Carnegie
Mellon
University
Software
Engineering
Institute

2019

YEAR IN REVIEW

The Software Engineering Institute (SEI) is a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

The SEI's mission is to support the nation's defense by advancing the science, technologies, and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring.

The *2019 SEI Year in Review* highlights the work of the institute undertaken during the fiscal year spanning October 1, 2018, to September 30, 2019.

A Message from the Director and Chief Executive Officer

The SEI sits right now in the middle of one of the key moments in the history of software, as our national defense and security organizations seek to attain competitive advantage through AI-enabled software systems.

Into that moment, we bring the unique combination of

- foundational, long-term, deep technical research, development, and deployment
- the capability to envision the future with the kind of academic rigor that comes naturally with being a part of Carnegie Mellon University, one of the world's elite academic research institutions

Everyone here is part futurist, part pragmatic problem-solver. Our charge is to be not on the cutting edge, but beyond it. For the women and men of the SEI, there is no status quo, no "this is the way things are"; our focus is on "the way that things look like they might become."

In a larger sense, our role remains as it was at our founding: to provide a higher degree of certainty to an uncertain future. In 1984, that future was about developing strong software engineering and development practices. Today, it's about developing even stronger practices to address the tight connection among software engineering, cybersecurity, and disruptive technologies, such as artificial intelligence (AI).

Our research and technology development inform the U.S. Department of Defense, federal government agencies, and the broader software engineering and cybersecurity communities about not only what to expect but also how to prepare for unexpected issues, problems, and opportunities. National defense and security organizations rely on our work and our people for

- assurance about software's behavior in any environment
- protection against threats that aren't even yet fully formed
- ways to gain the competitive advantage from emerging technologies

As told through examples from our fiscal year 2019 efforts, the SEI story is one of technology's threats, opportunities, and possible futures, and of the visionary thinkers here who are working to assure more certainty to a future that is in constant flux.

We recognize and embrace this moment for software technology, knowing that the mission we pursue for our sponsor has never been more essential.

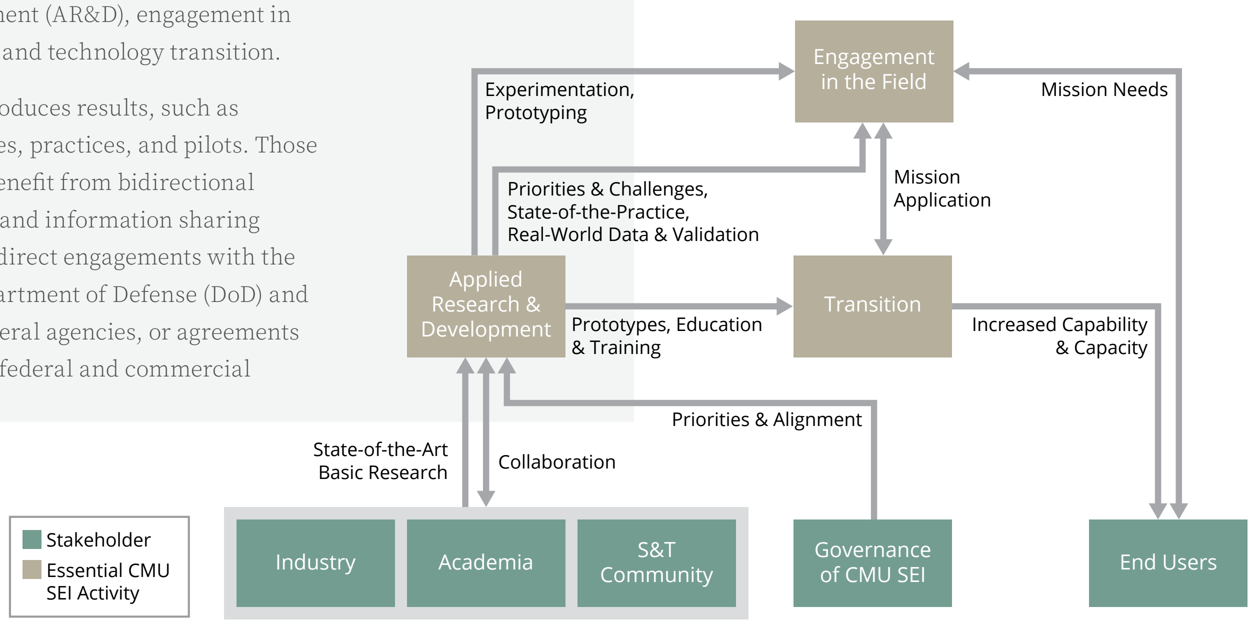
Paul D. Nielsen
Director and CEO

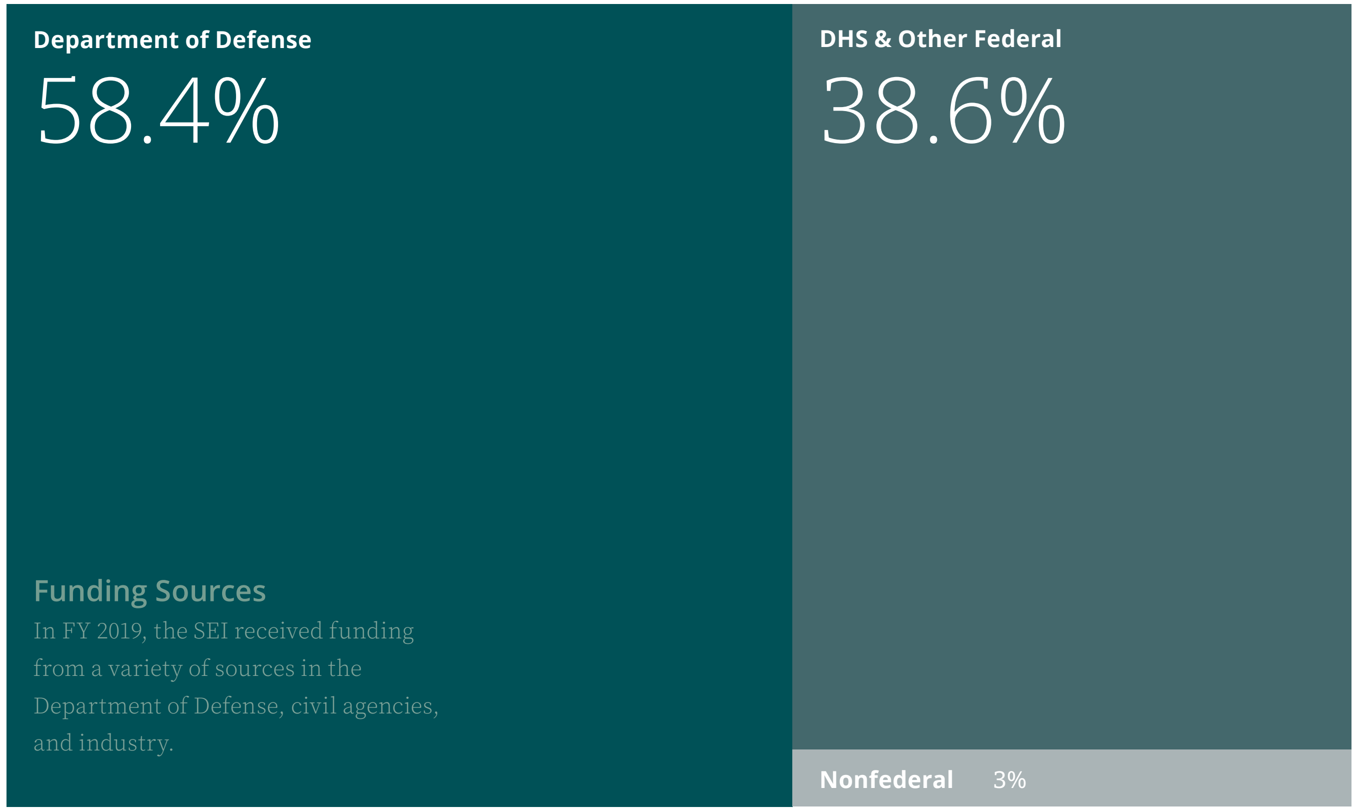
EXECUTION STRATEGY

The SEI employs an agile execution strategy, directing resources to the most critical ongoing and future challenges. This approach applies advances in technology and new insights to meet immediate needs, while developing capabilities to address larger underlying material and nonmaterial problems. The organization's essential activities are applied research and development (AR&D), engagement in the field, and technology transition.

