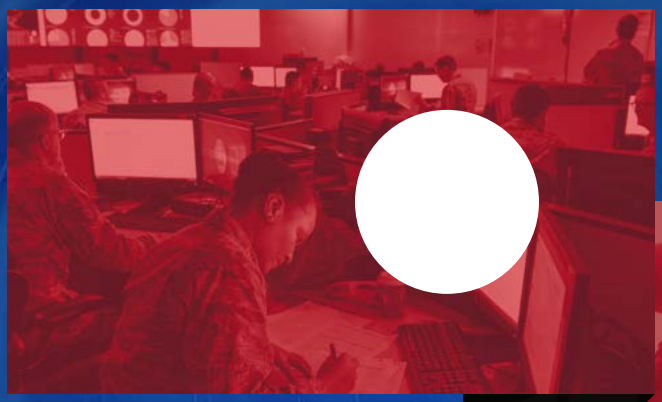
Carnegie Mellon University
Software Engineering Institute

2



YEAR IN REVIEW

2

4

Always focused on the future, the Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We lead research and direct transition of software engineering, cybersecurity, and artificial intelligence technologies at the intersection of academia, industry, and government. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD) and are based at Carnegie Mellon University (CMU), a global research university annually rated among the best for its programs in computer science and engineering.

The *2024 SEI Year in Review* highlights the work of the institute undertaken during the fiscal year spanning October 1, 2023, to September 30, 2024.

A MESSAGE FROM THE DIRECTOR AND CHIEF EXECUTIVE OFFICER

Making Software a Strategic Advantage for National Security

The Department of Defense's mission is to "provide the military forces needed to deter war and ensure our nation's security." Now and even more in the future, success in that vital mission can depend on the quality of software that the DoD acquires, operates, secures, and sustains. When the DoD created the SEI as a federally funded research and development center in 1984, it established a strategic partner for effectively and efficiently building, securely running, and evolving software capabilities that deliver asymmetric and decision advantage to U.S. warfighters.

The SEI contributes to the DoD mission by integrating three domains central to the development, application, and transition of mission-critical software technology. The first is artificial intelligence. The SEI tackles the DoD's need for leap-ahead capabilities that are trustworthy, safe, and fit for the mission. We build AI capabilities for real-world needs; research and define enabling processes, practices, and tools; and translate leading practices for national security. Our work results in the fielding of robust and secure, scalable, and human-centered AI systems that address current needs and are ready for future challenges.

Software is another essential domain. The SEI focuses on tools, technologies, and practices to rapidly deploy software capabilities. We ensure that complex software-reliant systems will deliver critical capabilities even in the most challenging environments. Part of our software acquisition process and policy work focuses on improving the capability delivered for every dollar invested in software systems by grounding policy and decision making in high-quality data and analysis. Our work spans acquisition through sustainment with a continual insertion of new and needed software technologies.

We also work to ensure that software capabilities are secure in development and operation. Our researchers, software engineers, security analysts, and digital intelligence specialists collaborate to find and mitigate software vulnerabilities, provide key improvements to combat threats to networked systems, and develop leading-edge information and training to improve the DoD's cybersecurity practice. Our work produces advanced methods and tools to counter increasingly sophisticated, large-scale cyber threats.

The SEI delivers, as no other organization can, innovation matched to DoD warfighter needs in AI, cybersecurity, and software engineering. The examples of our R&D in this *Year in Review* highlight only some of our best work in fiscal year 2024. I invite you to review our website, blogs, reports, podcasts, and webcasts to learn more, and I welcome every opportunity to discuss the needs of those who defend our nation.

Paul Nielsen

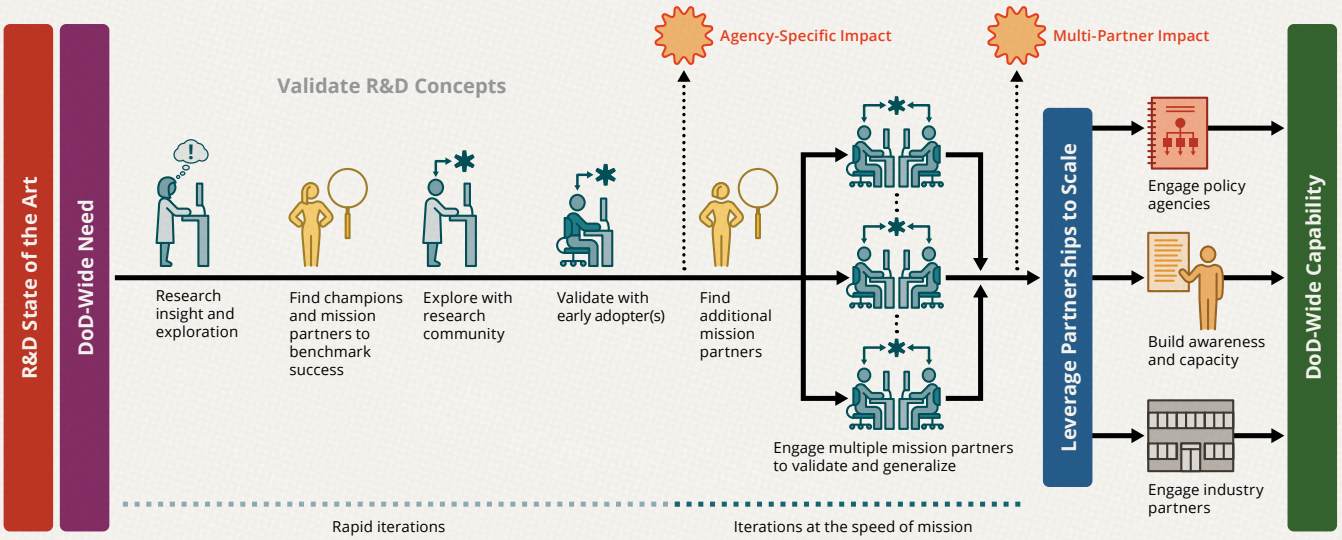
Execution Strategy

The SEI facilitates the transfer of research results to practice in Department of Defense (DoD) programs, the Office of the Secretary of Defense's science and technology initiatives, and non-DoD U.S. government organizations where improvements will also benefit the DoD. In doing so, we gain deeper insight into mission needs—insight that forms the basis for new research. In addition, we transition matured technologies more broadly to defense industrial base organizations and others in the DoD supply chain.

We execute applied research to drive systemic transition of new capabilities for the DoD. Our deep understanding of DoD needs and of the state of the art inform our selection of challenges in software, cybersecurity, and artificial intelligence.

To validate research and development concepts, we rapidly iterate with the research community and select mission partners. The results typically impact a single agency. We then scale the concept to multiple agencies and domains by iterating with additional mission partners based on their timing and needs. Finally, we engage policy agencies and industry partners and build the DoD's awareness of and capacity for the solution to create DoD-wide capability.

Our multidisciplinary approach informs prototype tools, innovative solutions, and input for our sponsor's policy decisions about software and related technologies. Through ongoing work and communication with customers, the SEI identifies priority areas for further research and development. We combine our body of knowledge with external material and systems engineering to deliver quantitative impact to U.S. government organizations, DoD organizations, and DoD end users.



Funding Sources

In fiscal year 2024, the SEI received funding from a variety of sources in the DoD, civil agencies, and industry.

Table of Contents

Carleton and Lewis Selected for IEEE Computer Society Leadership Posts

Two members of the SEI's Software Solutions Division (SSD) were selected for leadership posts in the IEEE Computer Society in 2024. Anita Carleton, director of the SSD, was elected chair of the advisory board for *IEEE Software*, one of the organization's journals. Grace Lewis, an SSD principal researcher and lead of the Tactical and AI-Enabled Systems Initiative, was elected the society's president for 2026 and will serve as president-elect in 2025.

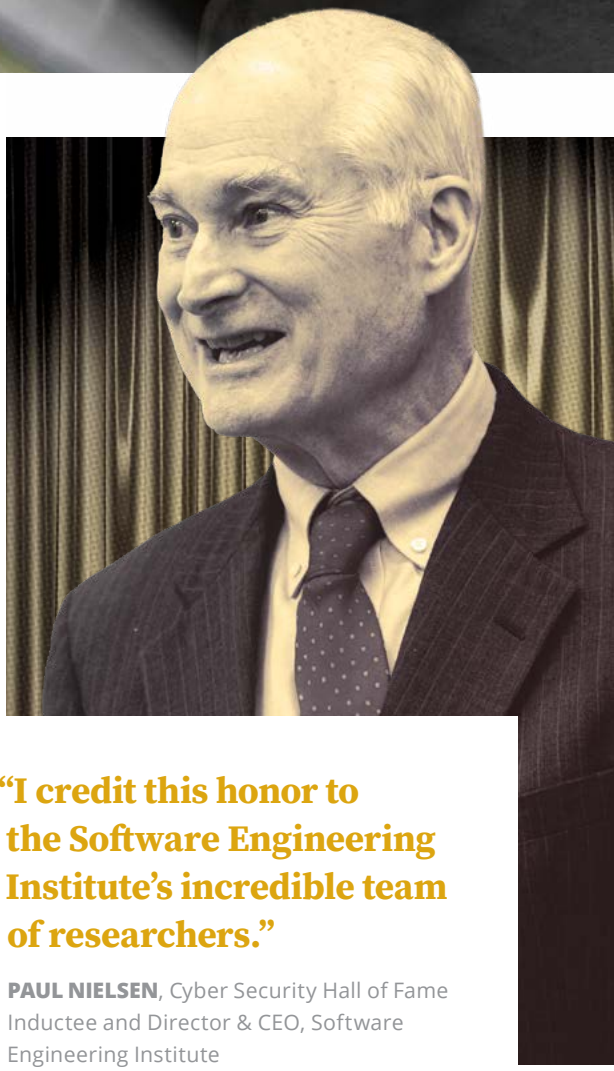
IEEE CS is the largest community of computer scientists and engineers. It publishes dozens of magazines and journals and runs many professional conferences and other programs to empower professionals in computer science and engineering and advance the field.

Nielsen Receives 2024 Cyber Security Hall of Fame Honor

SEI director and chief executive officer Paul Nielsen was inducted into the Cyber Security Hall of Fame in the fall of 2024. Since 2012, the Cyber Security Hall of Fame has celebrated global cybersecurity leaders' accomplishments. The Hall of Fame included Nielsen in its cyber technology and business category.

"I credit this honor to the Software Engineering Institute's incredible team of researchers," said Nielsen. "Across four decades, they laid the foundations for the security of networked systems and continue to innovate this crucial and always changing field. In addition, during my first career in the Air Force, I was fortunate to work with cybersecurity teams at the Air Force Research Laboratory, especially the Information Directorate in Rome, New York, and at the National Security Agency."

Nielsen has led the SEI since 2004. He previously served in the U.S. Air Force for 32 years, retiring as a major general and commander of the Air Force Research Laboratory. Nielsen is a member of the U.S. National Academy of Engineering (NAE) and a fellow of the American Institute of Aeronautics and Astronautics (AIAA), the Institute of Electrical and Electronics Engineers (IEEE), and the International Council on Systems Engineering (INCOSE).



"I credit this honor to the Software Engineering Institute's incredible team of researchers."

PAUL NIELSEN, Cyber Security Hall of Fame Inductee and Director & CEO, Software Engineering Institute

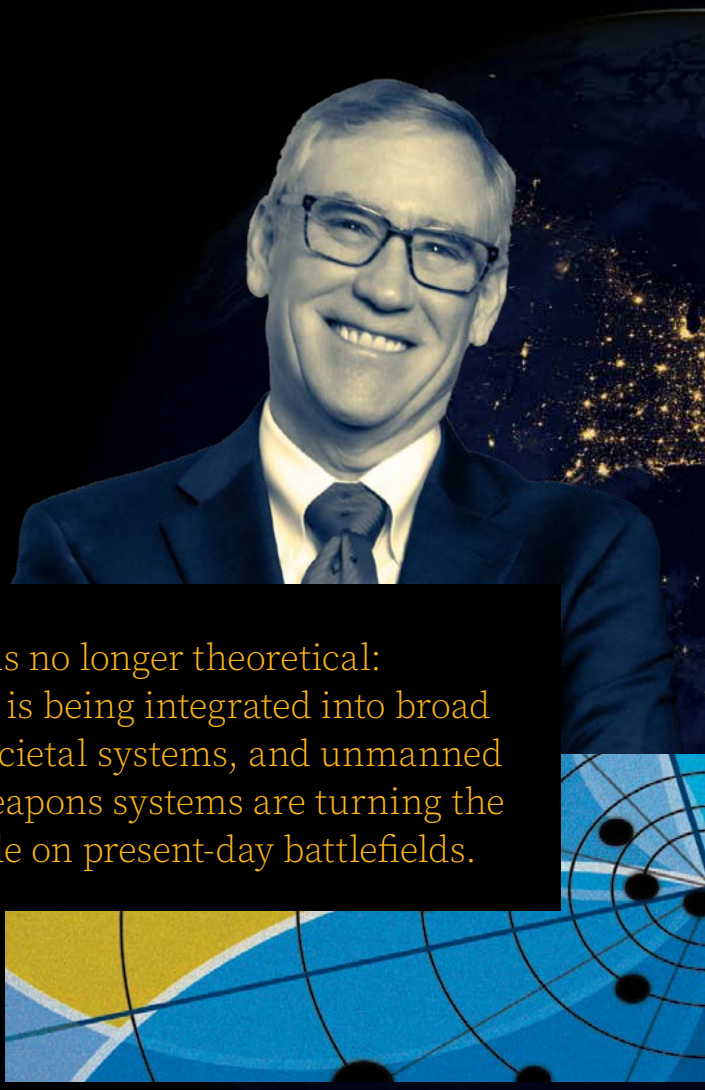
Danyliw Chosen to Lead Internet Engineering Task Force

In March 2024, Roman Danyliw, the SEI's deputy chief technology officer, was selected to be chair of the Internet Engineering Task Force (IETF), which develops voluntary standards that guide the evolution, architecture, and smooth operation of the internet. Danyliw oversaw the group's operations during 2024.

Danyliw is also the General Area director of the IETF's Internet Engineering Steering Group (IESG) and a member of the IETF's Internet Architecture Board (IAB). Together these bodies guide the immediate management of and long-range direction for internet standards.

