

SEI Overview – Part 1

Mark Sherman
Technical Director, SEI

JULY 19, 2023

Copyright 2023 Carnegie Mellon University.

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.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM23-0697

Carnegie Mellon University (CMU)

Pioneering discoveries on a global scale



- Leading-edge research global university turning disruptive ideas into successes
- 2022-2023 *U.S. News and World Report* rankings:
 - #1 in artificial intelligence, computer engineering, cybersecurity, management information systems, mobile/web applications, programming languages, software engineering, and quantitative analysis
 - #1 in overall computer science
- Creating inspired and inventive solutions through sponsored research, faculty and student engagement, executive education, licensing and tech transfer, start ups, and colocation

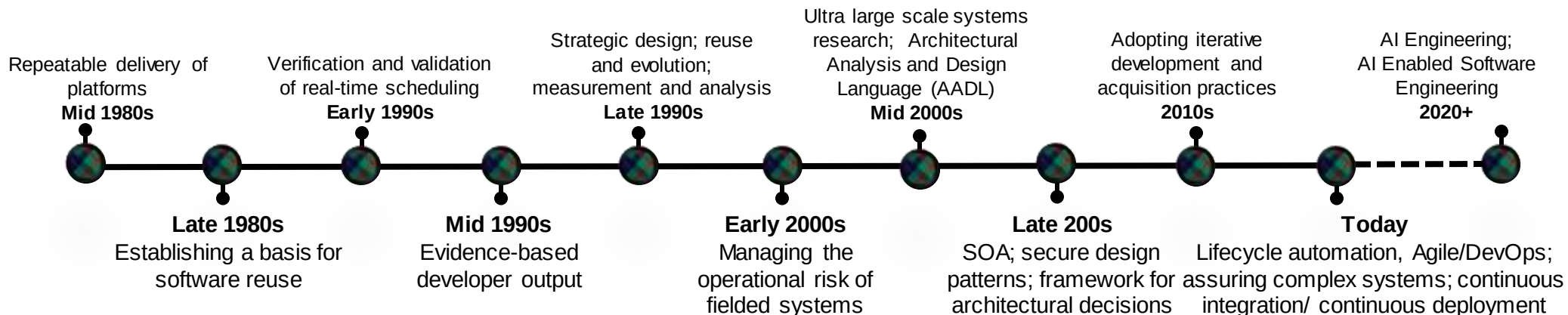
CMU Software Engineering Institute (SEI)

