



# THE MODERNIZATION QUANDARY

Emerging Technologies Institute Report

## WELCOME LETTER

“The Modernization Quandary” was the first workshop in what will be an ongoing series of activities focusing on the challenges and opportunities associated with accelerating the delivery of emerging technologies to our nation’s warfighters. This event was sponsored by the National Defense Industrial Association’s (NDIA) newly formed Emerging Technologies Institute (ETI). The mission of ETI is to serve as a non-partisan research center focused on the technologies that are critical to the future of national defense, and we can think of no more significant topic with which to launch this new enterprise.

Our hope for this workshop was to begin a reasoned discussion that the national security community needs to have but is not yet having. Much has been written and said about the need for the Department of Defense (DoD) to remain at the forefront of technological innovation—and to do so at a pace that will allow us to deter our rapidly advancing peer competitors. Yet, for a number of perfectly valid reasons, DoD has deferred major acquisition programs such that the Department will be experiencing simultaneous funding demands over the next decade. The quandary, then, is that DoD does not seem to have enough money to do all the things required for Nuclear Modernization, an expanded U.S. Navy fleet, a Next-Generation Air Dominance platform, and other modernization priorities—not to mention delivering hypersonic weapons at scale, enabling artificial intelligence, advanced electronic warfare, new directed energy systems, and so on. And, given both the unlikelihood of significant budget increases and the desire to sustain legacy systems, the Department of Defense simply does not have a program plan that would seem to close the existing gaps.

During the course of this workshop, we sought to explore solutions to this quandary from a technology development, process, and legislative perspective. We began with a panel on technology options and priorities that included some of our nation’s leading thinkers on emerging needs before moving into a panel of top thought leaders addressing what might be done to speed up acquisition, align funding, and allow more options in shorter order. We ended the day with a discussion among distinguished experts on legislative solutions and constraints.

On behalf of our speakers and the NDIA team, we thank you for your interest in this topic and look forward to your future engagement.

### Dr. Mark Lewis

Executive Director  
NDIA Emerging Technologies Institute

### The Honorable Alan Shaffer

Distinguished Visiting Fellow, NDIA ETI  
Former Deputy Under Secretary of Defense for  
Acquisition & Sustainment

## INTRODUCTION

Since the end of the Cold War, a number of factors have converged that together pose a significant national security challenge for the Department of Defense and United States as a whole. These factors include a series of decisions, or in some cases a lack of decisions, that has resulted in delays in defense modernization programs. Such delays have occurred at the same time as a dramatic increase in the capability of near-peer competitors, accompanied by an erosion of domestic industrial capacity in critical sectors. Any solution to this national security challenge—looking to address defense modernization—will have to acknowledge the significant budget pressures on the Department of Defense as it maintains legacy systems and capabilities, all while responding to the needs and expectations of executive branch leadership, Congress, and the American people. This is the Modernization Quandary.

NDIA’s Emerging Technologies Institute held a workshop on June 7, 2021, to address this challenge. “The Modernization Quandary: An NDIA ETI Online Workshop” convened speakers and three groups of panelists who explored possible solutions from three perspectives: 1) Prioritizing the technology areas to maximize capability for cost, 2) Examining process changes to improve delivery, and 3) Reducing legislative barriers to fielding the technologies.

This report outlines some of the key observations and recommendations derived from the workshop. While a single gathering could never offer a complete solution to such a complex problem, the collected experts set the stage for what will certainly be an ongoing dialogue.

An overall theme that emerged from this workshop is that the Department of Defense cannot address these modernization challenges in a vacuum. Given the budget constraints under which the Department operates, it will take a concerted effort—to include Congress, industry, and academia—to streamline processes and increase the tolerance for risk in technology development. Modernizing acquisition processes and leveraging existing authorities for flexibility and transparency will also be required, as will strengthened communication between Congress and the Department.

We look forward to continuing the important dialogue started during this workshop.

