Software Systems Engineering for the Development, Deployment, and Exploitation of Artificial Intelligence / Machine Learning-Based Systems at the Tactical Edge

RESEARCH TEAM

Student: Matthew M. Sheehan
Department of Systems Engineering
Naval Postgraduate School

Advisor: Dr. Oleg A. Yakimenko
Department of Systems Engineering
Naval Postgraduate School

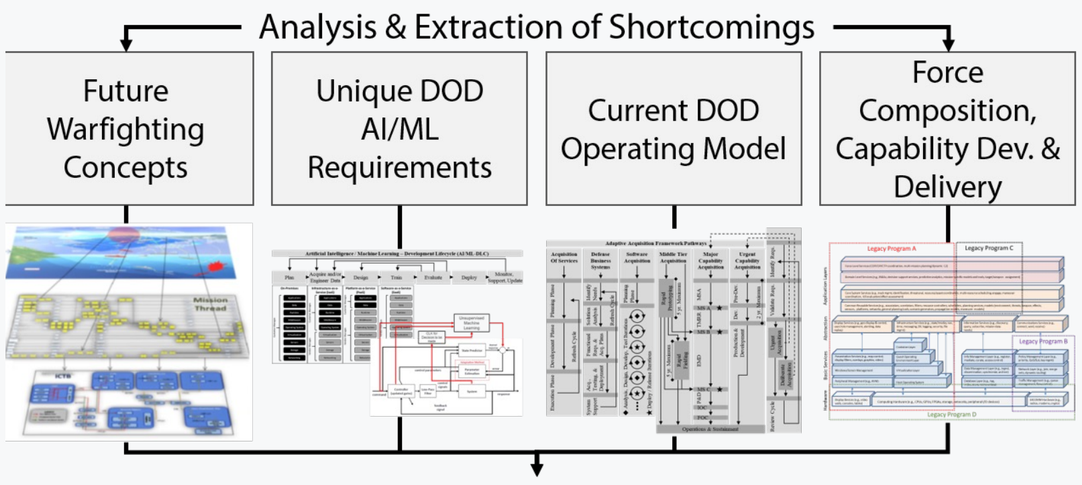
NAVAL POSTGRADUATE SCHOOL

RESEARCH TASK & OVERVIEW

The U.S. Armed Forces' future ability to **dominate the battlespace** will not be measured by the amount of exquisite platforms acquired by the Department of Defense (DOD), but how **well and fast** the DOD can deliver capability via artificial intelligence/machine learning (AI/ML).

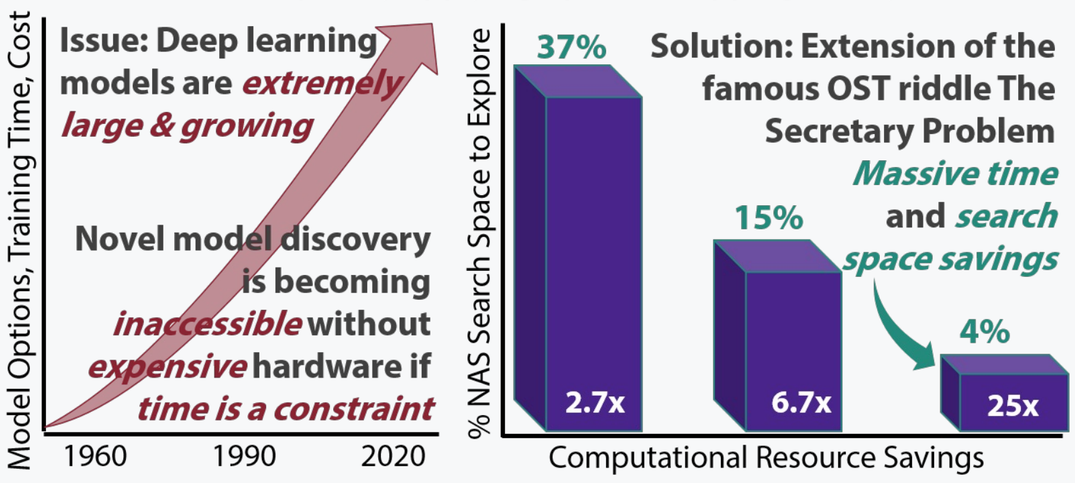
- The DOD is **dependent upon AI/ML to enable its future** warfighting concepts; however, it currently **struggles with basic** software development.
- The DOD has **unique** AI/ML requirements **beyond** the commercial sector; meaning DOD AI/ML development and delivery is **complex.**