Bringing innovation to the U.S. Government

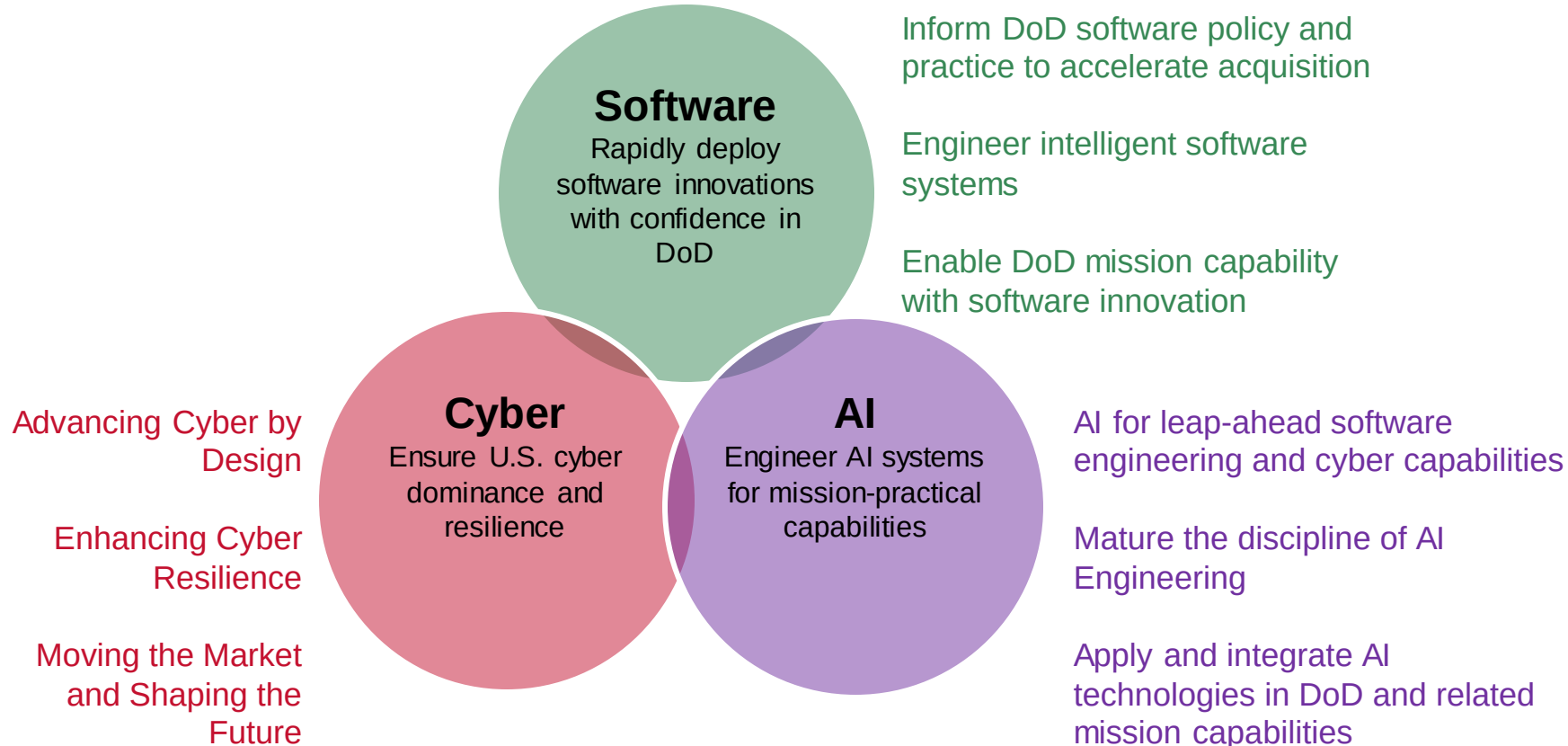


- Federally Funded Research and Development Center (FFRDC) chartered in 1984 and sponsored by the DoD
- Leader in researching complex software engineering, cyber security, and artificial intelligence (AI) engineering solutions
- Critical to the U.S. Government's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

CMU SEI: 35+ years of Software Engineering Leadership



Our technical research connects software, AI, and cyber strategies for **maximum** impact



SSD Division

Software research for a predictable tomorrow

SSD Division Focus Areas – 1

	Engineering Intelligent Software Systems	Architecture Design, Analysis, & Automation	Applying AI to automate architecture design and analysis activities; applying and accelerating adoption of architecture practices
		Tactical and AI-enabled Systems	Developing software engineering principles and practices for tactical and AI-enabled systems; advanced prototyping of the application of principles and practices
	Enabling Mission Capability at Scale	Systems and Software Development & Analysis	Scaling software development and deployment through AI/ML and automation for large, complex, real-time mission systems
		Resilient Critical Software Systems	Leveraging threat information and real-time software techniques to drive resilient solutions for mission critical embedded systems
		Advanced Deterrents	Contribute to the development of America's new 21st century deterrent platforms and weapons which will serve as the backbone of our nation's national security
	Assuring Cyber-Physical Systems	Formal Verification of Cyber-Physical Systems	Rapid and scalable automatic verification of cyber-physical systems built from verified and unverified components, ensuring outputs with the right value, at the right time, and with the right physical reaction (e.g., stop a crash)
		Model-Based Software Engineering	Virtual integration to discover flaws before implementation

SSD Division Focus Areas – 2

	Transforming Software Acquisition Policy and Practice	Software Acquisition Pathways	Assembling modern software acquisition/development approaches to inform policy and practice
		Software Engineering Measurement & Analysis	Data analytics to drive software acquisition policy and priorities
	Continuous Deployment of Capability	Agile Transformation	Modernizing software development and acquisition with Agile methods
		DevSecOps Innovations	Engineering for automated secure deployment and operations pipeline



Study available online at
<https://www.sei.cmu.edu/go/national-agenda>

Focus of National Agenda for Software Engineering

Software is vital to America's **global competitiveness**, **innovation**, and **national security**.

