SYM-AM-21-087

EXCERPT FROM THE PROCEEDINGS OF THE EIGHTEENTH ANNUAL ACQUISITION RESEARCH SYMPOSIUM

Artificial Intelligence Systems: Unique Challenges for Defense Applications

May 11–13, 2021

Published: May 10, 2021

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

Artificial Intelligence Systems: Unique Challenges for Defense Applications

Bonnie Johnson—has over 25 years of leadership and systems engineering experience in naval engineering research and development. She was a Senior Systems Engineer at SAIC and Northrop Grumman, researching automated decision aids for naval combat systems and missile defense capabilities. She joined the Naval Postgraduate School (NPS) Systems Engineering Department in 2011. She has a PhD in systems engineering from NPS, an MS in systems engineering from Johns Hopkins, and a BS in physics from Virginia Tech. [bwjohnson@nps.edu]

Abstract

Today's warfighters are bombarded with information and faced with challenging decision spaces as technology exponentially expands and threat environments become more complex. Artificial intelligence (AI) and machine learning (ML) are advancements that can lessen the burden on the warfighter. AI systems offer far-reaching benefits—improving situational awareness and detection and understanding of threats and adversary capabilities and intents; identifying and evaluating possible tactical courses of action; and offering methods to predict outcomes and effects of course of action decisions. AI systems are the key to understanding and addressing highly complex tactical situations.

AI systems offer advantages to the warfighter, but only if these systems are engineered and implemented correctly and in a manner that lessens the warfighter's cognitive load. Implementing AI systems for defense applications presents unique challenges. This paper identifies four unique challenges and describes how they affect the tactical warfighter, the engineering design community, and national defense. This paper offers solution ideas for addressing these unique challenges through defense acquisition and systems engineering initiatives.

Keywords: Artificial intelligence, machine learning, complexity, tactical decision aids, systems engineering, trust, human–machine teaming

Introduction

AI is a field that includes many different approaches with the objective of creating machines with intelligence (Mitchell, 2019). Figure 1 shows a simple Venn diagram with machine learning (ML) as a subset of AI, and with AI as a subset of the broader category of automation. Automated systems function with minimal human input and often perform repetitive tasks based on commands and rules. AI systems perform functions that mimic human intelligence. They incorporate learning from past experiences with new information received to make decisions and reach conclusions.

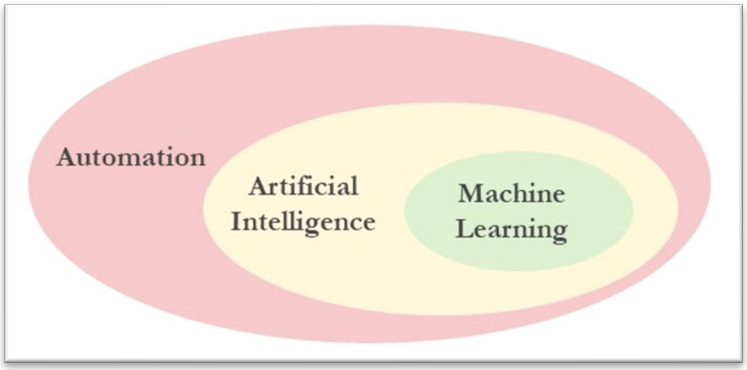

Figure 1. Venn Diagram of Automation, Artificial Intelligence, and Machine Learning

There are two primary types of AI systems, as described in Figure 2. The first type, which are explicitly programmed, are also known as Handcrafted Knowledge Systems. Allen (2020) described Handcrafted Knowledge Systems as "AI that use traditional, rules-based software to codify subject matter knowledge of human experts into a long series of programmed 'if given x input, then provide y output' rules" (p. 3). These systems use traditional, or normal, programming languages. The second type are ML systems that are trained from large sets of data. The ML systems "learn" from the trained data sets, and the "trained" system is then used operationally to produce predicted outcomes given new operational data.

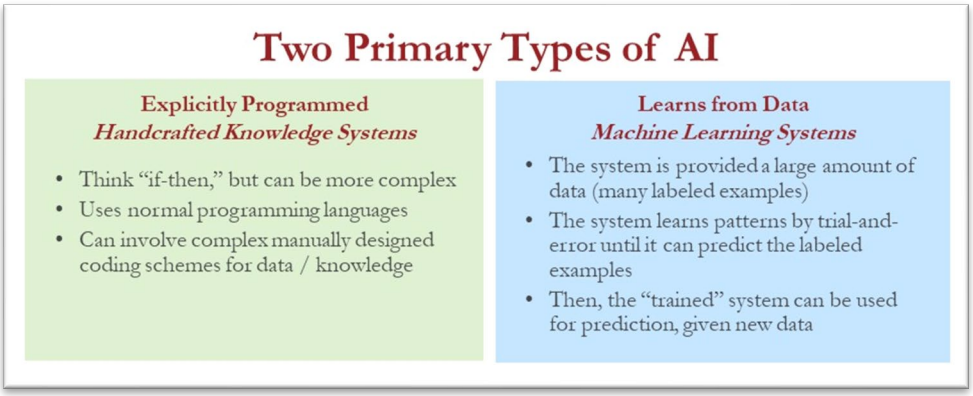

Figure 2. Two Types of Artificial Intelligence: Explicitly Programmed and Learning Systems

