Trusted Artificial Intelligence:

An Embedded Systems Security SCALE Effort to Develop Technologies and People

Dr. Nathaniel Husted, NSWC Crane Chief Scientist for Cyber and Electromagnetic Warfare Technologies

Sea Air Space 2022 (APR 4-6 2022)

NAVSEA
WARFARE CENTERS
CRANE

CAPT Duncan McKay, USN
Commanding Officer NSWC Crane

Dr. Angie Lewis, SES
Technical Director NSWC Crane

NAVSEA
WARFARE CENTERS
CRANE

BLUF

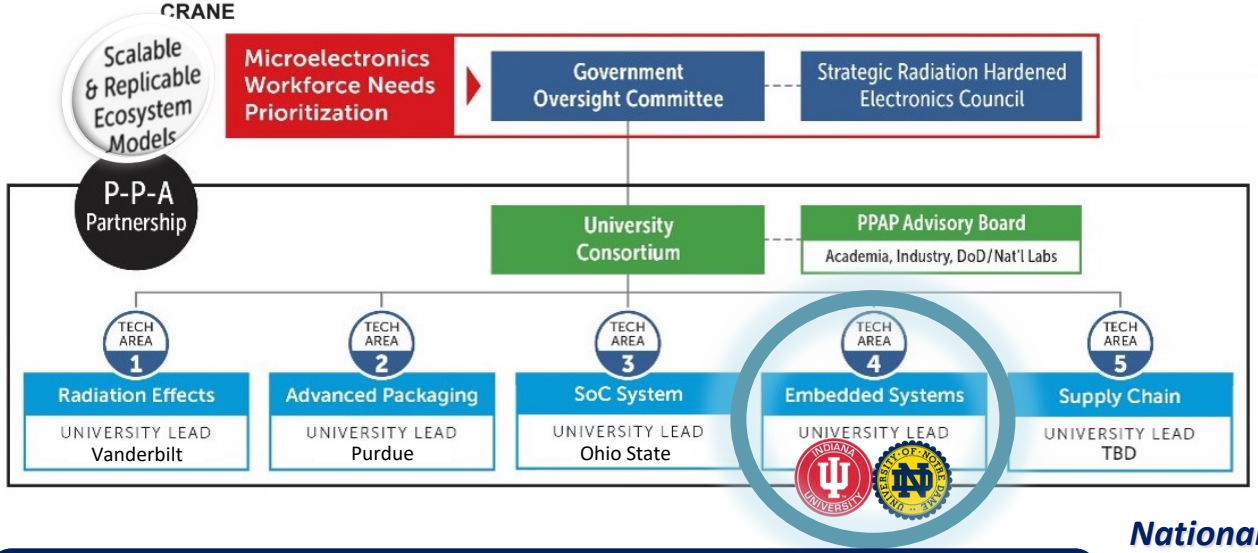
- OUSD(R&E) Trusted & Assured Microelectronics (T&AM) program launched the Embedded Systems Security/Trusted AI Vertical of their SCALE (Scalable Asymmetric Lifecycle Engagement) Workforce Development (WFD) program June 2021.
  - Focuses on the operational T&E of AI to expedite the deployment of AI solutions; development of both technologies and talent
  - Enabled by a $5M Congressional Add
  - Indiana University and the University of Notre Dame are the University Technical Leads
  - Purdue University is the SCALE Consortium Manager

- SCALE is a public-private-academic (PPA) model for workforce development
  - Technologies *and* people are developed and transitioned in parallel
  - There are university technical leads that coordinate activities across a larger consortium of university partners
  - Model is designed to be scaled to other university partners as needed (***the number of university consortium members is expected to grow***)

- NSWC Crane is serving as the technical lead for this effort

Trusted AI Vertical/Embedded Systems:
Scalable Asymmetric Lifecycle Engagement (SCALE)

NAVSEA WARFARE CENTERS
CRANE



SCALE Transitions Workforce *and* Technologies into the DoD/DIB

Workforce and Technical Capabilities:

- ***DoD Microelectronics Roadmap:*** **Education and Workforce Development**
- ***2018 NDS: Build a More Lethal Force – Cultivate Workforce Talent* (PME, Talent management, Civilian workforce expertise)**
- ***National Security Commission for Artificial Intelligence Interim Report, 1st & 3rd Quarter Recommendations 2020***
- ***National Defense Authorization Act (NDAA) 2020*, Section 224 – Defense microelectronics products and services must meet trusted supply chain and operational security standards**

FY-21

- Develop the Trusted AI Consortium and the SCALE Public Private Academic Partnership (PPAP) Model
- Co-develop the research themes required to assess the level of trust in artificial intelligence/machine learning (AI/ML)-enabled systems

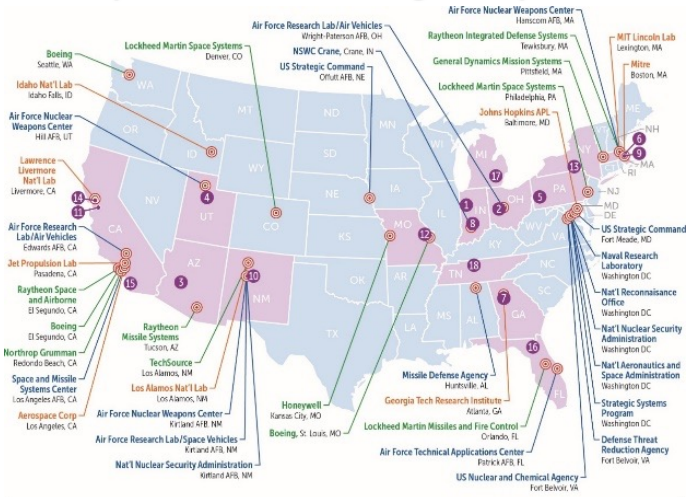
FY-21 and FY-22

- Co-develop research projects that will provide the tools, methodologies, and frameworks to assure AI
- US-citizen student recruitment; DoD oversight of projects and student engagement

FY-22 and Beyond

- Grow university, GOV, and DIB members
- Transition frameworks, methodologies, tools, and people to assess the trustworthiness of AI/ML-integrated systems

