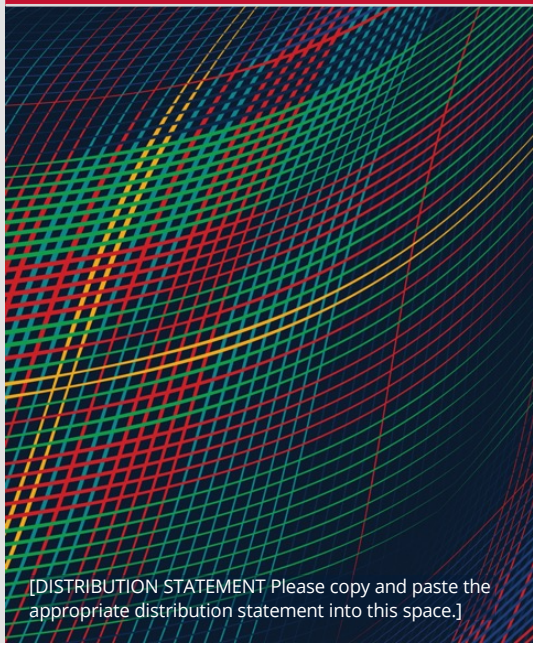
Advancing Cybersecurity: A Framework of Cybersecurity Research

AUGUST 24, 2026

Greg Touhill, CISSP, CISM, NACD.DC
Brigadier General, USAF (ret)
Director, CERT Division

© 2026 Carnegie Mellon University

Carnegie Mellon University
Software Engineering Institute



[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Document Markings

Carnegie Mellon University Software Engineering Institute

Replace the text on this slide with the markings generated by the form (and Controlled Information [CI] Handling, if needed) and update the distribution statement in the footer of each slide. (See slide 3 for instructions.) If you have a question about document markings, please contact the document marking team at DMARR-Team@sei.cmu.edu.

Release Review Document Markings

Please visit the Document Marking/Pre-Release Document Review SharePoint site and obtain the proper markings for this document.

Important: A notification that your markings have been validated does not mean that your document is approved for publication. You may need to complete extra steps to obtain RRO approval. Please follow the instructions in the automated messages you receive from the system.

The current DM Work Flow is here:
https://collaboration.sei.cmu.edu/forms/dm/FAQ/Document%20Marking%20Workflow.pdf

CI Handling Markings

If your slide presentation requires additional CI Handling markings (e.g., proprietary, confidential, for official use only, secret), place the details on this slide, and mark each slide as appropriate. Refer to https://wiki-int.sei.cmu.edu/confluence/display/ethics/Controlled+Information+Handling for more information.

DoD contract number FA8702-15-D-0002

© 2026 Carnegie Mellon University

Updating the Distribution Statement in the Footers

Carnegie Mellon University Software Engineering Institute

To update the distribution statement in the footers of your presentation, follow these steps:

1. Refer to the document markings to determine the distribution statement you'll need.
2. Copy the short version of the distribution statement provided by the document Marking System (e.g. [DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.].
   (See the table on the next slide for the short statements you can use. If you have questions, send email to DMARR-Team@sei.cmu.edu.)
3. Copy the appropriate short statement.
4. Access the slide masters by selecting View > Slide Master.
5. On the left side of your screen, select the first master slide at the top. (It is the bigger than the others)
6. Highlight the distribution statement listed on that slide, press CTRL-V to paste the short statement you copied in Step 3 making sure to select the *keep text only* option.
7. Repeat Step 6 for the Title Page master and Section Divider master.
8. Click Close Master View, and you're done!

© 2026 Carnegie Mellon University

Short Distribution Statements

Carnegie Mellon University Software Engineering Institute

Statement in Document Markings System	Short Statement You Can Use
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.	[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.
[INTERNAL SEI-USE ONLY] Further dissemination requires re-submittal through DM-RRO.	Internal SEI Distribution Only.