Automation, AI, and ML systems—both handcrafted knowledge systems and learning systems—offer great potential for the Department of Defense (DoD) with diverse applications in most mission domains. These intelligent systems can extend the DoD's abilities to make sense of complex and uncertain situations, to develop and weigh options, to predict the success of actions, and to assess the consequences. They offer the potential to support the DoD in strategic, planning, and tactical domains. AI systems can lessen the burden on the warfighter, but only if these systems are engineered and implemented correctly and in a manner that lessens the warfighter's cognitive load. Implementing AI systems for defense applications presents unique challenges. This paper identifies four unique challenges and describes how they affect the tactical warfighter, the engineering design community, and national defense.

The first unique challenge in implementing AI systems for defense applications is that tactical warfare presents highly complex situations. Tactical complexity can involve information overload, multiple concurrent missions that need to be addressed, time-critical decisions with dire consequences, unknowns/inaccuracies/incompleteness in situational awareness, and engineering challenges arising from the interoperability required among a diverse set of distributed warfare capabilities. Adding AI systems into this already-complex environment is a necessary but highly challenging endeavor.

The second unique challenge is that AI systems require large amounts of data for the systems to be trained. The quality of the resulting AI systems that are developed depends largely on the quality and quantity of the training data sets. Data in the military domain can be especially hard to come by. Military data may involve classification issues, cyber vulnerabilities, data validation challenges, and may simply be very costly and time-consuming to gather based on the need for fleet exercises and war games.

The third unique challenge is that the engineering of AI systems presents a new frontier for systems engineering. In traditional systems, behavior is set and is therefore predictable: given an input and conditions, the system will produce a predictable output. Some AI solutions

may involve systems that are complex in their own right—adapting and learning—and therefore producing unforeseen outputs and behaviors. In fact, the intent of some AI systems is to do just that—team with a human decision-maker by taking on some of the cognitive load and producing intelligent recommendations. Systems engineering methods are needed to engineer intelligent systems and ensure that they are explainable, trustable, and safe to human operators.

The fourth unique challenge is that for defense applications there is always a potential adversary that needs to be considered. In terms of AI systems, the acquisition community must be mindful that peer competitor nations are making their own strides in AI advancements. U.S. defense systems must also advance in this AI race. Cyberattacks are always a possibility in defense systems. As defense capabilities increase reliance on automation and AI systems, this may be creating more cyber vulnerabilities. Finally, technology is rapidly evolving, and the adversarial threat space is changing. The defense acquisition and systems engineering communities must ensure that AI systems evolve and adapt to address changes in the threat environment and do this in a trustable and safe manner.

Challenge: Complex Decision Spaces

The first unique challenge is that many defense domains present a complex decision space. Therefore, engineering and implementing appropriate AI systems to address this complexity will be highly challenging. Figure 3 highlights some of the many factors that contribute to decision complexity in the tactical domain. Naval strike force operations, as an example, can quickly change from a peaceful state to one of great peril-- requiring alertness to the threat and appropriate response actions—all within a highly compressed decision time line. Tactical threats may arise from underwater, on the surface, in the air, from the land, from space, or even virtually, resulting in the need to address multiple time-critical missions. With naval and defense assets on ships, submarines, aircraft, land, and in space; the tactical decision space must address the optimal collaborative use of these dispersed and diverse resources. Developing effective tactical courses of action must also occur in highly dynamic operational environments with only partial and uncertain situational knowledge. The decision space must also consider constraints imposed by command authority, rules of engagement, and tactical doctrine. The role of humans as tactical decision-makers adds to the complexity of the decision space—with the challenges of information overload, operator error, AI trust, and AI ambiguity and explainability issues. Finally, the stakes can be very high for tactical decisions and their possible consequences.