The economy, the nation's infrastructure, education, and healthcare all depend on software.

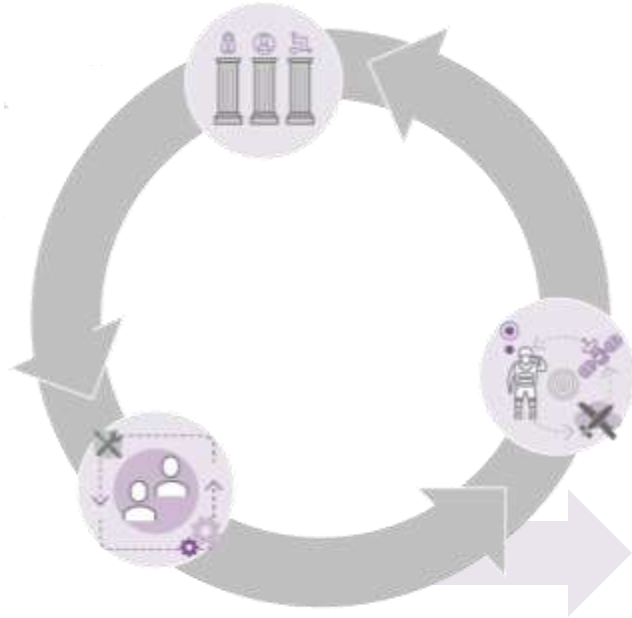
Lead a community effort to:

- **Identify future challenges** in engineering software-reliant systems.
- Develop a **research roadmap** that will drive advances in **foundational software engineering principles** across system types such as intelligent, autonomous, safety-critical, and data intensive systems.
- Raise the **visibility** of software to the point where it receives sustained recognition commensurate with its importance to national security and competitiveness.
- Enable strategic partnerships and collaborations to **drive innovation among industry, academia, and government**.

AI Division

Artificial Intelligence research for a reliable,
responsible, safe, fair, and transparent tomorrow

AI Division Focus Areas



Scalable, robust, and
responsible AI systems
for mission 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

AI Engineering

	Scalable AI Accommodate the size, speed, and complexity of mission needs	• Scalable management of data and models • Enterprise scalability of AI development and deployment • Scalable algorithms and infrastructure
	Robust and Secure AI Operate reliably when faced with uncertainty or threat	• Robustness of AI components and systems • Designing for security challenges in modern AI systems • Testing, evaluating, and analyzing AI systems
	Human-Centered AI Designed with the goal of working with, and for, people	• Understand context of use, sense changes over time • Scope and facilitate human-machine teaming • Methods, mechanisms, and mindsets for critical oversight

CERT Division

Cyber research for a secure tomorrow

CERT Division – Birthplace of Cyber Research



1988

Computer Emergency Response Team formed in response to the Morris Worm

2022

Cybersecurity Engineering and Resilience Team conducting collaborative and innovative evidence-based research to fortify the cyber ecosystem and protect national security and prosperity

Trusted

Conducting research for the U.S. Government in a non-profit, public-private partnership

Valued

Innovating solutions with a global collaboration of military, industry, and academia

