The Software Engineering Institute

27 SEP 2023

Carnegie Mellon University
Software Engineering Institute

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0981

CMU SEI is a DoD R&D federally funded research and development center

Established in 1984 at Carnegie Mellon University

Charged to improve the state of the practice of software engineering and cybersecurity

Added AI engineering in 2018

Collaborates with CMU and broadly in academia, government, and industry

Capable of conducting both fundamental research and classified work

~620 staff members

FY23 total funding ~$145M

Offices in Pittsburgh and Arlington, VA

Only DoD FFRDC focused on software

Carnegie Mellon University
Software Engineering Institute

Carnegie Mellon University
Software Engineering Institute

Our Vision

We are shaping the future of software for a better world.

Our Mission

We establish and advance software as a strategic advantage for national security.

We lead and direct research and the transition of software engineering and related disciplines at the intersection of academia, industry, and government.

Our leadership

Paul D. Nielsen
Director and CEO

David Thompson
Deputy Director
and COO

Thomas Longstaff
CTO

Matthew E. Gaston
Director
Artificial Intelligence Division

Anita Carleton
Director
Software Solutions Division

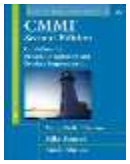
Greg Touhill
Director
CERT Division

Mary Catherine Ward
Chief Strategy Officer

Heidi Magnelia
Chief Financial Officer

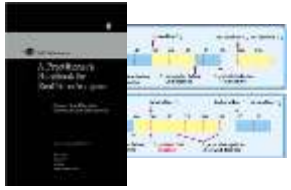
Sandra Noonan
General Counsel

Our Legacy: Over 35 years in software engineering leadership



Repeatable delivery of platforms

Mid-1980s



Verification and validation of real-time scheduling

Early 1990s

Strategic design; reuse and evolution; measurement and analysis

Late 1990s

Ultra-large-scale systems research; AADL

Mid 2000s

Adopting iterative development and acquisition practices

2010s

AI engineering; engineering for AI; AI for mission

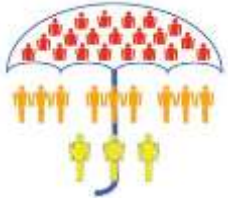
2030+

Late 1980s

Establishing a basis for software reuse

Mid 1990s

Evidence-based developer output



Early 2000s

Managing the operational risk of fielded systems

Late 2000s

SOA; secure design patterns; framework for architectural decisions

Today

Lifecycle automation, Agile/DevOps; assuring complex systems; continuous integration/continuous deployment

Our expertise: Assure secure, affordable, rapidly delivered, and innovative software

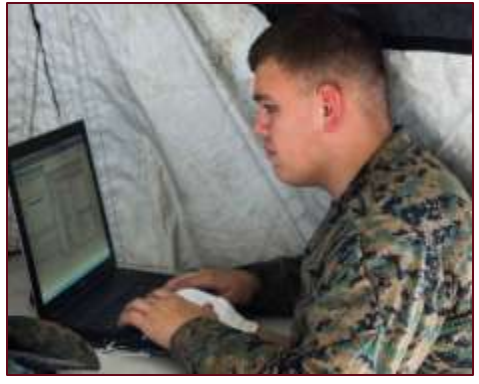
Carnegie Mellon University Software Engineering Institute

Bring capabilities that make new missions possible or improve the likelihood that existing ones will succeed