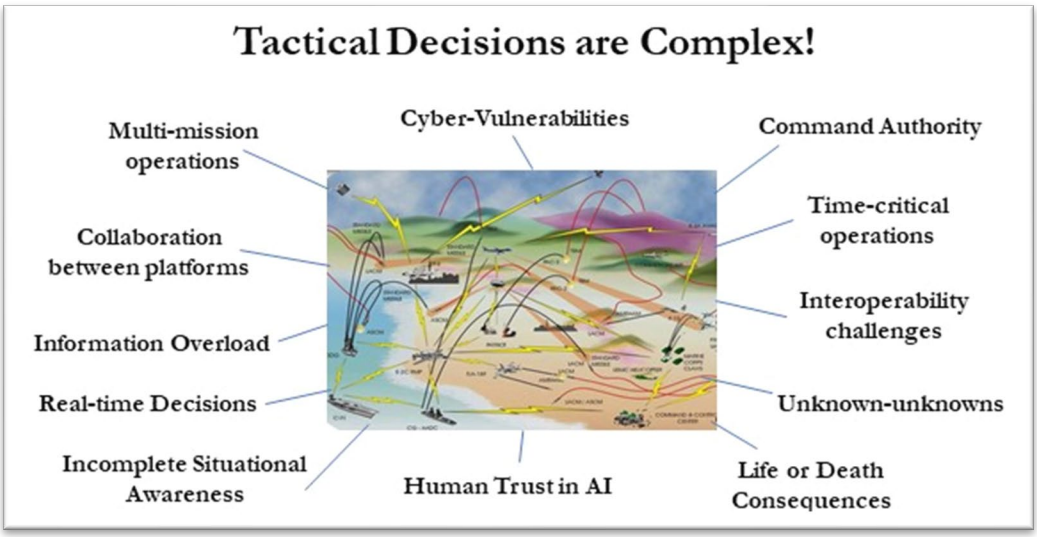

Figure 3. Factors that Lead to Tactical Decision Space Complexity

Addressing highly complex decision spaces is a challenge for the DoD. AI offers a potential solution to addressing this complexity—by handing large amounts of data, dealing with uncertainty, making sense of complex situations, developing and evaluating decision alternatives, and understanding risk levels and decision consequences. AI solutions can apply at the DoD strategic, planning, and tactical levels. The Naval Postgraduate School (NPS) has developed an engineering framework and theory for addressing highly complex problem spaces that require the use of intelligent and distributed AI systems for gaining situational awareness and making collaborative course of action decisions that adapt to a dynamic situation (Johnson, 2019). A complex tactical scenario was modeled to demonstrate the use of AI to validate the approach (Johnson, 2020a). NPS has developed a conceptual design for a predictive analytics capability to be implemented as an automated real-time war-gaming system that explores different possible tactical courses of action and their predicted effects and red force responses (Johnson, 2020b). NPS studies have identified the need to characterize the level of complexity during tactical operations and to implement an adaptive human–machine teaming arrangement to make tactical decisions where the level of automation adapts according to the level of situational complexity. Ongoing NPS research is studying the application of these conceptual engineered approaches in a variety of defense use case applications, including air and missile defense, over-the-horizon strike, ship self-defense, UAV operations, and laser weapon systems.

Complex decision spaces create challenging problems for AI systems to try and solve. Table 1 compares different AI application domains based on the complexity of their decision space. The table contains 10 factors that characterize the complexity of a decision space: epistemic uncertainty (the amount of uncertainty in the knowledge of the situation), situational dynamics, the decision time line (amount of time to make the decision), the complexity of the human interaction in the decision process, the resource complexity (the number, types, distance between them, and how dynamic they are), whether there are multiple missions involved, the existence of adversaries (competitors, hackers, or outright enemies that intend to destroy or overtake), the margin of allowable error (how much decision error is acceptable), and the severity of decision consequences.

Table 1. Comparison of Decision Complexity for Different AI Applications

	Epistemic Uncertainty	Situational Dynamics	Decision Time Line	Human Interaction in Decision Process	Resource Complexity (Number, Diversity, Geographical Dispersion, Dynamics)	Multi-Mission (Complexity in the Mission)	Training Data Sets (Ease of Obtaining, Data Rich vs. Data Poor)	Existence of Adversaries	Margin of Allowable Error	Decision Consequences
Loan Approval										
Advertising										
Medical Treatment										
Shipping Routes										
Self-Driving Cars										
Military Tactical Decisions										
Key		= little or no contribution to decision complexity			= medium amount of contribution to decision complexity			= high contribution to decision complexity		

The decision spaces involved in AI applications for advertising (determining which ads to stream to specific users based on their buying habits or Internet searches), loan approvals (determining loan eligibility based on loan amounts and credit scores), and medical treatments (determining diagnoses based on patient symptoms) are relatively straightforward. Large amounts of training data exist, calculations and human interaction in the decision process are straightforward, and the situations are relatively stable. The consequences of poor advertising are minimal. A bad loan approval decision can be audited. Poor medical diagnoses can have more serious consequences, but there is often enough time to seek more evaluation and opinions before treatment. Determining optimum shipping routes and engineering AI systems for self-driving cars are more complicated endeavors. These applications are dynamically changing and require shorter amounts of time to make decisions. Shipping routes will have complexity in the numbers of possible routes—which can result in many possible options. However, there is room for shipping errors, and the consequences are usually not too severe. The margin for decision error is very small for self-driving cars. Poor decisions in this application can cause serious accidents.

However, the military tactical domain presents extreme complexity in all areas of the decision space: uncertainty and limited knowledge/awareness, highly dynamic situations, very limited time lines, complicated human interaction, large numbers and types of resources, multiple missions, costly and hard-to-obtain training data sets, extremely small margins of allowable errors, and life-or-death consequences of actions (or inaction).

