirement, selecting a vendor, reaching back to a distant resource, or going through lengthy and onerous approval and contracting processes.

Recommendation 10: Make Computing and Bandwidth Abundant. Direct DoD to adopt a strategy for rapidly transitioning DoD Information Technology (IT) to current industry standards such as cloud computing, ubiquitous access to modernized wireless systems leveraging commercial standards, abundant computing power and bandwidth that is made available as a platform, integration of mobile technologies, and the development of a DoD platform for downloading applications.

Recommendation 11: Reward Bureaucracy Busting and Lower Barriers to Innovation. Establish incentives for process simplification, reduction of paperwork and reporting burdens, and "bureaucracy busting" activities such as a prize for proposals that simplify existing processes, increase performance or efficiency, save time or money, or reduce impediments to the mission. To the extent consistent with necessary constraints, use and publicize an organizing principle for innovation and creativity: "make it easier." Leaders need to compensate for the natural inertial pressure of large organizations by constantly repeating a mantra of simplification.

Recommendation 12: Forge New Approach to Data Collection, Sharing, and Analysis. Data is the 21st century equivalent of a global natural resource, like timber, iron, or oil previously – indispensable for sustaining military innovation and advantage. The next global conflicts will be fueled by data. The rapidly expanding power of new mathematical and computing techniques to reveal insights into intentions and capabilities, and to enhance accuracy, lethality, and speed, depend on immense data sets to train algorithms and from which to extract information. The data that provide the raw materials from which to identify patterns, as well as the anomalies that defy them, constitute the fuel that powers the engine of machine learning (ML). Whoever amasses and organizes the most data first will sustain technological superiority, so it is incumbent upon the Department to collect, store, share, analyze, and protect its data faster and better than its competitors. Data must be regarded as one of the most powerful resources in the Department's arsenal.

DEFENSE INNOVATION BOARD

RECOMMENDATIONS AND COMMENTARY FOR THE PUBLIC MEETING ON JANUARY 9, 2017

People & Culture

Recommendation 1: Appoint a Chief Innovation Officer and Build Innovation Capacity in the Workforce

Proposal: Appoint a DoD Chief Innovation Officer (CINO) to coordinate, oversee, and synchronize innovation activities across the Department, serve as a champion for innovation, and lead capacity-building efforts to promote innovation in the workforce. Working with relevant senior officials in the Department, the CINO should (a) design a template for innovation and set of principles that can be broadly applied; (b) establish a program office to build capacity to spur workforce-driven innovation, such as innovation tournaments and educational activities; and (c) launch a Defense Innovation Network (DIN), a community of interest and internal technology platform for information-sharing. The DIN will spearhead activities to increase rapid incorporation of the best available innovations and practices, and facilitate internal crowdsourcing activities.

Comment: To create a culture of innovation, the Department should create an office to supervise, coordinate, and spur the use of the best available ideas and approaches. The Department has an "innovation archipelago": many offices within DoD are engaged in excellent and important work on innovation, but each is an island, disconnected from the rest. This lack of communication and collaboration is hampering progress. A supervising and coordinating office, headed by a single person, and promoting a coherent strategy, can signal a sense of prioritization; further the use of best practices and information sharing; engage with the rest of government and the private sector; and draw attention to systemic barriers, including legal and regulatory barriers that might go unchallenged.

The Board is aware of the potential unintended consequences of centralizing innovation efforts into a single coordinating office, and acknowledges the need to balance the benefits of increased coherence with the advantages of diversity and planned redundancy. Adjustments to budget authority, reporting structure, and distribution of responsibilities can be difficult to implement and will require time to plan deliberately, especially in the context of other potential structural changes to adjacent organizational functions, such as the role of the DoD Chief Technology Officer, which the Board sees as distinct. Nevertheless, the benefits outweigh these potential challenges. Within the private sector, parts of the federal government, and in many states and cities, the establishment of chief innovation officers (or similar roles) has paid significant dividends. DoD may benefit most from this structural change and added emphasis.

Background: Today, CINOs – or their equivalents – are leading innovation efforts at organizations such as the U.S. Agency for International Development, Department of Veterans Affairs, and Department of Health & Human Services, MasterCard, Citi, Wells Fargo, AARP, Dentons, 1776, the State of Colorado,

and the City of San Francisco. CINO equivalents usually lead companies' designated innovation labs, such as the labs at Amazon, Walmart, CVS, Nordstrom, and others. These leaders have also spearheaded the kind of innovation tournaments that have been organized by companies such as Ford, Netflix, Google, Cisco, JP Morgan, Intel, Microsoft, GE, and PayPal.

The purpose of the DoD CINO is not to centralize the many innovation efforts taking place in disparate pockets across the DoD enterprise – indeed, doing so would undermine the very bottom-up culture of innovation DoD seeks to foster – but to better facilitate, support, empower, and connect these efforts. Many companies view innovation through a technology or research and development lens, but DoD is already strong in those arenas. A CINO focusing primarily in this space would be duplicative or worse. Through interviews with experts both within and outside of DoD and the federal government, in addition to the DIB staff's own research, it is clear that the CINO should focus on ways to enhance workforce capacity, human capital, professional training programs, and an underlying culture of innovation. Concentrating in these areas, which includes an emphasis on applying successful private sector methodologies to identifying and addressing problems, will enable DoD personnel in diverse locations, positions, and ranks to change the way DoD operates in vastly more constructive, collaborative, efficient, and effective ways. The Board views this function as separate, distinct, and complementary to the function of a Chief Technology Officer.

In the same interviews, the question of where the CINO would sit within the DoD structure and hierarchy surfaced often. There are a variety of approaches here, but there are two poles at each end of the spectrum that experts have identified:

- The CINO should report directly to the Secretary or Deputy Secretary of Defense to expedite timely and authoritative decision-making, even on controversial issues, ensure the role would carry weight alongside other senior DoD leaders, and accrue the budgetary resources and manpower to fulfill its mandate. This would require Senate confirmation, which would maximize the authority of the CINO. On the other hand, Senate confirmation would lengthen the process of implementation of this reform, and even stall it entirely. This approach carries with it greater risk of bureaucratic resistance to the new role, and a higher likelihood of tensions with other DoD organizations that have overlapping or adjacent missions.
- Making the CINO a term-appointed advisor to the Secretary within the Office of the Secretary of Defense (OSD) would carry less seniority, but have significant advantages and expedience. It could be done immediately, and would not need Senate confirmation. If the CINO was known to have support from OSD, the position would have the influence to make progress. The risk with such an approach is that it could relegate the CINO to a role where he/she would lack the proper support or resources, and would regularly fight from the sidelines to have equity in key efforts. This in turn would reduce the CINO's capacity to undertake the kind of activities that would be most helpful, and could create a position with insufficient heft to create sustainable change.

For the long-term health of the Department, an approach closer to the first option is preferable, even if an official CINO office would not be established in the near-term. If the CINO is to guide enterprise-wide

attitudinal changes in how DoD employees think about and solve problems, then the CINO must have significant resources, regular access to the Secretary of Defense, and an understanding with other DoD leaders on how the CINO can work with them. However, it is important not to ignore the second option, given the uncertainty around the required statute change and Senate confirmation process.