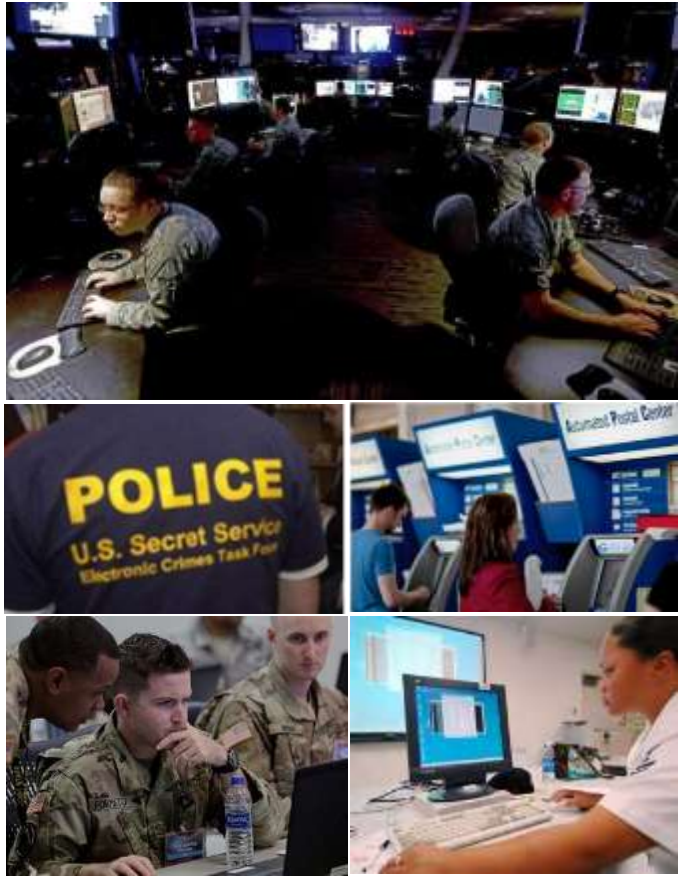
Be trustworthy in construction, correct in implementation, and resilient in the face of operational uncertainties

Be timely so that the cadence of fielding responds to and anticipates the operational tempo of the warfighter

Be affordable such that the cost of acquisition and operations, despite increased capability, is reduced and predictable



Our stakeholders



Major government customers

- U.S. DoD
- U.S. DHS

Researchers, developers, users, and acquirers—government, defense industrial base, commercial, and academic

Key industries and organizations with the potential to advance software engineering and related disciplines

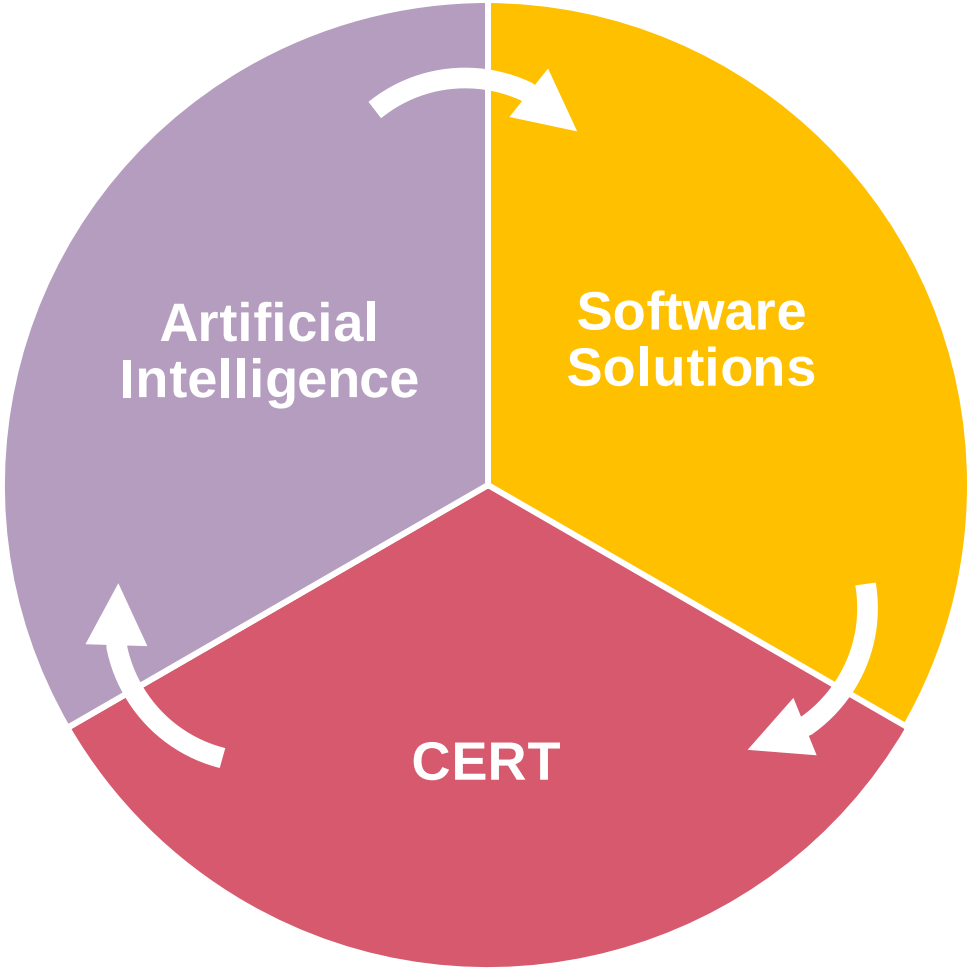
We pursue ways to integrate software, cyber, and AI