The Rapid Evolution of Scaled Software Solutions for National Defense

EDITORIAL *Tom Longstaff*



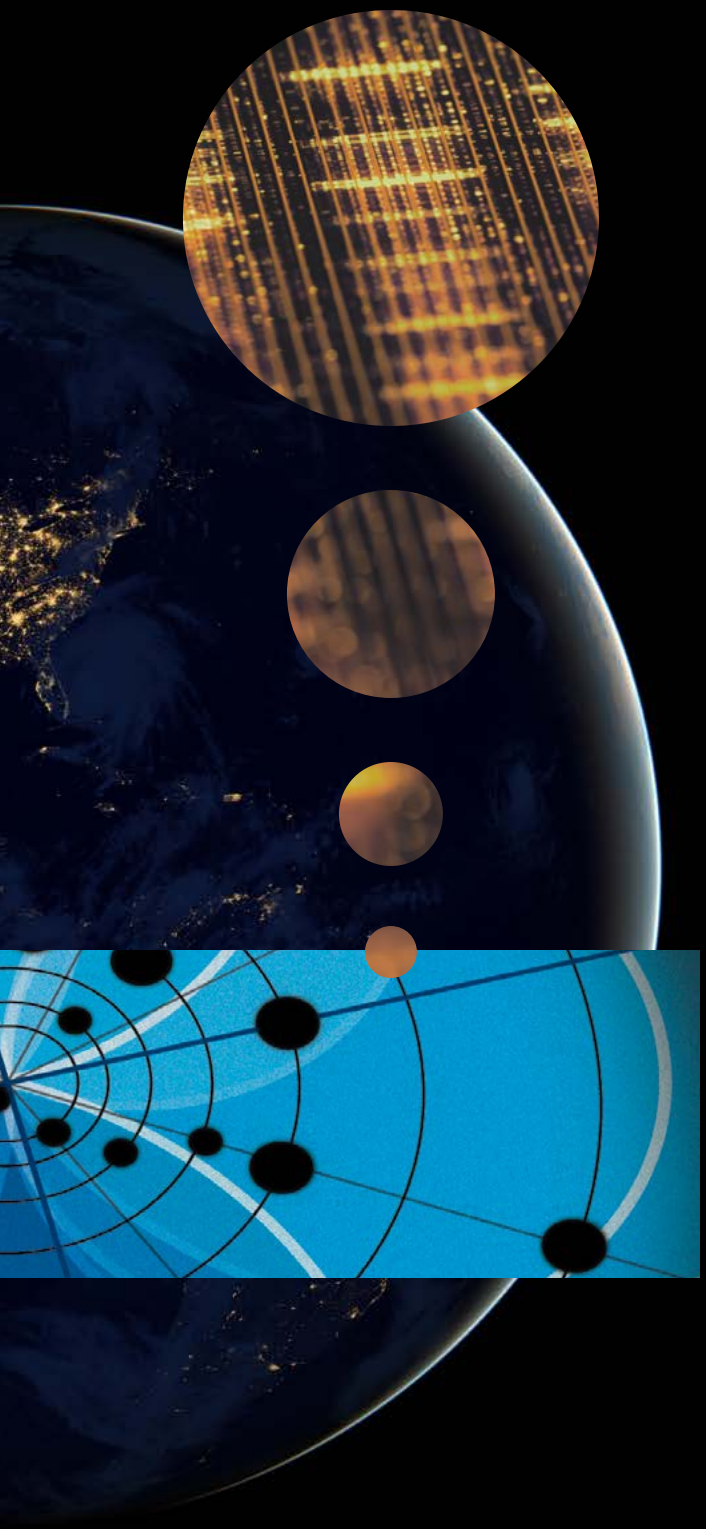
The urgency of the national defense mission is increasing the pressure to rapidly scale technology in the Department of Defense (DoD) and other security agencies. A January 2025 Defense Innovation Board study on scaling nontraditional defense innovation framed the challenge starkly: "We must act swiftly to ensure the DoD leads in global innovation and competition over AI and autonomous systems – and is a trendsetter for their responsible use in modern warfare. The importance of these tasks cannot be understated; our very democracy and way of life are at stake." Alongside this study, the DIB released another on scaling unmanned weapons systems.

Software lies at the heart of both artificial intelligence (AI) and autonomous systems, and the DoD has made great strides in keeping pace with the speed of software advancement. However, the need for these two crucial technologies to both advance technically and permeate the defense domain threatens to outstrip current paradigms for software acquisition, operation, and testing.

The SEI's 2006 report on ultra-large-scale systems and 2021 study on the future of software engineering research and development foresaw this moment. It is no longer theoretical: AI is being integrated into broad societal systems, and unmanned weapons systems are turning the tide on present-day battlefields.

It is no longer theoretical: AI is being integrated into broad societal systems, and unmanned weapons systems are turning the tide on present-day battlefields.

But we do not meet this moment empty-handed. The DoD and the defense industrial base can double down on the proven software development accelerators of Agile methodologies and continuous deployment of capability, The SEI has been, and will continue to be, instrumental to their evolution. More than ever, software system developers and operators need these methods in order to move at speed and with discipline to deliver capability to the warfighter. The SEI continues to improve them with



new tools like the Polar framework for DevSecOps data and a study of the state of DevSecOps within the DoD. Our recent Capability-Based Software Cost Estimation is a novel method, aligned to Agile and DevSecOps, built for flexibility and speed.

SEI work already transitioned to the DoD is bearing fruit. The SEI's Architecture Tradeoff Analysis Method has hastened the analysis of software architecture and design tradeoffs. The faster a development organization moves, the more it will need to manage its technical debt, another long-standing area of SEI expertise. We have also worked with DoD acquisition programs to improve their processes, as we did in the development of 2020's Software Acquisition Pathway, which a 2025 memo from the secretary of defense mandated as the preferred software pathway for all DoD components.

Where point solutions once satisfied end users, national defense now calls for large-scale solutions, such as development of the Universal Command and Control (UC2) program led by the SEI in 2022. SEI and Carnegie Mellon University researchers are working to accelerate assurance of large-scale systems through compositional techniques and automatic integration of verification results into certification claims. As software systems expand, so too do their attack surfaces. Vulnerability risk management has stretched to address the entire software supply chain, as has the SEI's Acquisition Security Framework. The scale of AI vulnerabilities will continue to rise, and the SEI's AI Security Incident Response Team (AISIRT) stands ready to lead the communal response. The federal workforce too must scale to overcome security threats, which is why the SEI develops automated malware reverse engineering tools and the DoD's first certification for malware reverse engineers.

The old software paradigm said you could make a system either quickly or at scale. Now we must do both, and in every warfighting domain: land, air, sea, cyberspace, and space. The SEI and other defense federally funded research and development centers have been laying the groundwork, but much work, innovation, and creativity lie ahead.

Photo: NASA

AI Eye in the Sky Improves Artillery Fire Missions

In artillery fire missions, binocular-equipped forward observers request multiple shots to close in on a target's coordinates. In the minutes between these bracketing rounds, the target may move and the observer remains in harm's way. An SEI artificial intelligence prototype is giving U.S. Army artillery observers a smart eye in the sky.

The Army has been experimenting with off-the-shelf unmanned aerial systems (UASs) to provide combat units a birds' eye view of enemy positions. The Army Artificial Intelligence Integration Center (AI2C) last year tasked the SEI with developing Shrike, a complementary prototype for recognizing and geolocating threats.

From its elevated vantage, the Shrike system uses computer vision and machine learning (ML) to identify potential threats. The system sends its aerial views, marked with potential targets and locations, to the forward observer's device. If the soldiers fire, Shrike's ML model detects the round's hit location and recommends targeting corrections. Shrike's sensors feed new data to its tactical ML pipeline for model retraining so the system gets smarter with every sortie.

"Shrike is about improving small-unit capability on the front line," said Jeff Mattson, the SEI's Shrike project lead. The project draws on areas of SEI expertise: ML in edge environments with memory and connectivity constraints, as well as integration into a package that is easily deployable on most UAS platforms. These research areas can inform Army fires modernization efforts.

Mattson conducted early field trials of Shrike with the 198th Infantry Brigade, 1st-19th Infantry Battalion's Infantry Mortar Leaders Course (IMLC) and the Army Test and Evaluation Center (ATEC). Using Shrike, operators decreased the time from the first round to the effective round by 80 percent and improved accuracy by 50 percent, when compared to the Expert Infantryman's Badge (EIB) call-for-fire standards.

"Shrike enables any soldier to accurately find, fix, and finish a target through digital fires with just minutes of training," said Captain Jarek Ingros, AI2C's perception team lead for robotics and autonomous systems. "This capability drastically increases the lethality of U.S. Army formations."

"Shrike enables any soldier to accurately find, fix, and finish a target through digital fires with just minutes of training."

CPT JAREK INGROS, Perception Team Lead for Robotics and Autonomous Systems, U.S. Army Artificial Intelligence Integration Center

Photos: (top) U.S. Army, *SPC Eric Cerami;* (bottom) U.S. Army, *CPT Avery Austin*

> **"Over the past five years, our collaboration with the SEI has been instrumental in advancing the AI Development Environment, AI Fusion, and Robotics and Autonomous Systems."**
>
> **COL ISAAC FABER**, Director, U.S. Army Artificial Intelligence Integration Center

SEI and AI2C Collaborate to Create Effective AI Solutions for the Army

The field of artificial intelligence (AI) is driving revolutionary capabilities to analyze data, automate systems, and support decision making. To leverage this potential, the Army launched a collaboration with Carnegie Mellon University (CMU) and the SEI in 2019 to explore the suitability of AI for addressing the Army's current needs and to advance capabilities that expand the U.S. advantage over its adversaries. The Army expanded this work in 2021, creating the Artificial Intelligence Integration Center (AI2C) to further develop and operationalize AI solutions.

The SEI delivers value and impact through its extensive experience leading novel research, testing and adapting new technologies to meet DoD needs, and delivering prototypes of effective capabilities. The SEI's collaboration with AI2C has been successful because of this research-to-practice paradigm, which has formed the basis for how the SEI provides a technical vision to help the Army discover, define, and develop AI-enabled capabilities.

Together the SEI and AI2C have established the technological underpinnings for several important AI systems and identified the metrics to ensure their success. "Over the past five years, our collaboration with the SEI has been instrumental in advancing the AI Development Environment, AI Fusion, and Robotics and Autonomous Systems," said Colonel Isaac Faber, director of AI2C. These AI-enabled solutions have given the Army the capability to develop AI quickly and effectively; acquire data to conduct high-confidence, real-time detection in operational environments; and deploy autonomous vehicles in the field. "Our work with the SEI has significantly helped AI2C fulfill its mission of accelerating AI innovations."

Photo: (bottom) U.S. Army Reserve, *CPT Katherine Alegado*

Training the DoD to Leverage AI for Strategic Advantage

Artificial intelligence (AI) is a transformational technology, but it has limitations in challenging operational settings. The Department of Defense (DoD) must understand how to build and employ reliable, secure AI capabilities that warfighters can trust in mission-critical environments. It has turned to the SEI for training in AI Engineering, the discipline of creating trustworthy, scalable, and robust and secure AI systems.

Rigorous engineering practices for AI and machine learning, especially in national security settings, are still nascent. Since 2022, the SEI has produced and delivered more than 150 hours of AI Engineering training to senior leaders, acquisitions personnel, technical teams, and end users in the DoD. The SEI's AI workforce development team leverages state-of-the-art technologies to develop highly engaging, hands-on learning environments that scale to the needs of participating organizations.

In alignment with U.S. strategies like the *National Artificial Intelligence Research and Development Strategic Plan* and the *National Defense Strategy*, the SEI works with DoD mission partners to fill the gaps in commercial AI training for the nation's defense workforce, from end users to senior leaders.

"The SEI understands the challenges that AI capabilities bring to high-stakes contexts where the DoD operates. We can apply the discipline of AI Engineering to help the DoD achieve strategic technical advantage," said Robert Beveridge, a technical manager in the SEI's AI Division.

The SEI's AI workforce development program collaborates with academic partners at Carnegie Mellon University and with DoD organizations. Going forward, the SEI will continue to produce and deliver DoD workforce training.

"The SEI understands the challenges that AI capabilities bring to high-stakes contexts where the DoD operates."

ROBERT BEVERIDGE, AI Engineering Center Technical Manager, SEI AI Division

Advanced Malware Academy Enhances Defense Cyberspace Capability

Malware analysts provide an important capability for national defense cyberspace operations. In this operational context, advanced skills and expertise are hard to acquire in part because the Department of Defense (DoD) does not have uniform definitions for an analysts' job role. To enhance this competency in the U.S. armed services, the SEI piloted the Advanced Malware Academy and developed a malware analyst certification for the DoD.

Jeff Gennari and David Belasco, researchers from the SEI's Malware Analysis team, created the academy's curriculum for the Air Force 867th Cyberspace Operations Group (COG). They drew on the SEI's decades of malware reverse engineering research and course creation for the government. The researchers mentored the first cohort academy interns in the summer of 2024.

For four weeks at the SEI, enlisted service members received hands-on training on advanced malware topics such as artificial intelligence, malware repurposing, and threats facing emerging technologies. A two-week, intern-directed project on novel malware scenarios culminated in a presentation to leaders in the 867th COG and the SEI.

"There's no shortcut to job experience, but this course jump-starts the student's ability to tackle new challenges," said Gennari.

The cadre of graduates is better prepared to tackle some of the most pressing and complex threats facing the DoD. But the academy also helped Gennari and Belasco define the DoD's first certification for Cyber Mission Force malware analysts. The certification outlines a set of skills that cross-service organizations such as the USCYBERCOM Cyber National Mission Force (CNMF) can use to inform analyst hiring and training.

The second cadre of service-member malware analysts completed another delivery of the Advanced Malware Academy in early 2025. Those interested in future deliveries can contact info@sei.cmu.edu.

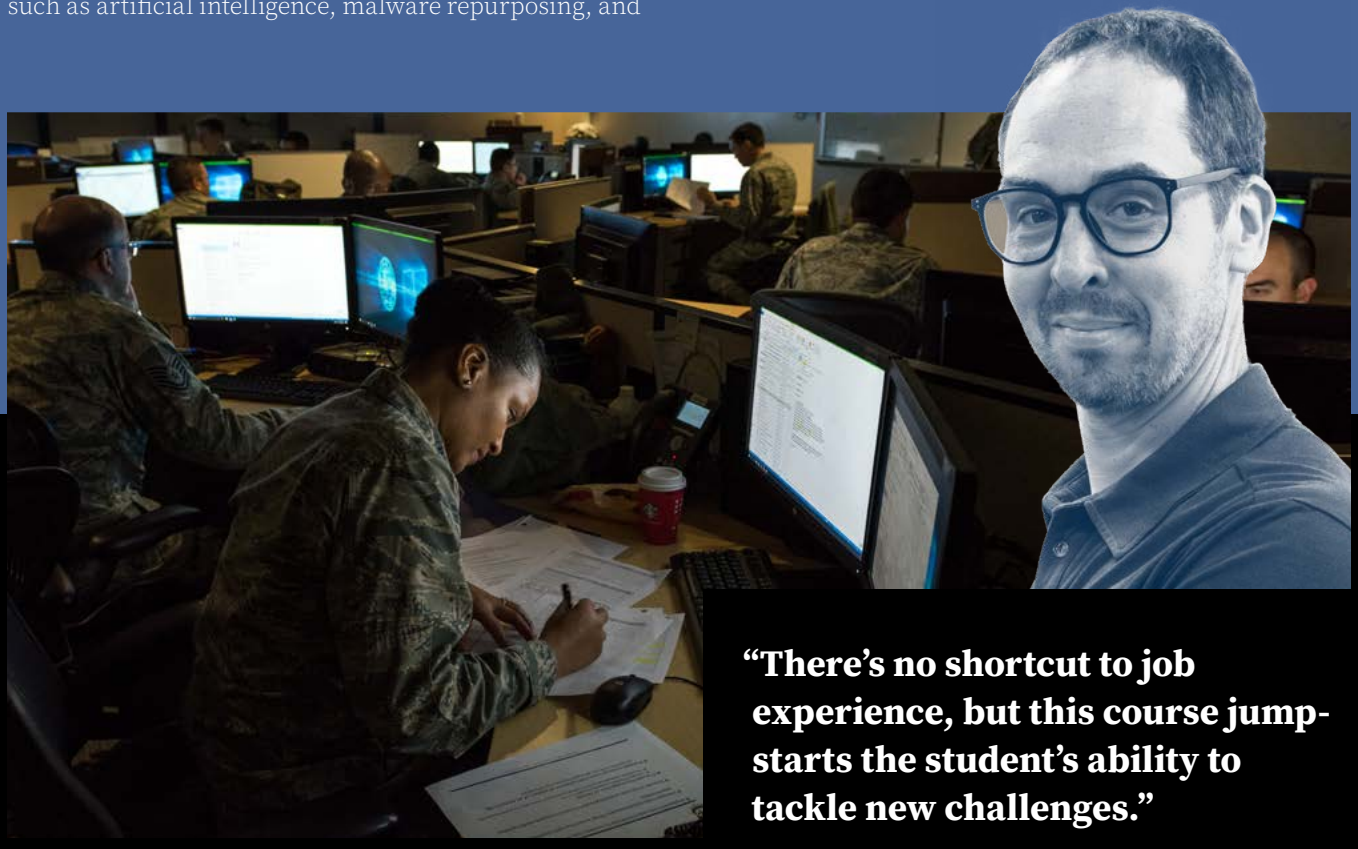


Photo: U.S. Air Force, *J.M. Eddins Jr.*

"There's no shortcut to job experience, but this course jump-starts the student's ability to tackle new challenges."

JEFF GENNARI, Senior Engineer, SEI CERT Division

First State of DoD DevSecOps Study Finds Excellence and Opportunities

The Department of Defense (DoD) started incorporating DevSecOps into its software development and acquisition practices in the last decade. To baseline the DoD's progress and facilitate planning for future DevSecOps adoption, the SEI studied the state of DevSecOps within the DoD in 2024.