Challenge: Data Can Be Hard to Acquire

The second unique challenge is that AI/ML systems require large amounts of relevant and high-quality data for training and development, and these data can be hard to come by in the military domain. Handcrafted knowledge systems that are explicitly programmed need data during the development process for evaluation and validation. ML systems have an even greater dependence on data during development. As shown in Figure 4, ML systems "learn" from data sets that represent what the operational conditions and events will be. The process of ML system learning is also called being trained, and the data used during the development phase are called training data sets. There are several types of ML learning or training—these are supervised, unsupervised, and reinforcement. All three types of ML learning require training data sets. The ML systems continue to need data during the post-deployment or operational phase. Figure 4 shows that during operations, the ML system, or "model," receives operational real-time data and determines predictions or decision outcomes by processing the operational data with its "trained" algorithms. Thus, throughout the systems engineering and acquisition life cycles, the ML system is intimately connected to data. The ML system "emerges" from the process of learning from the training data sets. ML systems are a product of the quality, sufficiency, and representativeness of the data. They are wholly dependent on their training data sets.

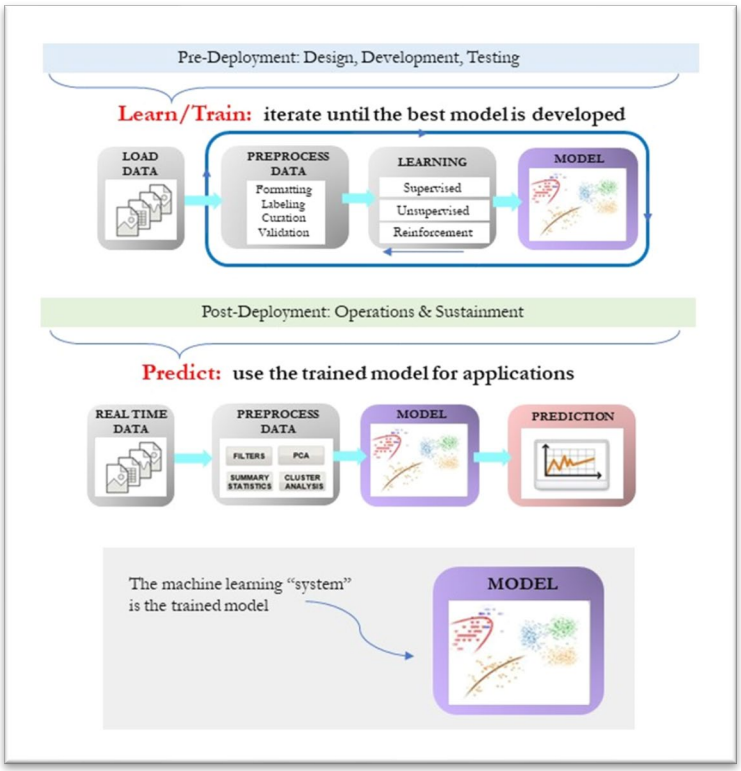

Figure 4. Developing and Implementing Machine Learning Systems

The DoD is beginning to recognize the need for these data sets as more AI developers in many domains (warfare, supply chain, security, logistics, etc.) are understanding the potential benefit of AI solutions and are embarking on AI system development. In some cases, the data exists and is ready to support AI system development. In other cases, the data exists but is not saved and stored. Finally, in other cases, the data does not exist and either needs to be simulated or gathered in fleet exercises or war games. Figure 5 illustrates a process of

considerations that need to be made to gather, obtain, and in some cases develop data for use in developing and training AI and ML systems.

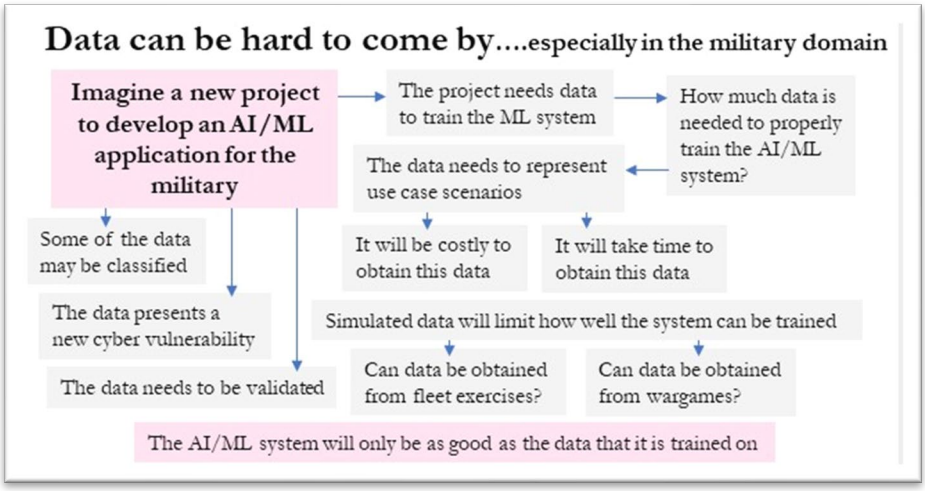

Figure 5. Development of Data Sets for Artificial Intelligence and Machine Learning System Training

The military domain presents some unique challenges for developing training data sets—the data may be classified, the data may present a cyber vulnerability (it could be hacked and purposely corrupted by an adversary), and if the data doesn't exist, it may need to be obtained from military/fleet exercises or war games. Data validation is a challenging endeavor as well.