Recommendation 2: Embed Computer Science as a Core Competency of the Department through Recruiting and Training

Proposal: Establish a career track for computer scientists in the military that provides incentives for service members to specialize in computer science and programming fields and to get the additional training and opportunities they require to advance, and protects them from pressures to rotate into unrelated roles. To attract Science, Technology, Engineering, and Math (STEM) talent to this cadre, establish new and expand existing programs that attract promising undergraduate and graduate students in computer science, engineering, and related fields to commit to military service for a period of time in exchange for scholarships or debt relief. These recruits should have recruiting standards and training that is tailored appropriately to their unique role.

Comment: The Board believes that the future of warfare will be increasingly software-centric. The Department's strategy documents recognize this and call for the development of futuristic weapons systems that depend almost entirely on the integration of state-of-the-art software. Yet the Department is significantly challenged in its ability to develop, use, update, or acquire modern software. This mismatch is a potential flaw in the Department's current approach to technology. Consequently, the Department must increase its emphasis on computer science as a core competency of warfighting. This is a decadal effort with profound implications for the Department's ability to fulfill its mission in the future. This will require a human capital strategy that will ensure that DoD can grow and maintain adequate computer science capability and capacity for the wide range of software-centric requirements that are unmet today and will only continue to grow.

It is important to note that recruiting more computer scientists has a broader intent than simply hiring talented people who know how to write code. Effective software comes from engineers as well as designers, product managers, security experts, and user experience researchers who understand the full scope of how and why software will be used. Since the goal is to make computer science a core competency of DoD, it is vital to recognize the diversity of talent needed to achieve this goal.

The Department benefits greatly from using distinctive career tracks for doctors and lawyers, which assists in recruiting, retention, and career management for scarce, highly trained professionals with specialized skills. With respect to computer science, DoD suffers from the fact that most personnel cannot specialize. In some cases, military personnel train for an extensive period (roughly two years) and then actually work in the field for a period that is not much longer (roughly two or three years). In view of the centrality of computer science to DoD's activities, it is necessary to allow a distinctive career path, with appropriately designed and specified expectations and requirements. Moreover, this would also enhance recruiting in this field.

However, the Department can't recruit its way out of its human capital shortage in computer science and related fields. Any effort at enhancing recruiting should be complemented with an increase in the capacity to conduct computer science and cyber training internally, ensuring that uniformed, Reserve, National Guard, and civilian units are properly equipped and prepared for a software-centric future.

Background: Unsurprisingly, the world's most innovative companies prioritize computer science as a core competency of their operations. Facebook, Google, Snapchat, and Dropbox are among the many companies that fight to attract the top talent among computer scientists and engineers. In addition, many Fortune 500 companies offer computer science internships to identify and recruit promising potential employees. These include Chevron, General Motors, Verizon, Boeing, Target, Comcast, Dow, John Deere, Morgan Stanley, Visa, Booz Allen Hamilton – a number of which are not traditional technology companies, indicating how important computer science is to the operations of virtually any successful company today.

As a specific case study, in the past few years General Electric (GE) has publicly sought to transform itself from an industrial company to a digital one focusing on the industrial internet, commonly known as the Internet of Things. GE's goals necessitated a new approach and additional resources dedicated to attracting talent, which has allowed GE to recruit top computer and data scientists from companies such as Apple, Facebook, Amazon, and Google. GE is a valuable analogue for DoD: a company that once was an industrial titan but has recognized the shifting strategic environment, remaking itself into an organization that embeds computer science at its core to remain competitive in the next century. The Board envisions a Department in the future where the software developer is as ubiquitous as the mechanic. The first steps of that transformation cannot be postponed.

Recommendation 3: Embrace a Culture of Experimentation

Proposal: Encourage evidence-based, outcome-driven policies and experimentation by (a) testing multiple strategies simultaneously and using evidence to assess them; (b) testing different operational approaches in real time to accelerate learning; (c) creating opportunities to incorporate diverse viewpoints into decision-making processes; (d) offering bonuses, recognition, awards, and other incentives for managers who promote innovation and experimentation, give employees greater voice, and encourage creativity and divergent views.

Comment: The Board observed several teams in the DoD that practiced evidence-based, outcome-driven, and experimental methods, such as rapid prototyping. Instead of being guided only by anecdotes or intuition, or relying solely on process and procedure, the leaders of these teams focus on the effects of their practices and test various possibilities of employing different practices to seek out empirical evidence indicating which products or approaches are optimal. Their approach is rapid, iterative, and risk-tolerant. Instead of giving processes pride of place, they focus on outcomes, and how to get there most efficiently. These practices should be generalized, and not only to products and services, but potentially to strategies and operations as well.

The Board observed that the predominant culture in the Department values authority, consensus, tradition, and an extreme form of professionalism sometimes described as a "zero defect mentality." These are admirable qualities, but they also tend to make employees risk-averse when it comes to creativity, experimentation, and dissent; and it makes nearly impossible for an ethos of experimentation to flourish. Experimentation – including embracing calculated risk-taking and learning from failure – is vital to improving decision-making and promoting innovation in the workforce. DoD leaders must find ways to embrace both sets of virtues; one way of doing that is to celebrate, reward, and provide incentives to those who take risks, learn from failures, and offer dissent. It is obvious there are situations unique to the military when the "no fail" attitude and authoritarian culture are the correct response to life-threatening situations or mission critical orders, but there are numerous circumstances where life and limb are not at risk, and an inflexible mindset is actually the greater risk to the overall mission.

Background: Experimentation and failure are built into the culture of Silicon Valley, and in the latter's case, it is not only accepted, but often encouraged. Perhaps the most famous example in Silicon Valley history around companies empowering employees to experiment is Google's 20% rule, which, while utilized less as an official policy today, allowed employees to spend 20% of their time on outside projects they believe would benefit the company. This idea – meant to harness employees' creativity and entrepreneurship – led to the creation of Google News, Gmail, and AdSense.

Google's R&D lab, known as X, specifically rewards employees who experiment and fail because not doing so diminishes the possibility that employees will take risks and discover key breakthroughs.

Facebook has posted on YouTube segments of its all-day or all-night internal sessions, which have taken place every several months for the past several years and during which employees work on projects

outside their usual scope of work. These projects are not just technological in nature, but can also include efforts such as improving or making more efficient the use and delivery of office amenities.

Beyond Silicon Valley, experimentation is becoming a core competency for leaders and managers across a variety of industries and functions. Experiments are necessary for innovation—there is evidence that half of all patents are the result of serendipitous, unplanned events. It is through tinkering, iterating, and making mistakes that creative ideas often emerge. Management researchers have gone so far as to argue that "failure is an essential prerequisite for effective organizational learning." Indeed, when governments and private companies attempt to launch rockets into orbit, the more they have failed in the past, the greater their odds of succeeding in the future.

Experiments are unlikely to happen without psychological safety—the belief that it is safe to take risks. Psychological safety has been identified as the single most important driver of team effectiveness at Google and as a key factor in organizational effectiveness in other settings. Leaders establish psychological safety when they invite critical feedback, show vulnerability, and admit fallibility. Research has shown that pilots foster psychological safety when they announce to cockpit crews that they are open to being challenged, stressing that everyone's first responsibility is not to respect authority but to land the plane safely. Physicians create psychological safety when they seek and value the input of every member of a healthcare delivery team. Manufacturing team leaders cultivate psychological safety when they frame mistake as learning opportunities—which in turn encourages people to run experiments.