Nationally Coordinated & Regionally Executed

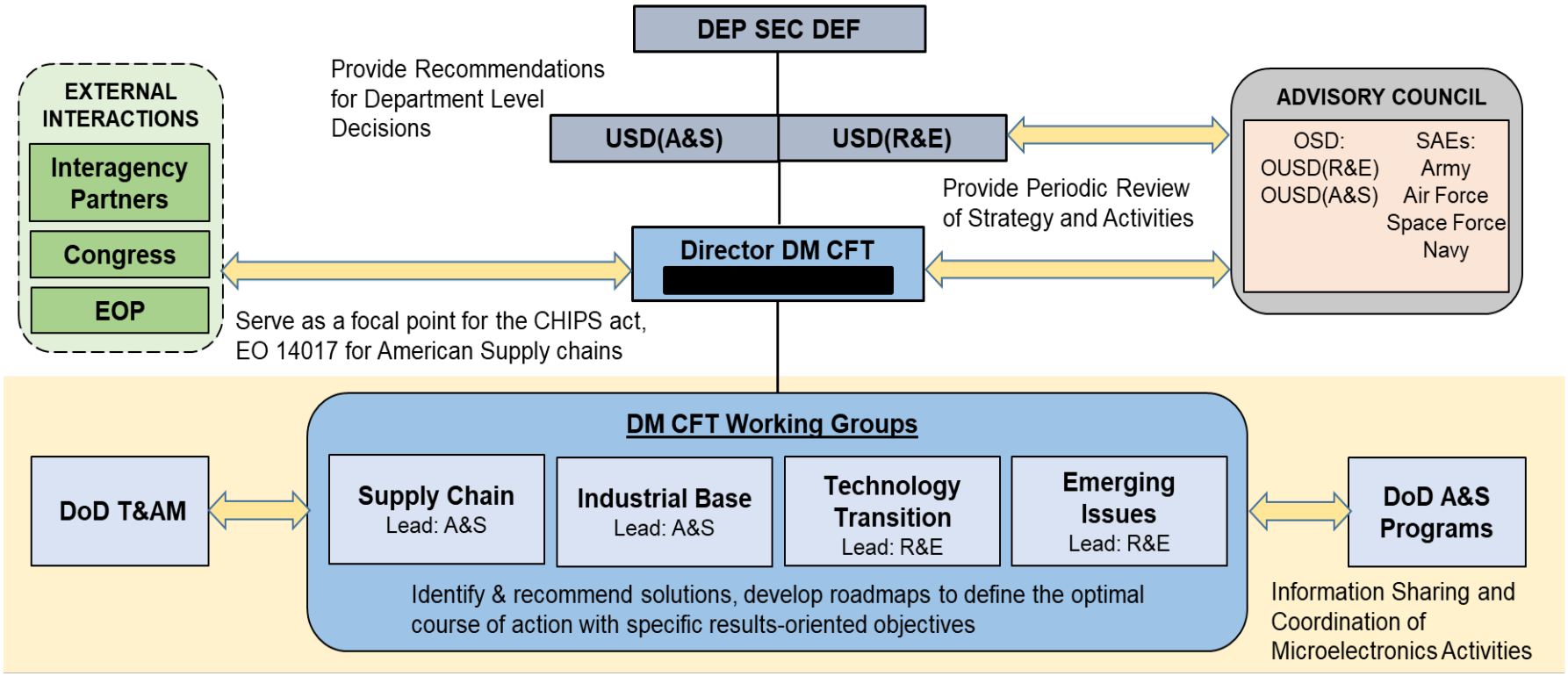


For a full list of partners, see: https://www.purdue.edu/discoverypark/scale/

NSWC Crane Technical Lead Role

Future Opportunities
DMCFT Microelectronics Workforce

DoD Microelectronics Cross Functional Team



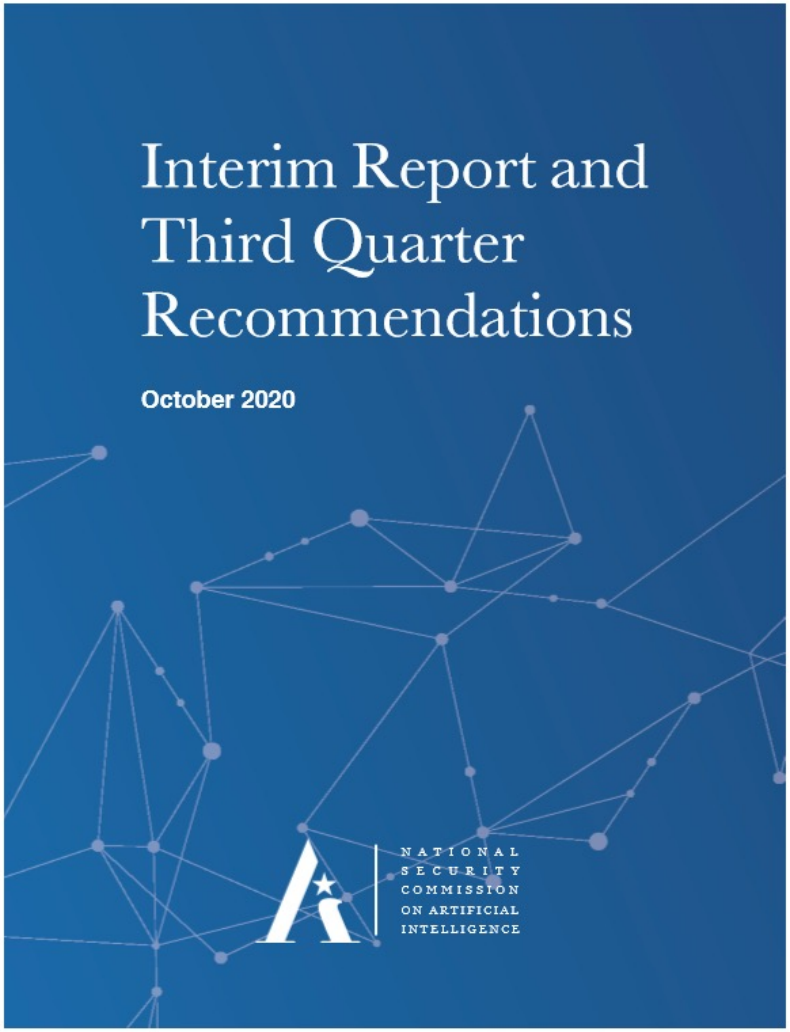
$612M Workforce Development Issue
POM-23 Request:
$122.4M FY23-FY27 to address Embedded Systems Security/Trusted AI

