Carnegie Mellon University
Software Engineering Institute

ETI EMERGING TECHNOLOGIES INSTITUTE | NDIA

CODING THE FUTURE: RECOMMENDATIONS FOR DEFENSE SOFTWARE R&D

Workshop Report • July 2023

NDIA Emerging Technologies Institute

CONTRIBUTORS

Dr. Maren Leed
Independent Consultant

NDIA Emerging Technologies Institute

Dr. Arun Seraphin
Executive Director

Undral Dalai
Meetings Manager

Camilla Shanley
Senior Manager

Jacob Winn
Associate Research Fellow

Carnegie Mellon University Software Engineering Institute

Dr. Forrest Shull
Lead for Defense Software Acquisition Policy

Alyssa LeSage
Legislative Analyst

Rebellion Defense

Gia DeHart
Marketing Engagement Lead

July 2023
First published in 2023 by NDIA's affiliate, the Emerging Technologies Institute. 2101 Wilson Blvd, Suite 700, Arlington, VA 22201, United States of America. (703) 522-1820

This report is made possible by general support to NDIA and the Emerging Technologies Institute. No direct sponsorship contributed to this report. This report is produced by NDIA, a non-partisan, non-profit, educational association that has been designated by the IRS as a 501(c)(3) nonprofit organization – not a lobby firm – and was founded to educate its constituencies on all aspects of national security. Its research is nonpartisan.

For more information please visit our website: EmergingTechnologiesInstitute.org

Written by Dr. Maren Leed, Dr. Arun Seraphin, Dr. Forrest Shull, Gia DeHart, and Alyssa LeSage
Typeset and produced by Hannah Meushaw, Alexander Feeser, and Eve Dorris.
Edited by Jacob Trask.

MEDIA QUERIES:
Habiba Hamid, Director of Public Affairs & Communications at hhamid@NDIA.org

FOREWORD

In today's world, rapid deployment of software capabilities to support the warfighter is more important than ever before. Rivals are acquiring military capabilities, especially digital capabilities, at a pace that challenges U.S. technological superiority.

Deterring or winning a future fight depends in part on the nation's ability to deliver fully integrated software-based capabilities in defense systems faster than our adversaries and to adapt those capabilities as needed to a highly dynamic threat and mission environment.

To compete in this context, the Department of Defense (DoD) must advance and accelerate the secure delivery of new software capabilities into weapon systems.

Sustaining accelerated capability delivery relies on both aggressively adopting currently emerging technologies and being able to adapt and adopt technologies that are today just "over the horizon" technologies with the potential to add value and disrupt expectations within the next several years.

The Department has made substantial recent progress in modernizing its software acquisition ecosystem. As part of these efforts, OUSD R&E released the DoD Software Science and Technology (S&T) Strategy to advance discussion on software S&T initiatives essential to achieving the Department's 2030 vision. The central focus of this S&T strategy is the need to "deliver resilient software capabilities at the speed of relevance," ensuring the Department can field software capabilities when and where needed. The strategy recognizes that collaborations are needed between the DoD and industry to leverage technologies and understand what is likely over the horizon.

I was pleased that the "Software as a Modernization Priority" workshop, co-hosted by NDIA Emerging Technologies Institute (ETI) and SEI, worked to explore these S&T needs, fostering the needed cross-talk and collaboration with industry and academia. The workshop brought together a cross-section of thought leaders, from the Department, the Defense Industrial Base, startups, and other stakeholders, to share thoughts, perspectives, and approaches to advance critical Software S&T areas and realize their potential. From these discussions, DoD and industry participants were able to identify priorities and recommendations for detailed focus areas consistent with the S&T strategy. This step was essential in the ongoing effort to meet the needs of the warfighter now and in the future. As we know, "software is never done," and likewise software technologies themselves continue to evolve rapidly. We look forward to continuing discussions and collaborations on these vital issues.

Thomas W. Simms

Acting Principal Deputy Director,
Systems Engineering and Architecture

Office of the Under Secretary of
Defense for Research and Engineering

OVERVIEW

The "Software as a Modernization Priority" workshop in November 2022 was hosted by the National Defense Industrial Association's (NDIA) Emerging Technologies Institute (ETI) in collaboration with the Department of Defense's (DoD) sole software-focused Federally Funded Research and Development Center, Carnegie Mellon University's Software Engineering Institute (SEI). The workshop focused on the challenges and opportunities associated with ensuring that software capabilities provide a competitive advantage to national defense. Speakers and panelists discussed their experiences with how DOD and industry are developing new defense capabilities and transitioning those capabilities into operational use.