Companies such as Autodesk, Microsoft, and Capital One encourage their employees to experiment in different ways:

- Autodesk prioritizes training employees not how to think differently – because the company recognizes that they already generate good ideas on their own – but rather how to operationalize them. Employees are encouraged to pitch business ideas and are trained to show why Autodesk is the right company to implement them for the benefit of the industry and consumers.
- Microsoft revamped its performance and evaluation metrics to allow employees to lead new innovation challenges for which they would not have been rewarded under the previous evaluation system.
- Capital One provides flexibility to teams to find and cultivate innovation champions among middle management – which usually focuses on core business processes and often rejects innovation activities they view as irrelevant to said processes – that allow more room for employees to test out new ideas.

High-tech companies have relied on split testing for years to understand their consumers' behavior, evaluate their products, and determine how to optimize the products and services they deliver. Digital companies routinely use experimentation to optimize performance. For example: Amazon and eBay customize search results for individual customers based on their searches to understand the behavioral patterns of purchasers; Google runs analytics on how different users behave online based on the number and type of search results listed on one page; and Netflix evaluates what viewers click on to

create more personalized homepages for them. Even small discoveries can have a massive impact on these companies' revenue, which explains why they devote significant resources to conduct this kind of split testing and analysis. It is central to how these companies operate, and it should be just as central for DoD to improve its extensive operations. Applying these principles to logistics, contracting, computing, maintenance, training, recruiting, and even strategy and operations could yield improvements in performance.

Technology & Capabilities

Recommendation 4: Assess Cyber Security Vulnerabilities of Advanced Weapons

Proposal: Direct U.S. Cyber Command, working in coordination with the National Security Agency, to conduct regular security reviews of embedded software and networks for weapons systems to identify vulnerabilities. Require that source code for such systems be made available on an ongoing basis for such testing, and that any detected vulnerabilities are removed. The DoD should identify new standards and practices to eliminate system vulnerabilities, particularly those that require collaboration between the DoD and the defense industry.

Comment: The fundamental premise of this recommendation is that the technological advances in weaponry are now advances in software, not hardware; the measures to maintain and protect them must reflect that. In other words, a state-of-the-art fighter plane is a software system with wings, whereas previous fighters were planes with computers aboard.

Most modern weapons systems were designed under the assumption that their computing, networking, and software components were developed in controlled environments and that the security of these components would be maintained through adherence to standardized security procedures. As these systems have been integrated into increasingly networked environments, the safeguards designed to protect them have become inadequate. Conventional operational test processes are not evaluating the embedded code for vulnerabilities. Attempting to protect these systems by hiding them behind a network firewall is no longer sufficient to protect them.

Meanwhile, the sophistication of cyber-attacks has increased, rendering these weapons systems more vulnerable to attacks from direct infiltration, spoofing of sensors and interfaces, or more sophisticated systems-level attacks. For example, the use of older operating systems is one particular vulnerability that may be common in weapons systems that are not updated at a pace that matches modern commercial computing environments.

The Board recommends that U.S. Cyber Command and NSA have the best expertise on identifying vulnerabilities in the DoD, so this requirement should be added to their mission. These organizations should apply state-of-the-art automated vulnerability testing technology to continually safeguard the software code embedded in weapons systems.

Background: Vulnerability to hacking and infiltration is of paramount concern to all major companies, which conduct routine security reviews to identify and root out bugs or other vulnerabilities. Apart from internal reviews, Facebook, Dropbox, Microsoft, Twitter, Google, Yahoo, PayPal, Snapchat, Tesla, and GE are among companies that have hired outside hackers – or acquired companies that conduct this work – to find vulnerabilities through “bug bounty” programs. These companies know that they will never find every vulnerability, so they solicit help from outside experts and white hat hackers.

In 2016, DoD instituted bug bounty programs of its own, such as Hack the Pentagon and Hack the Army, allowing anyone to search for and report vulnerabilities within the Pentagon and Army's unclassified websites. Hack the Pentagon attracted 1,400 white hat hackers who discovered 138 vulnerabilities.

In addition, the Pentagon announced a new policy that allows anyone to report vulnerabilities to the Pentagon at any time, not just during exercises such as Hack the Pentagon. While this is an important step forward, there will always be vulnerabilities that will go overlooked, so it is important to consider more programs such as Hack the Pentagon and Hack the Army to enhance the visibility of these opportunities for white hat hackers. This has a complementary benefit of developing a potential recruiting pool of computer scientists with a sense of duty that DoD needs.

However, identifying vulnerabilities solves only part of the problem. Just as large modern companies update their software and corresponding systems as technology becomes more advanced, DoD must do the same. Otherwise, an even wider range of adversaries, criminals, and opportunists will be able to identify vulnerabilities and even sell them on the black market for zero-day bugs.

Recommendation 5: Catalyze Innovations in Artificial Intelligence and Machine Learning

Proposal: Establish a DoD center for studying artificial intelligence and machine learning and building expertise and capacity in these areas across the department. Like the institutions established in the past to ensure the DoD's technological advantage in nuclear weapons, DoD now needs a centralized, focused, well-resourced organization to propel applied research in artificial intelligence (AI) and machine learning (ML). This center should coordinate research in these areas across the Department, and liaise with other labs in the private sector and universities, and should also conduct educational efforts to inform the Department about the implications of these advances for the Defense enterprise.

Comment: Across the broad landscape of information science and technology, two particular disciplines are maturing so rapidly that they will present transformational capabilities to the DoD: *artificial intelligence*, the capability for computational systems to execute tasks that are historically thought to require human methods, systems, and capabilities of reasoning; and *machine learning*, the capability for a computer system to grow its knowledge base without explicit pedagogical programming, and thereby extract information from large collections of data. After long periods of gestation, particularly for AI, and enabled by vast increases in computational capability, these two technologies are reshaping nearly every aspect of knowledge work in the private sector, from search to autonomous vehicles to pattern recognition for security applications.

The impact of AI and ML will be felt in every corner of the Department's operations, from critical tactical operations such as Intelligence, Surveillance, and Reconnaissance (ISR), targeting, cyber defense and autonomous land, air and sea vehicles; support operations such as personnel billeting, training, logistics, and threat analysis and war-gaming. These opportunities will be so ubiquitous and the adversary threat will be so competitive that it is critical the Department create and defend the asymmetric capability. Without exaggeration, the Board likens this situation to that which existed in the first (nuclear weapons) and second (precision munitions and stealth) offsets. Indeed, both AI and ML are key components of the Department's Third Offset thinking.

Against this backdrop, the Department should establish a DoD-wide center specifically dedicated to AI and ML. Such a construct should comprise research, experimentation, deployment, connection to global external private sector and academic expertise, and competitive threat analysis. Success will depend on having the necessary acquisition and retention tools to ensure the center is staffed by or has access to the highest quality scientific and technical expertise in these two fields. One model to consider are the dedicated nuclear weapons laboratories of the National Nuclear Security Administration (NNSA), but the Board does not suggest that centralized "brick and mortar" centers are the only option. Many of the most significant advances in commercializing and applying AI and ML research are occurring in open source collaboration forums and virtual research networks.