AR&D produces results, such as prototypes, practices, and pilots. Those results benefit from bidirectional learning and information sharing through direct engagements with the U.S. Department of Defense (DoD) and other federal agencies, or agreements with nonfederal and commercial organizations. The SEI engages with customer organizations that have high-priority challenges and problems it can address by closing lifecycle technology gaps. Direct engagement enhances AR&D activities with an understanding of the state of the practice, current and future challenges and gaps, adoption considerations, and access to real-world data and environments that support experimentation, validation, and the maturation of research approaches.

These engagements also provide the credibility and access that enable technology transfer to DoD organizations and the wider software engineering community.


Engagement in the Field
Experimentation, Prototyping
Mission Needs
Priorities & Challenges, State-of-the-Practice, Real-World Data & Validation
Mission Application
Applied Research & Development
Prototypes, Education & Training
Transition
Increased Capability & Capacity
Priorities & Alignment
State-of-the-Art Basic Research
Collaboration
Stakeholder
Essential CMU SEI Activity
Industry
Academia
S&T Community
Governance of CMU SEI
End Users



Funding Sources

In FY 2019, the SEI received funding from a variety of sources in the Department of Defense, civil agencies, and industry.

Table of Contents

Advanced Autonomous Systems

Resilient and Agile Logistics

Cyberspace as a Warfighting Domain

Command, Control, Communications, Computers and Intelligence, Surveillance, and Reconnaissance (C4ISR)

Cross-Cutting

A Note on the 2018 National Defense Strategy and the SEI

According to the Department of Defense, "The 2018 National Defense Strategy [NDS] underpins our planned fiscal year 2019-2023 budgets, accelerating our modernization programs and devoting additional resources in a sustained effort to solidify our competitive advantage." The SEI's work described in the *2019 Year In Review* supported the following NDS modernization capabilities:

Advanced Autonomous Systems—military application of autonomy, artificial intelligence, and machine learning, including rapid application of commercial breakthroughs, to gain competitive military advantages

Resilient and Agile Logistics—prepositioned forward stocks and munitions, strategic mobility assets, partner and allied support, as well as noncommercially dependent distributed logistics and maintenance to ensure logistics sustainment while under persistent multi-domain attack

Cyberspace as a Warfighting Domain—cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations

Command, Control, Communications, Computers and Intelligence, Surveillance, and Reconnaissance (C4ISR)—resilient, survivable, federated networks and information ecosystems from the tactical level up to strategic planning; capabilities to gain and exploit information, deny competitors those same advantages, and enable us to provide attribution while defending against and holding accountable state or nonstate actors during cyberattacks

Nielsen Selected as INCOSE Fellow

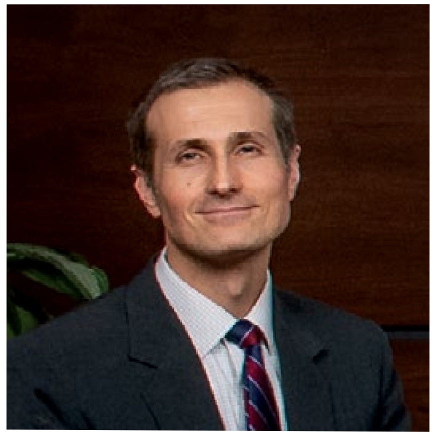
SEI Director and Chief Executive Officer Paul Nielsen was selected as a Fellow of the International Council on Systems Engineering, or INCOSE, in July 2019. INCOSE makes this lifetime award in recognition of "significant verifiable contributions to the art and practice of systems engineering in industry, government, or academia."

INCOSE connects nearly 17,000 systems engineering professionals in more than 70 countries. In its designation of Nielsen as a Fellow, it highlighted his "application of sound systems engineering to nationally significant defense and intelligence programs and for senior leadership in applying and advancing systems engineering in government R&D organizations."

"INCOSE has recognized the symbiosis between systems engineering and software engineering," said Nielsen. "It reflects the recognition that systems are evolving into using more software, and software is evolving into needing and using systems engineering. Working with INCOSE has been very productive and rewarding."

In receiving the award, Nielsen joins former SEI principal systems engineer Sarah Sheard, an INCOSE Fellow since 2006 and winner of the INCOSE Founders Award in 2002, and Barry Boehm, a member of the SEI Board of Visitors, a software engineering pioneer, and a 2000 INCOSE Fellow. Fellows are first nominated by other INCOSE members, then recommended by the Fellows Selection Committee to the INCOSE board of directors, which makes the final determination.

> *"INCOSE has recognized the symbiosis between systems engineering and software engineering."*
>
> **—PAUL NIELSEN, SEI DIRECTOR AND CHIEF EXECUTIVE OFFICER**



Danyliw Selected for Internet Engineering Steering Group

In early 2019, the SEI's deputy chief technology officer Roman Danyliw was selected to be a Security Area director for the Internet Engineering Steering Group (IESG), the committee responsible for the technical management of the Internet Engineering Task Force (IETF). The IETF is an open international standards development organization focused on the evolution of the Internet architecture and the smooth operation of the Internet.

As a Security Area director, Danyliw ensures that security and privacy are adequately considered in IETF work. He also oversees the Security Area of the IETF that focuses on enabling secure and privacy-preserving communications, threat mitigation, and end-point assessment, as well as on providing protocols and applications the means to handle the authentication, authorization, and accounting of users, applications, and devices.

"By serving on the IESG, I am able to transition the SEI's experience with operational security and security engineering to improve the next-generation Internet technologies," said Danyliw, who will serve from 2019–2021.

SEI Team Wins 2019 ISLA® Award

Program Manager's Guidebook for Software Assurance
Special Report
DoD Developer's Guidebook for Software Assurance
Special Report

(ISC)² awarded an SEI team the 2019 Information Security Leadership Award (ISLA®) Government, in the category of Most Valuable Industry Partner (Team):

- Timothy Chick, CERT Division
- William Nichols, Software Solutions Division
- Kenneth Nidiffer, Software Solutions Division
- Thomas Scanlon, CERT Division
- Carol Woody, CERT Division

The award recognized the SEI team's work for the Department of Defense (DoD) Joint Federated Assurance Center (JFAC), which supports software and hardware assurance efforts across the DoD. Over two years, the SEI team developed a pair of guidebooks on software assurance at the DoD.

Woody said that the award confirms the importance of the new guidance on software assurance. She further credited the award to the SEI's multidisciplinary approach. "The SEI brings expertise in acquisition, engineering, development, and security to the problem space," she said. "We are mission focused without pushing specific methods, practices, or tools, so we can be trusted to consider the needs of the DoD."

> *"The SEI brings expertise in acquisition, engineering, development, and security to the problem space."*
>
> **—CAROL WOODY, PRINCIPAL RESEARCHER**

Shull and Lewis Elected to IEEE Computer Society Leadership

Two members of the SEI's Software Solutions Division (SSD) were elected to leadership positions in the IEEE Computer Society (CS). Forrest Shull, the SSD's lead for defense software acquisition policy research, was voted 2020 president-elect. Grace Lewis, an SSD principal researcher, was elected to the board of governors.

Starting in 2021, Shull, a long-time IEEE CS member, will oversee IEEE CS programs and operations as president. "The Computer Society allows me to be part of a global community of computing professionals, with awareness of advances and challenges worldwide that can inform, and be informed by, the important work being done at the SEI and Carnegie Mellon University," said Shull.

Lewis, another long-standing IEEE CS member, will begin serving on the board of governors in 2020. "At the SEI, I have the privilege of working at the intersection of academia, government, and industry," she said. "This gives me the opportunity to see important advances that are happening in these three communities and identify synergy opportunities that can be supported by the Computer Society."