Security, efficiency, and speed are critical in the DoD's high-stakes environment and against fast-moving adversaries. DevSecOps principles and practices speed delivery of secure software capabilities by operations and security staff.

The SEI's study found that pockets of the DoD have had significant success with DevSecOps practices and that the DoD needs to implement those successes at scale. Major findings include the following:

- DevSecOps achieves success amid rapid change.
- Software factories are our digital arsenal and the catalyst to enabling software modernization.
- DevSecOps enables continuous Authority to Operate.
- Policy and guidance based on successful grass-roots efforts have enabled change.
- Success rests on forging a mission-ready DevSecOps workforce and strong leadership committed to driving to creative solutions.
- The path forward relies on data and effective measurement.

Photo: U.S. DoD, *U.S. Navy Petty Officer 2nd Class Alexander Kubitza*

Convening Community, Advancing Software for National Defense

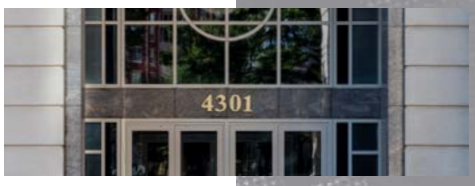
The SEI supports its Department of Defense (DoD) sponsor in ensuring software is capable, timely, trustworthy, and affordable by facilitating the community of experts working at the cutting edge of software engineering, cybersecurity, and artificial intelligence (AI) engineering.

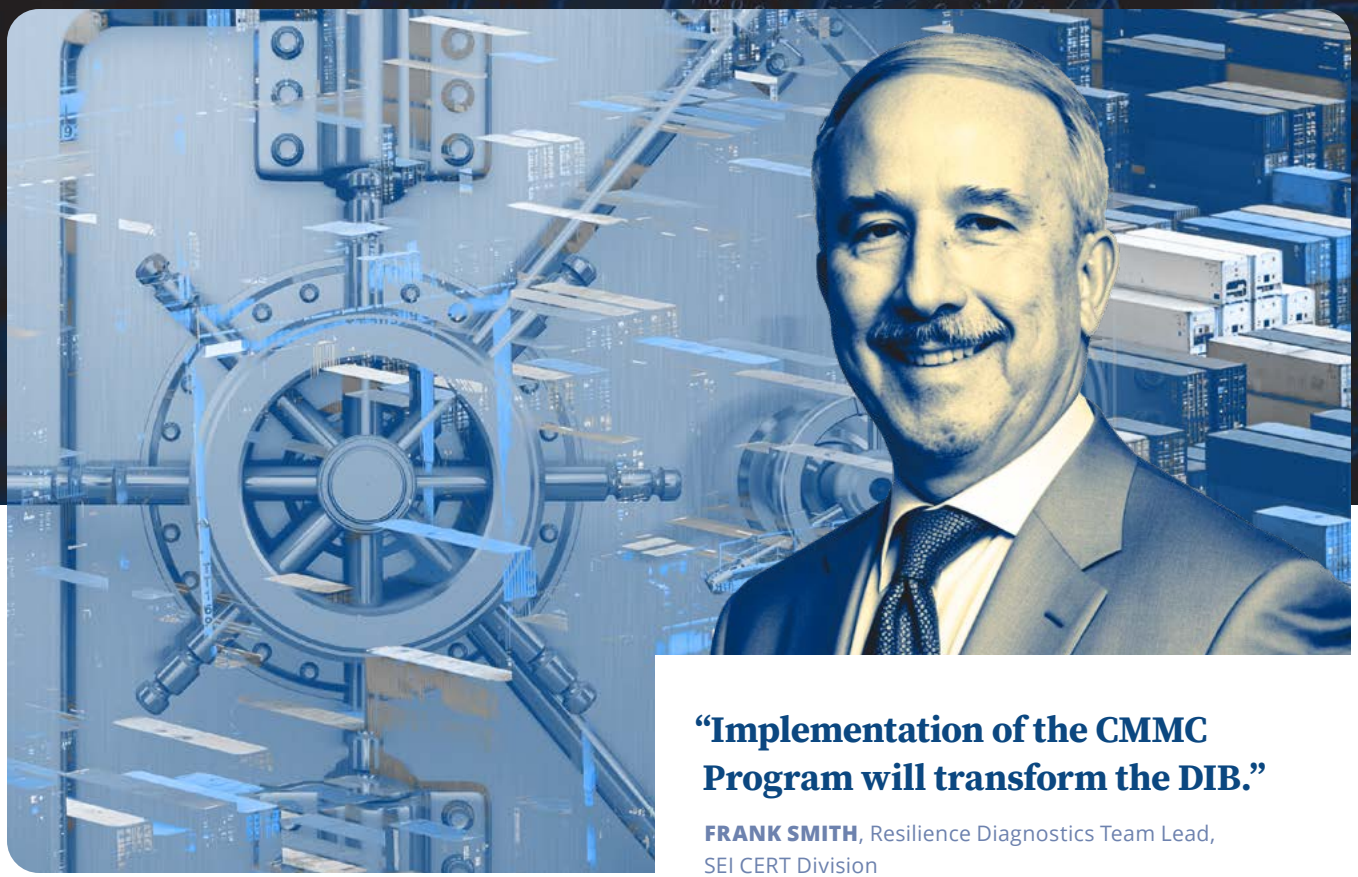
In late 2023, the SEI's Software Solutions Division (SSD) held the second International Workshop on Explainability of Real-Time Systems and Their Analysis (ERSA), which explored ways to include explanations, not just answers, in the verification of critical, real-time software systems. Focused on how to better integrate security into DevOps practices, DevSecOps Days 2024 was held in September. SSD also hosted the Assurance Evidence for Continuously Evolving Real-Time Systems (ASERT) Workgroup, which seeks to develop new system certification techniques based on automated formalized arguments.

The SEI's CERT Division hosted Secure Software by Design to promote security as an integral, early aspect of the software lifecycle. Deterrence of insider threats was the focus of the 11th annual Insider Risk Management Symposium, while the 20th FloCon brought together security operations experts. Zero Trust Industry Days 2024 gathered developers of solutions for implementing zero trust architecture. The 2024 Supply Chain Risk Management (SCRM) Symposium explored the field's challenges and best practices. Finally, NatCSIRT 2024 addressed the unique challenges of national Computer Security Incident Response Teams (CSIRTs).

The Artificial Intelligence (AI) Division of the SEI and Google co-hosted the AI Symposium: Collaborating Toward a Safer and More Responsible Future to discuss AI's impact on knowledge, information, and national security.

In 2025, the SEI will continue to engage thought leaders and practitioners in the advancement of the software as a strategic advantage.





"Implementation of the CMMC Program will transform the DIB."

FRANK SMITH, Resilience Diagnostics Team Lead, SEI CERT Division

CMMC Program Safeguards Information in the Defense Industrial Base

On December 16, 2024, 32 CFR Part 170 established the Cybersecurity Maturity Model Certification (CMMC) Program. The milestone marked a major transition for one of the SEI's most impactful projects.

A product of the Office of the Department of Defense (DoD) Chief Information Officer, CMMC improves security throughout the defense industrial base (DIB) supply chain against increasing and evolving cyber threats. The program defines the measures that DIB organizations must implement to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). The DoD verifies implementation of the measures through CMMC assessments of specified cybersecurity standards.

Since the inception of CMMC in 2019, the SEI has touched virtually every aspect of the program, from helping establish its structure based on proven cybersecurity practices, to developing certification and assessment standards, to creating training for an estimated 160,000 contracting officers, program managers, and others in the defense acquisition workforce.

"Implementation of the CMMC Program will transform the DIB," explained the SEI's Frank Smith, who leads the CMMC team. "CMMC protects sensitive DoD information from our adversaries. Beyond the DoD, it creates a baseline for DIB contractors to implement cybersecurity requirements according to a clear set of measures applicable across the federal space."

For details about the CMMC Program, contact the SEI CERT Division at info@sei.cmu.edu.

Establishing Modern Software Processes for Satellite Data Computing Laboratory

The United States Space Force's Overhead Persistent Infrared (OPIR) Tools, Applications, and Processing (TAP) Lab in Boulder, Colo., helps software developers build national defense tools that use satellite data. In 2024, SEI researchers helped the lab incorporate modern software development processes within its high-security environments.

Commercial software development teams mine the lab's satellite feeds to create mission applications, such as orbital object detectors, and test them with Space Force operators. The computing platforms support unclassified and classified work while also providing an open architecture for developers. While the setup fostered collaboration across external development teams, the mixed-classification environment provided a challenge for software delivery. But there was help on the way.

The SEI's long partnerships with industry and government, as well as a history of software process improvements, made it the right fit to support this challenge. SEI experts in software engineering, artificial intelligence and machine learning, and cybersecurity applied their expertise to the lab, designing well-architected end-to-end DevSecOps pipelines, creating modern workflows, facilitating training sessions, and recommending Agile method implementations to further enhance the lab's external development teams.

These process improvements will ultimately allow the Space Force to quickly integrate new data-processing capabilities.

SEI Machine Learning Prototype Helps the Air Force "Fuel More Fight"

When the U.S. Department of the Air Force (DAF) fuels its aircraft, it feels pain at the pump at a large scale: 1.5 billion gallons of fuel annually at a cost of about $5.5 billion. Aircraft modifications, or interventions, that reduce fuel consumption by even a small amount result in significant savings. However, faced with voluminous and variable data from in-service sorties, estimating fuel rate reduction is a laborious challenge for DAF experts. The SEI developed a prototype machine learning (ML) model to estimate fuel savings from aircraft interventions.

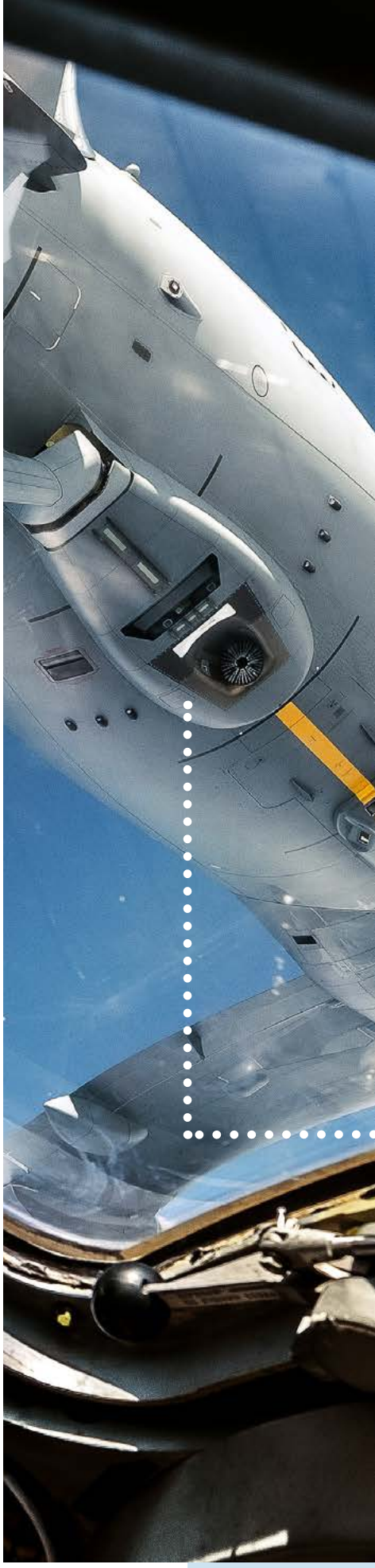
The DAF applies fuel cost savings to improve its combat readiness, or "fuel more fight," as those within the department say. The DAF asked the Defense Department's Defense Innovation Unit (DIU) to investigate a data-driven way to optimize flights for fuel savings. At the DIU's suggestion, the DAF asked the SEI to apply ML to flight data and derive fuel savings from aircraft interventions. This automation approach promised to speed an expensive process currently based on expert experience.

The SEI's expertise in ML, data science, and Air Force operations made it the perfect choice for tackling this problem. "This work is a good example of the SEI's applied research and prototype development for mission," said Keltin Grimes, an associate researcher in the SEI's AI Division and lead of the operational energy model project.

The SEI team recognized the challenges: collecting clean flight data, processing it into a usable format, overcoming data noise, and controlling for confounding hardware, software, and operational variables. Using common open source tools, the SEI team built and trained ML models and developed a prototype tool the DAF can use to specify aircraft type, input data from flights with and without aircraft intervention, and output the intervention's estimated fuel savings down to 0.5 percent. Even reductions that small in a single fleet of aircraft could save millions of gallons of fuel per year.

After validating the tool against expert estimates of a real-world intervention, the SEI delivered the prototype in May 2024 and trained DAF personnel to use it. Since then, the DAF has been applying the model to various aircraft interventions.

Dr. Jordan Eccles, former data scientist at the DAF's Operational Energy Program, said, "SEI's effort dramatically accelerated Air Force Operational Energy's efforts to analyze flight data recorder files to automate detection of fuel efficiency improvements. The tools developed by SEI demonstrated that machine learning can successfully identify very small improvements in efficiency that nonetheless have significant impacts on combat capability. Critically, cost savings identified with these tools can be recovered and reinvested in energy initiatives, a program expected to provide over $35 million for DAF initiatives in fiscal year 2024 alone."



> **"Cost savings identified with these tools can be recovered and reinvested in energy initiatives, a program expected to provide *over $35 million* for DAF initiatives in fiscal year 2024 alone."**
>
> **DR. JORDAN ECCLES**, (former) Data Scientist, U.S. Department of the Air Force Operational Energy Program

While the operational energy model is tuned for aircraft interventions, the data-driven approach could allow the DAF to identify other fuel-saving factors, such as flight location and performance parameters. Such techniques could be applied to any government or industry fleet that feels pain at the pump.

Accelerating Technology Adoption

The Office of the Undersecretary of Defense for Research and Engineering (OUSD(R&E)) has been fostering technology innovation initiatives, such as the Rapid Defense Experimentation Reserve (RDER), to rapidly develop solutions for warfighters. The SEI works alongside defense technology accelerators to support this research and development tempo.

The Defense Innovation Unit (DIU), which accelerates adoption of commercial and dual-use technology across the Department of Defense (DoD), is one of the SEI's most frequent innovation sponsors. The SEI provides technical advising and support as DIU evaluates potential vendors to address DoD mission needs. The SEI also collaborates with DIU on original projects:

- Responsible Artificial Intelligence Guidelines in Practice, a 2021 framework for building AI systems that align with DoD AI Ethical Principles. In 2025 the SEI will co-author updates that cover test and evaluation frameworks, generative AI, and operationalizing assured AI.
- xView2 Machine Learning Competition, a 2019 competition for computer vision algorithms examining satellite imagery to assess disaster damage. The SEI is part of a 2025 project to develop the xView2 program into a tool for warfighters to assess battle damage.

By partnering with innovation organizations, the SEI helps the DoD deliver solutions at the speed of relevance.

Photo: U.S. Air Force, *Senior Airman Joseph Morales*

Leading AI Security Incident Response

Artificial intelligence (AI) capabilities impact all corners of society and national security, yet cybersecurity processes have largely not been integrated into AI. Vulnerabilities occur throughout the complex, disparate AI ecosystem, and AI developers and researchers lack security tools and training. Meanwhile, attackers are leveraging this weak point to target AI-enabled assets.

In response to this threat, the SEI formed the first-of-its-kind Artificial Intelligence Security Incident Response Team, or AISIRT, to formulate tools, practices, and guidelines for AI cybersecurity. AISIRT members work with the governmental, industrial, and academic cyber community to identify, analyze, and respond to threats that affect AI systems and ensure the safe and effective development and use of AI technologies as they evolve and grow.

The AISIRT's initial focus is vulnerability management for AI systems, built on the SEI CERT/CC's capabilities for software cybersecurity: community-based intake, analysis, coordination, and disclosure of vulnerabilities. Since the SEI established the AISIRT in November 2023, the team has analyzed 103 community-reported AI vulnerabilities.

These cases have shown that while cybersecurity and vulnerability practices inform much of AI vulnerability management, AI has introduced new challenges. The deep, layered complexity of machine learning (ML) models and data within AI architectures complicates AI system security. New threats, such as model inversion and prompt injection, appear constantly. These emerging concerns, alongside the multi-vendor, dependency-heavy nature of most AI and ML environments, make coordinated vulnerability disclosure (CVD) more difficult.