The workshop delved into key capabilities that lead to software advances for defense, and where government investments can yield the greatest economic and national security impact. While software is an area of increasing attention, developing an understanding of where the government, and the DoD in particular, can and must invest to ensure that U.S. military capabilities remain at the forefront of technological innovation is a complex task. Commercial drivers of software may offer new capabilities that DoD can adopt, but in other areas market pressures may be less clearly aligned with DoD objectives. DoD faces two challenges: to understand where it should lead and where it should be a fast follower, and to be postured to integrate and adopt advances that might result from either path.

The workshop examined both challenges from a government, technical, and market perspective. It began with an overview of DoD's software science and technology (S&T) strategy, followed by a presentation summarizing a recent SEI report on trends in broader software engineering research and development (R&D)[1]. These presentations provided framing for two panel discussions, one featuring industry leaders offering their views on what DoD investments should look like, and the other representing perspectives on software acquisition challenges. The day concluded with a discussion among workshop participants to synthesize the discussion and resulting recommendations.

1 Anita Carleton et al., (2021). Architecting the Future of Software Engineering: A National Agenda for Software Engineering Research & Development. Software Engineering Institute, Carnegie Mellon University. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=741193.

INTRODUCTION

> *DoD must engage in a continual dialogue with industry, to include commercial entities who build and use software who may have no or limited involvement in national defense.*

The Department of Defense has identified advanced computing and software as one of its critical technology areas, including supercomputing, cloud computing, data storage, computing architectures, and data processing. The USD(R&E) 2022 strategic vision statement "Technology Vision for an Era of Competition" noted that:

"Software is ubiquitous throughout the Department, but the speed at which software develops outpaces the Department's ability to stay up to date. The Department must rapidly modernize its legacy software systems with resilient, affordable, and assured new software that has been designed, developed, and tested using processes that establish confidence in its performance."[2]

In response to language in Section 255 of the Fiscal Year 2020 National Defense Authorization Act, the Department of Defense (DoD) appointed a senior official to guide DoD in software, and to lead the development of a Software S&T Strategy. That Strategy, issued in November 2021, set a vision of delivering software capabilities at the speed of relevance, and identified four supporting pillars and associated focus areas.[3]

While the Strategy articulates a clear framework to help shape and inform DoD's software S&T efforts, NDIA's ETI, in partnership with SEI, held a workshop on November 14, 2022, to take the discussion a step further by fostering a not-for-attribution conversation around priorities within that framework. "Software as a Modernization Priority: An NDIA ETI/CMU Workshop" convened academic, industry, and government speakers and panelists who debated the relative merits of software S&T investments from multiple perspectives. This report outlines some of the key observations and recommendations that resulted from that discussion. The range of the day's dialogue made clear that while the importance of software to DoD's future is shared and well understood, there is a wide spectrum of enabling priority areas in which DoD needs to invest.

An overall theme that emerged from this workshop is that DoD must engage in a continual dialogue with industry, to include commercial entities who build and use software who may have no or limited involvement in national defense. The state of the practice in software is moving so quickly that sustained and purposeful engagement is necessary to maintain a clear picture of where private incentives are shaping investments and where they are not. SEI, as an FFRDC that works with government, industry, and academia, can help to bridge that gap. A second theme was that DoD has significant work it must continue to do to ensure it can leverage commercial developments, both technically and procedurally. The imperative for a knowledgeable civilian workforce was noted repeatedly throughout the day as an important, and perhaps most essential, enabler for success. Both ETI and SEI are committed to continuing the important dialogue started during this workshop.

WORKSHOP PARTICIPANTS

The workshop included participants from a range of DoD organizations, the private sector, and academia. Expertise spanned requirements, policy, acquisition, and software production and delivery, for both government and commercial customers. To convey the perspectives represented at the event, a list of participants' organizations is included in Appendix A.

> *DoD has significant work it must continue to do to ensure it can leverage commercial developments, both technically and procedurally.*

2 See USD(R&E)'s Technology Vision for an Era of Competition memo: https://www.cto.mil/wp-content/uploads/2022/02/usdre_strategic_vision_critical_tech_areas.pdf.