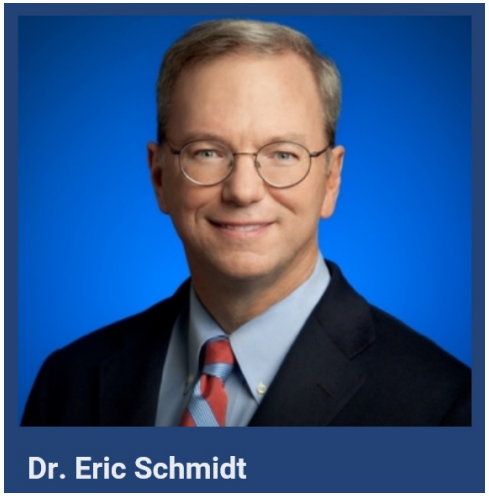
ORGANIZATIONS

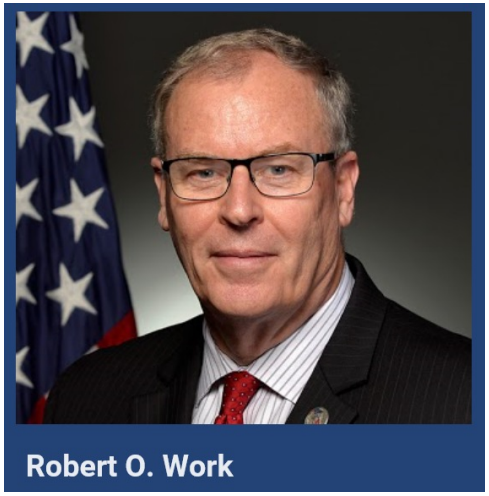
OUSD(A&S) – Office of Undersecretary of Defense for Acquisition and DoD Sustainment
OUSD(R&E) – Office of Undersecretary of Defense for Research & Engineering
EOP – Executive Office of the President
DoD T&AM – Trusted & Assured Microelectronics Program
SAEs – Service Acquisition Executives