DoD possesses data sets that no other university or company can access, and which would be immensely valuable, either commercially or intellectually. The center should grant access to DoD data strategically, in ways that further collaborative partnerships with external researchers. Provided the

data can be secured appropriately and intellectual property rights respected, mutual beneficial arrangements could lead to significant advancement for all parties.

Based on interviews with AI and ML experts within DoD and the federal government, and academics, technologists, and researchers outside the government, the Board recommends that the Department consider the following functions for the center:

- Consolidate the management and enhance the visibility of DoD's existing innovative and collaborative work on AI and ML. Focus on exploratory research by overseeing challenges and prizes, and strengthening DoD's existing exchange programs and connections with the private sector and academia.

- Develop a robust, rapid prototyping and experimentation function for making AI and ML technologies more applicable to the users. The Services should take leading roles in this endeavor, with the center serving as a relationship broker and facilitator to DoD labs, academia, and the private sector. The center would act as a "nerve center" that would funnel projects to the Services to deploy technologies to the field more quickly.

- Enmesh itself in a larger segment of the acquisition process to ensure that warfighters not only receive prototypes of new capabilities, but also continue to receive upgraded versions of them. This would require the use of some alternative acquisition mechanisms in Recommendation 6 allowing new technologies to reach service members on a large scale, but not as slowly as the usual procurement process demands. The success of this approach will depend on a more robust integration with the associated training, maintenance, budget, and doctrine required to sustain a speedy capability delivery process at scale.

Background: AI and ML are fundamental components of growth for nearly every major company across a wide range of sectors, yet this field is still nascent in many ways, paving the way for new research institutions or initiatives outside the federal government. The Association for the Advancement of Artificial Intelligence, the Allen Institute for Artificial Intelligence, the Machine Intelligence Research Institute, and the Fairness, Accountability, and Transparency in Machine Learning program are just a few examples, some of which are sponsored by Fortune 500 technology companies.

Leaders in the technology and other sectors recognize that AI and ML will have a transformative impact on society, creating new jobs and upending traditional industries. These leaders also know that this technology can be used with malicious intent. A significant segment of the public views AI and ML as enablers of "killer robots" that DoD and others might deploy. DoD leaders acknowledge the theoretical risk of these scenarios, the broader societal implications of advances in AI, and the legal and ethical implications of this emerging technology. If DoD is to grasp a fuller picture of this field, it is worth examining what the private and non-profit sectors are doing:

- OpenAI is a non-profit research company founded by Tesla's Elon Musk and others to showcase and research AI that benefits society rather than harms it. The company works with research institutions and individuals in an open-source environment, making its patents and research available to the public.

- In 2016, Amazon, Facebook, Google, IBM, and Microsoft launched the Partnership on Artificial Intelligence to Benefit People and Society, which aims to advance public understanding of AI and ML and develop best practices around the challenges and opportunities in the field.

The potential for transformative change from AI and ML – as well as misunderstanding its implications and applications in the military or other sectors – cannot be overstated, and DoD would do well to invest further in this field and collaborate where possible with outside expert researchers.

Recommendation 6: Expand Use of Available Acquisition Waivers and Exemptions

Proposal: Improve the speed and timeliness of acquisition processes by increasing the use of available mechanisms for waivers and exemptions, and by offering incentives for quick resolution of concerns. Identify and broaden the use of "best practices" by specifying aspects of acquisition approaches and techniques that are effective in the Special Operations community that could be applied more generally.

Comment: The acquisition and procurement process is too heavily bureaucratized, too slow, and too rigid to meet the needs of the Department. The Board is aware that the existing acquisition restrictions have legitimate motivations; and that many others have recommended an increase in flexibility. The Board thinks that those recommendations are correct and that it is past time to act on them. When the use of those authorities would bypass requirements that jeopardize the goals of speed and efficiency, balancing delivery to the warfighter against bureaucratic risk, officials should be encouraged to use existing exemption and waiver authorities more than they do today. In general, increasing decentralization will increase the Department's agility.

One of the most important and recurrent themes the Board notes is the need for a multi-track acquisition system rather than a one-size-fits-all approach. Some acquisition experts respond by pointing to the existing flexibilities in the system. While those who have mastered the Federal Acquisition Regulation (FAR) and DoD 5000 may be equipped to tailor acquisition approaches, many of those who can, do not. The professional incentives to adopt standard, consistent methods and the deep cultural imperatives to reduce bureaucratic risk have created enormous pressure to conform, at the expense of programmatic or operational progress and efficiency. Unfortunately, some of the most onerous requirements for documentation and reviews may be avoided, consistent with law, and in that sense are self-imposed. Rather than continuing the common refrain of only improving acquisition education, new incentives and norms need to be established if these behaviors are to change. Consequently, further intervention to improve the acquisition system should be guided not only by emphasizing what is technically feasible under law and regulation, but also by observing which behaviors, good and bad from the standpoint of innovation, are most common, and working to align risk and incentives to increase the behaviors sought.

The Board also observed the contrast between the differences in the approach to innovation, acquisition, and fielding in the conventional forces and the Special Operations community. Special Operations Forces (SOF) have funding and authorization to conduct tactical level development, while the conventional forces do not. Consequently, the culture of SOF is different. The widely recognized agility of the SOF acquisition process is not due to US Special Operations Command (USSOCOM) being more innovative per se, but because the USSOCOM systems and culture allow and encourage SOF to innovate in ways the conventional forces do not. To correct this, the DoD should identify how a rapid development capability at the conventional level could be established and allocate funding that can support those initiatives.

Background: Although few people have read the nearly 2,000-page FAR, those who have done so have noted that the FAR incudes specific language encouraging the acquisition process to be efficient, innovative, and agile. It is an open question whether this language fits with the multiple regulatory requirements the Department has layered on top of it. The FAR should be subjected to continuing scrutiny to test whether it strikes the right balance. Regardless, the idea of the FAR as a hidebound and cumbersome barrier to innovation and reform certainly endures. Even if knowledge of the FAR's flexibilities became more widespread among those acquisition professionals viewed as most tied to the status quo, a culture that prizes large long-term, high-dollar value projects still pervades the DoD.

In our view, the current system works relatively well – despite the need for some well-articulated modifications – for large programs such as aircraft carriers, nuclear submarines, and fighter jets. But smaller programs with specific and often more immediate applications, such as counter-unmanned aerial systems (UAS), should not be subjected to the normal acquisition process. The most egregious of these mismatches is software acquisition and procurement. There should be an entirely separate process for buying software whenever it can be decoupled from a system. There are current waivers, exemptions, and alternative authorities to facilitate this, but they are not used sufficiently, and they could should be revisited and expanded. Within the existing culture, they do not attack the root of the problem.