© 2026 Carnegie Mellon University

Agenda

Carnegie Mellon University Software Engineering Institute

- Our nano-second dilemma
- Analytic and operational tradecraft for cybersecurity
- Securing AI-based systems and workflows
- Cyber-physical system security
- Cybersecurity for complex integrated systems
- Insider threat and human-systems interaction
- Secure engineering and mission confidence
- Modeling and simulation in support of security
- Making applied research and development work for your mission

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Our Nano-Second Dilemma

Carnegie Mellon University Software Engineering Institute



Top: U.S. Army
Bottom: Skyler Wilson

- Our national security and national prosperity continue to rely on a safe, secure, and trustworthy digital environment.
- Cybersecurity is a risk management issue, not merely a technical challenge.
- Cyber engagements are considered an essential element of hybrid warfare.
- Today's cybersecurity capabilities were designed to thwart human-based threats.
- Rapid advancements in AI capabilities are overwhelming traditional defenses.
- Time is not our ally.

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Analytic and Operational Tradecraft for Cybersecurity

Carnegie Mellon University Software Engineering Institute



U.S. Air Force photo by Matthew McGovern

ANALYTIC TRADECRAFT: the tactics, techniques, and procedures (TTPs) of cybersecurity tradecraft to protect data and systems

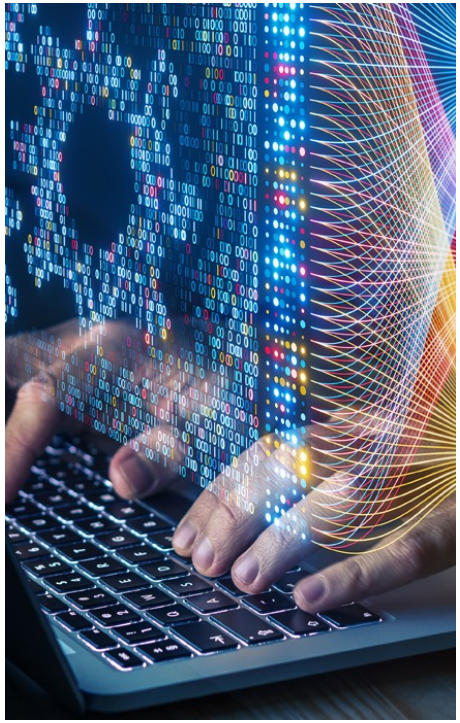
- Event analysis for networked and distributed systems
- Data retention and analysis
- Analysis of cyber adversary TTPs
- Reverse engineering and software understanding
- Secure system operations

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Analytic and Operational Tradecraft for Cybersecurity

Carnegie Mellon University Software Engineering Institute



Adobe Stock

OPERATIONAL TRADECRAFT: the advancement of capabilities that gain and maintain decisive cyber dominance in support of national security objectives

- Efficient and confident analysis and response
- TTPs for efficient and capable cyber red team operations
- Capacity to find and diagnose weaknesses and vulnerabilities
- Rapid creation and validation of software understanding
- Cyber hygiene for AI-based systems

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Securing AI-Based Systems and Workflows

Carnegie Mellon University Software Engineering Institute



Adobe Stock

THE CHALLENGE: conduct deliberate analyses of cybersecurity issues associated with AI to discover novel solutions that enhance AI mission readiness.

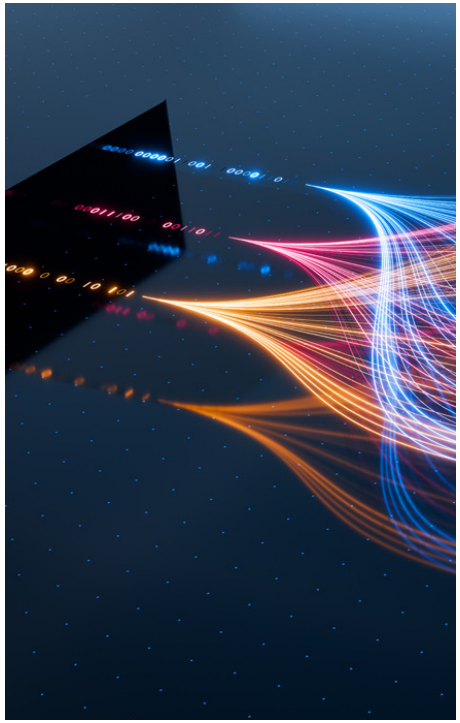
- Weaknesses and vulnerabilities for modern ML models
- Cybersecurity for AI-based systems and workflows
- Techniques to protect against attacks
- Red teaming for AI
- Special considerations for AI models trained with mission data
- Incident response for AI-based systems and workflows
- Mission engineering for AI-based systems and workflows

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Securing AI-Based Systems and Workflows

Carnegie Mellon University Software Engineering Institute



Adobe Stock

RESEARCH OPPORTUNITIES: develop a means to assure that aggressive AI-based systems concepts can be realized in ways that are acceptably secure without slowing the pace of mission-focused innovation.