NAVSEA
WARFARE CENTERS
CRANE

NSCAI 3rd Quarter Recommendations
October 2020




Dr. Eric Schmidt
Chairman


Robert O. Work
Vice Chairman

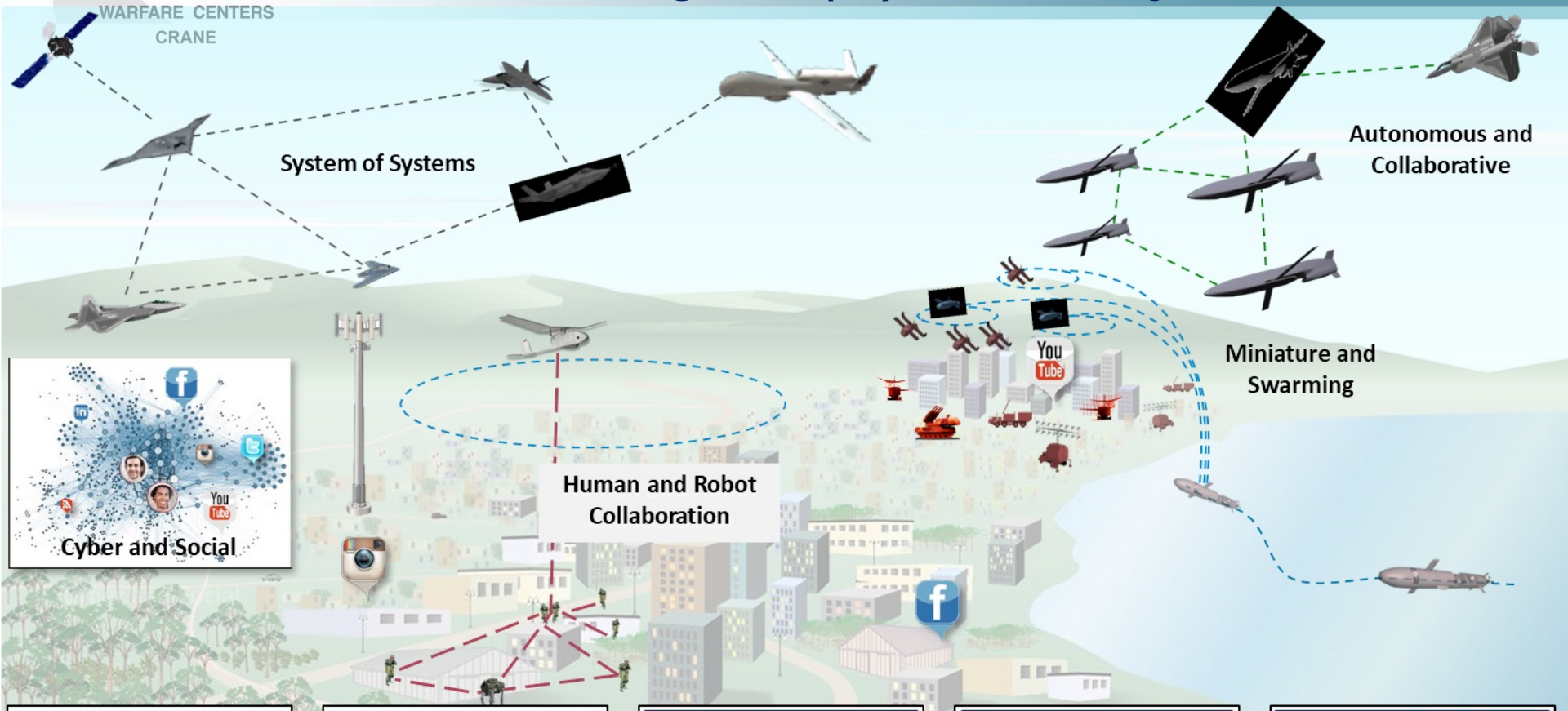
Recommendations for the Microelectronics Workforce Prototype, SCALE

"At minimum, **$24.7 million per year** over the next decade of additional funds are needed to address ***each*** critical technical area - $122.36 million per year over the next decade of additional funds are needed to initiate a parallel AI-specific consortium…"

The Future Battlespace

Artificial Intelligence (AI)-Enabled Systems Needs

NAVSEA WARFARE CENTERS CRANE



Big Data and AI Systems

Artificial Intelligence (AI) and Graph Processors

- 100B-1T node graphs
- Need 1000x performance and efficiency for real-time

Decentralized Systems

Open and Distributed Architecture & Processing

- Local processing raw data
- Rapid tech. insertion & upgrades using SotA

Human and Robot Systems

Vision, Semantic and Navigation Processing

- High performance imagers & local processing circuits
- Robust Navigation & local semantic processing

Diverse Protected Links

Frequency and Antenna Diversity Signal Proc.