## SETTING THE STAGE FOR THE MODERNIZATION QUANDARY WORKSHOP

Participants were reminded that the Department of Defense has made a number of decisions over the past 30 years that have had the effect of deferring or altering various modernization efforts. Whereas those decisions may have been made for tactically valid reasons, the result has been that the Department finds itself in a challenging strategic environment. Several recent works have explored this reality, most notably Mackenzie Eaglen’s report from

the American Enterprise Institute.<sup>1</sup> Over the past three decades, we have seen:

- The fall of the Soviet Union, allowing the United States to “skip a modernization cycle of nuclear modernization” (and other conventional platforms).
- The 9/11 attacks on America, which shifted the focus from conventional systems to those that would operate against the war on terror and insurgencies. For example, much of the focus of the ground tactical vehicle development in the 2000s was on Mine Resistant Ambush Protection vehicles, which led to a stretching of systems like the Joint Lightweight Tactical Vehicle.
- The Budget Control Act of 2011 effectively reduced Defense Budgets by 7-10%, most of which came out of readiness accounts. The resulting instability almost certainly stretched acquisition programs.

Because of deferred modernization, the Department seems to have reached a point where the existing budget simply cannot support the known requirements. Reasonable estimates suggest that DoD requires a 3-5% budget increase, *above inflation*, to meet the current modernization needs. Yet, the first budget submission of the Biden Administration (FY22) showed only a 1.6% increase for Defense—from \$703B to \$715B. Factoring in inflation, this budget represents reduced buying power. While prospects for future defense budgets are uncertain, this situation is likely to get worse in the short term as several key programs are entering their “expensive” phase. These efforts include:

- Nuclear Modernization (simultaneous modernization of Ohio Class sub to Columbia Class, Minute Man III to Ground-Based Strategic Deterrent, Air-Launched Cruise Missile to Long-Range Standoff weapon, and B-2 to B-21).
- Full-Rate Production of F-35 (roughly \$12B in the FY22 budget request).
- Expansion of the Navy, to include both crewed and unmanned surface and undersea vehicles. According to the Navy Modernization plan of December 2020, the procurement of the ships in the current pipeline will cost \$147B over the next Future Years Defense Program.
- Army development of a Long-Range Fires capability.
- The Missile Defense Agency’s recast of the cancelled RKV program with the NGL.
- Procurement of nearly \$2B of legacy microelectronics.
- Expansion of offensive hypersonics and artificial intelligence programs.

Compounding these challenges and for the first time in a generation, the United States is facing formidable conventional and asymmetric threats from China and Russia. In fact, with the fielding of the J-20, J-31, and Su-57, the United States no longer has the only fifth-generation aircraft.

1. Both the Chinese and Russians are expanding their naval fleets, to include a new indigenously designed and built aircraft carrier in China.
2. Russia continues to expand and practice its electronic warfare capabilities.
3. Russia and China are both ahead of the United States in modernizing their nuclear arsenals. In addition, both countries are reportedly pursuing the testing of nuclear capabilities.
4. Both China and Russia have active cyber intrusion programs—which could threaten the U.S. mainland (and should be considered a strategic weapon).
5. The continued development of advanced ballistic missiles in China and Russia, particularly with their introduction of hypersonic capabilities, puts the United States at a disadvantage in advanced munitions.

In addition to conventional military threats, there are fragilities in the defense supply chain that peer competitors can exploit. These fragilities include vulnerabilities in the supply of state-of-the-art microelectronics, rare earth elements, ship-grade steel, and even pharmaceuticals—all of which are coupled with the vulnerabilities of the defense industrial base to cyber attacks, as demonstrated by recent ransomware attacks on energy infrastructure and food supplies, and the ongoing theft of an estimated \$600B in U.S. intellectual property (IP) each year by China.

The last piece of the Modernization Quandary is the status of the U.S. economy and its implications for defense overall. As just one example, the National Debt of the United States has climbed to \$28.4T as of the publication of this report. If distributed uniformly across every American taxpayer, each would owe \$225,310. Furthermore, the ratio of debt to Gross Domestic Product, 127%, is the highest it has ever been—barring the spike during World War II—and is almost twice that of China, with no apparent improvement in sight.