In its first year, the AISIRT has learned valuable lessons, among which are four high-level takeaways:

- AI poses new security issues, but it also shares traditional software cybersecurity concerns.
- Software engineering is just as important for AI systems as for traditional software.
- Coordination and disclosure are the most important parts of CVD.
- Fixing an AI problem is more important than deciding whether it meets the definition of a vulnerability.

The AISIRT is working to identify the challenges of CVD for AI and ML systems and call the community to action. AISIRT experts are also working with researchers across the SEI and Carnegie Mellon University to provide other capabilities that advance the security and safety of AI: incident response; vulnerability discovery; situational awareness; identification of best practices, standards, and guidelines; and establishing a community of practice.

"We are working to extend cybersecurity best practices, such as coordinated vulnerability disclosure, to AI," said Lauren McIlvenny, who leads the AISIRT as the technical director of threat analysis in the SEI's CERT Division. "We are also performing cutting-edge research to stay ahead of the expanding set of critical issues and attack vectors born of the rapid adoption of AI-enabled systems in consumer, commercial, and national security applications."

In the long term, the AI community should invest in research that develops and improves processes, procedures, and mechanisms to prevent vulnerabilities from being introduced into AI systems in the first place. Such investments should develop vulnerability identification tools for AI security researchers and training for AI developers on secure development practices. The AISIRT is well positioned to support these investments and respond to incidents caused by AI vulnerabilities.

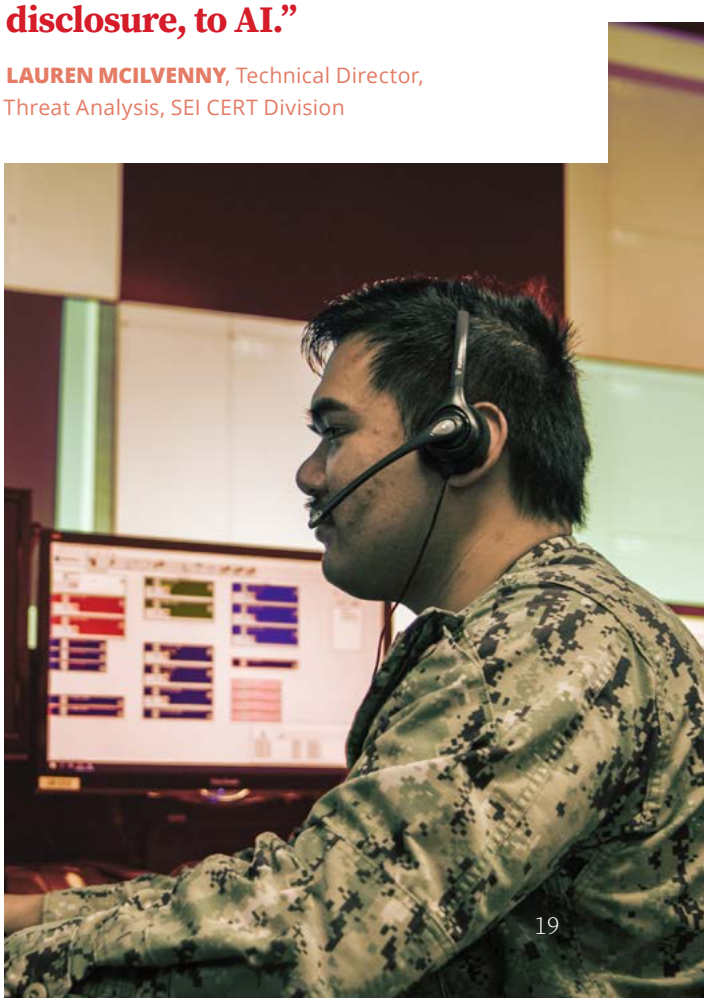
"Cybersecurity has always been a community activity," said Greg Touhill, director of the SEI's CERT Division. "AI vulnerabilities bring a new set of challenges to cybersecurity. That's why expanding the cyber neighborhood watch to include AI requires the kind of expertise, research, and trusted leadership that is foundational to the AISIRT mission."

Learn more about the AISIRT's *Lessons Learned in Coordinated Disclosure for Artificial Intelligence and Machine Learning Systems*. Report vulnerabilities in AI or traditional software to the AISIRT and CERT/CC at **kb.cert.org**.

Photo: (bottom) U.S. Navy, *Mass Communication Specialist 1st Class Benjamin A. Lewis*

"We are working to extend cybersecurity best practices, such as coordinated vulnerability disclosure, to AI."

LAUREN MCILVENNY, Technical Director, Threat Analysis, SEI CERT Division



Secure by Design Portfolio Supports Software Supply Chain Risk Management

Because software underpins so much of our daily life, attacks on software-reliant systems can pose a threat to public safety and well-being. To combat this threat, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) Secure-by-Design and Secure-by-Default initiative argues that "it is crucial for software manufacturers to make secure by design and secure by default the focal points of product design and development processes." The SEI has long advocated building security into early phases of software system development and acquisition. The SEI's 2024 portfolio of research and community outreach included multiple efforts to foster software security by design.

API Security

The application programming interface (API) is a fundamental component of most software applications. It makes system operations available to the user and enables engineers to build programs based on other programs without having deep knowledge of them. However, APIs invite attack because of their interconnectedness, the access they provide, their sometimes cryptic implementations, and their unexpected failures.

The SEI has been researching ways to create secure-by-design APIs by applying zero-trust principles, testing enabled by artificial intelligence (AI), DevSecOps approaches, supply chain security, and the SEI's Software Engineering Risk Assessment (SERA) framework. To learn more, read the SEI paper *On the Design, Development, and Testing of Modern APIs*.

Rust Software Security

The popular Rust programming language boasts a unique security model that promises memory and concurrency safety while providing the performance of C or C++. Rust, however, has not received the same scrutiny as older languages. Recent research by the

SEI examined claims and assumptions about the security of programs created with Rust and published its findings in a series of SEI Blog posts.

While Rust does provide memory safety and a degree of concurrency safety, it remains subject to a number of threats, such as supply-chain vulnerabilities. This year, the SEI examined several vulnerabilities that affected some Rust programs. One was a back door discovered in some versions of Rust crates, which are packages of Rust library code, and another was a command injection affecting programs running on Windows.

The Use of LLMs to Secure Source Code

There has been much hype about large language models (LLMs) replacing programmers. The SEI has been researching the use of LLMs in a variety of software engineering contexts, including identifying security flaws in source code.

A recent SEI study examined the benefits of using LLMs in DoD environments to automate static-analysis adjudication. Static analysis findings are often too voluminous for complete review, causing the DoD to accept unknown risk. SEI researchers developed a model of how an LLM-based tool could be used for static-analysis alert adjudication. They found LLMs hold promise for accurate static-analysis adjudication, automating code repair, and educating staff on alert adjudication.

Right Place, Right Expertise

In addition to these specific research efforts, SEI experts have provided commentary to CISA and White House Office of the National Cyber Director requests for information on secure by design practices and open source software security. To discover ways to reduce cybersecurity weaknesses earlier in the software development lifecycle, the SEI also holds an annual Secure Software by Design conference for security researchers, industry practitioners, and government officials. The SEI's history of connecting these communities, as well as its deep expertise in software engineering, acquisition, and cybersecurity, can help foster this holistic secure development approach.

Evaluating Risk Mitigation Practices for Generative AI in High-Sensitivity Domains

Generative artificial intelligence (AI) applications powered by large language models (LLMs) promise efficiency and efficacy for data-heavy enterprises, but the technology is particularly risky for the intelligence community. In 2024, the SEI researched three areas of generative AI called out by the Office of the Director of National Intelligence's *Principles of Artificial Intelligence Ethics for the Intelligence Community*: protecting privacy, mitigating bias, and immature security practices.

Benchmarks for Machine Unlearning

Removing sensitive data from a trained machine learning (ML) model normally requires expensive retraining. Machine unlearning algorithms are an efficient alternative for making neural networks forget specified data. This technique would allow organizations to address, in a scalable way, concerns about sensitive data exposure and privacy breaches.

However, research led by the SEI's Keltin Grimes suggests it is difficult to know if machine unlearning is successful. Current evaluation methods test unlearned models against relatively weak membership inference attacks and do not consider model update leakage, in which attackers infer deleted data by comparing model behavior before and after unlearning. The methods also do not account for declining model accuracy over iterations of unlearning.

For machine unlearning to help ML scale without expanding data exposure and privacy risks, practitioners will need ways to determine the success of the practice. Grimes and his colleagues plan to develop a comprehensive framework of machine unlearning evaluation benchmarks.

Scenarios for Auditing Bias in LLMs

While generative AI chatbots such as ChatGPT have safeguards against offensive outputs, they are imperfect, and biases within the underlying models remain. Auditing an LLM's inherent biases could be important in consequential settings such as intelligence analysis.

To uncover model bias, SEI research led by Katie Robinson and Violet Turri tested persona- and scenario-driven interactions with ChatGPT that circumvented the system's guardrails. They crafted a cowboy persona, had ChatGPT iterate a role-playing scenario as the cowboy, and prompted the persona to describe characters with a diverse set of names. The roles and personality traits ChatGPT provided revealed model stereotypes related to ethnic background and gender that were absent without the persona and role-playing scenario.

This work reveals that LLM bias can yield potentially harmful misrepresentations despite system safeguards. It also indicates the utility of exploratory methods of identifying bias and suggests paths for future investigation.

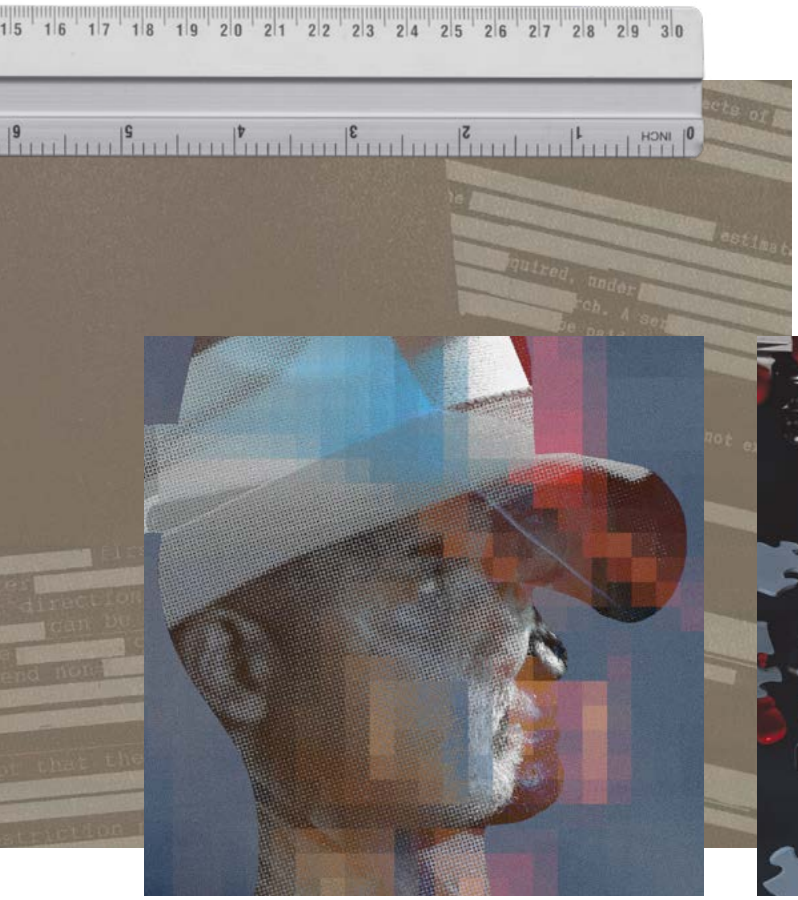
Red-Teaming Guidelines for Generative AI

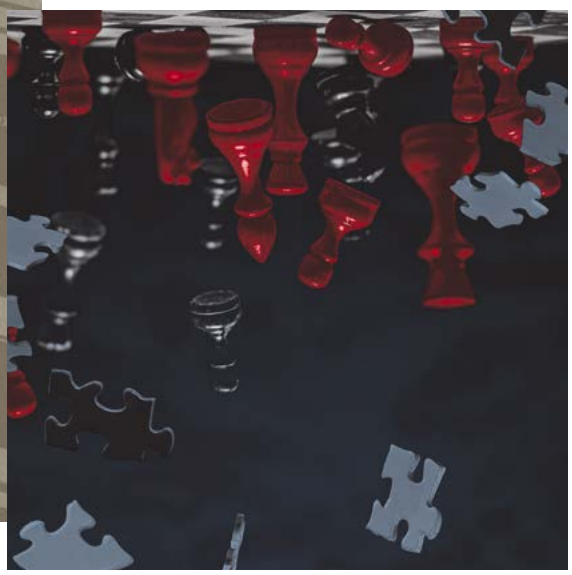
In AI red-teaming, testers emulate the exploitation of AI systems to find flaws and vulnerabilities. Faced with the broad risk surface of ML models, many champion red-teaming as a powerful way to mitigate safety, security, and trustworthiness concerns. However, the practice is poorly defined and its efficacy poorly understood. To determine the robustness of AI red-teaming, Carnegie Mellon University researchers led by the SEI's Michael Feffer and Anusha Sinha conducted an award-winning literature survey to characterize the practice's current scope, structure, and criteria.

They found that while red-teaming can identify risks and help evaluate the safety and robustness of generative models, it is not a comprehensive method and cannot guarantee safety. The practice is also inconsistently scoped and structured, with no consensus on evaluation team composition, threat models, resources, risks considered, or reporting and mitigation processes. The researchers proposed essential criteria to guide more effective AI red-teaming practices.

The New Edge of Generative AI

The edge of the field of generative AI is shifting to the tools and techniques for evaluating and mitigating the technology's risks. The three pillars of AI Engineering—scalable, operator-centered, and robust and secure—informed SEI research into these techniques to further ensure the benefits of AI and LLMs outweigh any risks for high-sensitivity, high-consequence domains.



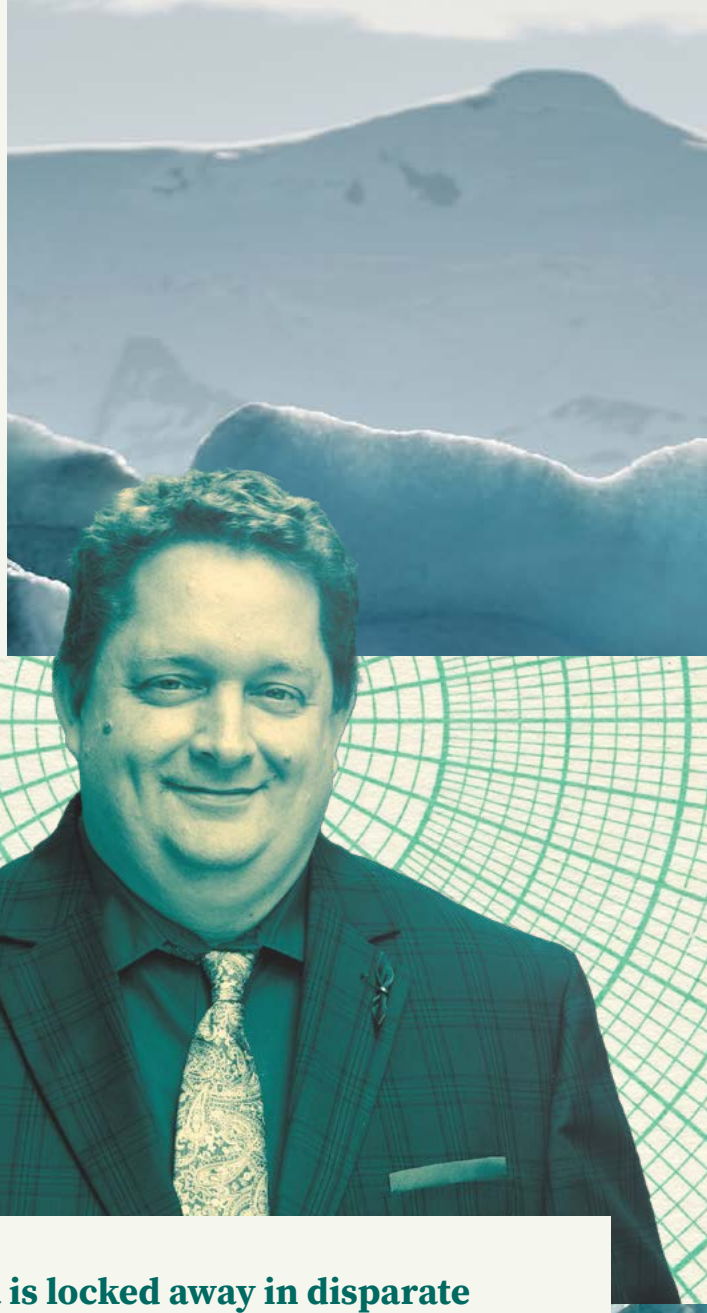


Polar Unlocks DevSecOps Data in Highly Regulated Environments to Improve Operational Decisions

Modern DevSecOps processes create a wealth of data that software producers can use to improve their development operations. However, traditional data-collection techniques obscure the full picture, limiting an organization's ability to leverage its data fully. To address this challenge, the SEI developed Polar, a secure and scalable framework that enables access to all of an organization's DevSecOps data to inform and streamline operational decision making and process improvement, even in highly regulated environments.