NPS is performing a needs analysis and conceptual design for a data management system for the Navy that will collect and provide data to many disparate organizations within the Navy that are developing AI/ML systems (French et al., 2021). Figure 6 is a context diagram of the Navy Central Artificial Intelligence Library (CAIL) that is envisioned as a data management system and process for identifying data sets and providing indexing, validation, auditing, and secure access to data that can be used by AI/ML developers working on naval applications. The CAIL would not be a data repository or database, but instead, a central organization that enables AI/ML developers to access validated and secure naval data—to help identify the existence of data sets, enable the authorized access, and help support developers when data that is needed does not yet exist and needs to be obtained—possibly through fleet exercises or war games.

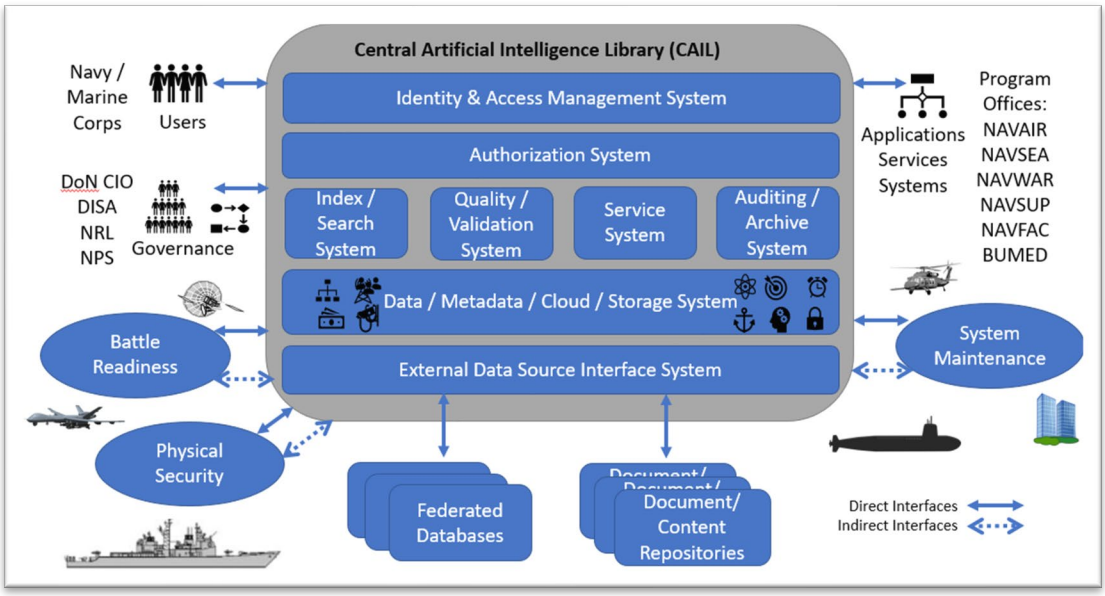

Figure 6. The Conceptual Central Artificial Intelligence Library (CAIL; French et al., 2021)

Challenge: AI Presents a New Frontier for Systems Engineering

The third unique challenge is that developing AI systems is presenting a new frontier for systems engineering. Systems engineering methods have been developed for engineering traditional systems that can be highly complicated but also deterministic (Calvano & John, 2004). Traditional systems have predictable behavior: for a given input and conditions they will produce a predictable output. Figure 7 illustrates the need for changes to traditional SE methods, like the SE Vee process, in order to engineer AI systems that are complex and nondeterministic. In particular, new methods will be needed to define requirements for a learning system that adapts over time, and the process of system validation may need to evolve and continue during operations to ensure safe and desired behavior. For military systems with high stakes consequences, there is very little room for error, so implementing a systems engineering process that can ensure safe and desired operations for AI systems is a requirement.

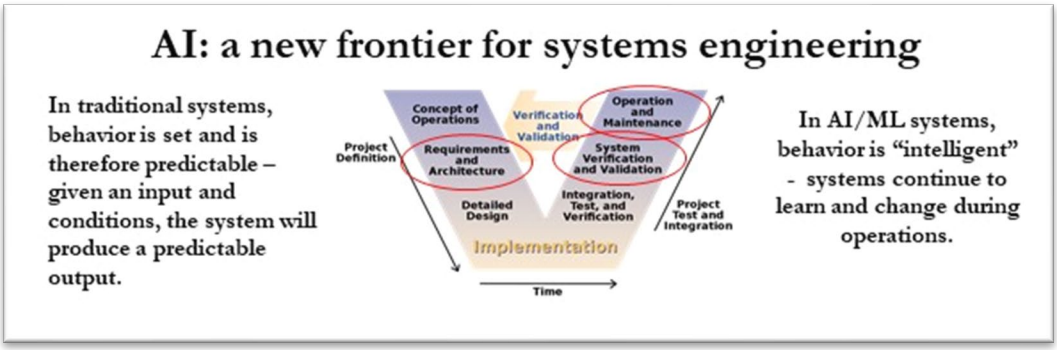

Figure 7. Artificial Intelligence: A New Frontier for Systems Engineering

A recent initiative by the International Council of Systems Engineers (INCOSE) has begun to explore what changes need to be made to systems engineering methods to effectively develop AI systems. Figure 8 was created as part of this initiative to highlight five aspects of AI systems that need to be considered during the SE process. In addition to nondeterministic and evolving behavior, AI systems may present new types of failure modes that are unanticipated, may occur suddenly, and whose root causes may be difficult to discern. Robust design—or ensuring that AI systems can handle and adapt to future scenarios—is another systems engineering design consideration. Finally, for AI systems with more involved human–machine interactions, careful attention must be paid to designing systems so they are trustworthy, explainable, and ultimately useful to the human decision-makers.