3 The four pillars are: (1) shift engineering and development left; (2) adopt an integrated framework of shared resources; (3) transform the software workforce; and (4) align software S&T with acquisition.

SOFTWARE MODERNIZATION PRIORITIES & RECOMMENDATIONS

Prior to the workshop, participants were provided with a simple poll (Appendix B) to solicit their views on the relative importance of DoD investments in three main software areas: tools and capabilities (in the short and long term), workforce, and infrastructure. That poll provided the basis for the concluding group discussion, and informed the findings and recommendations summarized below.

TECHNOLOGY PRIORITIES & RECOMMENDATIONS

The group discussed where DoD should focus its investments to address needs at different time horizons, and also how it should ensure that it keeps abreast of changes in the fast-moving commercial software field.

1.1 DoD should (1) create a process for surfacing and prioritizing long-term software-specific needs, both content (i.e., mission-supporting) and enabling, as a foundation for software S&T investments; (2) ensure S&T funding is applied to software needs; and (3) evaluate the degree to which current in house S&T performers are equipped to support software-specific advances, and make any necessary adjustments. While participants noted attempts to address more flexible funding for software through the new "Budget Activity 8" appropriation, this change does not extend into S&T activities. One participant observed that traditional S&T requirements generation and funding are not well aligned to software-specific future needs: Stakeholders within DoD are not accustomed to considering or articulating long term requirements. Another observed that the current ecosystem of in-house government S&T performers lack broad software expertise, and that DoD may need a different and/or expanded team to achieve the best results. Making more use of opportunities for bringing in software talent from industry may help to ensure that DoD remains aligned with industry practices and standards.

> *Making more use of opportunities for bringing in software talent from industry may help to ensure that DoD remains aligned with industry practices and standards.*

1.2 DoD should consider developing tools to support decisions about software pipeline content, as the next step after pipeline structure. One participant argued that as the use of modern software development and deployment tools and environments has expanded, they are generating a large set of performance data that could yield interesting insights. As environments become more standardized, tools that offer a better understanding of the relative value of operational system-specific algorithms created within those development and testing environments are needed to ensure the content being created is of greatest use. This should support efforts to develop and deliver new software capabilities into use in a more timely and cost effective manner.

1.3 DoD should prioritize the development of capabilities that will enable the maximum possible use of commercially-driven AI-enabled tools. This point was discussed in two specific contexts: with respect to classified data, and with respect to DoD-specific risk tolerance. One participant posited that DoD's system of security classification creates DoD-specific constraints that limit both the usability and the benefits for commercial software applications. He therefore emphasized the need for DoD investment in tools and capabilities to treat and manage data that would maximize secure accessibility across users with different levels of access to classified information, and secure ingestion for commercially developed applications. Automated capabilities would be needed to address these issues at scale. Beyond the data challenge, another barrier to commercial tool use is the lack of a clear framework, approach, or mechanism to establish acceptable risk levels or thresholds for their implementation. Creating automated capabilities to aid organizations within DoD to assess and characterize risk would enable clear policy and support a transparent and consistent mechanism for software evaluation across the Department.

1.4 DoD should focus on tools and capabilities that use automation to minimize the technical debt associated with legacy code. There was a robust discussion around the challenges that DoD will continue to face for the foreseeable future around the need to maintain a substantial amount of legacy code. Whereas commercial entities are more likely to replace or jettison legacy software, there are numerous reasons (cost, mission impact, etc.) why DoD is likely to continue supporting a large amount of legacy code. The breadth of this legacy codebase imposes many challenges, such as the need to sustain expertise in legacy coding languages that may be largely obsolete in the private sector. There is a need, therefore,

for DoD to have tools that can help it understand the scale and nature of outdated code (e.g. semi-automated extraction of the as-built architecture, detection of some types of technical debt), frame decisions about its disposition, and automate triage, interfaces, and/or updates to that code.

1.5 **DoD should create a software-focused S&T advisory board.** Given the speed and breadth with which software capabilities are advancing, and the amount of private investment pushing developments, DoD needs a routine touchstone to help it better understand and assess if they have their investment strategy "about right." This group should include software expertise from across the defense enterprise, including industry, academia, and FFRDCs, but also representatives of purely commercial software providers. It should include expertise with a variety of defense software experiences, including embedded software on weapons systems and platforms, network and communications systems, business systems, and software research and testing.