One way to do so is to ensure that acquisition professionals better understand and use available contracting vehicles that allow for a more nimble approach. As the DoD will require emerging technology at an increasing rate to offset any adversarial advantages, Defense Acquisition Workforce Development Funds (DAWDF) should be tapped to train acquisition professionals on the benefits of alternative contracting vehicles. In addition, the DoD should modify the incentive structure that typically rewards contract managers overseeing large long-term systems, so that contract managers will also be praised and promoted for managing shorter procurement cycles for technology that is equally critical to DoD but less visible or tangible than ships or planes. Without this culture change, which includes the spreading of best practices, no amount of education and training will be sufficient.

The DoD should also expand new vehicles and programs that, while not silver bullets, can help the DoD wean itself from the bulky acquisition process and respond to warfighter needs with the speed required to outpace competitors. Here are a few examples of what the department is already doing in this area:

- The Defense Innovation Unit Experimental (DIUx) funds commercial entities, many of which are startups or other types of small companies, that would not otherwise work with the defense sector due to lack of time and resources to comply with the burdensome acquisition requirements. Through a contracting mechanism known as the Commercial Solutions Opening (CSO), DIUx can help these companies complete the procurement cycle in 60 days or less, delivering important solutions in such areas as computer vision, high speed drones, simulations and war-gaming, indoor UAS that can operate without GPS, data analysis, and hands-free field communication systems. DIUx's use of the CSO is a model worth spreading across the DoD enterprise.

- The DoD participates in Hacking for Defense, an accredited academic course taught at a number of universities (first taught at Stanford in early 2016) that sees small teams of students solve unclassified problems that are sponsored by specific DoD commands, teams, and units, with the goal of providing sponsors with a Minimum Viable Product (MVP). Sponsors include the MD5 National Security Technology Accelerator at the National Defense University (NDU), Joint Improvised-Threat Defeat Organization (JIDO), US Army Asymmetric Warfare Group (AWG), US Special Operations Command (USSOCOM), US Navy Headquarters, 75th Ranger Regiment, the National Security Agency (NSA), US Army Communications and Electronics Research & Development Engineering Center (CERDEC), and numerous others. This approach focuses on understanding the root of the problem and using successful methods from the private sector to find the best solution. This differs from DoD's traditional model in which the military drafts the requirements for the solution it believes it needs – initiating the process that usually leads to large contractors vying to build a product that fits those requirements – even though a better solution may exist. Hacking 4 Defense helps find those better solutions the military may not be aware of, leading to some teams from the course receiving funding – either from their military sponsors or venture capital firms – after the semester ends to continue developing the product for rapid deployment. It is therefore important for additional offices and teams in DoD to submit their problem sets so university teams can help solve them and inject some outside creativity – at little cost – into the ideation and prototyping process.

- In 2016, the Army established the Rapid Capabilities Office (RCO), modeled after the Air Force RCO. The new RCO uses rapid prototyping and initial equipping, based in part on feedback from service members in the field, to deliver capabilities that will tackle high-priority threats (cyber and electronic warfare, positioning, navigation, etc.), with a delivery timetable of one to five years. The Army doesn't use the RCO to procure systems outright, but rather to close the gap between identifying the need and deploying the solution. The Navy's newly-created Maritime Accelerated Capabilities Office (MACO) is also modeled after the Air Force RCO, and should be given the resources requested in the Navy's current budget cycle.

- As a complement to MACO, the Navy's Rapid Prototyping, Experimentation and Demonstration (RPED) initiative deploys urgent capabilities to the fleet as soon as possible, quickly gauging their effectiveness to determine whether to discontinue prototyping or submit the capability to the usual procurement process to field the solution more broadly. RPED expands on the work of the Office of Naval Research's TechSolutions process, which develops and delivers technologies to warfighters within 12-18 months, based on their feedback and requests.

- The Army Rapid Equipping Force (REF) delivers technologies and capabilities to forward-deployed units requiring urgent solutions within a period of 180 days. REF focuses on the unit level, as military operations in the last decade and a half have seen the on-the-ground presence of more Army units than those of other Services, and often in remote areas. The thinking behind

focusing on units rather than the full scope of the Army is the necessary approach needed to support troops on the front lines.

- The Air Force's Revolutionary Acquisition Techniques Procedures and Collaboration (RATPAC) and "Ghost" programs convene junior and mid-level military and acquisition professionals to identify ways to make the acquisition process more nimble and innovative. An exchange program between the Air Force and US Special Operations Command (USSOCOM) empowers junior officers to implement new acquisition ideas when they are deployed to their Areas of Responsibility (AOR). This model should be expanded to the other Services as well.

- USSOCOM's SOFWERX is a collaboration lab that prototypes emerging technologies that can be quickly delivered to Special Operations Forces (SOF). While the lab is staffed by USSOCOM, anyone can come in off the street and suggest ideas. SOFWERX is working on capabilities such as thermal imagery to see behind walls, exo-skeletons as armor, vehicular modifications, more effective blood-clotting pellets, and more. While the Services have a wide network of labs, few are designed like SOFWERX. It is worth considering how they might invite outsiders to participate in the process the way SOFWERX does.

Recommendation 7: Increase Investment in New Approaches to Innovation

Proposal: Increase investment in and support for the Defense Advanced Research Projects Agency (DARPA), the Strategic Capabilities Office (SCO), the Defense Innovation Unit Experimental (DIUx), Defense Digital Service (DDS), rapid equipping units, and other small, agile, innovation-focused organizations within the DoD. Establish activities to improve communication and coordination between them and to educate DoD leaders and the workforce about their efforts to stimulate innovation as a means to enhance the Department's overall capabilities. An annual Innovation Synchronization Conference should be held semi-annually to increase information exchanges between these groups. One potential theme for this conference could be Third Offset technologies where each organization brings forward current challenges and potential technological solutions in fields that are relevant to the Third Offset.

Comment: The Department has made significant strides in innovation over the last decade by adding several new offices, initiatives, and approaches to its "innovation portfolio," such as DIUx. Simultaneously, the Department continues to support long-established, successful drivers of innovation, such as DARPA. There is a tendency to dismiss activities labeled as "innovation" as a fad and an equally misguided temptation to disguise conventional acquisition programs or research projects with "innovation" branding. The Department's leaders should take care to avoid both traps; nevertheless, the next year will be crucial for sustaining the current focus and intensity on innovation because these new activities are likely to encounter additional resistance.

Many of these new innovation or technology acceleration efforts, particularly the proliferating number of rapid equipping offices and processes that have cropped up as an adaptation to the operational demands of a decade at war, would be correctly perceived as the Department's efforts to disrupt itself. Because the Department's processes are optimized to reduce risk and enhance stability, the need for subversion and disruption is still increasingly urgent, perhaps more so, as the Department is likely to experience a countervailing tendency to eliminate workarounds as the Department resets. This will be exacerbated by budget pressures. Leaders should compensate for the institutional pressure to restore the status quo ante by seeking opportunities to lock in the progress and support current efforts even more aggressively. Incoming leaders should look to maintain current funding levels, sustain management focus, and, insofar as there is clear evidence that additional resources could be absorbed, look to increase resources.

The next step in advancing the Department's innovation agenda is to increase communication and coordination between the various nodes in the innovation network, and the various offices that have been established. Variation, planned redundancy, and competition are healthy for innovation in an ecosystem as large as DoD; however, there are too many missed opportunities for sharing information and best practices among groups working on complementary activities. Promoting more dialogue will accelerate innovation, particularly on emerging technologies that are crucial for the Department's continued competitive advantage, such as Third Offset. Working to lend greater coherence and information sharing through regularly schedule "synch" activities would be productive.