- Multi-antenna & frequencies
- Adaptive processing (Trillion Ops/sec/watt) for robust comm. & radar systems

Global Tech and Infrastructure

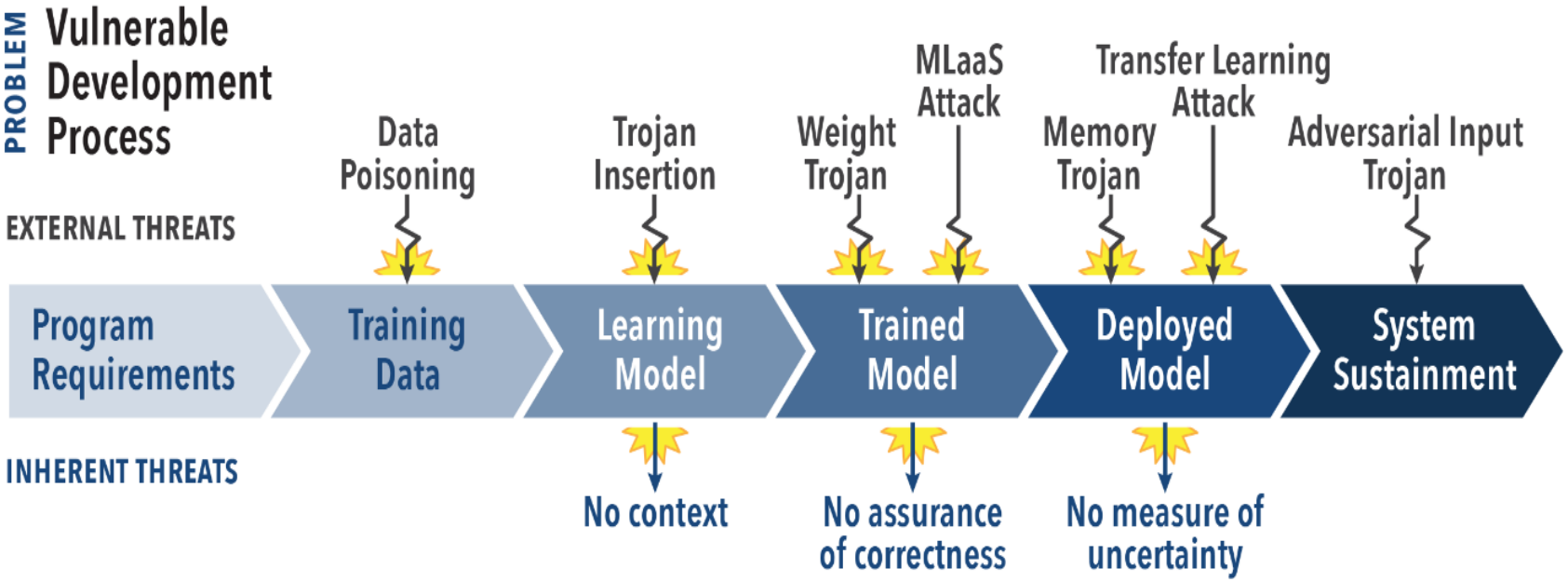
Leverage & Assure Access to the best Technology

- Use best global tech where it exists
- Assure domestic sources for state-of-art

NAVSEA
WARFARE CENTERS
CRANE

Trusted AI Overview

There is a critical gap in understanding risk and defending against attacks that can occur in the development and deployment of an AI system, even if the hardware and software works flawlessly.