- Mission-acceptable AI-based systems
- Security-focused test & evaluation, including red team operations
- Direct analytics for small-scale ML models
- Resilient and secure system architecture design patterns
- Relevant best practices and standards

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Cyber-Physical Security

Carnegie Mellon University Software Engineering Institute



Top: Mass Communication Specialist Seaman Apprentice Mark Bergado
Bottom: Adobe Stock

THE CHALLENGE: address cyber vulnerabilities in cyber-physical systems (CPS), often referred to as operational technology (OT), that are pervasive, span across all critical sectors, and are purpose-built, increasingly networked, and pivotal elements of military and critical infrastructure.

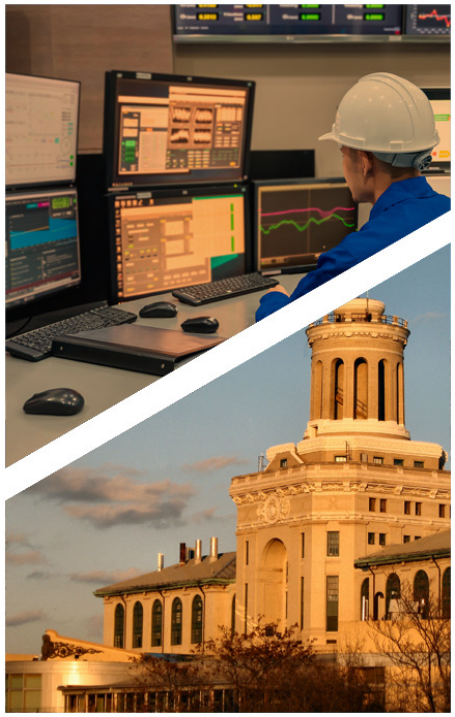
- Cyber-physical system design, security, and architecture
- Identifying and managing legacy CPS cybersecurity challenges
- CPS and OT resilience and autonomy

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Cyber-Physical Security

Carnegie Mellon University Software Engineering Institute



Top: Adobe Stock

RESEARCH OPPORTUNITIES: advance cyber resilience as an essential mission requirement to reduce the extent of consequences associated with internal faults, errors, and cyber attacks associated with cyber-physical systems (CPSs).

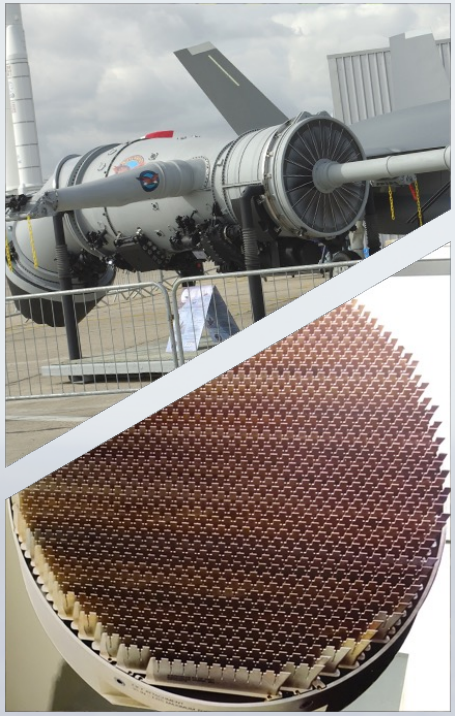
- Securable CPS elements
- Networked CPSs and communications
- CPSs and Autonomy
- Cybersecurity Protections for Legacy CPSs
- Configuration-aware CPS-based infrastructure
- CPSs and edge AI

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Cybersecurity for Complex Integrated Systems

Carnegie Mellon University Software Engineering Institute



Top: https://commons.wikimedia.org/wiki/User:Duch.seb
Bottom: Daderot

THE CHALLENGE: develop a means of confidently achieving cybersecurity situational awareness and risk management across the most consequential national security, critical infrastructure, and enterprise systems integrated from diversely sources elements.