The SEI envisions the confluence of advances in model-based engineering, AI engineering, cyber engineering, and software engineering for a more automated lifecycle.

As the SEI adapts, it continues to pursue software as a strategic advantage for the DoD (capable, timely, trustworthy, and enduring).

Further ahead, the SEI will continue to look beyond existing DoD requirements to anticipate where software can be a strategic advantage.

Collaborative technical divisions



Software Solutions Division: Rapidly deploy software innovations with confidence in DoD

CERT Division: Ensure U.S. cyber dominance and resilience

AI Division: Engineer AI systems for mission-practical capabilities

Software engineering strategy:
Rapidly Deploying Software Innovations with Confidence in DoD

Engineering Intelligent Software Systems	• Software architecture • AI-augmented software engineering • Technical debt
Enabling Mission Capability at Scale	• AI-enabled software analysis • Software resiliency • Software modernization at scale
Assuring Cyber-Physical Systems	• Model-based software engineering • Virtual integration • Automated software assurance practices
Transforming Software Acquisition Policy & Practice	• Operational test & evaluation • Software acquisition pathways • Automated software measurement
Continuous Deployment of Capability	• Agile methods • DevSecOps • Software tool chains
Architecting the Future of Software Engineering	• Advanced development paradigms • Advanced architectural paradigms

Software solutions: Army engagements for DevOps

Carnegie Mellon University Software Engineering Institute

Army Futures Command (Ai2C)

- Providing DevOps software engineering expertise to develop an architecture for a cloud-based pipeline that includes ML.
- Working with DoD IronBank to create, harden, and adjudicate containers with ML to be used by their system.

INSCOM

- Providing DevSecOps adaptations for the development and operational testing community.

CERT Division

Leader in Cybersecurity

	Advance Cyber by Design	**Identify and counter threats**	• Insider threat • Reverse engineering for malware analysis • Security vulnerabilities • System and platform evaluation
	Enhance Cyber Resilience	**Engineer for cyber resilience**	• Autonomy security and resilience • Situational awareness
		Measure risk and optimize cybersecurity investment	• Enterprise risk and resilience management
	Move the Market	**Cultivate essential skills and abilities**	• Cybersecurity center development • Cyber mission readiness
	Shape the Future	**Apply research for rapid capability transition**	• Cybersecurity engineering • Secure development

CERT: Army NETCOM Gaining Cyber Dominance Exercise

Carnegie Mellon University Software Engineering Institute

Mission rehearsals for teams on today's front lines of global cyber defenses
Impact: cyber exercise experience – better prepared teams – technical and leadership