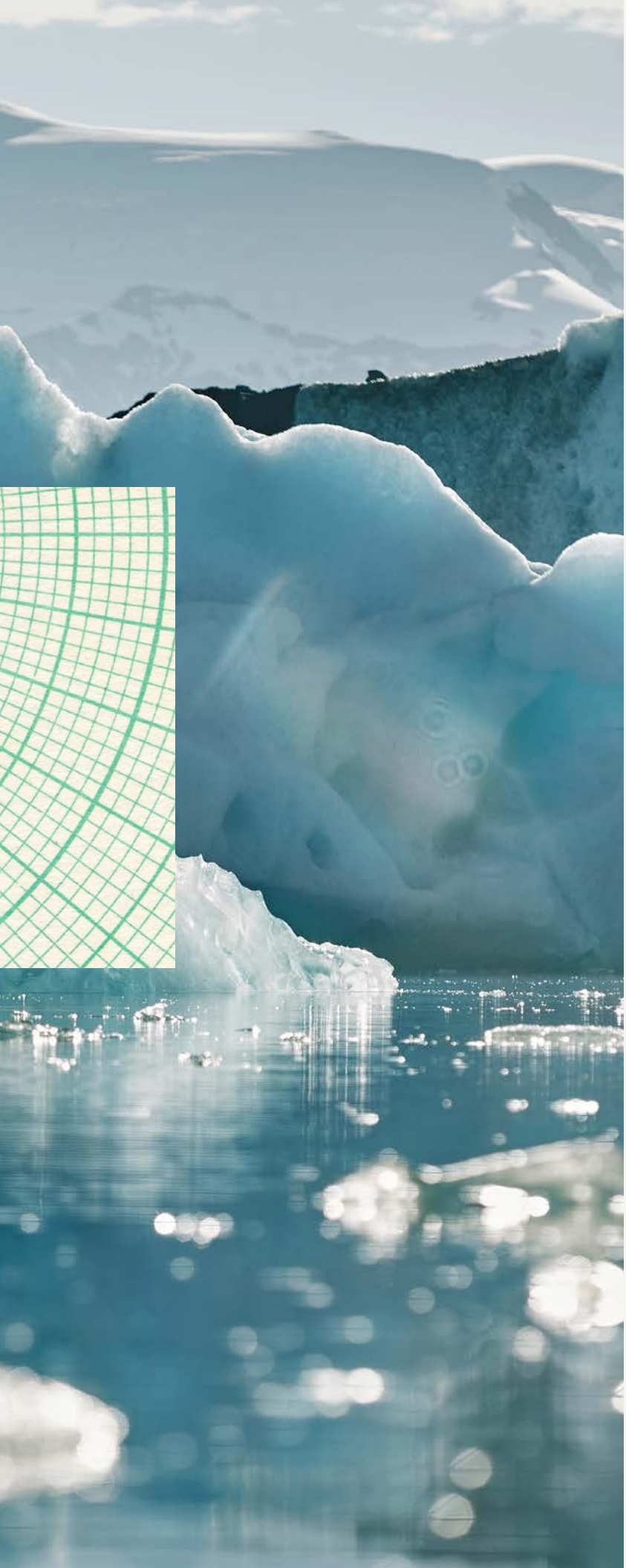
DevSecOps practices can help solve difficult service problems related to resilience, security, scale, and agility. But these practices may lead to complex deployment pipelines that are built from many different solutions and tools, each of which comes with its own inherent complexity and cost to adopt. The number and types of stakeholders who require information about the DevSecOps pipeline can be broad. They need different data from different systems and have different ways to access it. There may be no obvious way to use the information in one system to help answer questions and solve problems.

"The problem is complexity," said project lead David Shepard. "Data is locked away in disparate systems, and combining the data in meaningful ways often means custom application development. One-off solutions don't maximize the value of an organization's data because they're focused on a specific problem domain that is often not aligned with the needs of decision makers."



"Data is locked away in disparate systems, and combining the data in meaningful ways often means custom application development."

DAVE SHEPARD, Senior Engineer, SEI Software Solutions Division



Released in April 2024, the Polar tool dynamically maps the relationships in complex DevSecOps infrastructures and provides visibility into components that previously seemed unrelated. This kind of visibility can help users diagnose and track down problems when they arise. “The information can be used to build automation, monitoring, and alerting,” said Joseph Yankel, senior engineer at the SEI. “It can also help discover cost centers, reduce duplication, visualize end-to-end tool integration, manage licensing, and deliver additional insights.”

A knowledge graph is the core of the Polar architecture. It stores and manages data, using nodes containing organizational data and edges that build meaning between different types of data, enabling intuitive query and analysis. Polar’s schema can be changed at any time without a data migration, permitting the design to flex with evolving operating environments. Designed for highly regulated environments, Polar utilizes a publisher–subscriber architecture with mutual transport layer security for encrypted communications. Polar provides a

- framework for gathering observable data
- data model for organizing observations
- query engine for asking questions of the combined data
- distributable and repeatable environment for developing and testing software
- shareable development methodology for building secure and resilient software

Polar unlocks data that is captured by disparate tools within an organization, helping to answer complex questions about performance and security that are crucial for decision-making and agility in the face of threats.

> **The SEI encourages users to try Polar, available on GitHub at github.com/cmu-sei/polar, and provide feedback.**

LASTING IMPACT

SEI Core Capabilities Help Launch the F-35

The F-35 Lightning II Joint Strike Fighter has been one of the Defense Department's most complex weapons system acquisitions. The SEI started advising the F-35 Joint Program Office (JPO) in 2018, the same year an early F-35 flew in combat for the first time. Since then, SEI researchers and engineers have provided the JPO their expertise in some of the institute's core mission capabilities. The SEI's impact on the F-35 program continued into 2024 as a new batch of modernized planes started rolling onto tarmacs.

In 2018, the F-35 JPO was facing challenges adapting its internal processes to meet production plans. The SEI's first and perhaps most important task was to help the JPO and the program's contractors implement Agile and DevSecOps practices at scale. The practices applied not just to software development but also to contracting and administrative workflows. "We don't just work on software delivery, we help with the whole ecosystem around it," said Will Hayes, the SEI's Agile transformation team lead and technical lead for the engagement with the F-35 JPO.

Senior SEI technical staff were embedded with the JPO to speed tasking and real-time technical support for Lean and Agile systems engineering and software sustainment policy and practice. During the COVID-19 pandemic, the SEI helped sustain the program's Agile transformation by creating the Agile Virtual Schoolhouse. Program staff and international partners used this repository of online, self-paced modules, which were informed by the JPO's own experiences. The Schoolhouse was just one of many customized trainings the SEI delivered for the JPO and its contractors.

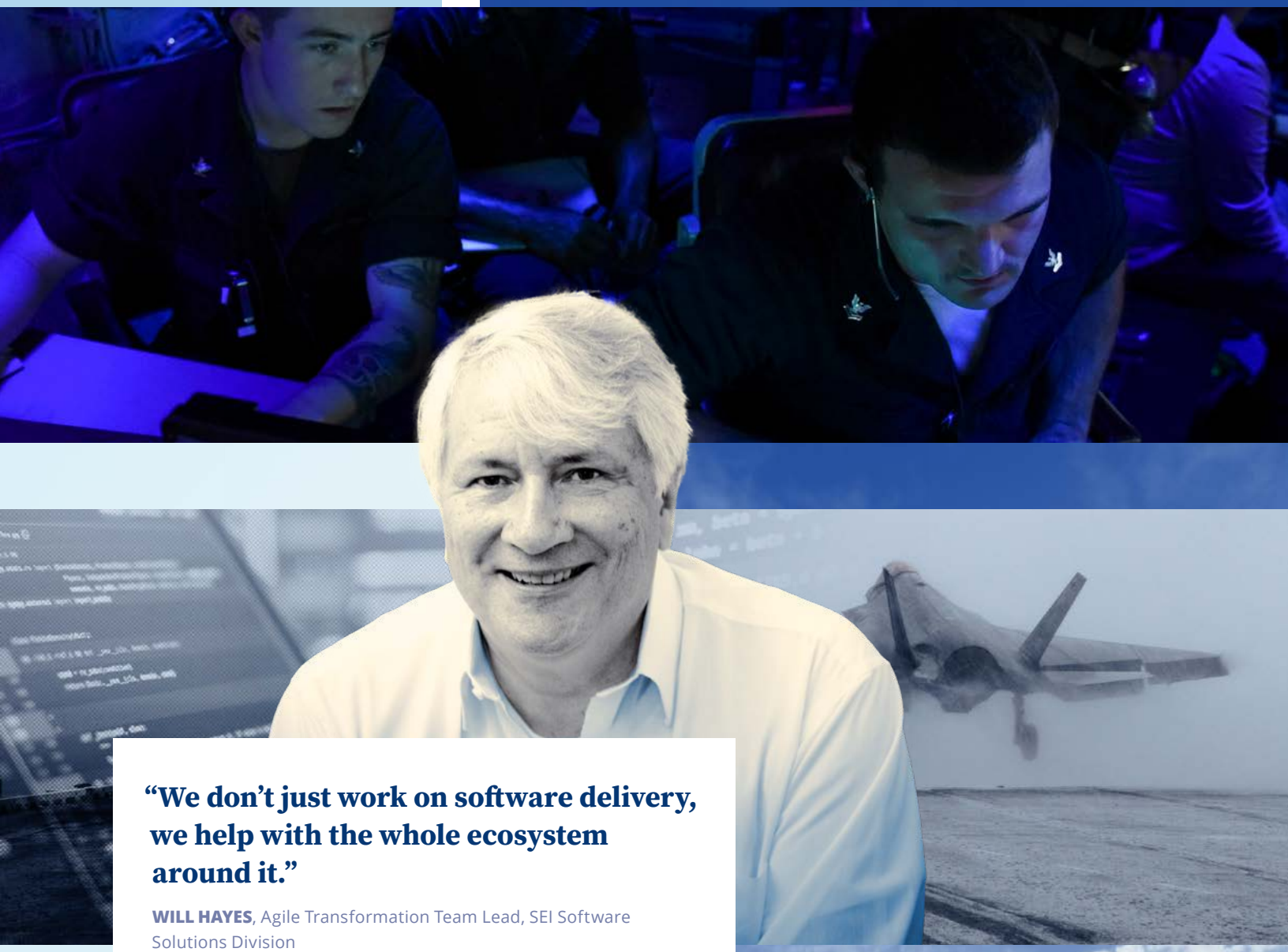
Software modernization was another early thrust of SEI work. Over the course of the F-35 program, software development in the Department of Defense had been transitioning from the waterfall style of system development to a faster, iterative style. In 2019, the SEI engaged with a JPO working group to produce a 10-year software modernization strategy and roadmap. It positioned the JPO and its contractors to focus on more efficient software capability delivery.

More recently, SEI researchers have participated in independent review teams (IRTs) to help break technical logjams. As part of the program's Tech Refresh 3, which enables the F-35's Block 4 capabilities, the SEI led an IRT on the aircraft's software architecture on behalf of the Secretary of the Air Force. SEI experts on another IRT helped identify software issues that had idled about 100 runway-ready jets.

In each engagement with the F-35 JPO and its contractors, the SEI has built up the program's own capabilities. In March 2024, six years after the SEI first met with the JPO, the Pentagon announced that the F-35 was approved for full-rate production. Later that year, planes started being delivered as they came off the assembly line.

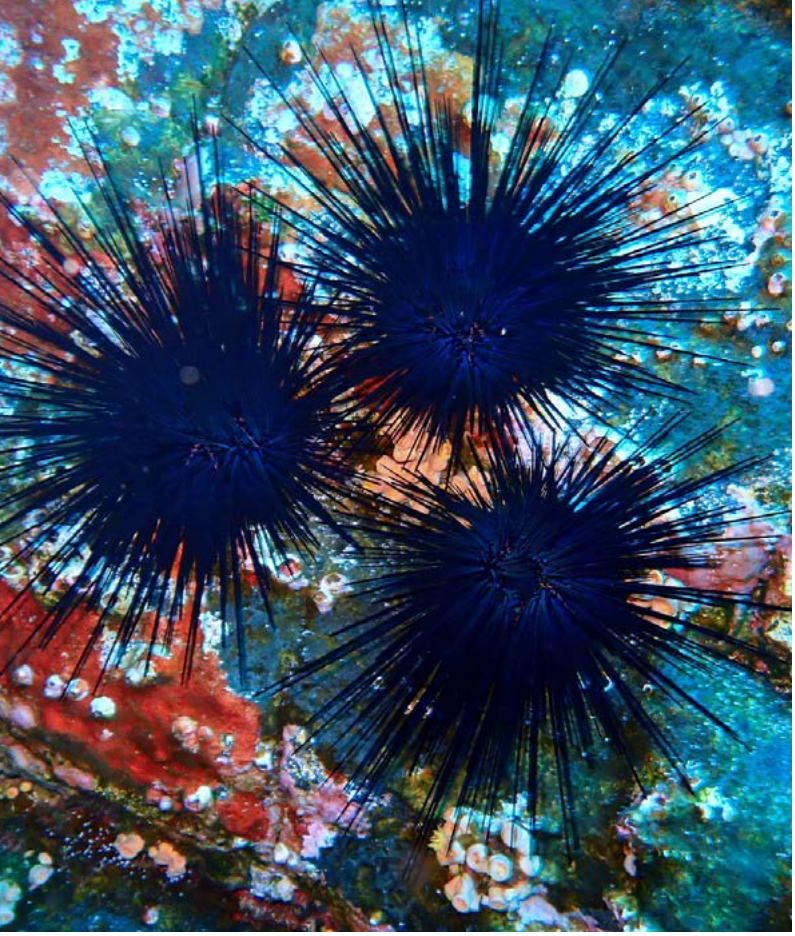
The SEI's placement at the intersection of government and industry enabled the institute to transition more than three decades of research and development in software engineering, Agile practices, and defense acquisition to this critical weapons acquisition.