> *DoD needs a routine touchstone to help it better understand and assess if they have their investment strategy "about right."*

WORKFORCE PRIORITIES & RECOMMENDATIONS

Throughout the day, the need for DoD organizations and the defense industry to either contain or have ready access to expertise in digital and/or software technologies arose frequently. While there were differences of opinion on how much, where, and how best to provide that expertise, some general themes and recommendations emerged.

2.1 **DoD should ensure that Program Executive Offices (PEOs) have sufficient digital/software expertise to understand the impact on the system of software decisions and trades, and the impact on software of system decisions and trades.** Participants' views on whether this expertise must be embedded within the PEO/resident within the senior leadership varied. However, there was a general consensus that, at a minimum, senior leadership needs to be supported by on-call expertise, and that they should have some level of familiarization training, with the ultimate goal of anticipating and understanding the importance of their decisions. There was a general observation that both military and civilian software experts lack a clear career pathway; one participant acknowledged that this was the case for military members assigned to Service software factories and suggested that leveraging their experience in follow-on acquisition assignments, like support for PEOs, might be one of the software factories' greatest contributions.

> *There was a general observation that both military and civilian software experts lack a clear career pathway.*

2.2 **DoD software workforce plans should deliberately seek to promote both retention of internal expertise and "leavening" with rotational positions for commercial practitioners.** The group discussed that retaining existing software expertise can be a double-edged sword, as some of those steeped in existing software practices lack familiarity and comfort with the state of the art. They agreed that the routine incorporation of "outside" experts through programs like the Defense Digital Service should remain an essential component of DoD talent management strategies in the software domain.

> *...incorporation of "outside" experts through programs like the Defense Digital Service should remain an essential component of DoD talent management strategies in the software domain.*

INFRASTRUCTURE PRIORITIES & RECOMMENDATIONS

With respect to software infrastructure, despite the progress to date on elements like a software-specific acquisition policy (DoDI 5000.87), there was a clear consensus that DoD needs to continue to push for the elimination of procedural and policy barriers. Rather than a lack of tools, the group was in strong agreement that authority to operate (ATO) remains the greatest barrier to progress in software implementation given the delays it imposes in deploying capability into use.

3.1 DoD needs to streamline the ATO process. Workshop participants quickly converged around ATOs as the largest barrier to rapid progress in software. From an S&T perspective, there may be some tools and capabilities that can make the process of attaining ATO faster and more straightforward. Greater shared understanding of what standards are applicable across environments would also speed the determination of where reciprocity was appropriate. The discussants were aware of the recent DoD CIO memo and guidance on institutionalizing institutionalizing Continuous Authorizations to Operate (cATOs).[4] However, the group discussion suggested challenges remain to greater use of cATOs which are primarily policy-and culture-related, and that continued attention and leadership on this challenge is essential. One participant pointed out that the sheer number of systems means that greater use of reciprocity is the only feasible path forward. However, it was noted that the authority of individuals responsible for certifying a system does not always extend to the environment through which software is produced. It was suggested that DoD should consider moving to certification as a service, in which a central organization would be charged with providing development and deployment environments to program customers that would be tailored to user needs.

> *Workshop participants quickly converged around ATOs as the largest barrier to rapid progress in software.*

3.2 DoD should explore standardization of requirements for evidence about software systems. Participants noted that the lack of standardization is a hurdle in being able to field capabilities quickly. While some of what needs to be demonstrated for a software system to be fieldable is going to be context-dependent, a substantial amount of the needed evidence around software quality and security could be common across multiple domains. Having a better sense of standard data that need to be collected to support these decisions would enable software factories to be ready as soon as they are deployed to produce a body of evidence which could be machine readable and help satisfy fielding decision needs in a variety of contexts more quickly.

3.3 DoD needs to establish better and more regular communication channels around software, with a spectrum of stakeholders. As mentioned above, to keep abreast of rapidly evolving technologies, DoD must collaborate and communicate more with industry. Such communication does not happen by accident; Department stakeholders need to consciously develop such opportunities at a regular cadence. Likewise, although some progress has been made recently, the Department's usual tendency to do problem solving within specific silos is a challenge. Ensuring that different perspectives within the Department can collaborate on software solutions early and often is key. Finally, good software companies know how to build effective capabilities by talking directly to their customer. Removing the customer from the equation (or burying expertise under too many subcontracting relationships) needs to be avoided. Using roadmaps to help communicate and set clear expectations among the various parties will result in better outcomes.