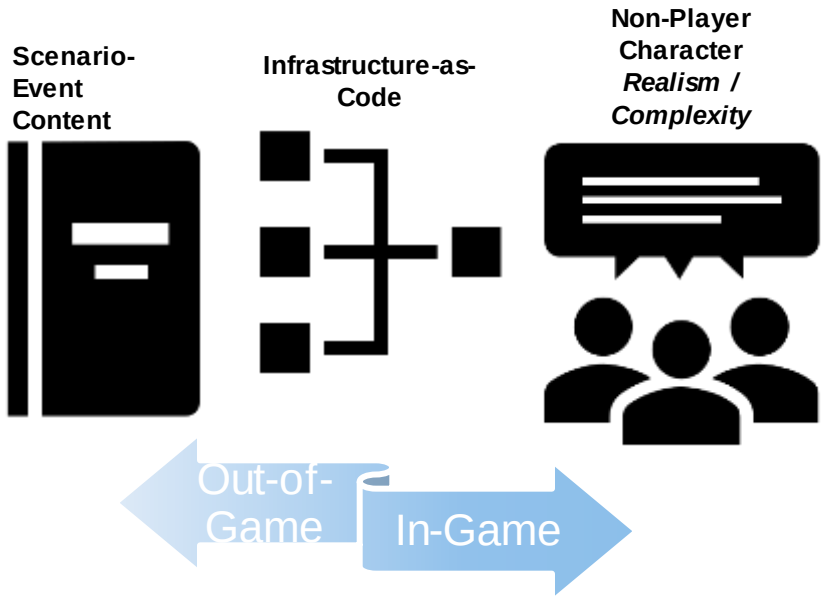
2023

20 Army Regional Cyber Center (RCC) Exercises
- Five teams
  - Arizona, Germany, Kuwait, Korea, Hawaii
- Three 4-hour training exercises for each
- One 8-hour certification exercise for each
  - Regional Cyber Center of the Year

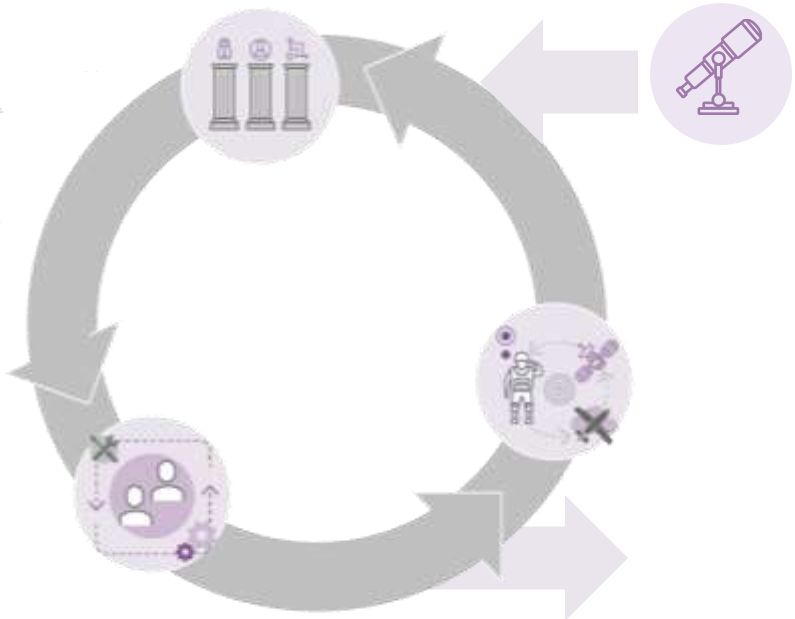
40 Army Cyber Protection Team (CPT) Exercises
- 19 threat-hunting teams – out of Augusta, GA
- Duration: 5 days each

Impacts of cyber-team exercising
- **Technical "stick time"**
- **Team building**
- **Cyber data science – analytic testbed**