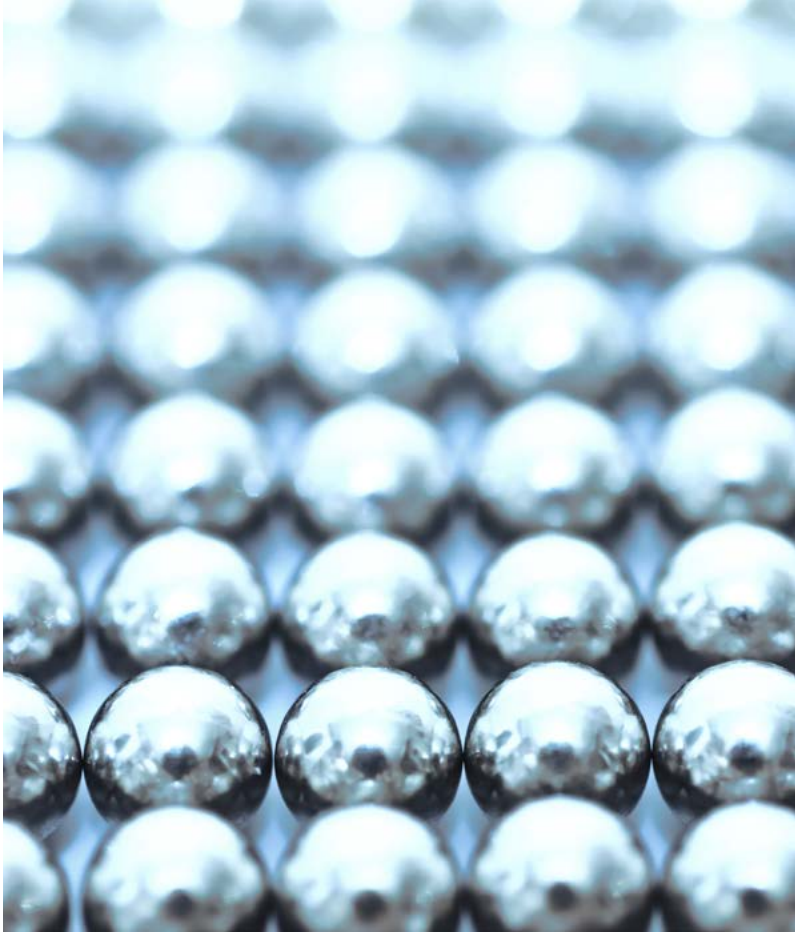
Photos: (top) U.S. Navy, *Mass Communication Specialist 1st Class Brian M. Brooks*; (middle) U.S. Navy, *Mass Communication Specialist 1st Class Brian M. Wilbur*; (bottom) U.S. Air Force, *Tech. Sgt. Alexander Cook*



“We don’t just work on software delivery, we help with the whole ecosystem around it.”

WILL HAYES, Agile Transformation Team Lead, SEI Software Solutions Division





LASTING IMPACT

The CERT Secure Coding Initiative

Twenty years ago, software security researchers were struggling with a troubling observation: Software vulnerabilities with known solutions continued to be reported. The CERT Secure Coding Initiative was formed at the SEI to discover what programmers could do about it. The initiative would go on to pioneer secure coding, a field that has made a lasting impact in software security and resilience.

By the early 2000s, the software community had been studying and categorizing vulnerabilities for years, but guidance for prevention was basic and left much to programmers' interpretation. Existing guidance reflected the perspective of how computers interpret and process software, not how programmers should write it, and it lacked any clear recommendations for different programming languages.

The SEI was uniquely suited to address this problem. SEI researchers could take a bird's-eye view by analyzing vulnerabilities reported to the CERT/CC and seek patterns in code. They could also dive deeply into programming language details and software analysis to unpack specific vulnerabilities, their causes, and their mitigations.

The Secure Coding Initiative developed guidance and training for developers on secure coding practices for C and C++, the most prominent languages at the time. This effort resulted in 2005's *Secure Coding in C and C++* and its second edition.

The work progressed into formalized descriptions of rules and recommendations for secure coding in C, developed through a broad-based, collaborative effort with the software development and software security communities. The result was *The CERT C Secure Coding Standard*, first published in 2008.

Photo: (left) *Sylvain Le Bris*

(left to right) Dan Plakosh, Archie Andrews, David Svoboda, Dean Sutherland, Brad Rubbo, Jason Rafael, Robert Seacord, Chad Dougherty

"SEI CERT standards will forever be a vital part of securing code."

ROBERT SCHIELA, Deputy Technical Director, Cybersecurity Foundations, SEI CERT Division

Since then, Robert Seacord, David Svoboda, and other SEI authors and collaborators have written secure coding standards for C++, Java, Perl, and Android. The SEI continues to revise the standards in response to language updates and programmer feedback.

The *SEI CERT Coding Standards* have had wide impact. Companies such as Cisco and Oracle have adopted them. The *SEI CERT C Coding Standard* formed the basis for the ISO/IEC standard on C secure coding rules. All major static analysis tool vendors support checking for standards adherence. Secure coding courses, such as those pioneered at the SEI's CERT Division, are now incorporated into university curricula.

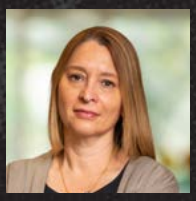
As more AI is applied to software development, the standards are now being used to train automated analysis tools to detect weaknesses in source code. One example is CodeQL, GitHub's code analysis engine developed to automate security checks. GitHub advanced security specialist Jose Palafox noted, "Microsoft and GitHub implemented checks for CERT C and C++ into CodeQL. This enables auto manufacturers, other regulated industries, and open source enthusiasts to demonstrate meeting the standard through continuous code scanning during the software development lifecycle."

SEI research and development on secure coding continues. Its experts are studying newer, memory-safe languages, such as Rust, and expanding into other aspects of secure coding: using large language models to augment software development and analysis, automatically repairing code, and detecting malicious information flow in source code. The SEI participates in the ISO C committee and contributes to security improvements of the ISO C language standard.

Use of the *SEI CERT Coding Standards* embeds best practices into the foundation of software engineering, making software less vulnerable by reducing system attack surfaces. As more tools implement the standards, their use will become a more natural part of the software product development lifecycle. The SEI's Cybersecurity Foundations deputy director and former Secure Coding technical manager Robert Schiela noted, "SEI CERT standards will forever be a vital part of securing code."

Learn more about the *SEI CERT Coding Standards* at **securecoding.cert.org**.


Anita Carleton


Grace Lewis

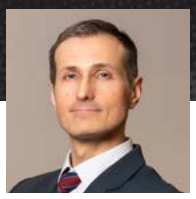

Bjorn Andersson

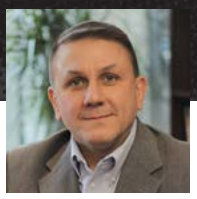

Linda Parker Gates


Anandi Hira


Michael Mattarock


Tracy Bills


Roman Danyliw


Jason Hawk


Angel Hueca


Craig Lewis


Dan Plakosh

Professional Organization Leadership Promotes National Defense Mission

The active participation of SEI staff members in professional societies and organizations helps the SEI serve its Department of Defense (DoD) sponsor, external customers, and the nation. In 2024, many SEI researchers held leadership positions in professional organizations.

Professional Society Leadership

Anita Carleton, elected chair of the *IEEE Software* advisory board

Grace Lewis, elected 2026 president of the IEEE Computer Society

Conference Committee Leadership

Bjorn Andersson, journal track co-chair and keynote session chair, 2024 Ada-Europe International Conference on Reliable Software Technologies

Linda Parker Gates, conference chair, International Association for Strategy Professionals (IASP) 2024

Anandi Hira, general chair, 2023 Boehm Center for Systems and Software Engineering COCOMO & Practical Software and Systems Measurement Forum

Grace Lewis, program co-chair, 2024 Conference on AI Engineering (CAIN)

Michael Mattarock, AI session chair, 2024 Aerospace TechWeek Americas

Leigh Metcalf, practitioner session program chair, 2023 IEEE Secure Development Conference

Jasmine Ratchford, co-chair, Nonlinear Dynamics II session at the 2024 IEEE Conference on Decision and Control

Carol Smith, keynote chair, 13th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2024)

Hasan Yasar, general chair, 43rd International Conference on Conceptual Modeling (ER 2024)

Robin Yeman, conference track chair, 2023 National Defense Industrial Association (NDIA) Systems Engineering, Agile Delivery for Agencies, Programs & Teams (ADAPT)

Mark T. Zajicek, co-chair, conference program committee of the 2024 Open Cyber Security Conference

Standards Bodies and Other Organizational Leadership

Tracy Bills, chair, Board of Directors of the Forum of Incident Response and Security Teams (FIRST)

Roman Danyliw, chair, Internet Engineering Task Force (IETF); director, board of the IETF Administration LLC; General Area director, IETF Internet Engineering Steering Group

Jason Hawk, chair, Federally Funded Research and Development Centers and University Affiliated Research Centers (FFRDC/UARC) Security Council


Leigh Metcalf

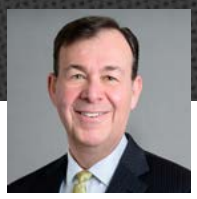

Jasmine Ratchford

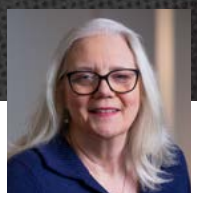

Carol Smith


Hasan Yasar

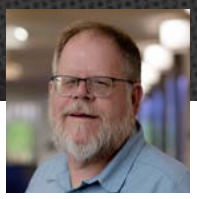

Robin Yeman


Mark T. Zajicek

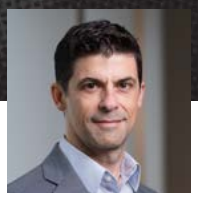

Greg Touhill


Laurie Tyzenhaus


Sharon Mudd


Tim Shimeall


Marisa Midler


Gabe Moreno

Angel Hueca, vice chair, Information Technology Security Community Steering Committee, American Society for Industrial Security (ASIS) International

Craig Lewis, co-chair, DoD Defense Industrial Base Small Business Working Group

Dan Plakosh, secretariat, ISO/IEC C standards committee

Greg Touhill, board of directors, Internet Security Alliance

Laurie Tyzenhaus, co-chair, Standards Special Interest Group, FIRST Standards Committee

Hasan Yasar, elected vice-chair of the Open Group Security Forum; chair, FFRDC Advanced Technology Academic Research Center DevSecOps Working Group; co-chair, IEEE 2675 DevOps Standard Development Working Group

Editorships

Angel Hueca, **Sharon Mudd**, **Tim Shimeall**, guest editors, Association for Computing Machinery (ACM) *Digital Threats: Research and Practice*, December 2023

Marisa Midler, guest editor, *SANS OUCH!* newsletter, June 2024

Gabe Moreno, associate editor, *ACM Transactions on Autonomous and Adaptive Systems*

Destiney Plaza, guest editor, *SANS OUCH!* newsletter, July 2024

Professional Awards

Linda Parker Gates, International Association for Strategy Professionals' Janice Laureen Award for Outstanding Service

Greg Touhill, Air Force Cyberspace Operations & Support Hall of Fame, Air Force Cyberspace and Air Traffic Control Association

Carol Woody and the IEEE P2933 working group, IEEE Standards Association's Emerging Technology Award for Standard on Clinical Internet of Things Data and Device Interoperability with Trust, Identity, Privacy, Protection, Safety, Security


Destiney Plaza


Carol Woody

Leadership

CMU Leadership

Farnam Jahanian
President

James H. Garrett, Jr.
Provost and Chief Academic Officer

Theresa Mayer
Vice President for Research

SEI Executive Leadership

Paul Nielsen
Director and Chief Executive Officer

David Thompson
Deputy Director and Chief Operating Officer

Tom Longstaff
Chief Technology Officer

Anita Carleton
Director, Software Solutions Division

Gregory J. Touhill
Director, CERT Division

Matt Gaston
Director, Artificial Intelligence Division

Heidi Magnelia
Chief Financial Officer

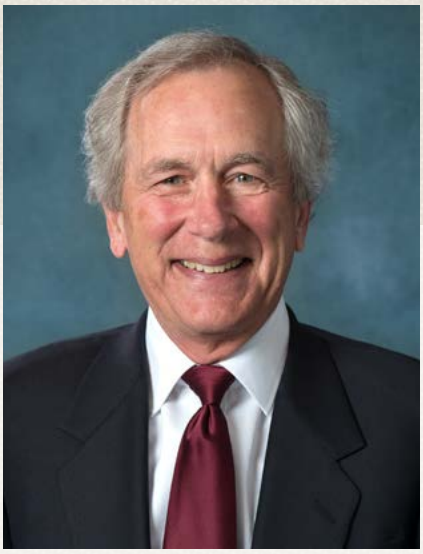
Mary Catherine Ward
Chief Strategy Officer

Sandra Noonan
General Counsel

Board of Visitors

The SEI Board of Visitors advises the Carnegie Mellon University president, university provost, and SEI director on SEI plans and operations. The board monitors SEI activities, provides reports to the president and provost, and makes recommendations for improvement.

Russell Crockett
Cofounder of Aeon Blue Technologies; Principal and Owner of RTC Energy LLC; Trustee, Carnegie Mellon University



Philip Dowd
Private investor; former Senior Vice President, SunGard Data Systems; Emeritus Trustee, Carnegie Mellon University

John M. Gilligan
Chair, SEI Board of Visitors; President and CEO, Center for Internet Security (CIS); former President and COO, Schafer Corporation; former President, Gilligan Group; former Senior Vice President and Director, Defense Sector of SRA International; former CIO for the Department of Energy and the U.S. Air Force

J. Michael McQuade

Director of the Program on Emerging Technology, Scientific Advancement and Global Policy at the Belfer Center for Science and International Affairs in the Harvard Kennedy School; Special Advisor to the President of Carnegie Mellon University

Laura Richardson

General, retired, U.S. Army. Former: Commander, U.S. Southern Command; Commanding General, U.S. Army North; Dep. Commanding General, U.S. Army Forces Command; Chief of Army Legislative Liaison to Congress; Dep. Chief of Staff for Communications, HQ International Security Assistance Force, Afghanistan; Dep. Commanding General, 1st Cavalry Div.; Commanding General, U.S. Army Operational Test Command

Cedric T. Wins

Superintendent, Virginia Military Institute; Major General, retired, U.S. Army; former Commanding General of the Army Combat Capabilities Development Command (CCDC); former Commander, Army Research, Development, and Engineering Command (RDECOM); former Director of Force Development in the Army Office of the Deputy Chief of Staff

Key Publications and Conference Presentations

Articles

Cai, Yuanfang and Kazman, Rick. Software Design Analysis and Technical Debt Management Based on Design Rule Theory. *Information and Software Technology*. Volume 164. December 2023. **https://doi.org/10.1016/j.infsof.2023.107322**

Cara, Marçal Comajoan; Dahale, Gopal Ramesh; Dong, Zhongtian; Forestano, Roy T.; Gleyzer, Sergei; Justice, Daniel; Kong, Kyoungchul; Magorsch, Tom; Matchev, Konstantin T.; Matcheva, Katia; & Unlu, Eyup B. Quantum Vision Transformers for Quark–Gluon Classification. *Axioms*. Volume 13. Number 5. Article 323. May 13, 2024. **https://doi.org/10.3390/axioms13050323**

Cyphert, Amy; Perl, Samuel J.; & Tu, S. Sean. AI Cannibalism and the Law. *Colorado Technology Law Journal.* Volume 22. Issue 2. July 8, 2024. Pages 301–316. **https://ctlj.colorado.edu/?p=1280**

Dong, Zhongtian; Cara, Marçal Comajoan; Dahale, Gopal Ramesh; Forestano, Roy T.; Gleyzer, Sergei; Justice, Daniel; Kong, Kyoungchul; Magorsch, Tom; Matchev, Konstantin T.; Matcheva, Katia; & Unlu, Eyup B. $\mathbb{Z}_2 \times \mathbb{Z}_2$ Equivariant Quantum Neural Networks: Benchmarking against Classical Neural Networks. *Axioms*. Volume 13. Number 3. Article 188. March 13, 2024. **https://doi.org/10.3390/axioms13030188**

Đorđević, Milica; Albonico, Michel; Lewis, Grace A.; Malavolta, Ivano; & Lago, Patricia. Computation Offloading for Ground Robotic Systems Communicating Over WiFi – An Empirical Exploration on Performance and Energy Trade-Offs. *Empirical Software Engineering.* Volume 28. October 2023. **https://doi.org/10.1007/s10664-023-10351-6**

Ernst, Neil A.; Klein, John; Bartolini, Marco; Coles, Jeremy; & Rees, Nick. Architecting Complex, Long-Lived Scientific Software. *Journal of Systems and Software.* Volume 204. October 2023. **https://doi.org/10.1016/j.jss.2023.111732**