Background: Information sharing and coordination in large companies is not just a way to increase efficiency – it's a fundamental building block for success and mission achievement. DoD is a notoriously diffuse enterprise, with millions of employees around the world engaging in myriad jobs. Connecting them – particularly the pockets of innovation located in every corner of DoD but rarely in touch with or even aware of one another – is an important step in achieving mission success.

A few examples in the private sector underline that communication platforms are not only about connecting employees to share best practices, but also challenging one another. These platforms include opportunities for information sharing, knowledge management, crowdsourcing, competitions, and more:

- Slack: cloud-based team collaboration tool
    - Companies that use Slack include Airbnb, Pandora, Buzzfeed, Pinterest, LinkedIn, Samsung, Ebay, Autodesk, and Ticketmaster
- Socialcast: a social networking and collaboration platform; bought by VMWare in 2011
    - Companies that use Socialcast include 3M, Humana, Philips, Siemens, and SAS
- Yammer: a social network for companies' internal use; bought by Microsoft in 2012
    - This was one of the earliest information sharing and collaboration platforms, so fewer companies use it now, particularly as other platforms have been launched, but some major companies, such as Xerox, still rely on it

Some large companies have developed their own collaboration platforms that are available as a service that other companies can purchase. One example is Cisco's Collaborative Knowledge, a "digital workplace" solution that helps employees access information and experts, train and update their skills, build social communities, and solve challenges collaboratively.

Practices & Operations

Recommendation 8: Improve DoD Access to Code

Proposal: Require that all systems purpose-built for the DoD should have their source code available to DoD. The Department should have the rights to and be able to modify the code.

Comment: A large number of modern defense systems are built and maintained in a manner that leaves control of the source code that runs the systems in the hands of industry. In some cases, changes to the code to adapt to new conditions, incorporate new features, or eliminate flaws require that contractors who control the code make the changes. This often incurs significant delays and costs. To enable more rapid innovation and customization that is required for modern defense operations, the DoD should have access to code running on its major purpose-built systems and to be able to make changes to that code. An additional benefit is the ability to reuse software in other parts of DoD.

The Department will honor existing contracts where DoD does not currently have access to the code, though modifying them if possible would be welcome. New contracts and systems should incorporate this recommendation, though, as with most major DoD policies, waivers and exemptions should be made available. This change should not prevent DoD from purchasing Software as a Service (SaaS) products that are open-source and would otherwise be ineligible for purchase due to contractual restrictions.

Background: As weapons and other systems become primarily software-driven platforms, and consistent with modern understanding of software systems as organic, evolving and improving, the Board places a very high premium on the native ability to rapidly fix and improve codes in delivered systems. DoD must have the ownership and capability to do so.

The Board recognizes three important challenges that must be addressed in this view of the world: First, DoD must have the necessary capability and capacity to understand, modify, verify, and validate code. Recommendations 2 and 9 speak to this issue. Second, transfer of risks and rewards must be managed. Clear requirements for what comprises delivery of major systems must protect the department from inheriting less than adequate original code that it will then have to maintain. Conversely, new business models will be required if systems providers do not have the financial returns that come from support of deployed systems. And, third, care must be taken to ensure IP rights are properly valued and protected.

Recommendation 9: Establish Software Development Teams at Each Major Command

Proposal: Establish embedded software development teams of government employees -- "human clouds" of computer programmers and software developers responsive to local commanders -- who are available on-demand to swiftly solve software problems by working directly with the owner of the requirement. Small teams of these developers should be assigned to commanders to provide an organic, on-demand resource that is immediately responsive to warfighter needs without necessitating writing a requirement, selecting a vendor, reaching back to a distant resource, or going through lengthy and onerous approval and contracting processes.

Comment: Throughout the DoD enterprise, our warfighters are often confronted with computer programming obstacles that are compounded by the lack of speed and agility to address even the simplest system software development problems. Moreover, there are numerous opportunities to gain a tactical advantage, increase efficiency upgrade, or improve data analysis, visualization, and sharing that are currently missed due to a lack of awareness and lack of capability to do rapid software development. The absence of dedicated computer science resources "in the field" that are capable of addressing emerging requirements and the drawn-out approval processes mandated by current acquisition regulations are inadequate to address the increasingly complex and high-tempo demands our troops face across all domains. This has a negative impact to mission readiness and effectiveness that is simply accepted as the cost of doing business in the DoD.

In keeping with the industry best practices, the DoD should embrace a localized approach that pairs users and software developers sitting side by side with the ability to do rapid deployment of new code that is responsive to rapidly evolving requirements. In this scenario, the Board envisions that commanders would have at their disposal a small cadre of talented specialists that can easily be deployed to provide fast and innovative solutions the most pressing programming and software needs. This "human cloud" rapid reaction force should be empowered to work side by side with operators on the ground and apply their expertise to the front line of the DoD's software challenges.

In addition, these teams of developers would not be restricted to fixing broken programs, but could also develop new capabilities and speed them to warfighters and commanders. The solutions may have broader applications elsewhere in the Department; for example, developers might be able to create customized solutions for automating the processing, exploitation, and dissemination of data. The natural evolution of this project is to create a secure "GitHub-like" platform for DoD developers.

Background: Modern software companies take advantage of the ability of small teams of programmers to develop and deploy new capabilities into their products in a rapid fashion. SAP is one such example. Equipped with the right capabilities, access to computing, and network-centric infrastructure, these teams can implement a new product feature, continuously check it against a set of unit and system tests, deploy it to a test group for feedback, and eventually deploy the new feature in a matter of days, weeks, or months, depending on the complexity of the change. In the DoD, this type of change can take years.

Most companies do not typically deploy on-demand teams of programmers or developers to swiftly solve software problems in the field – the rough equivalent of the Pentagon sending these teams to different theaters or Areas of Responsibility (AOR). If this dynamic played out in the private sector, it is likely that the company that built the code or sold the resulting product would send teams to the user that would experience software problems with the product. While this may occur when large enterprises with complex systems experience problems, individual users generally do not have access to this type of non-virtual support directly from the software developer.

However, the nature of the unique environment faced by Combatant Commands, and the need to be able to rapidly respond to changing conditions, motivates a different approach in the DoD. And despite the ability for rapid "reach back" support, the ability to have software developers "in the field," working directly with the warfighters whose lives they are helping protect, would significantly enhance the value that this "human cloud" would bring.

In addition to the deployment of software development assets, it will also be necessary to provide the modern computing and communications capability to allow this group to share their results with others in the DoD enterprise and build off of the work that others have done in similar situations. GitHub provides one model for this, where thousands of programmers share their code with others in a manner that allows creative contributions to be rapidly disseminated, tested and critiqued, in addition to providing continuous integration (e.g., unit testing code revisions as they are committed) and sophisticated revision tracking. Creating a secure "GitHub-like" platform can be modeled after the way different companies use GitHub, including MailChimp, Hootsuite, PayPal, Etsy, Vimeo, and SAP.