AI Research



Today's AI applications, tomorrow's AI discipline



Scalable, robust, and responsible AI systems for mission outcomes

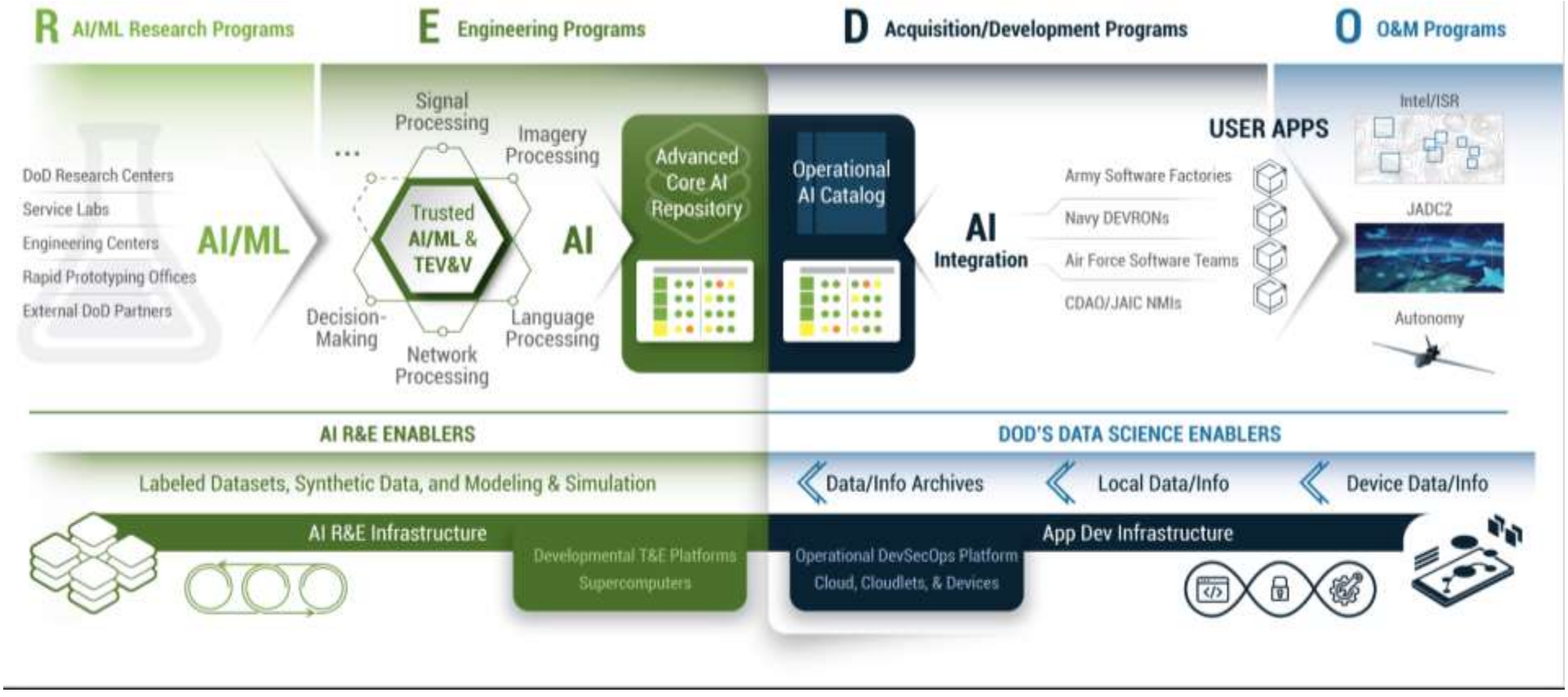
AI ENGINEERING
Research and define the processes, practices, and tools to support operationalizing robust, secure, scalable, and human-centered AI systems.

AI FOR MISSION
Build real-world, mission-scale AI capabilities

DIGITAL TRANSFORMATION
Prepare our customers to be ready for the unique challenges of adopting, deploying, using, and maintaining AI capabilities

EMERGING TECHNOLOGY
Identify and investigate emerging AI and AI-adjacent technologies that are rapidly transforming the technology landscape

AID: DoD's AI workforce and REDO pipeline



We are an integrated part of CMU

Carnegie Mellon University Software Engineering Institute

By design, we are operated by Carnegie Mellon University, which uniquely enables an S&T FFRDC to bring the power of CMU to the table to solve some of the DoD's most challenging problems.