DATA & ANALYSIS



Creation of reusable artifacts: (1) Required infrastructure for development and operation, (2) Digital System Architecture, (3) Integration and modernization methods for legacy systems, (4) Acquisition guidelines for resourcing and contracting, (5) Training/testing datasets, (6) Adversarial AI/ML safeguards

Reusable artifact example: Efficient neural architecture search (NAS) method developed by applying optimal stopping theory (OST)

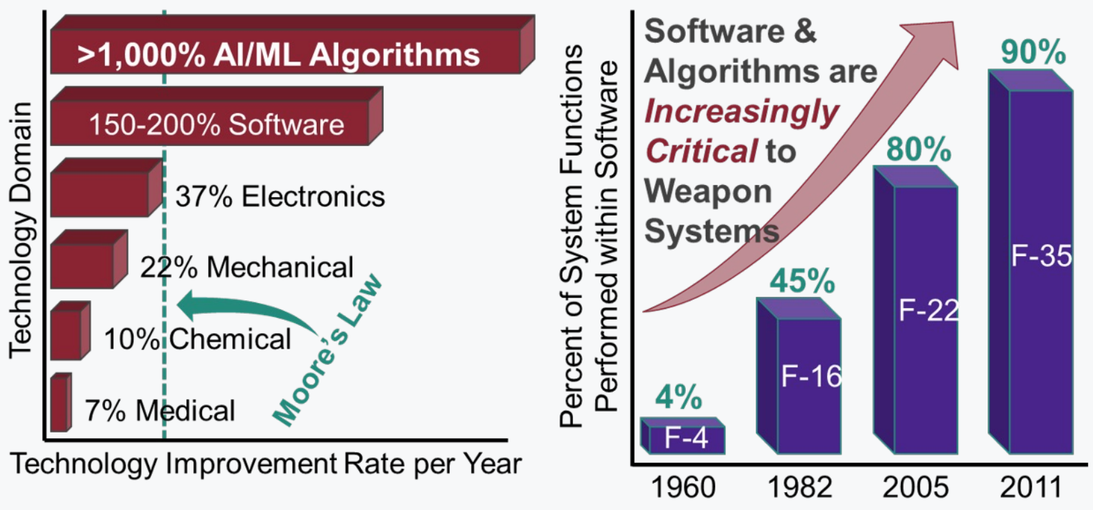


GOALS & OBJECTIVES

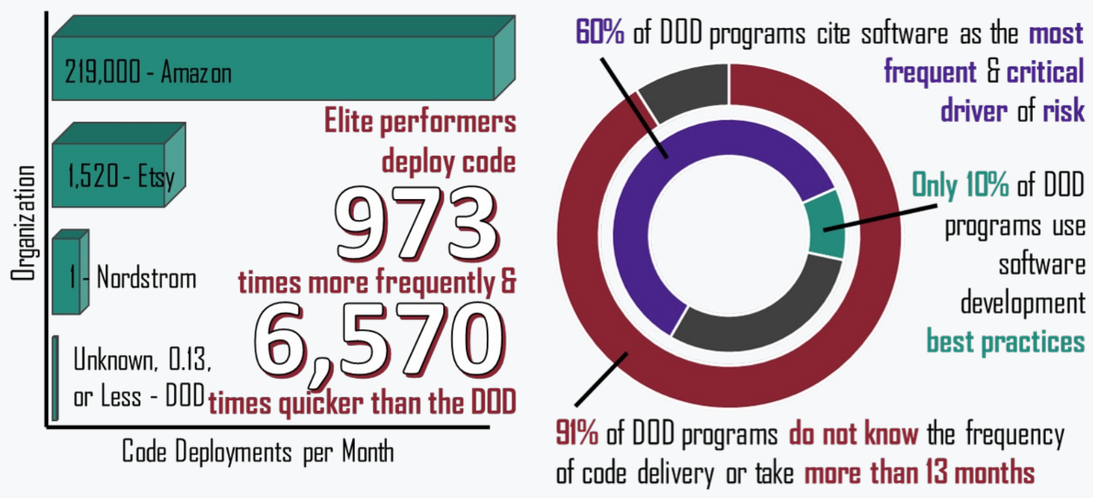
Develop a **holistic** theoretical framework to successfully enable DOD AI/ML solutions at every phase of their lifecycle.