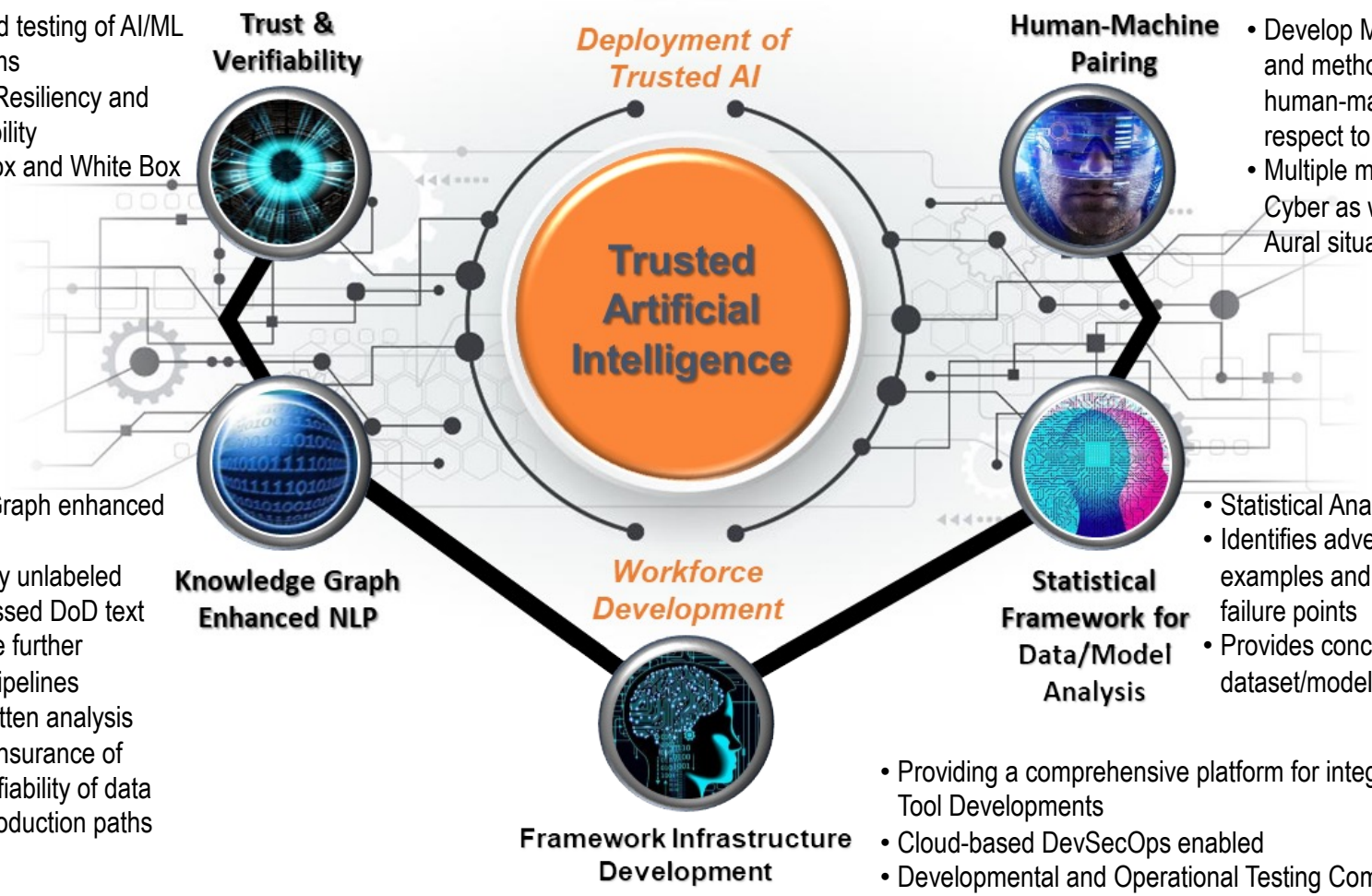


When warfighters' lives depend on AI, trust is not optional

NAVSEA
WARFARE CENTERS
CRANE

Overview: Trusted AI Research Themes

AI-enabled systems must be trusted in order to expedite the deployment of trusted AI solutions test capabilities & people must be developed to assess the trustworthiness of these systems



- Improved testing of AI/ML algorithms
- Testing Resiliency and Survivability
- Black Box and White Box Support