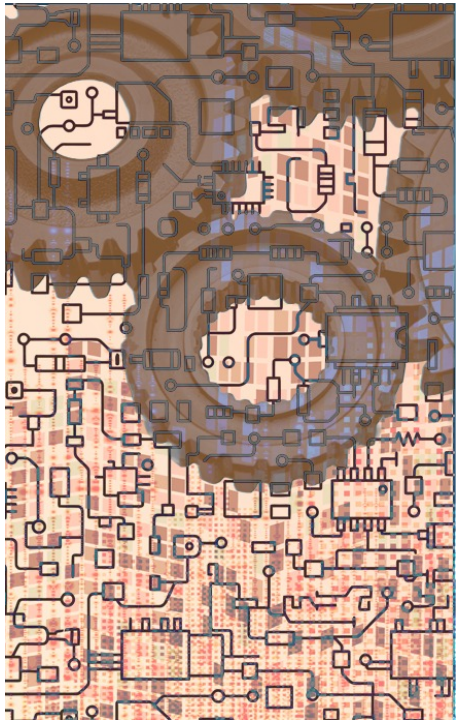
- Complexity, abstractions, and vulnerabilities
- Operational scoping, and functional and quality requirements
- Integration with complex supply chains
- Interconnected systems and data exchange
- Long lifespans and information loss

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Cybersecurity for Complex Integrated Systems

Carnegie Mellon University Software Engineering Institute



Adobe Stock

RESEARCH OPPORTUNITIES: as the ambition, complexity, and sophistication of systems continue to increase, such as with the evolution of AI models, create novel capabilities that secure both legacy and emerging complex systems.

Systems integration practices

- Models for integrated systems and their operating environments
- Systems engineered for cybersecurity
- Sourcing practices to create incentives for security
- Capacity to monitor configuration integrity
- Security and integrity of open source system elements
- Security for cloud-based services

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Insider Threat and Human-Systems Interaction

Carnegie Mellon University Software Engineering Institute



U.S. Air Force photo illustration/Staff Sgt. Don Branum

THE CHALLENGE: reduce the opportunity for attackers to gain access to systems and data by exploiting human weaknesses and vulnerabilities.

- Cybersecurity applied to human-system interaction (HSI)
- Anthropomorphism and other human weaknesses
- Engineering designs that accommodate HSI realities

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Insider Threat and Human-Systems Interaction

Carnegie Mellon University Software Engineering Institute



Photo Staff Sgt. Collette Brooks

RESEARCH OPPORTUNITIES: develop designs for systems and workflows that reduce opportunities for human actions to create significant adverse consequences in the operational context of the system.

- HSI design practices for systems and their workflows
- Models to inform HSI design practices
- Data from operational monitoring of critical systems
- AI models in advisory roles
- Red team practices that facilitate risk assessment

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Secure Engineering and Mission Confidence

Carnegie Mellon University Software Engineering Institute



Adobe Stock

THE CHALLENGE: reduce the extent of of weaknesses and vulnerabilities in systems, including weapons systems and critical infrastructure, through implementation of cost-effective secure engineering practices, including Secure-By-Design policies and procedures.

- Trustworthy critical systems
- Tactics, techniques, and procedures (TTPs)
- Formal methods
- Security-focused architectural designs
- Roles of AI

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Secure Engineering and Mission Confidence