## WORKSHOP PARTICIPANTS

### Hon. Alan Shaffer

Distinguished Visiting Fellow, NDIA ETI  
Former Deputy Under Secretary of Defense for Acquisition & Sustainment

### Hon. James “Hondo” Geurts

Performing the Duties of the Under Secretary of the Navy, U.S. Navy

### Dr. Mark Lewis

Executive Director, NDIA ETI

### Dr. Eric Evans

Director, MIT Lincoln Laboratories

<sup>1</sup> Eaglen, Mackenzie, and Coyne, Hallie, *The 2020s Tri-Service Modernization Crunch*, American Enterprise Institute, Washington, DC, March 2021.

**Dr. Dana “Keoki” Jackson**

Senior Vice President and General Manager,  
National Security Sector, MITRE

**Nicole Petta**

Former Principal Director, Microelectronics,  
Office of the Under Secretary of Defense for  
Research & Engineering

**Hon. Kevin Fahey**

President and Chief Operating Officer, Cypress International

**Hon. Elaine McCusker**

Resident Fellow, American Enterprise Institute

**Hon. Katherina McFarland**

Former Assistant Secretary of Defense for Acquisition and  
Acting Assistant Secretary of the Army for  
Acquisition, Logistics, & Technology

**Gen Hawk Carlisle, USAF (Ret)**

President and Chief Executive Officer, NDIA

**Paul Arcangeli**

Staff Director, House Armed Services Committee,  
U.S. House of Representatives

**Dr. William Greenwalt**

Visiting Fellow, American Enterprise Institute

**Kate Käufer**

Professional Staff Member, Senate Appropriations Committee,  
U.S. Senate

## TECHNOLOGY OPTIONS AND MODERNIZATION PRIORITIES

The workshop began by noting that the 2018 National Defense Strategy called upon the Department of Defense to build a more lethal force through modernizing its key capabilities. The Strategy identified a list of modernization priorities that were then given a central role under the auspices of the Office of the Under Secretary of Defense for Research & Engineering. This focus was done with the creation of the Director of Defense Research & Engineering for Modernization, overseeing a cadre of Principal Directors with a responsibility for providing technology roadmaps. While the successful adoption and fielding of each of these identified emerging technology areas can offer the United States a capability advantage over peer competitors, there may also be other technologies or processes that could reduce the cost of systems or make the Department more efficient. Additionally, modernization is essential for maintaining existing capabilities, including the nation’s aging nuclear arsenal, and other key pieces of our aging military

technology. Modernization is therefore not just about doing entirely new things but also about doing existing things better and fixing those things that are already failing or becoming obsolete.

## Key Recommendations

### **The Department of Defense and Congress should build a margin of failure into the budget of new programs.**

Since budgets are static and allocated months or years in advance, it was pointed out that failure is typically seen as a waste of time and money. While this statement may be true for *destructive* failure, many notable and successful programs have failed—*constructively*—numerous times before achieving success. The Department needs to be less risk averse and, in turn, Congress must be willing to allocate budget margins in new or existing programs to account for failure. Additionally, there must be a cultural shift in both the Department and Congress in how failure is viewed. If the Department, and specifically program managers, could be less concerned about program cuts due to failure, the Department would likely be more transparent with Congress. In essence, failure needs to be an option, which means that the Department needs to avoid what might be termed “dumb” failures—failures due to poor engineering, poor program management, or unrealistic expectations. Accordingly, the Department must recruit and retain the best and the brightest technical leaders and program managers.

### **The Department of Defense should implement Zero-Trust principles across all technology areas.**

One participant highlighted the importance of adopting Zero-Trust principles across many technology areas. Zero-Trust is a concept formulated initially for cybersecurity, where no user or data on a network is granted access beyond its direct scope, and where everything is verified. The Zero-Trust approach represents a very different view from the more traditional network security methods that have focused primarily on establishing seemingly secure perimeters that are intersected by trusted connections. The problem with this latter approach is that absolutely secure perimeters are all but unattainable, and trusted connections may in fact not be trustworthy. The Zero-Trust concept should be expanded and applied to additional technology areas, particularly in the microelectronics area but also to autonomous systems, networked command and control, and next-generation communications. In practice, this expansion might include authorizing all personnel entering and exiting a given laboratory, monitoring data transfers on laboratory computers, and similar practices—all without exception. To do so, the Department should consider commercial standards and advanced monitoring strategies as it applies Zero-Trust principles internally. Of note, another panelist pointed out some challenges with implementing Zero-Trust, including transitioning from current approaches, as well as the certification of new Zero-Trust systems.