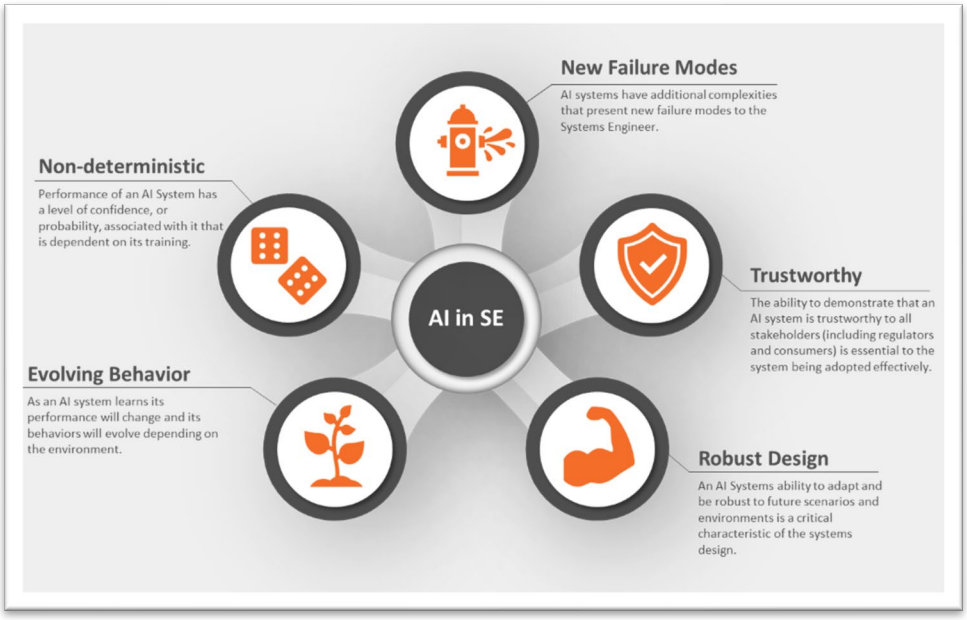

Figure 8. Challenges in the Engineering of Artificial Intelligence Systems (Robinson, 2021)

NPS is studying systems engineering methods that can support the design and development of complex, adaptive, and intelligent AI systems. A systems engineering framework and methodology has been developed to engineer complex adaptive systems of systems solutions (Johnson, 2019). The methodology supports the development of systems of systems that, through the use of AI, can collaborate to produce desired emergent behavior. A current research project is studying safety measures that can be engineered into AI systems during the design process to ensure safety during operations (Cruz et al., 2021). NPS is studying a design solution called *metacognition* as an approach for an AI system to identify internal errors (Johnson, 2021). Another current NPS thesis project is studying how to engineer "trust" into AI systems to ensure effective human–machine teaming arrangements (Hui, 2021). Several NPS research projects have studied the use of an SE design approach called *coactive design* to determine interdependences between human operators and AI systems (Blickley et al., 2021; Sanchez, 2021).

Challenge: Adversaries

The fourth unique challenge is the presence and role of the adversary in defense applications. The DoD must keep up in the race with adversaries to advance AI capabilities, AI systems must be protected from cyberattacks, and AI systems must adapt to the ever-changing evolution of the threat environment. Figure 9 highlights this unique set of challenges that the existence of adversaries presents for AI systems being developed for the DoD.