Featured Researchers **Matt Gaston, Bobbie Stempfley, Anita Carleton**

A Pivotal Moment: AI Engineering for Defense and National Security

Often called the new electricity, artificial intelligence (AI) stands to revolutionize our lives. Organizations all over the world, including the U.S. Department of Defense (DoD), are implementing rapidly developed AI solutions. The 2018 National Defense Strategy cites advanced autonomous systems, just one area enabled by AI and machine learning (ML), as a focus for capability modernization. The DoD's AI Strategy recognizes the importance of where we are in the unfolding history of this technology: "The present moment is pivotal: we must act to protect our security and advance our competitiveness, seizing the initiative to lead the world in the development and adoption of transformative defense AI solutions that are safe, ethical, and secure."

Current AI solutions resemble early software creations: often brilliant, but difficult to replicate, verify, and validate. The speed of their deployment could lead to a chaotic landscape far from the DoD's vision of safe, ethical, and secure solutions. In response, the SEI is leading the creation of a professional AI engineering discipline to enable the DoD to realize the full benefit of AI for defense and national security and to provide a foundation for creating viable, trusted, and extensible AI systems.

"At the SEI, we focus on the interplay between AI for mission and AI engineering," said Matt Gaston, director of the SEI's Emerging Technology Center, which is leading the institute's AI efforts. "We apply AI to actual mission challenges and use the lessons we learn to inform the AI engineering discipline we're developing."

Bobbie Stempfley, director of the SEI's CERT Division, agrees that applying AI in the areas of cybersecurity and software engineering informs the development of an AI engineering discipline. "Establishing a discipline for AI means doing the things in our core areas of expertise, recognizing that everything is deployed into contested space," said Stempfley. "We are doing everything we can to modernize software engineering and cyber engineering as precursors to AI engineering."

Software Solutions Division Director Anita Carleton connects AI engineering with the SEI's rich history of building mission solutions underpinned by rigorous software engineering. "We've known for years that the stakes are very high if software fails, and things only become more complex when we add AI and ML," she said. "All the things we're thinking about for modern software engineering processes—sound architecture design, coding, DevOps, and measurement practices—can bring trustworthiness to AI systems."

Carleton noted that automation will play a key role in lending repeatability to AI systems. This motivates the SEI's research in automated code generation, automated code repair, and automated architectural analysis.

In September 2019, the SEI released its first guidelines for the new discipline. *AI Engineering: 11 Foundational Practices* is an initial set of recommendations for organizations attempting to build, acquire, and integrate AI capabilities into business and mission systems. "These foundational practices offer some initial insights in a chaotic landscape where AI and ML technologies are evolving and advancing rapidly," said Gaston. "An AI engineering discipline can help the DoD create and adopt solutions that are reliable, reproducible, trustworthy, and maintainable."

In 2019, the SEI also assembled the first-ever community of interest workshop on AI engineering for defense and national security. This workshop brought together leaders from defense, industry, and universities to identify challenges and opportunities for AI engineering. The SEI will release a workshop report in 2020 and continue to work with the community of interest.

Thirty-five years ago, the SEI was founded to bring discipline to the chaos of software development for the DoD. Today, AI demands the same rigor. The SEI's deep expertise in software and data, trusted leadership in cybersecurity, and exploration of emerging technologies uniquely position the SEI to bring discipline to the twenty-first century's new electricity.

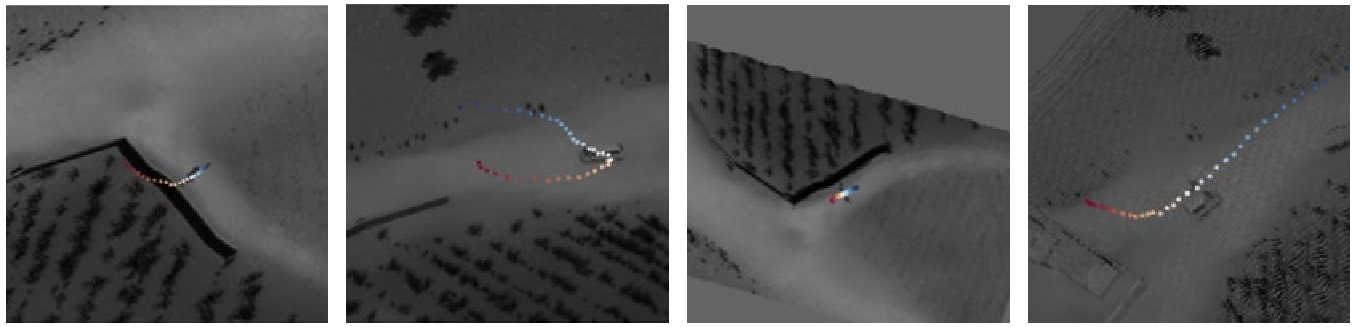
To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."

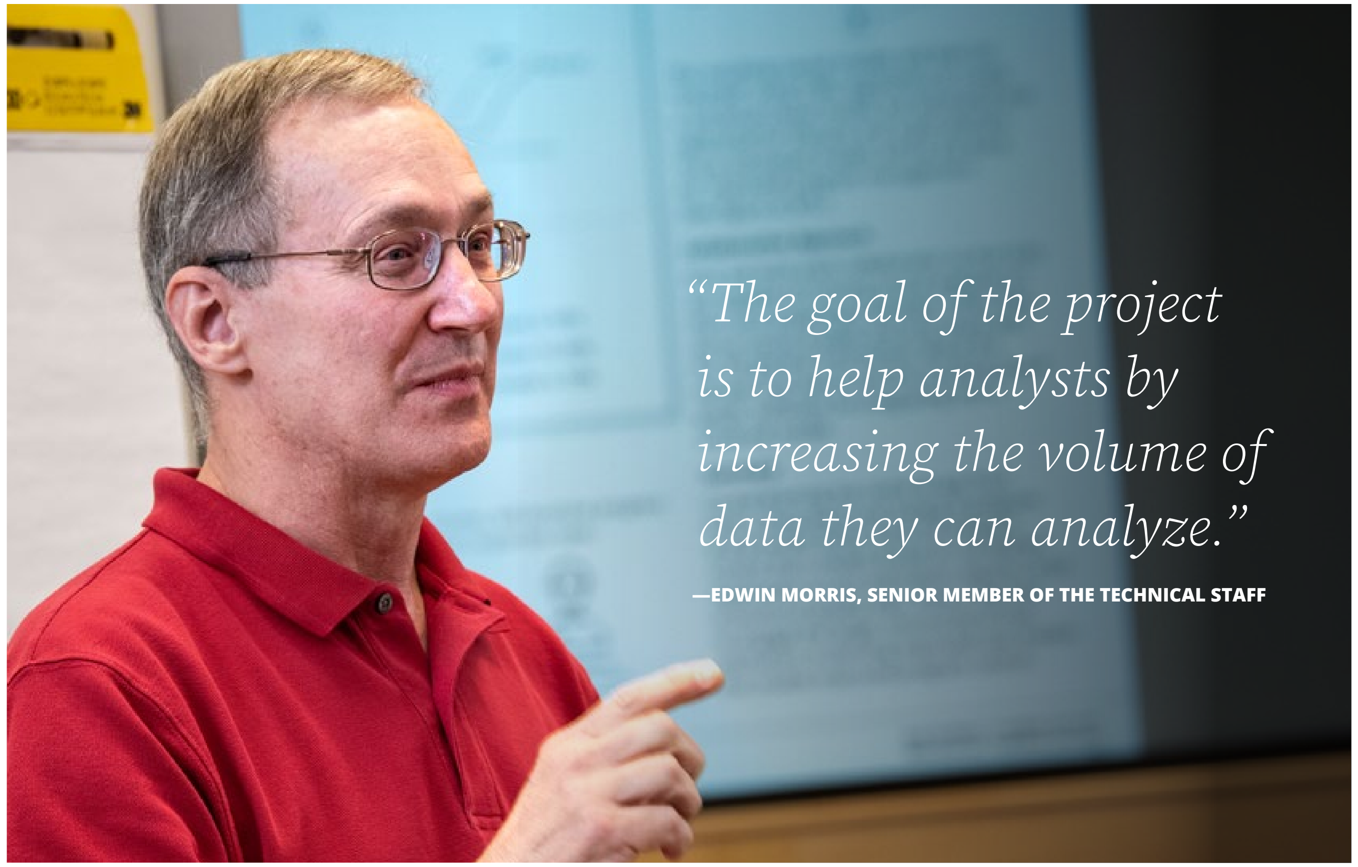
"An AI engineering discipline can help the DoD create and adopt solutions that are reliable, reproducible, trustworthy, and maintainable."