> *...good software companies know how to build effective capabilities by talking directly to their customer. Removing the customer from the equation (or burying expertise under too many subcontracting relationships) needs to be avoided.*

4 See OSD's 2022 memo on Continuous Authorization to Operate (cATO): https://media.defense.gov/2022/Feb/03/2002932852/-1/-1/0/CONTINUOUS-AUTHORIZATION-TO-OPERATE.PDF.

OVERALL TAKEAWAYS

The workshop concluded with a brief discussion about what DoD is getting right in the software S&T area, and where it is off-base. Participants offered two main areas in which things are going well. One is the new pilot funding mechanism for software (Budget Activity 8, or BA-8), which is an attempt to address software-specific programming and budgeting obstacles that hamper DoD software purchases. Another participant cited the DoD's software acquisition pathway policy, which is built around agile and iterative software practices. It was noted that this approach improves performance, as the iterative delivery timelines expose actual performance more rapidly and consistently than longer traditional acquisition pathways. Another positive area that participants highlighted was around the general culture of software "fluency": that attention to software is more prominent, that software-specific vocabulary is becoming more common, that the priorities for toolsets and environments are more frequently and explicitly articulated, and that programs and PEOs are doing a better job of articulating what they need (in terms of help and capabilities). All of these behaviors were pointed to as signs of a growing organizational acknowledgment of the importance of software to DoD. One participant observed that a key sign of the shift in culture is that it is now helping to shape private capital flows, as evidenced by unprecedented investments in the DoD software industrial base.

In terms of areas of future improvement, participants noted that barriers continue to exist for most programs when it comes to buying software, including licenses. This led to a discussion about Congressional views of the need for DoD to provide more insight into the benefits of the BA-8 appropriation, and the challenges associated with quantifying those benefits. A participant offered a reframing of the pilot effort's true benefits: they are not primarily in the areas of cost, schedule, or performance, but in the ability of program managers to rapidly acquire innovative capabilities once they are identified without having to work at the pace of the Department's lanning, Programming, Budgeting, and Execution (PPBE) cycle.

CONCLUSION

The centrality of software to DoD's present and future is becoming increasingly evident and recognized across the defense community. The implications of this reality for the subset of the community that focuses on long-term technological development – investments in foundational technologies that unlock emergent capabilities – are still being fleshed out and debated. DOD's Software S&T Strategy represents an important milestone in the evolution of that understanding, creating a sustained dialogue among key stakeholders and articulating a clear framework as a point of departure. The Software S&T workshop was intended to be another step in the long process of further socializing and refining that framework, and of surfacing recommendations for priority areas of action from a cross-section of the software community that both feeds and is influenced by DoD's actions in this space.

The overall message that emerged from the day's discussions is that progress is palpable, but that continued focus and effort is essential. Careful consideration of DoD-unique software needs and how they relate to the likely direction of commercially driven advancements will be essential both for DoD to ensure it can make the most of privately developed capabilities and, as has been true in so many other technology areas, for industry to have access to new kernels of seed corn from which currently unimaginable capabilities can be built. The challenges are familiar, including the limitations of the current budgeting and acquisition processes, and ensuring the application of the right kinds of expertise in the right situations. DoD and Congress should continue to emphasize the imperative for overcoming these challenges, and support investments in this essential area. Just as software is "never done," so too the work of software advancement will continue. There is no steady state where the Department will be "caught up" in terms of software capabilities. Rather the Department needs to put processes and relationships in place that will enable it to make use of continued advances from industry and academia. DoD's success depends on its ability to partner effectively with industry to identify the areas where it can have the greatest impact, and with the legislative branch to support policies and investments to realize progress. ETI and SEI look forward to continuing their efforts to facilitate this success.

APPENDIX A: WORKSHOP REGISTRANTS

The list below represents organizations which registered for the workshop. Registrants who participated did not represent the official positions of their organizations; this list is only indicative of perspectives present.