Recommendation 10: Make Computing and Bandwidth Abundant

Proposal: Direct DoD to adopt a strategy for rapidly transitioning DoD Information Technology (IT) to current industry standards such as cloud computing, ubiquitous access to modernized wireless systems leveraging commercial standards, abundant computing power and bandwidth that is made available as a platform, integration of mobile technologies, and the development of a DoD platform for downloading applications.

Comment: The computing environment available to DoD application developers and end users is substantially behind the current state of the art in industry and academia, and is not agile enough to support the mission needs. The DoD acquisition process is extremely slow, taking on average a year for an Authorization to Operate (ATO) to get accredited. Furthermore, the DoD IT policy is inundated with detailed requirements, such as adaptation to the Risk Management Framework (RMF), and is not fast enough to keep pace with industry standards. In addition, there is a lack of transparency on how IT commodities are acquired across the DoD, which then faces the problem of having inadequate technology and maintenance cost for hardware and software that is either obsolete or no longer valuable to the Department. To enable an elastic and scalable computing environment sufficient for DoD IT needs, there must be a shift to accrediting the review processes and not just the product, and there must be a focus on service delivery instead of just managing IT.

Modern software development and execution environments require access to cloud services, modern networking (including mobile), and large scale computational infrastructure. While providing these computing capabilities in a DoD-compatible environment will require overcoming obstacles that may not be present in many commercial environments, failing to provide this infrastructure has severe consequences in terms of software-enabled innovation. For those services or software programs that cannot be run in a secure manner on DoD networks, development of an appropriately secured virtual environment could enable access to modern software development tools (including open source) that would avoid bottlenecks and inefficient computing practices.

One way many companies make computing power abundant is by adopting cloud-based cost reduction strategies based on setting and achieving metrics across the enterprise. By setting targets for reducing the unit cost of computing, storage, and network transport every year by a certain amount across the enterprise, these companies can offset volume growth with increased efficiency. DoD should adopt a similar metric for assessing progress in increasing computing abundance. DoD could even benchmark against such companies (e.g. Amazon, Google, Rackspace) to set the targets for cost per Central Processing Unit (CPU) core, cost per gigabyte of storage, and cost per gigabit per second of network transport, albeit at a less aggressive rate. This would force DoD to modernize practices, hardware, and software in ways that make usage more efficient and treat computing as a commodity. Adopting this practice is far more than simply a cost-saving measure: where computing and bandwidth is scarce, behavior will be risk averse and technological progress will slow; where it is abundant, innovation flourishes.

While there seems to be broad consensus on the flaws in DoD's IT infrastructure, it appears that the limitations are widely perceived as an inconvenience that can be overcome by the workforce. But with an estimated 600 open IT billets and the inability for the DoD to efficiently recruit for these priority placement opportunities through the USAJobs.com platform, DoD should explore using alternative routes to attract the next generation of IT talent that will help DoD meet its IT mission needs.

The general acceptance of DoD IT being a decade or more behind the private sector has secondary and tertiary effects that have not been fully explored or documented, but are likely associated with other challenges facing the Department: difficulty recruiting and retaining human capital, especially for top STEM and cyber talent; significant costs in money, time, and productivity; unquantifiable missed opportunities to analyze all of the Department's data; negative impact on morale; and significant cyber vulnerabilities from obsolete software and networks.

Background: Despite concerns over the use of cloud computing, DoD cannot operate as a modern organization without adapting to the digital age. Abundant cloud computing power is foundational to digital organizations from large firms such as Microsoft, Oracle, IBM, and Amazon to small companies throughout the US commercial landscape.

Recommendation 11: Reward Bureaucracy Busting and Lower Barriers to Innovation

Proposal: Establish incentives for process simplification, reduction of paperwork and reporting burdens, and "bureaucracy busting" activities such as a prize for proposals that simplify existing processes, increase performance or efficiency, save time or money, or reduce impediments to the mission. To the extent consistent with necessary constraints, use and publicize an organizing principle for innovation and creativity: "make it easier." Leaders need to compensate for the natural inertial pressure of large organizations by constantly repeating a mantra of simplification.

Comment: Many of DoD's process are far too complex, with multiple levels of review, and with excessive administrative burdens. Much of this is necessary and appropriate, of course, but some of it is not. Simpler may be better. There should be a dedicated effort to reduce centralization and layers of review, and to remove obstacles to new thinking. In many institutions, creativity has been spurred by eliminating paperwork and reporting burdens and by adopting "make it easy" as an orienting theme. DoD should move rapidly in that direction.

That effort is best undertaken, in large part, by DoD personnel themselves who are now subject to the requirements and processes that are sapping productivity and morale. One way to do that is to take account of dispersed knowledge within DoD and to give employees an opportunity to exercise their own creativity. Sometimes those who have good ideas, or could develop them if asked, do not speak out, because they think that it would be fruitless to do so, and who fear that creativity on their part might be deemed inappropriate, especially if it is directed against longstanding requirements. Incentives should be created to reward good ideas. There should be a process for recognizing those who come up with them.

Background: Large organizations, both private and public, often suffer from undue complexity. Layers of review are increased rather than decreased, and that can stifle creativity. Caution becomes the watchword, and the desire to try new approaches is sapped. The Board repeatedly observed this stifling influence in the Department.

In the private sector, "bureaucracy busting" is often the very reason that new companies are born, as many innovators who find new and faster ways of doing business found startups to do precisely that. Irrespective of a company's origins, however, bureaucracy is inevitably present, even among the most innovative companies in the world. Their goal is not necessarily to stamp it out entirely, but to manage it in a way that enables the company to remain agile in important aspects and empowers employees to find ways to make the company even more agile. The White House, Office of Management and Budget, Office of Personnel Management, and a variety of federal agencies have offered cost saving awards; DoD has as well, to a limited degree relative to its size. Walmart and Sprint reward employees for cutting waste within their companies. Under the auspices of Management Innovation eXchange (MIX), Harvard Business Review and McKinsey have teamed up to sponsor several challenges around innovative approaches to management. Past winners or finalists include GE, Microsoft, Statoil, Electronic Arts, Vodafone, and Genentech.

Rather than simply cost-saving awards, time-saving awards should be equally valued. DoD should build on these practices here. A good first step would be to canvas DoD employees in a dedicated effort to catalogue layers of complexity and review what seem redundant or duplicative, or what weakens incentives to innovate. Respondents should be rewarded for ideas that seem especially promising or are implemented.

Recommendation 12: Forge New Approach to Data Collection, Sharing, and Analysis

ARGUMENT

Data is the 21st century equivalent of a global natural resource, like timber, iron, or oil previously – indispensable for sustaining military innovation and advantage. The next global conflicts will be fueled by data. The rapidly expanding power of new mathematical and computing techniques to reveal insights into intentions and capabilities, and to enhance accuracy, lethality, and speed, depend on immense data sets to train algorithms and from which to extract information. The data that provide the raw materials from which to identify patterns, as well as the anomalies that defy them, constitute the fuel that powers the engine of machine learning (ML). Whoever amasses and organizes the most data first will sustain technological superiority, so it is incumbent upon the Department to collect, store, share, analyze, and protect its data faster and better than its competitors. Data must be regarded as one of the most powerful resources in the Department's arsenal.