### **The U.S. government should expand the limits of data that can be released to academic institutions to the maximum extent possible without compromising security.**

It was pointed out that academic institutions often lead advanced research in many of the emerging technology areas, including artificial intelligence and biotechnology. They also offer an incredibly cost-effective solution to exploring new ideas and developing existing ones. Much of their work is actually funded by the Department, through the laboratories and basic research offices of the Services and agencies such as the Defense Advanced Research Projects Agency and the Missile Defense Agency. While universities with Federally Funded Research and Development Centers (FFRDCs) and University Affiliated Research Centers (UARCs) do classified work, there are challenges that remain for other universities when it comes to handling classified research. A number of universities have expanded their willingness and ability to handle classified information; in turn, the Department has created expanded opportunities for universities to participate in the development of emerging technologies, including the University Consortium for Advanced Hypersonics. Nevertheless, universities often lack access to relevant data, thus inhibiting their contributions to the development cycle. It was suggested that the U.S. government could improve this situation by following best practices that maximize the opportunities for willing partners in academia to work on unclassified aspects of classified projects, or even by providing controlled access to classified data as possible while still protecting information vital to our national security.

**The Department of Defense should emulate digital engineering and data collection techniques used by industry.**

Several of the participants noted that the Department of Defense has embraced a significant push towards digital engineering practices. Partly in response to this embrace, elements of the defense industrial base have pioneered the use of digital engineering to efficiently tighten the development process. The Department can learn from successful examples in order to accelerate development, reduce delivery cost, and—most importantly—reduce sustainment costs, which is especially important in a budget-constrained environment. However, it was also pointed out that the Department should standardize its software and data structures to maximize interoperability both now and in the future. The Department also struggles to collect real-time data and share it rapidly. It would benefit from expanded collaborations with industry to modernize its hardware and software used in data collection.

## ACQUISITION PROCESSES AND THE NEED TO SPEED DELIVERY

A panelist observed that the Department of Defense's current acquisition processes, used to generate requirements and then develop, manufacture, and purchase all equipment and technology, have their roots in principles established almost six decades ago by then-Secretary of Defense Robert S. McNamara. In the intervening years, the adversaries and threats that the United States has faced have changed dramatically—as have the time scales for the development of new technologies. To respond to these changes, it was suggested that the Planning, Programming, Budgeting, and

Execution (PPBE) process must also change. The Department lacks a flexible PPBE process that can effectively respond to shifts in real time without the entanglement of burdensome bureaucracy. Parallel paths of development that might reduce risk are often not encouraged for budget constraint-related reasons, and the Department is not always willing to discontinue or redirect a project when better options are identified. Defense organizations lack the flexibility necessary to shift funding between projects so that time and purchasing power are not lost.

At the same time, participants pointed out that issues involving the ownership, use, and protection of collected data have not been adequately addressed. This data includes that which is part of digital engineering and might be used to help streamline production and maintenance while reducing long-term costs.

Overall, it was suggested that there are tremendous opportunities for improvement in the acquisition processes. The Department would benefit greatly from a critical evaluation of the current architecture with an eye towards simplifying processes for increased agility and transparency.

## Key Recommendations

**The Department should overhaul the Planning, Programming, Budgeting, and Execution process to allow for increased flexibility and transparency.**

One workshop participant argued that the PPBE process should be updated to permit iterative development and testing. It was suggested that this update could be done by making improved management and oversight tools available within DoD while incentivizing improved behavior among both funders and contractors. More open communication between the Department and Congress would help consolidate the necessary information in budget justification documents, thereby reducing errors and acquisition process times. Greater flexibility in the use of available funds will provide the agility required to improve the fielding of evolving technologies today.