—MATT GASTON, DIRECTOR, EMERGING TECHNOLOGY CENTER

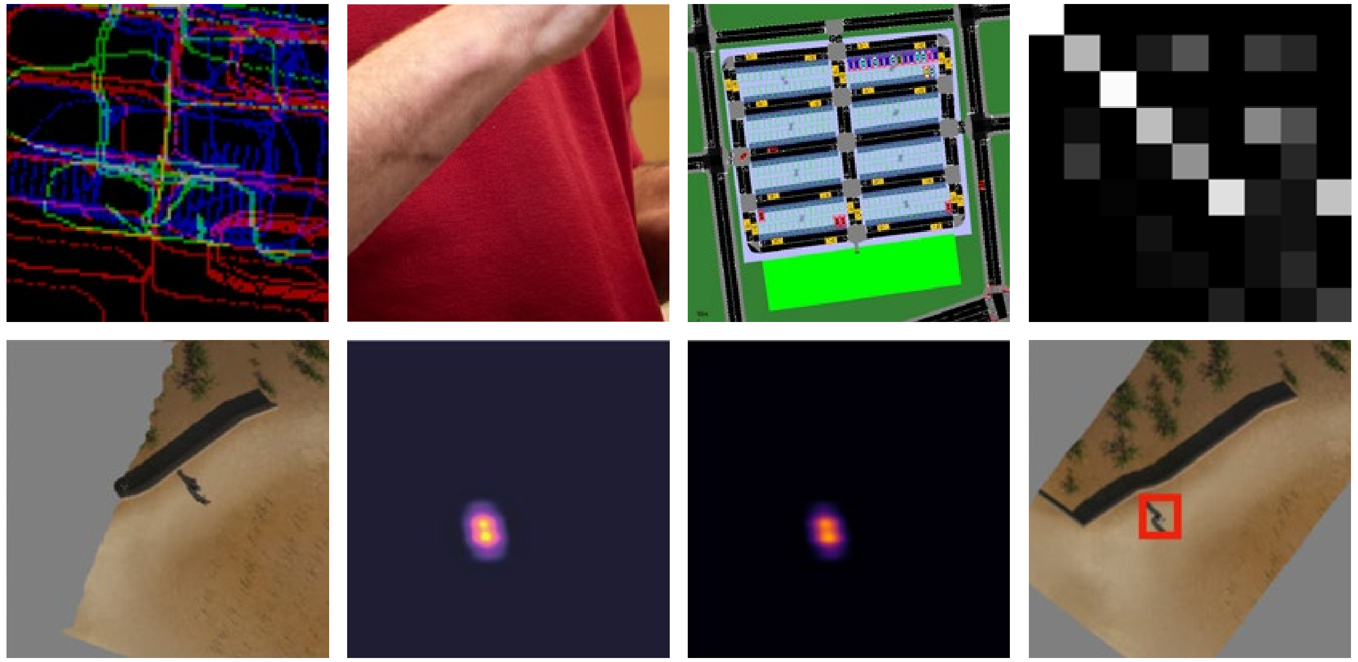
BOBBIE STEMPFLEY, DIRECTOR, CERT DIVISION

ANITA CARLETON, DIRECTOR, SOFTWARE SOLUTIONS DIVISION





> *“The goal of the project is to help analysts by increasing the volume of data they can analyze.”*
>
> —EDWIN MORRIS, SENIOR MEMBER OF THE TECHNICAL STAFF



Featured Researcher **Edwin Morris**

Supporting AI Engineering Challenges in the DoD: Summarizing Aerial Surveillance Video

The Department of Defense (DoD) has committed to the use of artificial intelligence (AI) and machine learning (ML) techniques, broadly, to modernize its capabilities in advanced autonomous systems and, specifically, to improve the timeliness and accuracy of decision making in next-generation intelligence, surveillance, and reconnaissance platforms. To achieve this goal, the DoD must address challenges related to the availability and fitness of data. It must also engineer these next-generation, AI-enabled systems in a way that accommodates how AI components and ML models will be trained, updated, deployed, and sustained.

The SEI is taking on a particularly thorny area of AI engineering for the DoD: working with data that is imperfect because of the conditions under which it was gathered. Aerial surveillance is one area in which the SEI is pursuing this objective. While aerial surveillance video is rich in information, extracting that information is difficult, labor intensive, and error prone. A lack of automated tools means analysts must dedicate their full attention to video streams, limiting the situational awareness of warfighters.

SEI researcher Edwin Morris and his team are developing algorithms for analyzing aerial surveillance data. Specifically, the algorithms improve the detection and tracking of objects and recognize patterns among them, including the ways they interact. “The goal of the project,” said Morris, “is to help analysts by increasing the volume of data they can analyze by providing them insights into patterns of life that would be difficult to otherwise identify.”

Morris and his team are working on three core technologies that make video summarization and search possible in the DoD problem space:

- *Domain adaptation to address limitations of training data.* Morris’s team is exploring ways to get around a chronic lack of labeled training data necessary to build good ML algorithms. They are using technologies such as the Cycle Generative Adversarial Network (CycleGAN), which employs ML to transform labeled data from past situations into good training data for a new situation. This technique will enable the DoD to supplement limited training data for ML classifiers with synthetic data, potentially from different contexts (e.g., open desert versus urban), and real data gathered from other locations and adapted to the new context.
- *Geometry-aware visual surveillance to improve the detection, tracking, and classification of moving objects.* Tracking moving objects in a video is a fundamental problem in surveillance, especially if the camera is constantly moving, as in drone surveillance. The team is developing a pipeline that estimates camera motion on-the-fly while tracking, eliminating the camera motion before deploying the team’s tracking algorithm. The tracker works by matching a detected object in a stabilized frame against a subsequent stabilized frame. This tracking method has shown promise and achieved better Intersection Over Union scores compared to unstabilized trackers. The technique is a step toward 3D processing of aerial surveillance data.
- *Pattern-of-life (PoL) analysis to characterize detected, tracked, and classified objects by their relationships and behaviors.* A PoL analyzer might identify targeted types of behaviors (e.g., insurgents planting an IED) or report anomalous or suspicious activity. More sophisticated PoL analyzers might refine these analyses to identify situations (e.g., a compound being used to hide hostages).

“By using a combination of techniques, we’ve been able to improve aspects of aerial video surveillance, such as identifying more objects correctly,” said Morris.

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for “2019 SEI Year in Review Resources.”

Featured Researcher **Oren Wright**

Graph Convolutional Neural Networks to Bolster AI Analysis of Irregular Data

Figuring out how artificial intelligence (AI) can learn structure is one of the most important AI questions for the defense community. As Department of Defense (DoD) datasets become larger, more complex, and more heterogenous, their structures are becoming increasingly irregular. Because of these complicated structures, AI tools—including machine learning (ML)—often fail to deliver useful analyses of this data. To obtain the benefits ML can offer, such as modeling uncertainty or navigating complex dependencies and differing data velocities, new ML techniques are needed that can learn the irregular structure of modern datasets.

The SEI is collaborating with Carnegie Mellon University's Electrical and Computer Engineering Department to develop graph convolutional neural networks (GCNNs), a new generation of techniques to apply deep learning, a form of ML, on graphs that represent complex datasets. GCNNs make use of convolutional neural networks (CNNs), a set of deep learning techniques that have revolutionized fields like computer vision, and extend them into irregular data domains that require graphs to explicitly model, such as sensor feeds, web traffic, and supply chains. The goal is to produce practical tools for mission problems, such as cybersecurity, infrastructure monitoring, and social network analysis. In addition, use of GCNNs can help the DoD modernize the National Defense Strategy capability of advanced autonomous systems and apply it to diverse prediction and pattern recognition problems, such as bot identification on social networks.

"The problem with state-of-the-art deep learning techniques like CNNs is that they work on Euclidean data—data that has a uniform, grid-like structure," said Oren Wright, a research scientist at the SEI's Emerging Technology Center. "These techniques, however, don't perform well on non-Euclidean data, like social networks, telecom networks, or biological systems. When operating over irregular data structures, these techniques discard useful information and often make wrong assumptions. The research effort to improve these techniques by extending deep learning to non-Euclidean data is called geometric deep learning."