PROBLEM STATEMENT

DoD does not view data as strategic resource. Without a data strategy to collect, protect, and make available this critical resource, DoD will not be able to create or sustain competitive advantages over our adversaries. Meanwhile, the lack of a modern approach to data is consuming vast financial and personnel resources.

BENEFITS

DoD should establish a new paradigm for the collection, exchange, availability, analysis, and protection of all DoD data. Data should be mined for patterns to train ML systems that will provide strategic and tactical insights no human could ever generate. This advancement will transform the Department in four ways:

1. Data-enabled capabilities will enhance the lethality, speed, precision, and survivability of warfighters
2. Storage of data will allow artificial intelligence (AI) and ML-based systems to identify significant cost and time efficiencies that can be deployed across the enterprise
3. Ubiquitous and deep data sources will advance our capabilities past those of our adversaries
4. Encrypting and aggregating data will allow us to protect them using new sophisticated cyber security techniques

The scope of this recommendation comprises all development, operational, tactical, and strategic data across the total DoD enterprise. Any data repositories or similar architecture will therefore require use of the encryption and access rights technologies necessary to protect secure and third party proprietary data. This approach is more secure than our current one, as DoD would be protecting the data, not merely the networks that surround them. Moreover, aggregating data allows us to use ML to pattern

who accesses data and why, which enables anomaly detection that can be used to counter insider threats.

FIXABLE PROBLEMS

Every time a U.S. fighter plane takes the air or a submarine slips below the surface, it collects enormous amounts of data from its sensors, picking up vital information about targets in all domains. It generates a continuous stream of data on the performance characteristics of its systems, the mission profile it is assigned, and the behavior of the crew operating the controls. If captured and analyzed over time, these data provide unprecedented insight into enhancing performance of the operators, maximizing the performance of the platforms, detecting patterns across a fleet of planes or vessels, understanding the capabilities and patterns of potential adversaries, and reducing the cost of maintenance. However, these data are virtually never collected, and when they are, they are seldom organized in a helpful way, often discarded, and not stored in a way to discern patterns that could show us how to reduce IED-related casualties, defend against cyber attacks, identify which zip codes tend to produce the most talented recruits, or map out how our adversaries attempt to wage hidden economic warfare against us. Our inability to track these patterns disadvantages us against our competitors.

This challenge is characterized by three interdependent areas: 1) data systems; 2) data policies; and 3) data talent.

Data systems: DoD does not adopt the latest technology needed to capture and understand data, creating an infrastructure gap that becomes harder to bridge the longer it is neglected.

Data policies: Since many of the Department's challenges with data are cultural (i.e. DoD organizations are not used to collecting or sharing data), the Secretary's role in this endeavor is critical, particularly because new policy and legal frameworks will be necessary to change the status quo.

Data talent: DoD should recruit and develop data scientists that can prioritize speed and agility, and apply data science techniques common in the private sector but novel to DoD. A new breed of talent is necessary because without the requisite understanding of how to build and interpret algorithms at all levels of organizations – which is profoundly lacking among DoD personnel – advanced analytics will provide a false sense of security for prediction of catastrophic risks.

WHAT CHANGE LOOKS LIKE

Modern data set storage and analysis capabilities no longer make it necessary to devise a common labeling scheme for all data that might be addressed by an application; rather, it is more effective to connect and collect already-labeled data and then, using ML-enabled algorithms, automatically label non-labeled data based on similar available labeled data. Google Scholar, Apple photos, and Evernote work this way, for example.

To this end, it is useful to describe how DoD *currently* treats data and how it *should* treat data, per the standard of the most advanced software companies.

Access

- Current approach: DoD agrees on a set of common tags, sets up a database, and forces everyone to enter and/or convert data into a standard form and submit it to the database that responds to standard queries.
- New approach: Make existing data "discoverable" by putting it on NIPRNet or other accessible networks, create code that scans all databases, assemble a knowledge base (such as a Knowledge Graph) to store structured and unstructured information, and start to create linkages between the data (the goal is not just to view the raw data but also to create pattern-matching APIs (Application Programming Interfaces) that allow access to whatever structure exists for those data).

Analytics (data integrity protection)

- Current approach: Using the same database for transactions and analytics.
- New approach: Making an offline copy of data for analytics and decision support.

Usage

- Current approach: Each use case constructs and maintains a separate database.
- New approach: Data can be pulled from various databases for many different purposes, some of which we can't even identify right now, but will be useful in the future.

Standards

- Current approach: Joint standards committees develop mandated one-size-fits-all schemas.
- New approach: DoD promotes flexible opt-in cooperation across the Department to respond to emerging demands and opportunities.

COURSES OF ACTION

While these are not mutually exclusive, they represent tiered options, from the most comprehensive to the most specific:

1. *Establish a new DoD-wide data agency*

   This new agency would make all of DoD's information available to employees, possess the authority to access all data on NIPRNet, and establish a distributed cloud-based set of services that enable DoD personnel to write applications that tap into the database and provide access to this information.

   With a budget of $500 million to $1 billion per year, creating one virtualized and distributed logical facility to store data and provide the tools and methods to access and analyze it, will form the foundation – common among the private sector's largest innovative organizations – of strategic and tactical data analytics and machine learning.

2. *Make data accessible across silos*

   Modern data access and translation APIs now provide the power to make existing data across disparate silos available without the need to comprehensively process and store data according to unified standards. In myriad DoD verticals (budgeting, personnel, acquisition, healthcare, logistics, etc.), there are often dozens of databases that are not interoperable, a software design flaw that severely undermines DoD's ability to understand what its vast arrays of data can tell it. Sample topics amenable to analysis from more comprehensive data extraction might include: money flows, why certain officers succeed more than others, how we can purchase superior weapons systems for a greatly reduced price, how best to keep service members and their families healthy, and where and why breakdowns in supplying warfighters with materiel occur.

   Traditionally, it has been very difficult to access data across multiple databases within one vertical or Service or Combatant Command or single installation/facility (a "location"), undercutting DoD's ability to analyze its own data. By creating an application at each data storage "location" that mines the data and feeds them into an ML-enabled system, DoD personnel will be able to view patterns never seen before that help them make better decisions in each vertical, Service, COCOM, etc.

3. *Apply machine learning to existing data within silos*

   This approach is a straightforward effort that DoD can and should do now, but it won't solve the underlying data challenges outlined in this recommendation. In this case, data in one location, agency, Service, etc. that has already been labeled can be mined by an ML-enabled application that pre-labels data to enable an exponentially larger increase in efficiency in looking at data normally viewed by humans.

   For example, whether it is drone footage viewed by analysts at Creech Air Force Base or sonar scans viewed by analysts in the Fifth Fleet, there is simply too much incoming data for humans to analyze quickly and accurately. As DoD's sensor collection ability increases, this problem will only get worse, and increasing the number of humans watching monitors is neither practical nor effective. Image and video recognition by machines, which are demonstrably faster, more accurate, and more resilient than humans, will provide the needed, timely analysis mission commanders need. Project Maven is an example of how DoD is addressing this issue the right way, showing that this approach is feasible and replicable across all DoD verticals, agencies, or locations.