**The Department should clearly define ownership, use, and protection as they relate to data and intellectual property.**

With the transition to digital engineering, it has been observed that there is an increasing need to examine data and IP rights. To do so, it was suggested that the Department not only be diligent in negotiating with industry partners about the ownership of data but also clearly delineate that data's intended use. Multiple production and maintenance processes could be accelerated through greater access to collected data. Equal focus should also be given to protect this data and intellectual property through encryption methods and Zero-Trust policies. Cybersecurity standards ought to be followed to defend against potential cyber attacks, particularly those conducted by peer competitors.

**The Department should continue to integrate digital engineering into production processes to accelerate timelines and reduce costs.**

It was suggested that digital engineering can lead to a shift towards a more efficient model-analyze-build methodology across

the Department. The more that a comprehensive digital representation of virtual systems can be used to emulate actual physical systems, the more that programs will be able to analyze, experiment with, and identify potential issues early in the production process. This method will ultimately lead to an increase in success rates in the field. Creating digital twin models will also help the process of incorporating new capabilities into existing systems and then adapting those systems to emerging risks.

## OVERSIGHT AND APPROPRIATIONS: PERSPECTIVES FROM CAPITOL HILL

Several participants agreed that modernizing the U.S. military and reorienting it towards the Great-Power Competition as outlined in the 2018 National Defense Strategy are priorities for both Congress and the Department of Defense, and are seen as having bipartisan support. Yet, despite this shared interest, the Department and Congress often struggle to effectively communicate with each other, impeding the push for modernization. Communication errors, failure to follow through, overreactions to programmatic failures, and poor incentive structures have all contributed to the problem. To modernize the Department, Congress will have to enable the Department to move with the speed and flexibility it needs while accounting for its role in maintaining oversight authorities. It was also candidly pointed out by participants that the Department of Defense does not always communicate with a single voice, nor do its representatives always recognize the political implications of their requests. The Department has not always done an effective job when educating members of Congress on the importance of specific aspects of defense modernization. Moreover, DoD representatives have damaged their credibility with shifting priorities and by seeming dissembled. Overall, despite a shared understanding of the threats that the United States faces and even an acknowledgment of the changes required to meet those threats, friction between Congress and the Department of Defense remains a limiting factor.

### Key Recommendations

**The Department of Defense should communicate with Congress more effectively, especially in relation to limiting or ending non-vital programs in congressional districts, to build trust in the common goal of a modernized force.**

Though most members of Congress strongly support defense technology modernization, recommendations to cut legacy systems in order to fund new capabilities are often a politically tough pill to swallow. Though it is ideally an apolitical organization, it was suggested by one participant that the Department of Defense should do better in understanding the political implications of ending specific programs, which can often be a long process stretching beyond the election cycles of the members of Congress in affected districts. Therefore, the Department should not ignore the economic

and political impacts in its efforts to explain the benefits of modernization to members of Congress and their staffs.

**The Department of Defense and Congress should do a better job of signaling to the defense industrial base which emerging technologies the Department is prioritizing in its modernization efforts—and then be consistent in their support.**

It was agreed that signaling which emerging technologies are of greatest importance to the military will encourage members of the private sector to invest in these technologies as they see the potential of long-term profits. The result will strengthen the defense industrial base, spur private investment in the military's top priorities, and help bridge the so-called acquisition "Valley of Death" that makes it difficult to get innovative concepts out of the laboratories and into the hands of the warfighters. These demand signals can be provided through annual fiscal year budgets, clear statements delivered by senior members of the Department of Defense, and commitments by Congress that funds allocated to these technologies will not be immediately eliminated upon failures during the testing and procurement phases.

**The Department and Congress should better articulate the threat that peer competitors such as China pose to America's national security as well as how defense spending will be used to ensure the U.S. military remains second to none.**

According to one panelist, large investments in military modernization have historically occurred in response to existential crises. The need to confront China and ensure it does not supplant the United States as the leader of the international order is one of the few areas of true bipartisanship on Capitol Hill. However, since there has not yet been one moment or crisis that defines the threat China poses to average Americans, it was pointed out that a thorough commitment to the U.S.-China competition is not shared by the American public more broadly and, thus, is not always reflected in the priorities of its representatives. Without a shared sense of urgency and a better understanding of what modernization entails, it was stated that there will be no appetite among the public to increase defense spending to the levels required to rapidly modernize the military or even maintain current military funding levels relative to inflation.