- Develop DOD **acquisition guidelines** to address management, contracting and resourcing **shortcomings** of AI/ML solutions
- Develop a **flexible** and **scalable** AI/ML delivery platform architecture along with **legacy platform** integration and modernization methods
- Create **reusable** artifacts for **model training** and **architecture discovery**

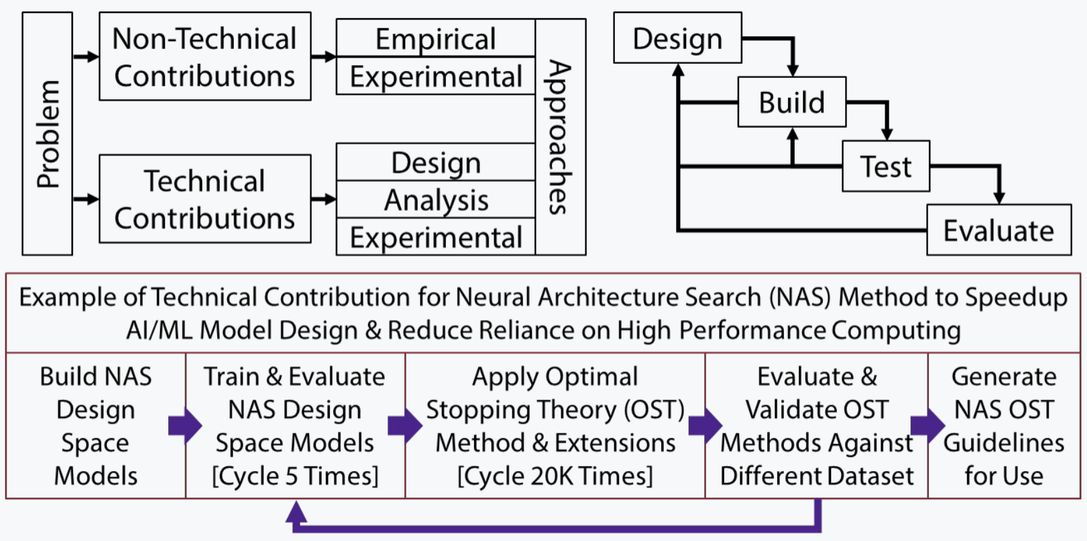
AI/ML is ***rapidly evolving*** and ***actively transforming*** the battlespace



To be ***great*** at AI/ML, an organization must first be ***fluent in modern software practices***



METHODOLOGY



Example of Technical Contribution for Neural Architecture Search (NAS) Method to Speedup AI/ML Model Design & Reduce Reliance on High Performance Computing

Build NAS Design Space Models	Train & Evaluate NAS Design Space Models [Cycle 5 Times]	Apply Optimal Stopping Theory (OST) Method & Extensions [Cycle 20K Times]	Evaluate & Validate OST Methods Against Different Dataset	Generate NAS OST Guidelines for Use

FUTURE RESEARCH

Future directions for this work include: automated AI/ML system security exploit detection, multiplatform resource optimization and coordination, and autonomous legacy platform AI/ML integration.

CONTACTS & REFERENCES

mmsheeha@nps.edu & oayakime@nps.edu

Due to space limitations, please contact for references (>150).

SYSTEMS ENGINEERING RESEARCH CENTER

SERC DOCTORAL STUDENT FORUM 2022
NOVEMBER 17