GCNNs are a particularly attractive geometric deep learning approach because they bring the most effective attributes of CNNs—such as a relatively small memory footprint, low computation cost at inference time, and a hierarchical structure that leads to high accuracy—to graph data. Graph signal processing (GSP), which generalizes theories from classical signal processing to graph-structured data, is the key to making GCNNs possible.

The SEI and its collaborators have applied GSP concepts to build elements of GCNNs, compare different GCNN variants, and perform experiments on benchmark graph datasets. The project demonstrated a state-of-the-art convolution and pooling architecture that improved the average baseline accuracy of graph classification from 77.9 percent to 80.2 percent. Another demonstration, of GCNN joint representation with graph spectral distances, improved graph classification accuracy from 80.7 percent to 90.1 percent. The SEI and its collaborators have also contributed GCNN code to open source geometric deep-learning tools, such as PyTorch Geometric, and they have published multiple peer-reviewed research papers.

To learn more about this and other topics discussed in the *Year in Review,* visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."

> *"The research effort to improve these techniques by extending deep learning to non-Euclidean data is called geometric deep learning."*
>
> **—OREN WRIGHT, RESEARCH SCIENTIST**

Photo: U.S. Air Force

Featured Researchers **Scott McMillan & John Wohlbier**

SEI Collaborations Tackle Big-Data Analytics

Commanders and warfighters in the field rely on data. The Department of Defense (DoD) and U.S. intelligence community have an overwhelming data collection capability that far outpaces the ability of human teams to process, exploit, and disseminate information. Graph algorithms and large-scale machine learning (ML) algorithms are a key component of intelligence analysis of large datasets. However, these approaches are computationally expensive, energy inefficient, data intensive, and difficult to implement efficiently in increasingly complex computer hardware and architectures.

For more than five years, the SEI's Emerging Technology Center (ETC) has been researching a portfolio of work in advanced computing that addresses these challenges. Multiple efforts mark the latest step in the ETC's research on big-data analytics.

Graph algorithms analyze problems represented by graphs of interconnected nodes, such as those used in social network analysis, cybersecurity, and intelligence, surveillance, and reconnaissance. However, graph analytics must be custom-developed to work with the underlying hardware. A project headed by ETC research scientist Scott McMillan aims to separate graph algorithm development from the tasks required to optimize their performance on the underlying hardware systems.

Part of the approach to achieving this separation was the development of the Graph Basic Linear Algebra Subprograms (GraphBLAS) application programming interface (API). GraphBLAS is a community-driven, open source programming specification for graph analysis. McMillan, supported by ETC colleagues, has provided instrumental GraphBLAS development, publication, and promotion. The specification makes the development of high-performance graph algorithms simpler—and hardware agnostic—by defining the algorithms in the language of linear algebra. This freedom will allow graph algorithm developers to leverage the latest in high-performance computing without having to be experts in its hardware.

John Wohlbier, a senior research scientist in the ETC, is collaborating with Eric Hein at Lucata Corporation (formerly Emu Technology), a company developing an exascale-capable computing architecture designed specifically to tackle big-data applications. "Lucata is working on a fundamentally different computer paradigm," said Wohlbier, "where the program moves to the data, rather than vice versa."

Lucata's programming model reduces traffic on computation networks and nets improved computational and energy efficiency. This advance holds great promise for the field of graph analysis, and Wohlbier is working to implement algorithms built using the GraphBLAS API, co-created by ETC researchers, on Lucata's innovative hardware. The purpose is to evaluate algorithm programmability and performance with an eye toward advancing future mission capability.

"GraphBLAS is a natural fit for the Lucata platform and will provide numerous opportunities for algorithm development and enhancement of mission capabilities," said Lucata's Hein. "The SEI–Lucata collaboration is a key factor in achieving this goal."

With a variety of hardware configurations available for big-data analysis, the challenge becomes fitting the right software to the right hardware. Another ETC project involves the use of Spiral, an automated code-generation system developed at Carnegie Mellon University (CMU) to produce efficient implementations of digital signal processing algorithms for targeted hardware platforms.

McMillan is working with CMU's Spiral team, led by professor Franz Franchetti, to extend the system to achieve hardware–software co-optimization. For a specified computation, Spiral will search for and select optimized hardware configurations and generate optimized code for them, all automatically. The SEI and CMU team is also expanding Spiral's capabilities to tackle the irregular, data-intensive computations required for artificial intelligence (AI) and ML algorithms.

If successful, Spiral's automatic generation of hardware-optimized code will allow platform developers to realize high-performance AI/ML applications on leading-edge hardware architectures faster and cheaper. These advances will allow for rapid development and deployment of capabilities across the DoD enterprise and the spectrum of national and tactical needs. They will also support the 2018 National Defense Strategy's modernization of the key capability of advanced autonomous systems.

> To learn more about this and other topics discussed in the *Year in Review,* visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."

Featured Researcher **Dio de Niz**

Can We Trust Our Cyber-Physical Systems?

Kicking up a cloud of dust, a drone takes off to gather overhead video—a typical intelligence, reconnaissance, and surveillance task. The drone flies a wide circle around its operator and disappears over the horizon. Can we trust it to safely complete its mission?

We can ask this question about any cyber-physical system: ground vehicles, robots, weapons, manned aircraft, ships, and all computer-based systems that interact with their physical environment. New cyber-physical systems are constantly being developed and deployed that enable the Department of Defense to respond and adapt to an ever-evolving array of threats. Being able to enforce safe behavior will speed up the deployment and use of new technologies and increase trust in the systems military personnel depend on. How can we validate and verify that these systems do not endanger their users?

The SEI's Dio de Niz is leading a team of researchers to develop the rapid certifiable trust approach: a lightweight, scalable method to rapidly validate whether cyber-physical systems are behaving safely. Rapid certifiable trust focuses on how systems and components act, not on their internal algorithms. "For a cyber-physical system, safe behavior means safe actions at the correct time, for instance, to avoid a crash," said de Niz.

Rapid certifiable trust techniques could be incorporated into any type of cyber-physical system to improve its safety: autonomous, semiautonomous, remotely teleoperated, or directly controlled by human beings. Rapid certifiable trust does not require access to the source code of components. Instead, it verifies that their output and corresponding behavior are safe. An enforcer monitors these outputs to ensure that they do not violate safety constraints, which are determined by verification models based on physics, logic, and timing.

- Physics models verify the interaction between software and physical components, including the system's physical properties such as mass, velocity, and torque.
- Logical models ensure that the code computes the correct values.
- Timing models guarantee that the values are produced at the right time, for example, to correct the behavior of the physical components before a crash can occur.

"For a cyber-physical system, safe behavior means safe actions at the correct time."