Flynn, Lori & Klieber, Will. Using LLMs to Automate Static-Analysis Adjudication and Rationales. *CrossTalk: Journal of Defense Software Engineering.* August 2024. **https://afscsoftware.dso.mil/crossTalkIssues/AI_Part_2_Aug_2024.pdf**

Forestano, Roy T.; Cara, Marçal Comajoan; Dahale, Gopal Ramesh; Dong, Zhongtian; Gleyzer, Sergei; Justice, Daniel; Kong, Kyoungchul; Magorsch, Tom; Matchev, Konstantin T.; Matcheva, Katia; & Unlu, Eyup B. A Comparison between Invariant and Equivariant Classical and Quantum Graph Neural Networks. *Axioms*. Volume 13. Number 3. Article 160. February 29, 2024. **https://doi.org/10.3390/axioms13030160**

Fotiadis, Filippos; Kanellopoulos, Aris; Vamvoudakis, Kyriakos G.; & Hugues, Jérôme. On the Effect of Clock Offsets and Quantization on Learning-Based Adversarial Games. *Automatica*. Volume 167. Article 111762. September 2024. **https://doi.org/10.1016/j.automatica.2024.111762**

Fungprasertkul, Suwichak; Bahsoon, Rami; & Kazman, Rick. Technical Debt Monitoring Decision Making with Skin in the Game. *ACM Transactions on Software Engineering and Methodology.* Volume 33. Issue 7. Article 168. August 26, 2024. **https://doi.org/10.1145/3664805**

Hugues, Jérôme. Mechanization of the Ravenscar Profile in Coq. *Ada User Journal.* Volume 44. Number 2. June 2023. Pages 157–160. **https://www.ada-europe.org/archive/auj/auj-44-2-withcovers.pdf#page=67**

Morrison, Katelyn; Spitzer, Philipp; Turri, Violet; Feng, Michelle; Kühl, Niklas; & Perer, Adam. The Impact of Imperfect XAI on Human-AI Decision-Making. *Proceedings of the ACM on Human-Computer Interaction.* Volume 8. Issue CSCW1. Article 183. April 26, 2024. **https://doi.org/10.1145/3641022**

Paradis, Carlos; Kazman, Rick; & Tamburri, Damian. Analyzing the Tower of Babel with Kaiaulu. *Journal of Systems and Software.* Volume 210. April 2024. **https://doi.org/10.1016/j.jss.2024.111967**

Robert, John E.; Ivers, James; Schmidt, Doug; Ozkaya, Ipek; & Zhang, Shen. Future of Software Engineering and Acquisition with Generative AI. *CrossTalk: The Journal of Defense Software Engineering.* May 2024. Pages 26–43. **https://community.apan.org/wg/crosstalk/m/documents/464157**

Singhoff, Frank; Hugues, Jérôme; Tran, Hai Nam; Bardaro, Gianluca; Blouin, Dominique; Bozzano, Marco; Denzler, Patrick; Dissaux, Pierre; Senn, Eric; Xu, Xiong; & Yang, Zhibin. ADEPT 2022 Workshop: A Summary of Strengths and Weaknesses of the AADL Ecosystem. *Ada User Journal.* Volume 44. Number 2. June 2023. Pages 125-128. **https://beru.univ-brest.fr/svn/CHEDDAR/trunk/docs/publications/adept22.pdf**

Sridhar, Upasana; Tukanov, Nicholai; Binder, Elliott; Low, Tze Meng; McMillan, Scott; & Schatz, Martin D. SMaLL: Software for Rapidly Instantiating Machine Learning Libraries. *ACM Transactions on Embedded Computing Systems.* Volume 23. Issue 3. May 13, 2024. **https://doi.org/10.1145/3607870**

Tucker, Brett. Building a New Assessment: How to Assess Ransomware Attack Readiness and Recovery. *CrossTalk: The Journal of Defense Software Engineering.* November 2023. **https://community.apan.org/wg/crosstalk**

Unlu, Eyup B; Cara, Marçal Comajoan; Dahale, Gopal Ramesh; Dong, Zhongtian; Forestano, Roy T.; Gleyzer, Sergei; Justice, Daniel; Kong, Kyoungchul; Magorsch, Tom; Matchev, Konstantin T.; & Matcheva, Katia. Hybrid Quantum Vision Transformers for Event Classification in High Energy Physics. *Axioms.* Volume 13. Number 3. Article 187. March 13, 2024. **https://doi.org/10.3390/axioms13030187**

von Stein, Meriel; Shriver, David; & Elbaum, Sebastian. DeepManeuver: Adversarial Test Generation for Trajectory Manipulation of Autonomous Vehicles. *IEEE Transactions on Software Engineering.* Volume 49. Number 10. October 1, 2023. Pages 4496–4509. **https://doi.org/10.1109/TSE.2023.3301443**

Woody, Carol S. Addressing Today's Software Risks Requires an Assurance Educated Workforce. *Journal of Systemics, Cybernetics and Informatics.* Volume 22. Number 5. 2024. Pages 62–67. **https://doi.org/10.54808/JSCI.22.05.62**

Wrubel, Eileen. Editorial: AI in the DoD: Power, Potential, and Risks. *CrossTalk: The Journal of Defense Software Engineering.* May 2024. Pages 4–6. **https://community.apan.org/wg/crosstalk/m/documents/464157**

Books

Cervantes, Humberto & Kazman, Rick. Designing Software Architectures: A Practical Approach, 2nd Edition. Addison-Wesley Professional, SEI Series in Software Engineering. 2024. 978-0-13-810810-6. **https://insights.sei.cmu.edu/library/designing-software-architectures-a-practical-approach/**

Conference Papers

Andersson, Bjorn; de Niz, Dionisio; & Klein, Mark. A Tool for Satisfying Real-Time Requirements of Software Executing on ARINC 653 with Undocumented Multicore. In *2023 IEEE/AIAA 42nd Digital Avionics Systems Conference (DASC).* November 2023. **https://doi.org/10.1109/DASC58513.2023.10311291**

Athalye, Surabhi; Fotiadis, Filippos; Vamvoudakis, Kyriakos G.; & Hugues, Jérôme. An Output Feedback Game-Theoretic Approach for Defense Against Stealthy GNSS Spoofing Attacks. In *2024 American Control Conference (ACC).* September 2024. **https://doi.org/10.23919/ACC60939.2024.10644369**

Avgeriou, Paris; Ozkaya, Ipek; Chatzigeorgiou, Alexander; Ciolkowski, Marcus; Ernst, Neil A.; Koontz, Ronald J.; Poort, Eltjo; & Shull, Forrest. Technical Debt Management: The Road Ahead for Successful Software Delivery. In *2023 IEEE/ACM International Conference on Software Engineering: Future of Software Engineering (ICSE-FoSE).* March 2024. **https://doi.org/10.1109/ICSE-FoSE59343.2023.00007**

Brower-Sinning, Rachel; Lewis, Grace A.; Echeverría, Sebastián; & Ozkaya, Ipek. Using Quality Attribute Scenarios for ML Model Test Case Generation. In *2024 IEEE 21st International Conference on Software Architecture Companion (ICSA-C).* August 2024. **https://doi.org/10.1109/ICSA-C63560.2024.00058**

Chen, Hong-Mei; Kazman, Rick; Catolino, Gemma; Manca, Massimo; Tamburri, Andrew Damian; & van den Heuvel, Willem-Jan. An Empirical Study of Social Debt in Open-Source Projects: Social Drivers and the "Known Devil" Community Smell. In *57th Hawaii International Conference on System Sciences (HICSS).* January 2024. **https://scholarspace.manoa.hawaii.edu/items/13215152-e131-4d43-929b-50209872b6dd**

Dey, Tapajit; Loungani, Jonathan; & Ivers, James. Smarter Project Selection for Software Engineering Research. In *PROMISE 2024: Proceedings of the 20th International Conference on Predictive Models and Data Analytics in Software Engineering.* July 2024. **https://doi.org/10.1145/3663533.3664037**

Dramko, Luke; Lacomis, Jeremy; Schwartz, Edward J.; Vasilescu, Bogdan; & Le Goues, Claire. A Taxonomy of C Decompiler Fidelity Issues. In *SEC '24: Proceedings of the 33rd USENIX Conference on Security Symposium.* August 2024. **https://dl.acm.org/doi/10.5555/3698900.3698922**

Fotiadis, Filippos; Kanellopoulos, Aris; Vamvoudakis, Kyriakos G.; & Hugues, Jérôme. Poisoning Actuation Attacks against the Learning of an Optimal Controller. Pages 4838–4843. In *ACC 2024 American Control Conference*. September 2024. **https://doi.org/10.23919/ACC60939.2024.10644755**

Gallagher, Shannon K.; Ratchford, Jasmine; Brooks, Tyler; Brown, Byron P.; Heim, Eric; Nichols, William R.; McMillan, Scott; Rallapalli, Swati; Smith, Carol J.; VanHoudnos, Nathan; Winski, Nick; & Mellinger, Andrew O. Assessing LLMs for High Stakes Applications. In *ICSE-SEIP '24: Proceedings of the 46th International Conference on Software Engineering: Software Engineering in Practice*. May 2024. **https://doi.org/10.1145/3639477.3639720**

Grimes, Keltin; Abidi, Collin; Frank, Cole; & Gallagher, Shannon. Gone but Not Forgotten: Improved Benchmarks for Machine Unlearning. In *7th Deep Learning Security & Privacy Workshop, co-located with the 45th IEEE Symposium on Security & Privacy.* May 2024. **https://dlsp2024.ieee-security.org/papers/dls2024-final3.pdf**

Healy, Robert; Conboy, Kieran; Dey, Tapajit; Lewzey, Edwin; & Fitzgerald, Brian. Comparing Stability and Sustainability in Agile Systems. In *Agile Processes in Software Engineering and Extreme Programming, XP 2024*. May 2024. **https://doi.org/10.1007/978-3-031-61154-4_9**

Hira, Anandi. Capability-Based Software Cost Estimation (CaBSCE): Proposing a New Method to Estimate Software Costs. In *Proceedings of the Twenty-First Annual Acquisition Research Symposium*. April 2024. **https://dair.nps.edu/retrieve/e3b0a02e-d1fd-4eb0-a53a-1e66bf80ad4d/SYM-AM-24-106.pdf**

Hristozov, Anton Dimov & Matson, Eric. Dynamic Architecture Description Language for System of Systems. In *2024 IEEE International Systems Conference (SysCon)*. June 2024. **https://doi.org/10.1109/SysCon61195.2024.10553612**

Hristozov, Anton Dimov. Fast and Secure Mission Description, Validation and Deployment for Safety-Critical Operations. In *2024 IEEE International Systems Conference (SysCon)*. June 2024. **https://doi.org/10.1109/SysCon61195.2024.10553550**

Järvenpää, Hel; Lago, Patricia; Bogner, Justus; Lewis, Grace; Muccini, Henry; & Ozkaya, Ipek. Synthesis of Green Architectural Tactics for ML-Enabled Systems. In *ICSE-SEIS'24: Proceedings of the 46th International Conference on Software Engineering: Software Engineering in Society*. June 2024. **https://doi.org/10.1145/3639475.3640111**

Kimmerer, Raye; Mattson, Timothy G.; McMillan, Scott; Brock, Benjamin; Welch, Erik; Pelletier, Michel; & Moreira, Jose E. The GraphBLAS 3.0 Project. In *2024 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW 2024).* May 2024. **https://doi.ieeecomputersociety.org/10.1109/IPDPSW63119.2024.00099**

Magalhães, José M.; Zhai, Lijing; Fotiadis, Filippos; Kanellopoulos, Aris; Vamvoudakis, Kyriakos G.; & Hugues, Jérôme. Real-Time and Experimental Reactive and Proactive Defense in a Multi-Agent Scenario. In *AIAA SciTech Forum and Exposition 2024*. January 2024. **https://doi.org/10.2514/6.2024-0343**

Malich, Stefan; Cervantes, Humberto; & Kazman, Rick. Developing and Applying an Essence-based Description of the Attribute-Driven Design Method. In *2024 IEEE/ACM International Workshop on Designing Software (Designing).* April 2024. **https://www.computer.org/csdl/proceedings-article/designing/2024/056300a021/209sHmCVlp6**

Mead, Nancy; Woody, Carol; & Hissam, Scott. Open Source Software (OSS) Transparency for DoD Acquisition. In *Annual Acquisition Research Symposium Proceedings & Presentations*. May 2024. **https://dair.nps.edu/handle/123456789/5159**

Moore, Andrew P.; Grzenia, Stephanie; Morales, Jose; Ickes, Cody; Fallon, Joshua; & Casey, William. Game-Theoretic Modeling and Analysis of Insider Compliance with Security Policy. In *WRIT 2023: 8th Workshop on Research for Insider Threats.* December 2023. **https://www.acsac.org/2023/workshops/writ/WRIT-Moore.pdf**

Morales, Jose Andre; Antunes, Luiz; Earl, Patrick; Edman, Robert; Hamed, Jeff; Reynolds, Douglas; Maffey, Katherine R.; Yankel, Joseph; & Yasar, Hasan. Insights on Implementing a Metrics Baseline for Post-Deployment AI Container Monitoring. In *ICSSP '24: Proceedings of the 2024 International Conference on Software and Systems Processes*. September 2024. **https://doi.org/10.1145/3666015.3666018**

Papke, Barry; Kratzke, Ronald; Span, Martin; & Shevchenko, Nataliya. Enabling FuSE Security Objectives through Cyber Survivability Methods. In *34th Annual INCOSE International Symposium (IS)*. September 2024. **https://doi.org/10.1002/iis2.13133**

Paradis, Carlos V.; Kazman, Rick; & Peruma, Anthony. Making Team Projects with Novices More Effective: An Experience Report. In *57th Hawaii International Conference on System Sciences (HICSS)*. January 2024. **https://dblp.org/rec/conf/hicss/ParadisKP24**

Pitstick, Kevin; Novakouski, Marc; Lewis, Grace A.; & Ozkaya, Ipek. Defining a Reference Architecture for Edge Systems in Highly-Uncertain Environments. In *2024 IEEE 21st International Conference on Software Architecture Companion (ICSA-C).* August 2024. **https://doi.org/10.1109/ICSA-C63560.2024.00064**

Rebello, Sasha; Sunil, Smriti; Lewis, Grace; & Shaikh, Shainila. FortiShare: A Predictive Cloud File Sharing System for Detecting Intrusions. In *2023 6th International Conference on Advances in Science and Technology (ICAST)*. March 2024. **https://doi.org/10.1109/ICAST59062.2023.10454961**

Robinson, Katherine-Marie; Turri, Violet; Smith, Carol J.; & Gallagher, Shannon K. Tales from the Wild West: Crafting Scenarios to Audit Bias in LLMs. In *1st HEAL Workshop at CHI Conference on Human Factors in Computing Systems*. May 2024. **https://heal-workshop.github.io/chi2024_papers/24_tales_from_the_wild_west_craft.pdf**

Rodman, Christopher; Kraus, Breanna; & Novak, Justin. SOC Service Areas: Identification, Prioritization, and Implementation. In *Workshop on SOC Operations and Construction (WOSOC) 2024*, co-located with *Network and Distributed System Security (NDSS) Symposium 2024*. March 2024. **https://dx.doi.org/10.14722/wosoc.2024.23001**

Schenker, Alfred; Guertin, Nikolas H.; Schmidt, Douglas. A Model for Evaluating the Maturity of a Modular Open Systems Approach. In *Proceedings of the Twenty-First Annual Acquisition Research Symposium*. April 2024. **https://dair.nps.edu/bitstream/123456789/5140/1/SYM-AM-24-077.pdf**

Smith, Carol J. Augmenting Intelligence: Ethical Challenges in the Age of AI. In *SIGUCCS '24: Proceedings of the 2024 ACM SIGUCCS Annual Conference*. March 2024. **https://doi.org/10.1145/3599732.3641496**

Smith, Carol J. Trustworthy by Design. 1–4 In *ICSE '24: Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*. May 2024. **https://doi.org/10.1145/3597503.3649400**

Smith, Justin & Hayes, William. Independent Verification & Validation (IV&V) for Agile Developed Projects. In *2024 IEEE Aerospace Conference*. May 2024. **https://doi.org/10.1109/AERO58975.2024.10521415**