- Develop Measures, metrics, and methods to assess human-machine pairing with respect to decision making
- Multiple modalities including Cyber as well as Visual and Aural situational awareness

- Knowledge Graph enhanced NLP
- Take relatively unlabeled and unprocessed DoD text data to create further information pipelines
- Automate written analysis and provide insurance of trust and verifiability of data in other AI production paths

- Statistical Analysis Toolkit
- Identifies adversarial examples and neural network failure points
- Provides concrete metrics for dataset/model robustness

- Providing a comprehensive platform for integrating Trusted AI Tool Developments
- Cloud-based DevSecOps enabled
- Developmental and Operational Testing Communities focused

Trusted AI Status

NAVSEA WARFARE CENTERS CRANE

Dec 20

$5M Congressional Add OUSD/RE/T&AM SCALE program

Jan 21

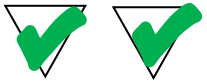
Assemble the NSWC Crane team, TPOCs and Sr. Advisors; TPOCs supported ¼ FTE from T&AM

Feb 21

Topic Development Meeting; NSWC Crane TPOCs and IU/ND PIs

Feb-Mar 21

SOW Refinement: TPOCs and IU/ND PIs



Mar 21

1) AWARD: SCALE/ESS/ Trusted AI awarded to consortium manager via the Cornerstone OTA
2) NSWC Crane approved IU/ND SOWs enabling Purdue to proceed with sub-awards

Mar 21

June 21

Kickoff; Keynotes: Mr. Thom Kinney, USSOCOM Chief Data Officer and Dr. José-Marie Griffiths, NSCAI Commissioner

June 21

1) AWARD: NSWC Crane PIA partner NTI for "Strengthening the Public-Private-Academic Partnership through the Indy Autonomous Challenge"
2) NTI PIA kick-off

June-Sept 21

TPOC oversight and insight, including monthly status report reviews and participation in group meetings

Current

Oct 21-June 22

Continued TPOC oversight/insight, including engagements with the PIs and students and monthly status report review

Dec 21

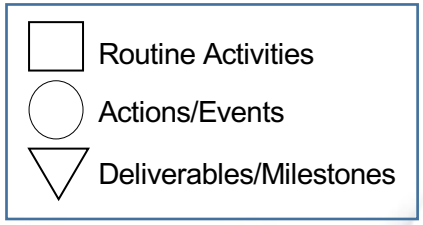
TPOC support of Technical Execution Review

Feb 22

Stakeholder Discovery Meeting; hosted by NSWC Crane and the Midwest Tech Bridge

Jun 22

TPOC support of the final Technical Execution Area Review



NAVSEA
WARFARE CENTERS
CRANE

FY-21, FY-22, & Future Direction

FY-21

- Develop the Trusted AI Consortium and Public Private Academic Partnership (PPAP) Model
- Co-develop the research thrusts required to assess the level of trust in artificial intelligence/machine learning (AI/ML)-enabled systems

FY-21 and FY-22

- Co-develop research projects that will provide the tools, methodologies, and frameworks to assure AI:
  - Develop tools, techniques, and procedures to measure human trust of AI/ML algorithms linked with the trustworthiness of the AI/ML system to help inform stakeholders about the levels of trust across the developmental process
  - Develop methods to reduce data source bias and create modularity
  - Develop a cybersecurity and risk model to ensure AI/ML algorithms maintain robustness in situations where a given set of sensors used to train the system are no longer used in the system
  - Develop ways to measure success of a system during the full lifecycle
- US-citizen student recruitment and training
- DoD oversight of projects and student engagement
- Transition frameworks, methodologies, and tools to assess the trustworthiness of AI/ML-integrated systems

- Position NSWC Crane as a resource for IV&V assessment of AI/ML-enabled systems
- Customer supported refinement of existing assessment tools and frameworks and development of new methods as AI technology evolves
- Continue to develop and transition the Trusted AI workforce