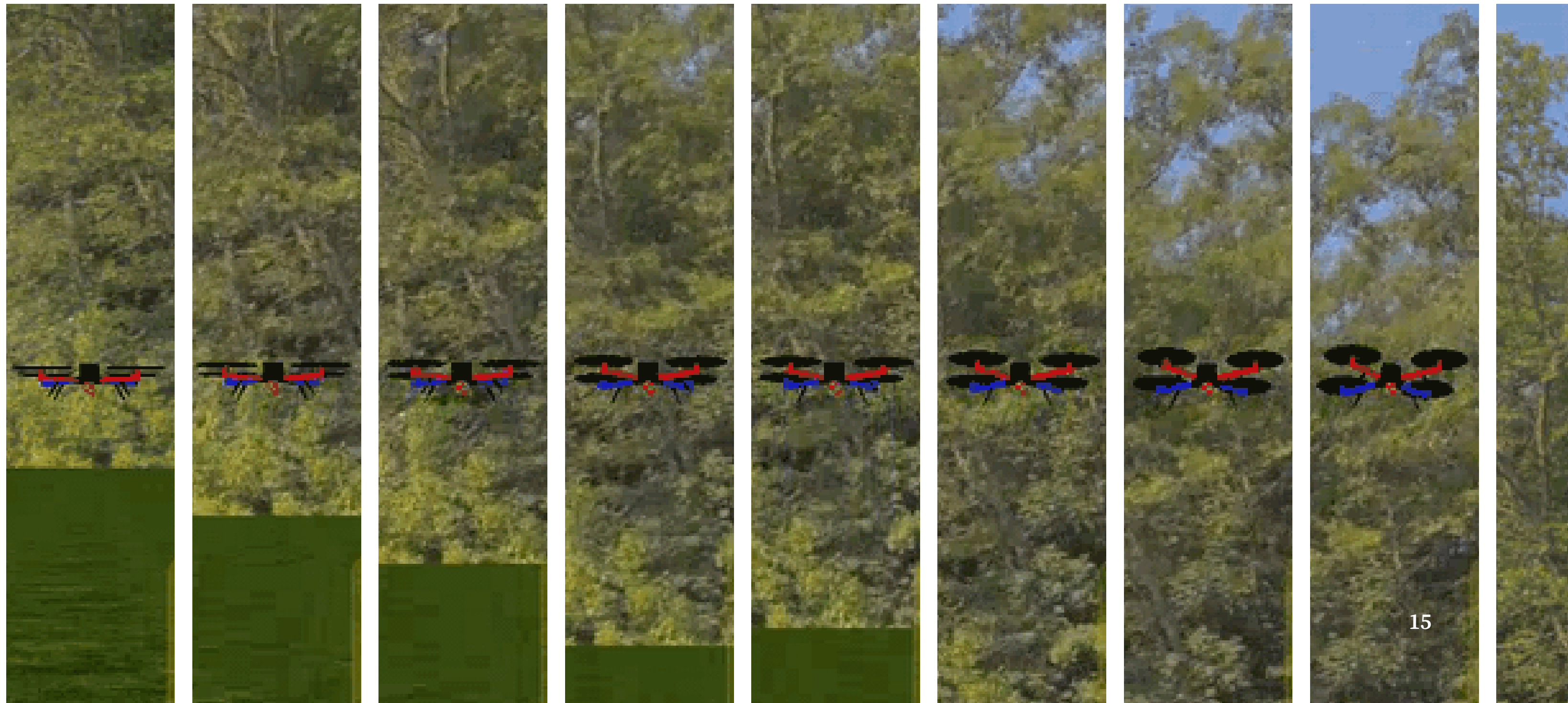
—DIO DE NIZ, TECHNICAL DIRECTOR, ASSURING CYBER-PHYSICAL SYSTEMS

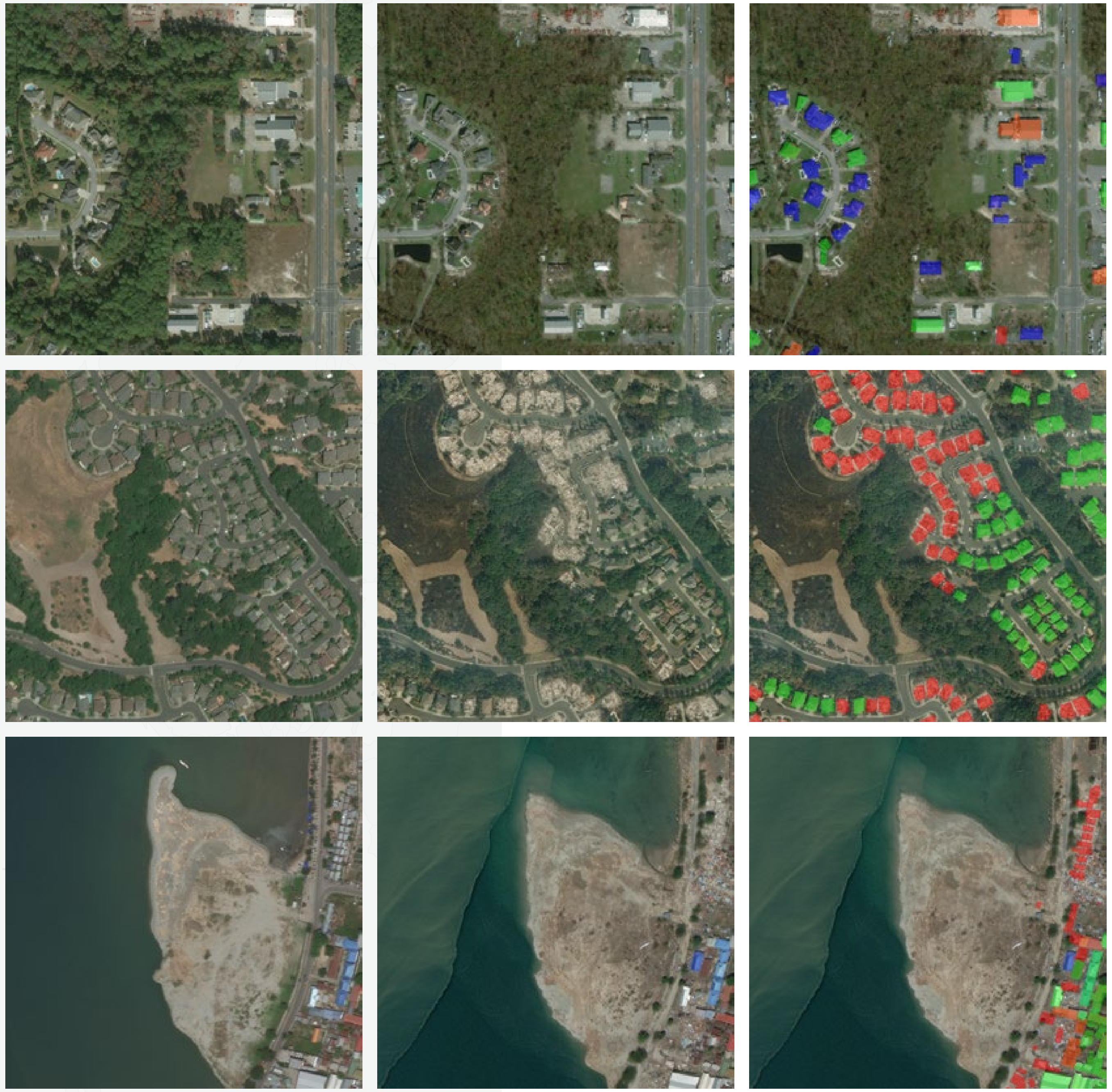
This published verification framework can be used to model specific problems in cyber-physical systems and, using the accompanying algorithms, verify their safe condition. While the models provide irrefutable mathematical proof of correctness, they are difficult to scale up in size. To use them with large, real-world systems, rapid certifiable trust applies these methods only to smaller enforcers that are specifically designed to monitor safety-critical properties. The enforcers operate in a real-time, mixed-trust computing system: verified, trusted components enforce unverified, untrusted components. A tamper-proof, verified hypervisor protects the enforcers from accidental or malicious modification by the unverified code. This hypervisor is available as open source software.

As a proof-of-concept, de Niz and his team are currently implementing rapid certifiable trust techniques on a Navy system. Future plans include transitioning it to a deployed system and investigating how it interacts with autonomy, supporting the National Defense Strategy's focus on modernizing advanced autonomous systems. Artificial intelligence would be a strong candidate for the rapid certifiable trust approach.

To learn more about this and other topics discussed in the *Year in Review,* visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."

Photo: U.S. Army





Examples of before and after a disaster event, with polygons overlaid to assess the scale of damage (left to right)

Raw images Copyright 2019 Maxar/DigitalGlobe. Used under a Creative Commons Attribution-NonCommercial 4.0 license (CC BY-NC 4.0). Polygons added by Carnegie Mellon University Software Engineering Institute.

Featured Researchers **Ritwik Gupta & Ricky Hosfelt**

Building Damage Assessment Dataset Advances Machine Learning for Disaster Recovery

When disaster strikes, Department of Defense (DoD) personnel are often among the boots on the ground. Responders can work more safely and effectively if they are aware of nearby building damage. Currently, gathering this information requires either dangerous on-the-ground observation or time-consuming human analysis of satellite photographs.

Recent work by the SEI's Emerging Technology Center (ETC) has enabled machine learning (ML) developers to create automated assessments of building damage from satellite imagery.