Smith, Justin. The Value of an Agile Approach to Independent Verification and Validation (IV&V) for Acquisition. In *Proceedings of the Twenty-First Annual Acquisition Research Symposium*. April 2024. **https://dair.nps.edu/bitstream/123456789/5101/1/SYM-AM-24-033.pdf**

Snyder, Shay; Gobin, Derek; Clerico, Victoria; Risbud, Sumedh R.; & Parsa, Maryam. Parallelized Multi-Agent Bayesian Optimization in Lava. In *2024 International Conference on Neuromorphic Systems (ICONS)*. December 2024. **https://doi.org/10.1109/ICONS62911.2024.00051**

Turri, Violet; Morrison, Katelyn; Robinson, Katherine-Marie; Abidi, Collin; Perer, Adam; Forlizzi, Jodi; & Dzombak, Rachel. Transparency in the Wild: Navigating Transparency in a Deployed AI System to Broaden Need-Finding Approaches. In *2024 FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency*. June 2024. **https://doi.org/10.1145/3630106.3658985**

Woody, Carol; Alberts, Christopher; Wallen, Charles; & Bandor, Michael. Improve Acquisition Cybersecurity Risk Using the Acquisition Security Framework and Software Bills of Materials Risk Framework. In *Proceedings of the Twenty-First Annual Acquisition Research Symposium*. April 2024. **https://dair.nps.edu/bitstream/123456789/5075/1/SYM-AM-24-031.pdf**

Zhai, Lijing; Vamvoudakis, Kyriakos G.; & Hugues, Jérôme. Safe Stochastic Model-Based Policy Iteration with Chance Constraints. In *2023 62nd IEEE Conference on Decision and Control (CDC)*. January 2024. **https://doi.org/10.1109/CDC49753.2023.10383730**

Conference Presentations

Benitez, Mario & Ivers, James. *Role of Automation in Reducing Software Refactoring Costs.* 2023 DoD Weapon Systems Software Summit. December 2023. **https://custom.cvent.com/6CA8784A95BD4574A858FFA862468AC0/files/02ff1cbe2ac04ce5bef872771aed4314.pdf**

Benoit, Thomas. *Demystifying the Shape of Traffic in the Cloud: How Cloud Monitoring Differs from Traditional On-Prem Solutions.* FloCon 2024. January 2024. **https://insights.sei.cmu.edu/library/flocon2024-demystifying-the-shape-of-traffic/**

Chick, Timothy A. *Secure Systems Don't Happen by Accident.* Cybersecurity Summit: North America Midwest. June 2024.

Chick, Timothy A. *Are Your DevSecOps Capabilities Mature?* DevSecOps Days Washington D.C. October 2023. **https://insights.sei.cmu.edu/library/are-your-devsecops-capabilities-mature/**

Flynn, Lori & Klieber, Will. *Using LLMs to Adjudicate Static-Analysis Alerts.* Secure by Design Conference. August 2024. **https://insights.sei.cmu.edu/library/2024-secure-software-by-design-presentations/**

Gomez, Alejandro. *Modern API Security.* Secure by Design Conference. August 2024. **https://insights.sei.cmu.edu/library/2024-secure-software-by-design-presentations/**

Hira, Anandi. *Capability-Based Software Cost Estimation: Proposing a New Method to Estimate Software Costs.* BCSSE COCOMO and PSM Forum 2023. November 2023. **https://docs.google.com/presentation/d/1JuqksGBVkWBXQCup0mI1cwAGcI2MT67b**

Hira, Anandi. *Capability-Based Software Cost Estimation: Proposing a New Method to Estimate Software Costs.* 2023 ISBSG IT Confidence Conference. November 2023. **https://www.isbsg.org/wp-content/uploads/2023/11/Capability-Based_ISBSG-2-tccd.pdf**

Johnson, Suzette & Yeman, Robin. *Industrial DevOps - Building Better Systems Faster.* IT Revolution Event - DevOps Enterprise Summit. October 2023.

Johnson, Suzette & Yeman, Robin. *Industrial DevOps and Digital Twins for Cyber-Physical Systems.* 34th Annual INCOSE International Symposium (IS). July 2024.

McDowell, Angel. *Is Prompt Engineering the New Divide?* WomenTech Global Conference 2024. April 2024.

Mellon, Jeffrey & Worrell, Clarence. *Cyber-Informed Machine Learning: End-User Value through Explainability.* RSA Conference 2024. May 2024. **https://www.rsaconference.com/library/presentation/usa/2024/cyber-informed%20machine%20learning%20end-user%20value%20through%20explainability**

Miller, Elias; Sconiers-Hasan, McKinley; & Morrow, Timothy B. *Zero Trust + DevSecOps Workshop.* Secure Software by Design 2024. August 2024. **https://insights.sei.cmu.edu/library/2024-secure-software-by-design-presentations/**

Nichols, William R.; Clausner, Brent; Miller, Chris; Antunes, Luiz; Bandor, Mike; O'Hearn, Brigid; Cohen, Julie; Hira, Anandi; & Novak, William. *Automated Continuous Estimation for Pipelines of Pipelines.* BCSSE COCOMO and PSM Forum 2023. November 2023. **https://drive.google.com/file/d/1MZqjlFH0wl65GZ2a-c-iN6FavcyLLdgE/**

Nielsen, Paul D. *Engineering the Future.* 34th Annual INCOSE International Symposium (IS). July 2024.

Ozkaya, Ipek. *Is Generative AI Fit for Your Use Case?* ICSE 24: International Conference on Software Engineering. April 2024.

Ruef, Dan. *Fusing AWS VPC Flow Logs and Traditional Netflow.* FloCon 2024. January 2024. **https://insights.sei.cmu.edu/library/flocon2024-fusing-aws-vpc-flow-logs-and-traditional-netflow/**

Scanlon, Thomas P. *What Threats Do Deepfakes Present?* ISC2 Security Congress 2023. October 2023.

Scanlon, Thomas P. *Protecting the ML Pipeline: Practical Guidance for Securing Machine Learning Systems.* ISC2 Security Congress 2023. October 2023.

Scanlon, Thomas P. & Worrell, Clarence. *Data Science for Cybersecurity Workshop.* InfoSec World 2024, AI Security Summit. September 2024.

Scanlon, Thomas & Ross, Dominick. *Generative Artificial Intelligence (AI) — Part 1 — Deepfakes 101.* 2024 ISAC Annual Meeting. June 2024.

Sherman, Mark. *Should I Trust the Next Generation of LLMs to Check My Program?* InfoSec World 2024, AI Security Summit. September 2024.

Sherman, Mark. *Using ChatGPT for Evaluating Computer Programs.* 2023 DoD Weapon Systems Software Summit. December 2023. **https://custom.cvent.com/6CA8784A95BD4574A858FFA862468AC0/files/d880036742c749d58eaadee0b8a1f348.pdf**

Sherman, Mark. *Should I Trust ChatGPT to Review My Program?* 2023 INFORMS Annual Meeting. October 2023.

Shimeall, Tim. *Working with Cloud Flow Data.* FloCon 2024. January 2024. **https://insights.sei.cmu.edu/library/flocon2024-working-with-cloud-flow-data/**

Shriver, David; von Stein, Meriel; & Elbaum, Sebastian. *DeepManeuver: Adversarial Test Generation for Trajectory Manipulation of Autonomous Vehicles.* ICSE 24: International Conference on Software Engineering. April 2024.

Smith, Justin & Hayes, William. *Agile Programs.* 2023 DoD Weapon Systems Software Summit. December 2023. **https://custom.cvent.com/6CA8784A95BD4574A858FFA862468AC0/files/c2f710b510bf4605ad44c85566ad4284.pdf**

Svoboda, David. *Automated Repair of Static Analysis Alerts.* Secure by Design Conference. August 2024. **https://insights.sei.cmu.edu/library/2024-secure-software-by-design-presentations/**

Touhill, Gregory & McIlvenny, Lauren. *Creating an AI Security and Incident Response Team.* RSA Conference 2024. May 2024. **https://www.rsaconference.com/Library/presentation/usa/2024/creating%20an%20ai%20security%20and%20incident%20response%20team**

Trzeciak, Randall F. *Avoiding Unanticipated Consequences of Implementing an Insider Threat Program.* InfoSec World 2024, AI Security Summit. September 2024.

Trzeciak, Randy & Tucker, Brett. *Insider Payback: Using Metrics to Demonstrate Insider Risk Program Value.* RSA Conference 2024. May 2024. **https://www.rsaconference.com/Library/presentation/usa/2024/inside%20payback%20using%20metrics%20to%20demonstrate%20insider%20risk%20program%20value**

Tucker, Brett. *Striking the Balance: Measuring and Managing the Complexity of Cyber Environments.* InfoSec World 2024, AI Security Summit. September 2024.

Tucker, Brett. *Spend What on This Risk Nightmare? Appetite Development and Application.* RSA Conference 2024. May 2024. **https://www.rsaconference.com/library/presentation/usa/2024/spend%20what%20on%20this%20risk%20nightmare%20appetite%20development%20and%20application**

Tucker, Brett. *Foresight: Using Incident Reports to Improve Measurability of Risk Exposure for Predictability.* FloCon 2024. January 2024. **https://insights.sei.cmu.edu/library/flocon2024-foresight-using-incident-reports-to-improve-measurability-of-risk-exposure-for-predictability/**

Turri, Violet; Robinson, Katie; Smith, Carol J.; & Gallagher, Shannon K. *Large Language Models (LLMs) & Me.* 2023 IEEE Women in Engineering (WIE) Forum USA East. October 2023.

Vesey, Alex. *Contract Programming: Formalizing APIs.* Secure by Design Conference. August 2024. **https://insights.sei.cmu.edu/library/2024-secure-software-by-design-presentations/**

Woody, Carol. *Acquisition Security Framework (ASF): Informing Software Bill of Materials (SBOM) Use Cases and Risk Reduction.* 34th Annual INCOSE International Symposium (IS). July 2024.Woody, Carol. *Meeting Challenges of Software Assurance and Supply Chain Risk Management.* Secure by Design Conference. August 2024. **https://insights.sei.cmu.edu/library/2024-secure-software-by-design-presentations/**

Worrell, Clarence & Shimeall, Tim. *Netflow Data Cleaning and Feature Engineering.* FloCon 2024. January 2024. **https://insights.sei.cmu.edu/library/flocon2024-netflow-data-cleaning-and-feature-engineering/**

Worrell, Clarence. *Implementation-Friendly Approximation Algorithm for the "Meet-in-the-Middle" Facility Location Problem.* AFCEA TechNet Mid-America Conference. June 2024.

Yasar, Hasan. *Addressing Technical Debt in AI System Development with DevSecOps.* 2023 DoD Weapon Systems Software Summit. December 2023. **https://custom.cvent.com/6CA8784A95BD4574A858FFA862468AC0/files/9aebf20b596948829de9f8d89f05799b.pdf**

Yeman, Robin. *Industrial DevOps — Building Better Systems Faster.* DevOps Experience 2023. October 2023.

Keynotes

Gallager, Shannon. *Deepfakes: Generating and Detecting Deepfakes.* National Cybersecurity Conference in Finland March 2024.

Hugues, Jérôme. *Model-Based Systems Engineering and Multi-Paradigm Modeling and Simulation: Two Faces of the Same Coin.* 5th International Workshop on Multi-Paradigm Modeling for Cyber-Physical Systems (MPM4CPS'23). October 2023.

Ozkaya, Ipek. *Beyond Automation: Human-AI Partnership and Redefining Roles in Software Architecture.* ICSA 2024 21st IEEE International Conference on Software Architecture. June 2024.

Ozkaya, Ipek. *Is Generative AI Fit for Your Use Case?* ICSE 24: International Conference on Software Engineering. April 2024.

Smith, Carol J. *Trustworthy by Design.* ICSE 24: International Conference on Software Engineering. April 2024.

Smith, Carol J. *Augmenting Intelligence: Ethical Challenges in the Age of AI.* ACM International Conference of the Special Interest Group on University and College Computing Services (SIGUCCS) 2024 Annual Conference. April 2024.

Smith, Carol J. *Letting Go of the Numbers: Measuring AI Trustworthiness.* 13th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2024). February 2024.

Touhill, Gregory. *Lessons Learned from the U.S. CISO.* Pittsburgh ISACA Information Security Awareness Day. December 2023.

Touhill, Gregory. *Cybersecurity: I Don't Think That Word Means What You Think It Means.* 2023 CyberShare Summit. October 2023.

Touhill, Gregory. *The Future of Cybersecurity: Trends, Challenges and Strategies.* NACD Directors Summit 2023. October 2023.

Woody, Carol. *Measurement of Supply Chain Risk.* 28th World Multiconference on Systemics, Cybernetics and Informatics (WMSCI 2024). September 2024.

Technical Reports

Alberts, Christopher J.; Bandor, Michael S.; Wallen, Charles M.; & Woody, Carol. *Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk (Expanded Set of Practices).* Software Engineering Institute, Carnegie Mellon University. October 2023. **https://insights.sei.cmu.edu/library/acquisition-security-framework-asf-managing-systems-cybersecurity-risk-expanded-set-of-practices/**

Moreno, Gabriel; Hristozov, Anton; Robert, John E.; & Klein, Mark H. *A Model Problem for Assurance Research: An Autonomous Humanitarian Mission Scenario.* Software Engineering Institute, Carnegie Mellon University. July 2024. **https://insights.sei.cmu.edu/library/a-model-problem-for-assurance-research-an-autonomous-humanitarian-mission-scenario/**

Ozkaya, Ipek; Shull, Forrest; Cohen, Julie B.; & O'Hearn, Brigid. *Report to the Congressional Defense Committees on National Defense Authorization Act (NDAA) for Fiscal Year 2022 Section 835 Independent Study on Technical Debt in Software-Intensive Systems.* Software Engineering Institute, Carnegie Mellon University. December 2023. **https://insights.sei.cmu.edu/library/congressional-report-section-835-technical-debt-cmu-sei-2023-tr-003/**

Sconiers-Hasan, McKinley. *Application Programming Interface (API) Vulnerabilities and Risks.* Software Engineering Institute, Carnegie Mellon University. June 2024. **https://insights.sei.cmu.edu/library/application-programming-interface-api-vulnerabilities-and-risks/**

Updyke, Dustin D.; Podnar, Thomas G.; & Huff, Sean. *Simulating Realistic Human Activity Using Large Language Model Directives.* Software Engineering Institute, Carnegie Mellon University. October 2023. **https://insights.sei.cmu.edu/library/simulating-realistic-human-activity-using-large-language-model-directives/**

Walsh, Matthew; Worrell, Clarence; & Scanlon, Thomas. *Toward the Use of Artificial Intelligence (AI) for Advanced Persistent Threat Detection.* Software Engineering Institute, Carnegie Mellon University. August 2024. **https://insights.sei.cmu.edu/library/toward-the-use-of-artificial-intelligence-ai-for-advanced-persistent-threat-detection/**

Wrage, Lutz. *Reachability of System Operation Modes in AADL.* Software Engineering Institute, Carnegie Mellon University. May 2024. **https://insights.sei.cmu.edu/library/reachability-of-system-operation-modes-in-aadl/**

2024 Featured Research Teams

Copyright

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.

DM25-0616

Credits

Managers

Communication Services
Janet Rex

Strategic Communication & (Acting) Public Relations
Amanda Parente

Communication Design
Cat Zaccardi

Technical Communication
Tamara Marshall-Keim

Staff

Editor-in-Chief
Paul Ruggiero

Editorial
Hollen Barmer

Ed Desautels

Megan Dietz

Felicia Evans

Tricia Flinn

Analisa Goodmann

Lope Lopez

John Morley

Sheela Nath

Sandy Shrum

Barbara White

Design
Christopher Baum

Illustration
Christopher Baum

Kurt Hess

Photography
Carnegie Mellon University Communications & Marketing Photography

David Biber

Digital Production
Mike Duda

40 years

SOFTWARE ENGINEERING INSTITUTE

SEI Pittsburgh, PA
4500 Fifth Avenue
Pittsburgh, PA 15213-2612

SEI Arlington, VA
4301 Wilson Boulevard
Suite 200
Arlington, VA 22203