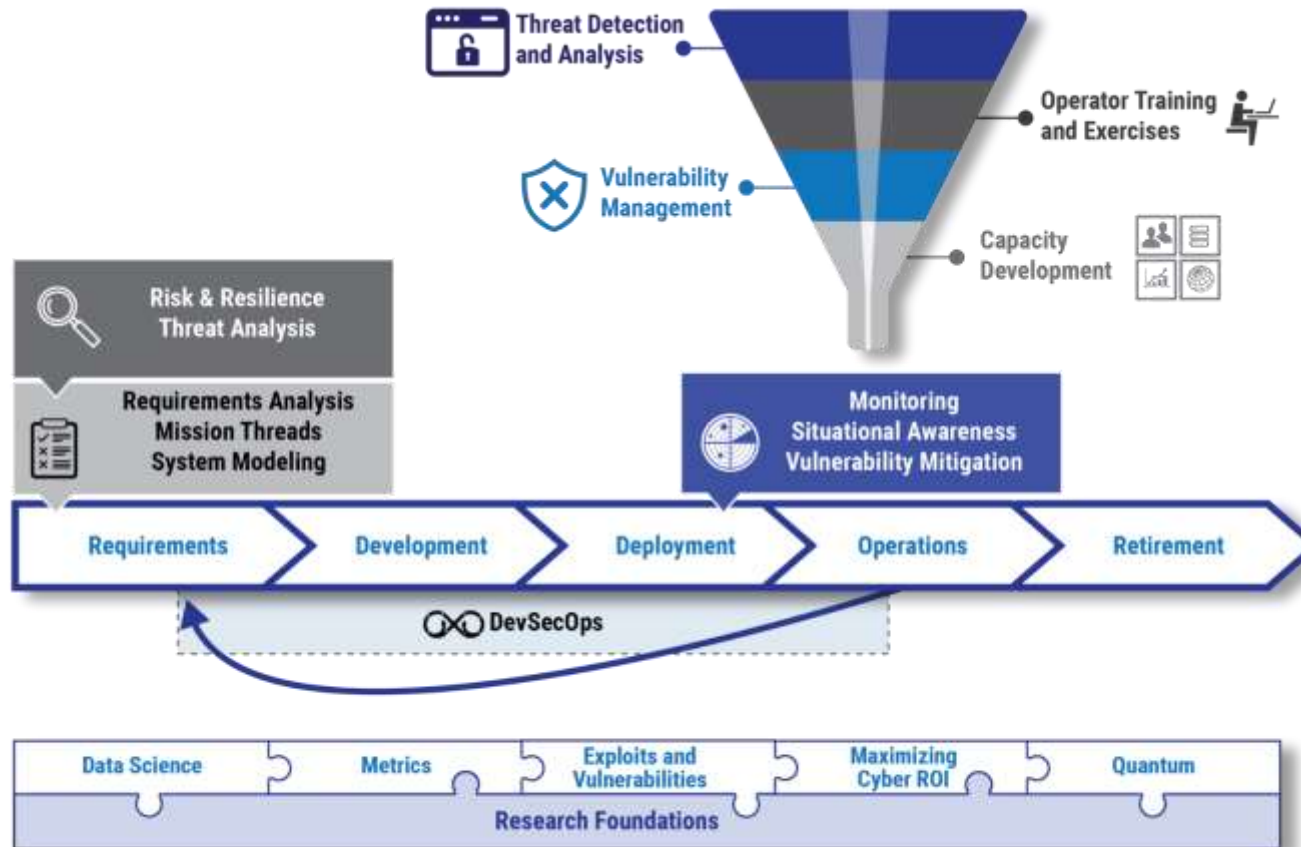
Relevant

Achieving results for our mission partners

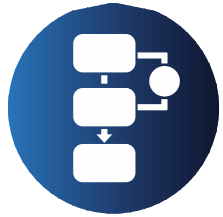
CERT Division Focus Areas

	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 • Cybersecurity for and by AI

Improving the Full Lifecycle



Identify and counter threats



super
mediator



YAF

Scalable network analysis

- Large scale network collection
- Data exploration in large scale data
- Cloud and on-prem

Network and security architecture and design

- Monitoring
- Protection and segmentation
- Host, cloud, network monitoring

Putting cyber into context for mission

Engineer for cyber resilience

Security Requirements Engineering

System Modeling and Analysis

Mission Threads

Code security and cyber supply chain

- Binary analysis
- Software Bill of Materials (SBOM)