Ritwik Gupta, an ML research scientist in the ETC, and Ricky Hosfelt, an ETC software engineer, helped assemble the world's largest dataset of pre- and post-disaster building damage assessment. The xBD dataset (xview2.org/dataset) labels satellite images of more than 850,000 buildings with degrees of disaster-caused damage.

Using supervised learning, ML-automated damage assessment tools would need to train with images of buildings before and after a disaster, with labels for post-disaster levels of damage. The xBD dataset provides this ground-truth training data for ML tools that may someday quickly and automatically scan satellite photos to assess damage to structures caused by natural or human-made disasters. Automated assessment could save critical time and financial resources for DoD responders and others in the humanitarian assistance and disaster recovery (HADR) community.

The xBD dataset was first used in the Defense Innovation Unit's (DIU) xView2 Challenge, for which the ETC developed xBD, sample ML algorithms, and the metrics for determining the contest's winners. In the fall of 2019, DIU called on the ML community to create computer vision algorithms that would scan xBD's satellite images of buildings before and after wildfires, landslides, dam collapses, volcanic eruptions, earthquakes, tsunamis, wind events, and floods. The algorithms would then automatically identify the buildings and classify their damage.

Gupta and Hosfelt curated imagery of pre- and post-disaster buildings. The researchers and collaborators at the California Department of Forestry and Fire Protection, California Air National Guard, Federal Emergency Management Agency, NASA, DIU, and the HADR community then created the Joint Damage Scale to enable consistent labeling of damage across different types of disasters, structures, and geographies.

The next step was to manually label the buildings in the post-disaster images with a degree of damage, using the Joint Damage Scale, and the cause. Gupta and Hosfelt guided the crowdsourced labeling effort and quality checked the results with HADR partners and experts in satellite imagery and remote sensing.

> *"We want these challenges to make a difference to agencies and their partners in their day-to-day operations."*
>
> **—RITWIK GUPTA, MACHINE LEARNING RESEARCH SCIENTIST**

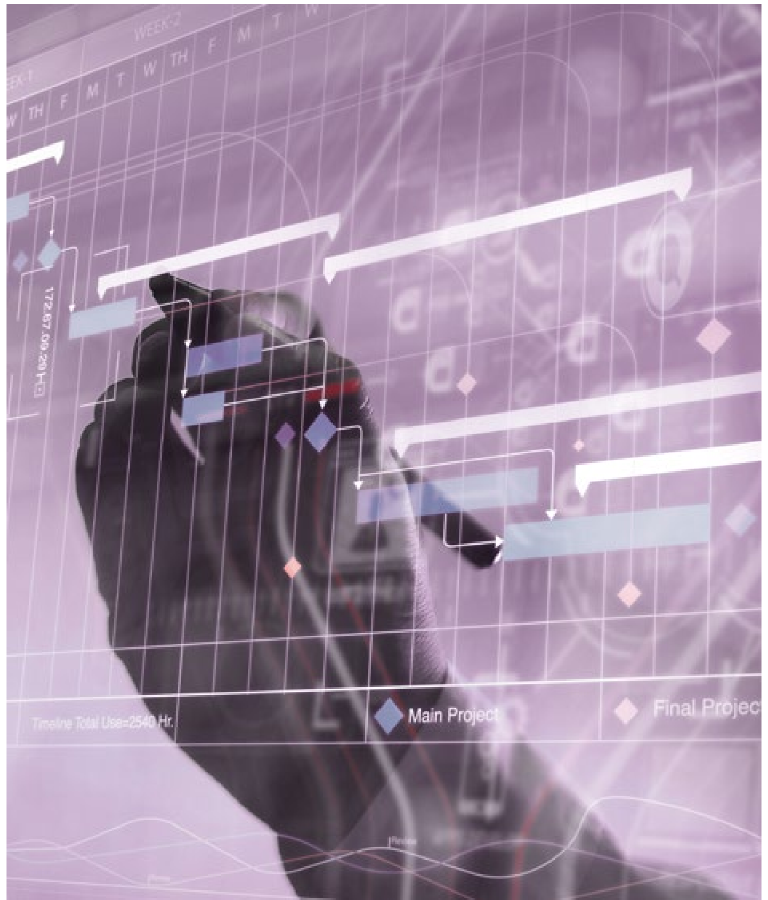
The resulting xBD is the largest satellite imagery dataset for building damage assessment. It constitutes the ground truth against which xView2 competitors' automatically generated damage assessments will be scored. Gupta said he aimed to make the xView2 Challenge academically rigorous but operationally relevant. "We want these challenges to make a difference to agencies and their partners in their day-to-day operations."

While technologists tout the power of ML and artificial intelligence (AI), they will require training datasets to create truly advanced autonomous systems, one of the key modernization capabilities in the 2018 National Defense Strategy. For the nascent field of applied ML and AI in HADR, the SEI and DIU collaborators behind xBD expect the dataset to be a breakthrough source of training data.

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."

> *“The SEI’s rare combination of experience in software engineering and acquisition practice informed analysis of DoD acquisitions data and helped shape the report’s recommendations.”*
>
> **—EILEEN WRUBEL, TECHNICAL DIRECTOR, TRANSFORMING SOFTWARE ACQUISITION POLICY AND PRACTICE**

FORREST SHULL, LEAD FOR DEFENSE SOFTWARE ACQUISITION POLICY RESEARCH



Featured Researchers **Forrest Shull & Eileen Wrubel**

The SEI Helps Shape Software Acquisition Policy Reform

To stay ahead of our adversaries and respond to operational needs in today’s mission space, the Department of Defense (DoD) must accelerate the delivery of new capabilities by adopting new methods of software development and acquisition. Longstanding acquisition, development, and governance policy evolved in response to a hardware development and production model. Progress requires new policies better suited to the reality that software drives many new capabilities.

The 2018 National Defense Authorization Act (NDAA) contained a number of provisions related to software acquisition improvement. In selecting the SEI to support these efforts, the DoD recognized the SEI’s expertise, developed through years of technical research on the application of Agile and lean practices in the DoD context as well as studies and analyses of software development, acquisition, and sustainment processes.

Beginning in fiscal year 2018 and continuing through fiscal year 2019, the SEI contributed its expertise to the Software Acquisition and Practices (SWAP) study. Required by 2018 NDAA Section 872, the SWAP study identified ways to streamline software development and acquisition regulations. SEI staff analyzed DoD software acquisition data, conducted case studies, and engaged with stakeholders from across the DoD acquisition ecosystem to advise SWAP authors and inform the study’s conclusions. Prepared by the Defense Innovation Board (DIB) and released in May 2019, the SWAP study advocated for speed of development as a primary metric, the cultivation of workforce digital talent, and the recognition that software is different from hardware.

Technical work being conducted by the SEI contributes to all the themes outlined in the SWAP study and helps to make the study’s recommendations actionable. This work also supports the DoD’s need, described in the 2018 National Defense Strategy, for resilient and agile logistics by streamlining rapid, iterative approaches to acquisitions. Anita Carleton, director of the SEI’s Software Solutions Division, pointed out the importance of this shift in acquisition philosophy. “No matter how innovative the software technologies and processes we come up with are,” she said, “we cannot affect the warfighter unless DoD acquisition policies—and in fact, the entire acquisition ecosystem—support their adoption.”

Acquisition programs adopting Agile and lean software acquisition approaches, as directed by 2018 NDAA Sections 873 and 874, have also worked with the SEI. These pathfinding programs provide experience and data concerning how Agile approaches can be adopted in the DoD and how stakeholders throughout the acquisition ecosystem must adapt their practices to support this transformation. Prior SEI work in this space, including the Readiness and Fit Analysis model characterizing programs’ Agile acquisition activities, has been instrumental in shaping the effort.

Forrest Shull, the SEI’s lead for defense software acquisition policy research, served as a member of the SWAP study team and worked with the Agile pathfinders. “This work engaged stakeholders from throughout the acquisition ecosystem,” said Shull, “not just within the DoD, but government, defense contractors, and FFRDCs such as the SEI. Together, all of these parties are realizing meaningful, positive change.”