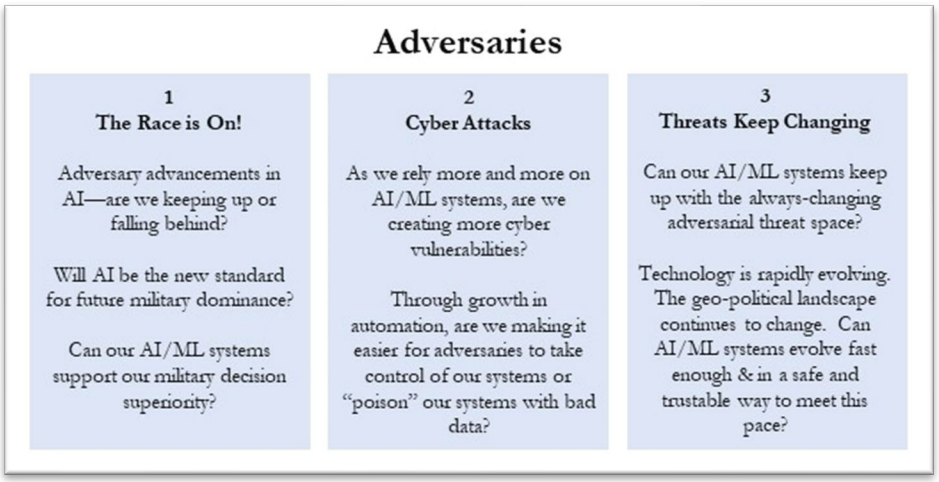

Figure 9. Adversarial Challenges

The race among peer competitor nations to develop AI capabilities is ultimately about getting inside the adversary's decision cycle to decide and act faster than the adversary can (Rosenberg, 2010). AI systems offer the potential to improve the quality and speed of decisions and are therefore critical to gaining decision superiority. As the DoD explores AI solutions, peer competitor nations are doing the same. Ultimately, realizing the goal of using AI for the DoD depends on more than AI research. It requires proper data gathering and management, effective systems engineering and acquisition methods, and careful consideration of the human interaction with AI systems. The DoD must ensure that it meets all the challenges involved with implementing AI systems in order to win the race. An NPS research initiative is studying how to apply AI and game theory to get inside an adversary's tactical decision cycle (Johnson, 2020b). This project is developing a concept for creating models of the tactical situation, the adversaries' location and capabilities, and a prediction of what the adversaries know about the situation. The conceptual system would then play a real-time "war game" to analyze tactical decision options based on predicted adversarial responses and second- and third-order effects. This is an example of studying what future tactical warfare might be like with enhanced knowledge and decision aids for both blue and red forces. Other NPS initiatives to prepare the DoD for the AI race include studying new SE methods and acquisition practices for developing AI capabilities, studying the data management needs of the Navy and the DoD (French et al., 2021), and studying AI system safety risks to develop engineering practices that ensure safe AI capabilities (Cruz et al., 2021; Johnson, 2021).

Cyber warfare is another race that the DoD must successfully compete in to stay ahead of the constant onslaught of hacking attempts. As the DoD implements more automation, it naturally results in more cyber vulnerabilities. The use of AI systems that are intrinsically dependent on both trained and operational data, opens up opportunities for hackers to poison the systems with corrupt data during the development phase and also during the operational phase. If an adversary gains control of an operational AI system, the possible harm they can inflict will depend on the application domain. For automation that supports weapon control

decisions, the consequences can be deadly. In a recent study on automotive cybersecurity, a car company posted a fake vehicle electronic control unit online, and in under 3 days, 25,000 breach attempts were made (Taub, 2021). The DoD must be mindful of the particular cyber vulnerabilities presented as AI systems are developed. Careful cyber risk analysis and cyber defense strategies must be implemented for each new AI system. NPS is studying data security requirements for ensuring that ML training data sets are safe from hacking and will require secure authorization to access (French et al., 2021). NPS is studying the use of metacognition as a method for AI systems to perform self-evaluation as a means to identify cyber intrusions, tampering, or any unusual behavior (Johnson, 2020b). NPS is also studying the use of ML to identify malicious spoofing and tampering with the Global Positioning System (GPS; Kennedy, 2020).

The evolution of the threat environment is the third adversarial race for the DoD as it develops AI systems. As the adversarial threat space is constantly changing over time with faster and more lethal weapons, more autonomy, greater surveillance assets, more advanced countermeasures, and more stealth, this poses a challenge for the DoD to be able to anticipate and identify new threats and cope with unknowns in the battlespace. NPS research is focused on engineering systems that continue to adapt and learn during operations to detect and identify unknown unknowns in the battlespace and quickly respond to new threats through innovative courses of action (Grooms, 2019; Jones et al., 2020; Wood, 2019). NPS is studying ML methods for identifying anomalies in patterns of life by studying data over time for a given region to identify unusual changes (Zhao et al., 2016). An example is the study of commercial aircraft flight patterns and identifying suspicious aircraft based on unusual flight patterns. Ground-based operations can be surveilled over time to identify new and unusual construction projects that could signify military operations.

Conclusions

AI systems offer the DoD significant advances in achieving and maintaining knowledge and decision superiority. However, implementing AI systems for defense applications presents unique challenges. The military tactical domain presents extreme complexity in all areas of the decision space: uncertainty and limited knowledge, highly dynamic situations, very limited time lines, complicated human interaction, large numbers and types of resources, multiple missions, costly and hard-to-obtain training data sets, extremely small margins of allowable errors, and life-or-death consequences of actions (or inaction). AI systems, and ML systems in particular, require representative, sufficient, secure, and validated data sets for their development. Gathering suitable data for defense application has the additional challenges of handling classified data sets and ensuring that data is secure and protected from cyberattacks; it will also be a major endeavor to gather real-world data that represents tactical operations. New systems engineering methods will be required to effectively specify, design, and evaluate AI systems that present new levels of complexity through their non-determinism, new types of human–machine teaming challenges, and new safety failure modes that are hard to anticipate and prevent. Finally, the existence of adversaries in the military domain presents an AI race in three forms: a race to develop AI systems as quickly as adversaries, a race to stay ahead of possible cyberattacks, and a race to train AI/ML systems that can cope with the ever-advancing adversarial threat space.