Architecture Analysis and Acquisition Guidance

- Zero trust

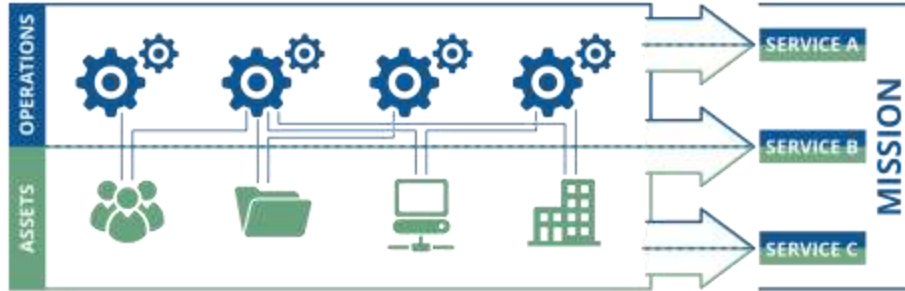
DevSecOps improvements

- Platform Independent Model – DevSecOps maturity
- Continuous Authorization to Operations (CATO)

Risk and resilience models and planning

 This image cannot currently be displayed.

Measure risk and optimize cybersecurity investment

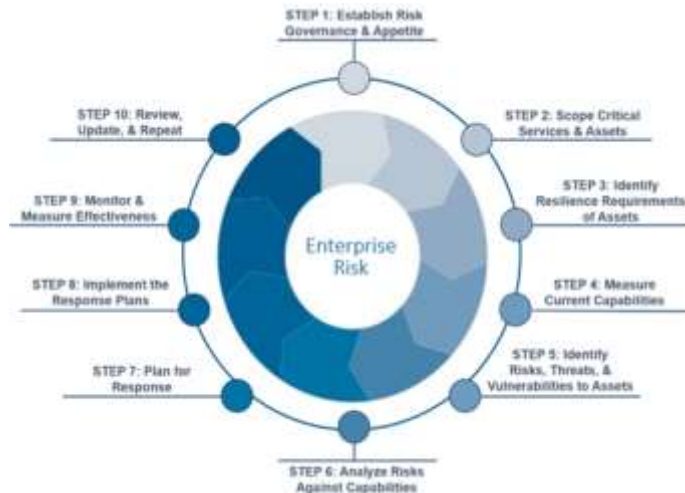


People: those who operate and monitor the service

Information: data associated with the service

Technology: tools and equipment that automate and support the service

Facilities: where the service is performed



Risk Quantification and Management

- Risk-informed cyber control selection and evaluation
- Econometrics of cybersecurity and return on cybersecurity investment
- Cybersecurity to resilience transformation

Resilience Diagnostics

- Adversary emulation and penetration testing
- Rigorous measurement of capabilities and benchmarking
- Cyber incident study and control analysis

Cultivate essential skills and abilities



SOC implementation

- Team construction
- Skill mapping
- Processes and workflows

Incident response

- Planning
- Processes and workflows

Mission Readiness

- Cyber exercises, simulations, testbeds
- Game-based training/competitions
- Adversarial tactics
- Disruptive technologies

Targeted platform understanding

- Theory of operation of platforms

Apply research for rapid capability transition



Data science

- AI for cyber
- Media manipulation
- AI Verification & Validation

Cyber metrics

Automated exploit discovery and vulnerability analysis

- Concolic execution
- SMT solvers

Maximizing cyber return on investment

Quantum information science

Example of SEI Work Products



Technical and Process-Driven Solutions



Training and Exercises



Analysis and Recommendations

Discover more about our research at sei.cmu.edu



Download [software and tools](#)
Participate in [education](#) offerings
Attend an [event](#)
Search the [digital library](#)
Read the [SEI Year in Review](#)
Explore our [research and capabilities](#)
[Collaborate](#) with the SEI on a new project

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Avenue
Pittsburgh, PA 15213
412-268-5800
info@sei.cmu.edu