Carnegie Mellon University Software Engineering Institute

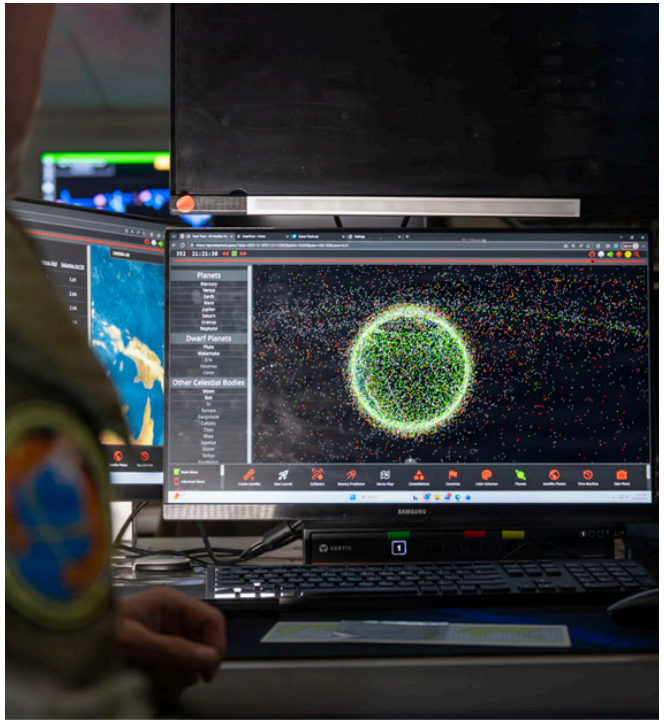


Photo: U.S. Space Force, David Dozoretz

RESEARCH OPPORTUNITIES: directed research can accelerate the rapid evolution of secure engineering practices, particularly involving formal methods and AI, to enable its effective application to mission systems.

- Memory-Safe(r) programming languages and beyond
- Secure coding and Application Programming Interface (API) design
- Architecture design and modeling
- Integration of secure engineering and formal methods
- Supply-chain practices
- Means to organize and analyze bodies of evidence

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Modeling and Simulation (M&S) in Support of Security

Carnegie Mellon University Software Engineering Institute



U.S. Space Force photo by Airman 1st Class Olya Houtsma

THE CHALLENGE: create agile, easy to employ, and cost-effective modeling and simulation capabilities that enable proactive security assessments, simulations, digital twins, and other techniques that accelerate innovation, enhance preparedness, and function as a force multiplier.

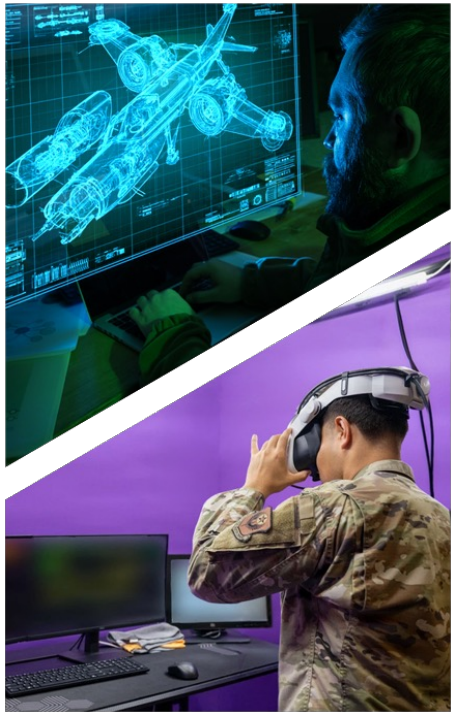
- M&S of cybersecurity systems and operations
- M&S integration and interoperability
- Model realism and validity
- Human elements

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Modeling and Simulation (M&S) in Support of Security

Carnegie Mellon University Software Engineering Institute



Top: Adobe Stock
Bottom: U.S. Air Force photo by Airman Olivia Perkins

RESEARCH OPPORTUNITIES: conduct novel applied research and development activities designed to create novel, mission-focused M&S capabilities that operators can effectively adapt to rapid changes in the threat environment; the evolution of mission concepts; and the pace of emerging technologies.

- M&S as a key linking element
- Experience-based capability development
- M&S standards and requirements development

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Your Role in Advancing Cybersecurity

Carnegie Mellon University Software Engineering Institute



Top: Adobe Stock
Bottom: af.mil/About-Us/Biographies/Search/touhill/

- Make cybersecurity a key requirement of every project and program
- **Think like a hacker; act as a commander**
- Invest in applied R&D to enhance your warfighting capabilities
- Partner with department applied R&D activities
- Test novel ideas and concepts leveraging new and emerging technologies
- Be bold and challenge the status quo as you envision the future
- Don't Be afraid to ask for help

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]

Want to Learn More?

Carnegie Mellon University Software Engineering Institute



Greg Touhill
Director
CERT Division

Telephone:
+1 412.268.4728

Email:
info@sei.cmu.edu

© 2026 Carnegie Mellon University

[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]