NPS is addressing the four unique challenge areas through a series of ongoing research initiatives. NPS researchers are studying the implementation of AI systems in the naval tactical warfighting domain, conducting needs analysis and requirements development for military data sets, studying systems engineering methods for developing complex AI systems, and developing methods to engineer AI systems that are safe, trustable, and mindful of the role of potential adversaries. NPS is providing AI research and educational opportunities for military

officers and civilian students. NPS welcomes collaboration with the DoD and naval organizations to continue studying AI systems for defense applications and to continue exploring solution strategies and methods for overcoming the challenges of developing and implementing AI capabilities.

References

Allen, G. (2020). *Understanding AI technology*. Joint Artificial Intelligence Center, U.S. Department of Defense.

Blickley, W., Carlson, J., Mariana, M., Pacheco, A., & Roscher, J. (2021). *The cognitive laser weapon system: An understanding, architecture design, and integration of an automated decision aid within a laser weapon system*. Naval Postgraduate School.

Calvano, C., & John, P. (2004). Systems engineering in an age of complexity. *Systems Engineering*, *7*(1).

Cruz, L., Hoopes, A., Pappa, R., Shilt, S., & Wuornos, S. (2021). *Evaluation of the safety risks in developing and implementing automated battle management aids for air and missile defense*. Naval Postgraduate School.

French, R., Fukumae, W., Hun, K., Matuga, O., & O'Shaughnessy, C. (2021, March). *Data management for artificial intelligence/machine learning implementation* [Presentation]. Naval Applications for Machine Learning (NAML) Conference.

Grooms, G. (2019). *Artificial intelligence applications for automated battle management aids in future military endeavors* [Master's thesis, Naval Postgraduate School]. NPS Archive: Calhoun. https://calhoun.nps.edu/handle/10945/62722

Hui, P. (2021). *Proposing a strategy to develop a trustworthy artificial intelligence enabled air and missile defense system* [Thesis proposal]. Naval Postgraduate School.

Johnson, B. (2019). *A framework for engineering complex adaptive systems of systems* [Doctoral dissertation, Naval Postgraduate School]. NPS Archive: Calhoun. https://calhoun.nps.edu/handle/10945/63463

Johnson, B. (2020a). Modeling and simulation analysis of a complex adaptive systems of systems approach to naval tactical warfare. In D. Braha et al. (Eds.), *Unifying Themes in Complex Systems X: International Conference on Complex Systems (ICCS)*. Springer.

Johnson, B. (2020b). Predictive analytics in the naval maritime domain. In Y. Zhao (Ed.), *Proceedings of the AAAI Symposium on the 2nd Workshop on Deep Models and Artificial Intelligence for Defense Applications: Potentials, Theories, Practices, Tools, and Risks 2020*, co-located with the Association for the Advancement of Artificial Intelligence 2020 Spring Symposium Series (AAAI-SSS 2020).

Johnson, B. (2021, April). Metacognition for artificial intelligence system safety [Manuscript submitted for publication]. *Proceedings of the 16th International Conference on Systems (ICONS).*

Jones, J., Kress, R., Newmeyer, W., & Rahman, A. (2020). *Automated battle management aids for air and missile defense: Leveraging artificial intelligence* [Systems engineering capstone report, Naval Postgraduate School]. NPS Archive: Calhoun. https://calhoun.nps.edu/handle/10945/66088

Kennedy, R. (2020). *Applying artificial intelligence to identify cyber spoofing attacks against the global positioning system* [Thesis proposal]. Naval Postgraduate School.

Mitchell, M. (2019). *Artificial intelligence: A guide for thinking humans*. Picador.

Robinson, K. (2021, January 31). *Engineering artificial intelligence with systems engineering* [Presentation]. INCOSE International Workshop, Artificial Intelligence-Systems Engineering Primer Workshop.

Rosenberg, B. (2010, April 21). Military seeks to disrupt the enemy's decision cycle. *Defense Systems*. https://defensesystems.com/articles/2010/04/26/cover-story-getting-inside-the-enemy-decision-cycle.aspx#:~:text=Success%20in%20battle%20is%20increasingly,quickly%20than%20your%20adversary%20can.&text=As%20a%20result%2C%20military%20forces,known%20as%20the%20OODA%20loop.

Sanchez, K. (2021). *A study of human interactions with artificial intelligence systems for naval tactical applications* [Unpublished manuscript].

Taub, E. (2021, March 18). Carmakers strive to stay ahead of hackers. *New York Times*.

Wood, S. (2019). *Leveraging artificial intelligence in support of decision superiority: Enabling artificial intelligence, a system of systems approach* (NPS-19-N157A). NPS Archive: Calhoun. https://calhoun.nps.edu/handle/10945/65039

Zhao, Y., Kendall, W., & Johnson, B. (2016). Big data and deep analytics applied to the common tactical air picture (CTAP) and combat identification (CID). In *Proceedings of the 8th International Joint Conference on Knowledge Discovery, Knowledge Engineering, and Knowledge Management* (Vol. 1, pp. 443–449).

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net