## CONCLUSION

Peer competitors pose an existential threat to the future security of the United States. Other nations have had ample time and opportunities to study America's technology-based approach to fighting wars. In some cases, they have been able to replicate, or even surpass, our technical capabilities; in other cases, they have developed effective countermeasures and asymmetric levelers. Both Russia and China have invested significant resources into modernizing existing systems and introducing new ones.

At the same time, the United States faces a perfect storm of expensive modernization bills. All three legs of the nuclear triad

are aging and require replacement; additionally, navy shipbuilding requirements and standing up the F-35 fleet require significant investments, all at a time when the Department is realizing the importance of investing in emerging technologies such as artificial intelligence and hypersonics.

The goal of “The Modernization Quandary: An NDIA ETI Online Workshop” was to plant the seeds for an ongoing discussion and to provide an analysis of possible ways to address these challenges. It is tempting, when faced with such complex issues, to merely “admire the problem”—that is, to identify the issues without offering substantive, actionable solutions. For this workshop, we sought suggested solutions and mitigating options while our participants offered a number of promising ideas. Unsurprisingly, no magic solutions were identified, though some unifying themes were apparent.

The overall message that came from each of the three groups of panelists was the need for cultural change. This sort of cultural change includes changes to the way we think about trust, changes to the way we handle data and intellectual property, and changes to the way we communicate across the government. We also heard a collective realization that the current budgeting and acquisition processes are antiquated and not sufficiently agile to meet our modernization needs. However, we heard few concrete examples of how that problem might be fixed. Perhaps most surprising was the apparent disconnect between the Department of Defense and Capitol Hill staff, especially given the collective appreciation of the pending challenges. Finally, we heard that the Department’s moves towards Zero-Trust, the infusion of digital engineering, and a focus on retaining access to intellectual property are all positive steps with the potential to improve our ability to modernize.

As Honorable Geurts explained in his keynote address opening the workshop, the Department needs to be open to constant and bold experimentation in all aspects—technological, process, and legislative—to overcome the Modernization Quandary. Modernizing the Pentagon is a challenge everyone agrees on; however, without consistent public and political commitment, it may prove impossible, thereby putting American security and prosperity at risk. As this report makes clear, the Biden Administration has inherited a military at an inflection point. Making the right policy changes and investments now can ensure American supremacy for decades to come; the wrong policies and investments risk ceding global leadership.

## CONTRIBUTORS

### **Dr. Mark Lewis**

Executive Director, NDIA ETI

### **The Honorable Alan Shaffer**

Distinguished Visiting Fellow, NDIA ETI

Former Deputy Under Secretary of Defense for Acquisition & Sustainment

### **Camilla Shanley**

Senior Program Associate, NDIA ETI

### **Rebecca Wostenberg**

Research Fellow, NDIA ETI

### **Rahul Jain**

Research Intern, NDIA ETI

### **Shrividya Subramanian**

Research Intern, NDIA ETI

### **Sean Dack**

Research Intern, NDIA ETI

## **ADVANCING THE TECHNOLOGIES OF TOMORROW TO ADVANCE OUR ECONOMY AND SECURE OUR NATIONAL DEFENSE**

The Emerging Technologies Institute of NDIA is a new organization that provides leadership, bolsters public awareness, and creates independent, reliable research about the technologies critical to our nation's economy and national defense.

Led by Dr. Mark Lewis, former Acting Deputy Under Secretary of Defense for Research & Engineering, and supported by a preeminent advisory board, the research staff and leadership at ETI are among our nation's top experts on technological innovations.

ETI provides the leadership outside the government to bring together government, industry innovators, academia, investors, and the American public in pursuit of economic integration, defense modernization, and technological primacy. As part of a nonpartisan 501(c)(3) organization, ETI supports the modernization of the national industrial base and our military through the development, acquisition, and integration of emerging technologies—specifically those essential to our national defense strategy and our economic future. For more information, visit **[EmergingTechnologiesInstitute.org](https://EmergingTechnologiesInstitute.org)**



[ETI@NDIA.org](mailto:ETI@NDIA.org)