- Adnet
- Applied Intuition
- Bell Textron
- Boeing
- CACI
- Citizen Consulting Solutions
- DCS Corp
- DragonSpears
- Embassy of Singapore
- Etherton and Associates Inc
- GE Aerospace
- Georgia Tech Research Institute
- Google
- Harmonia
- Keysight Technologies
- Leonardo DRS
- Maximus
- McLaughlin Research Corporation
- MIT Lincoln Laboratories
- MITRE Corporation
- Nimbus Services
- Northrop Grumman
- Palantir Technologies
- Rebellion Defense
- Royal Australian Air Force
- Second Front
- Softwarfare
- Sosi
- Specialty Systems
- Spectrum Partners
- Trident Technologies
- U.S. Army
- U.S. Air Force
- U.S. Department of Defense
- U.S. Department of Veterans Affairs

APPENDIX B: POLLING QUESTIONS

Prior to the workshop, participants were provided with a simple poll to solicit their views on the relative importance of DoD investments in three main software areas: tools and capabilities (in the short and long term), workforce, and infrastructure. That poll provided the basis for the concluding group discussion.

Q1: Which of the following should be prioritized for *near-term* impact?

- Software and systems models to assist with integration and assurance
- Automating the software lifecycle to reduce cost and complexity
- Integrated framework of shared resources
- Tools to assess cost and complexity of large-scale DoD software integration
- Tools to analyze and suggest improvements to legacy code

Q2: Which of the following should be prioritized for *long-term* impact?

- Software and systems models to assist with integration and assurance
- Automating the software lifecycle to reduce cost and complexity
- Integrated framework of shared resources
- Tools to assess cost and complexity of large-scale DoD software integration
- Tools to analyze and suggest improvements to legacy code

Q3: Which of the following is most important for addressing workforce challenges?

- Training opportunities for the existing workforce
- Retention of SMEs in the DoD workforce
- Recruitment of SMEs to the DoD workforce from industry
- Winning the competition with private sector for new talent
- General software skills for broader workforce

Q4: What should be the biggest priority for infrastructure to support a successful modernization portfolio?

- Shared, accessible DevSecOps environments
- Modeling and simulation
- Test labs
- Streamlined authorities to operate
- Connection to research and prototyping opportunities

Q5: In 1-2 words, what is one thing that the software modernization activities are getting right?

Q6: In 1-2 words, what is one thing that the software modernization activities are getting wrong?

Q7: Is there anything else you want to share?

EVENT AGENDA

(November 14th, 2022)

Welcome Remarks

Mark Lewis
Executive Director, NDIA Emerging Technologies Institute

Brief: Software S&T and Modernization Area

Allan Dianic
Director of Software Engineering, Policy, and Systems
OUSD(R&E)

Brief: SEI Study on Software Research

Forrest Shull
Lead for Defense Software Acquisition Policy at Software Engineering Institute, CMU

Panel: Industry Perspectives on Software S&T Portfolio

Joshua Marcuse
Head of Strategy & Innovation, Google
Moderator

Chris Lynch
Co-Founder, Rebellion Defense

Jerry McBrearty
B-2 Deputy Program Manager, Northrop Grumman

Courtney Barno
Chief Operating Officer, Defense Unicorns

Panel: Acquisition Community Perspectives on Software S&T Portfolio

Maren Leed
Independent Consultant
Moderator

Jane Rathbun
Deputy Assistant Secretary of the Navy IWAR & Enterprise

Kyle Fox
Air Force Sentinel

Facilitated Discussion: Recommendations on Shaping the DoD S&T Software Portfolio

Bess Dopkeen
Senior Advisor to the Under Secretary for Research & Engineering (OUSD(R&E))

Next Steps

Arun Seraphin
Deputy Director, NDIA Emerging Technologies Institute

SUPPORTING EMERGING TECHNOLOGIES TO SECURE U.S. NATIONAL DEFENSE AND ADVANCE U.S. ECONOMIC STRENGTH

The National Defense Industrial Association's Emerging Technologies Institute (ETI) performs research, hosts events, and bolsters public awareness through educational products and webinars focused on defense technology modernization and innovation. ETI also works to create a policy environment most conducive to the efficient development and delivery of new systems and technologies for the defense enterprise. ETI engages industry, academia, policymakers, and the public to explore emerging technologies' impact on national security and opportunities for industry-government partnerships to increase U.S. competitive advantage.

ETI reports, events, and workshops support NDIA's membership and the defense science & technology enterprise as part of its nonpartisan 501(c)(3) mission.

ETI was founded in 2021 and is staffed by researchers and subject matter experts and backed by a preeminent advisory board.

For more information, visit **EmergingTechnologiesInstitute.org**

EmergingTechnologiesInstitute.org