Michael McQuade, Carnegie Mellon University’s Vice President for Research, is a member of the DIB and co-chaired the SWAP study. In remarks made on the study’s release, McQuade pointed to the study itself as exemplary of a sea change in defense acquisition. “We tried to do this the way you do software, not just because that’s a clever way to do a study, but because that’s part of the cultural change that has to happen in the way the Department approves the implementation of the recommendations in this study. It is an iterative process,” he said.

The SEI’s Eileen Wrubel, technical director, Transforming Software Acquisition Policy and Practice, underlined the SEI’s contributions to the DIB SWAP study. “The SEI’s rare combination of experience in software engineering and acquisition practice informed analysis of DoD acquisitions data and helped shape the report’s recommendations,” said Wrubel. “We believe we are uniquely positioned to help the DoD adopt the study’s recommendations and provide leadership across the acquisition ecosystem’s community of practice.”

To read the SWAP study report, *Software Is Never Done*, visit innovation.defense.gov/software/.

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for “2019 SEI Year in Review Resources.”

Featured Researchers **Cory Cohen & Jeff Gennari**

Updated Pharos Binary Analysis Framework Speeds Malware Analysis

In the landscape of cyberattacks, those using malware are among the costliest, according to a 2019 study by Accenture and the Ponemon Institute. Some of the most notorious malware attacks, such as WannaCry in 2017, have been linked to nation-states, and the 2018 National Defense Strategy recognizes cyberspace as a warfighting domain. In most cases, malware infections begin because of users who unwittingly download, open, and propagate dangerous files, and users in the federal computing environment are no exception.

Reverse engineering of malware can help analysts better understand the malware's abilities and improve their response to it. However, malware, like much other software, is increasingly built with object-oriented programming, whose abstractions present considerable challenges to reverse engineering. For example, C++ classes are high-level structures that lead to complex arrangements of assembly instructions. Malware rarely has source code available, forcing analysts to extrapolate sophisticated, complicated data structures from the low-level machine code. This work is difficult and time consuming. The Pharos suite of tools encodes expert knowledge of software compilers to automatically do some of reverse engineering's heaviest lifting.

Analysts have used the Pharos toolset, made publicly available on the SEI's GitHub site since 2015 (github.com/cmu-sei/pharos), to automatically reverse engineer binaries, the files available in wild-caught malware. Pharos, built in collaboration with Lawrence Livermore National Laboratory (LLNL) on its ROSE compiler infrastructure, provides a platform for binary static analysis capabilities, including disassembly, control flow analysis, instruction semantics, and more ways to reason about the behavior of, and data structures in, binary files.

In August 2019, the CERT Division released an updated version of Pharos. While the update represents more than a year's worth of bug fixes and improvements, one Pharos tool received an important new ability. OOAnalyzer determines the behavior and structures of object-oriented programs by automatically recovering C++ class abstractions from executables. Users have long been able to work with OOAnalyzer output by importing it into other reverse engineering frameworks, such as IDA Pro. The Pharos update added a plugin to OOAnalyzer that imports its outputs into Ghidra, the National Security Agency's recently released software reverse engineering tool. Ghidra can now display imported OOAnalyzer results in its user interface.

"Ghidra's decompiler automatically applies imported C++ data structures recovered by OOAnalyzer to decompiled code," said Jeff Gennari, a senior malware reverse engineer in the CERT Division and a developer of the Pharos toolset. "This greatly improves an analyst's ability to reason about complex data structures at the binary level by getting the representation even closer to source code."

Cory Cohen, a senior member of the technical staff in the SEI's CERT Division, and Pharos project lead, noted that the Ghidra plugin should expand OOAnalyzer's impact. "Since Ghidra is freely available," he said, "the improved analysis produced by OOAnalyzer will be able to reach a much broader audience of program analysts."

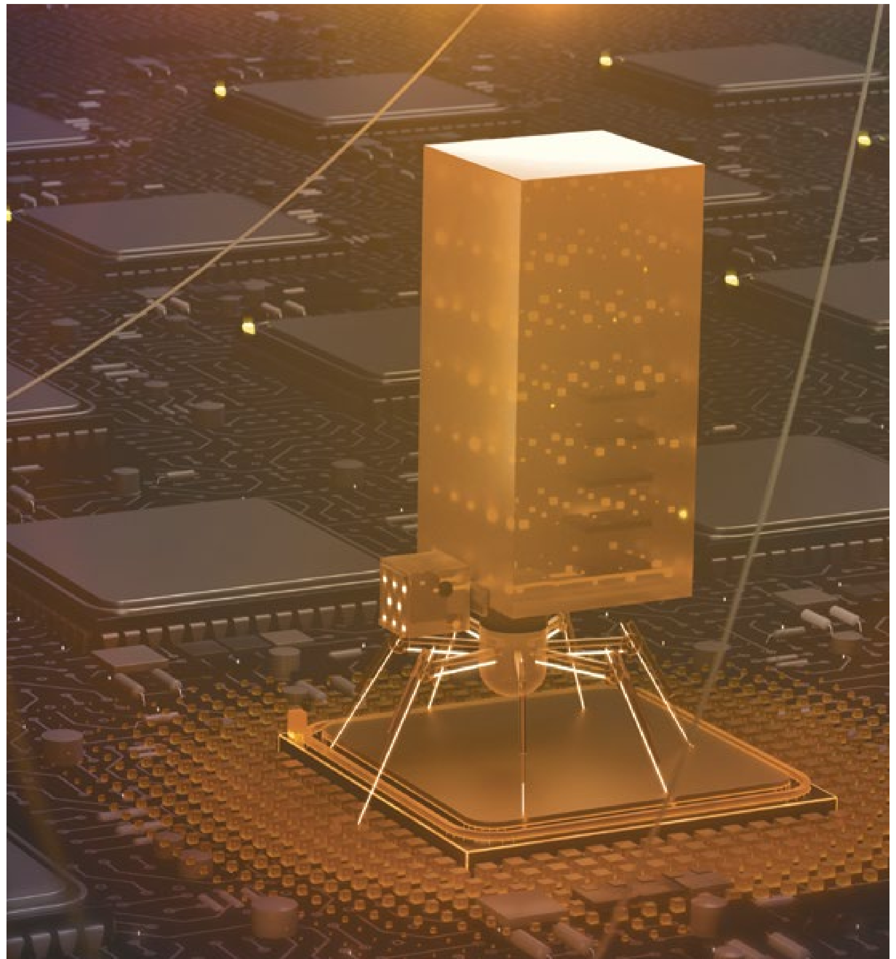
The other significant update to Pharos is improved path analysis. Path finding identifies the steps in the code that lead to program execution, from start to finish. The binary code of malware leaves out or obscures critical source-code locations and instructions along the execution path, making path finding notoriously difficult. The updated Pharos tool models the complete execution path by filling in the missing pieces with logically constrained symbolic representations. This technique has limitations, but it is a leap forward in path analysis that has applications in vulnerability discovery and malware feature identification and removal.

Cohen said the Pharos update represents the SEI's mission at work. "This is how the SEI has transitioned the latest research in program analysis capabilities into a platform that's actually usable by the Department of Defense and others."

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."

"*This is how the SEI has transitioned the latest research in program analysis capabilities into a platform that's actually usable by the Department of Defense and others.*"

—CORY COHEN, SENIOR MEMBER OF TECHNICAL STAFF



JEFF GENNARI, SENIOR MALWARE REVERSE ENGINEER

Featured Researcher **Jared Ettinger**

SEI Report Reveals the State of U.S. Cyber Intelligence

In May 2019, the SEI capped 17 months of research with the *Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States*. Jared Ettinger, technical lead and intelligence researcher, authored the report. He and his team interviewed 32 organizations, across a wide range of sectors, to understand their challenges and most effective practices. The team used 33 factors to categorize more than 2,000 different practices. This research updated a 2013 study; both were sponsored by the U.S. Office of the Director of National Intelligence.

The report presents actionable steps organizations can take to adopt high-performing cyber intelligence practices. It includes a top-10 best practices list and three implementation guides on how organizations can incorporate machine learning, the Internet of Things, and cyber threat frameworks into their cyber intelligence programs. The report is intended for readers of every level and role type, from incident responders to analysts to CISOs to Department of Defense staff defending cyberspace as a warfighting domain.

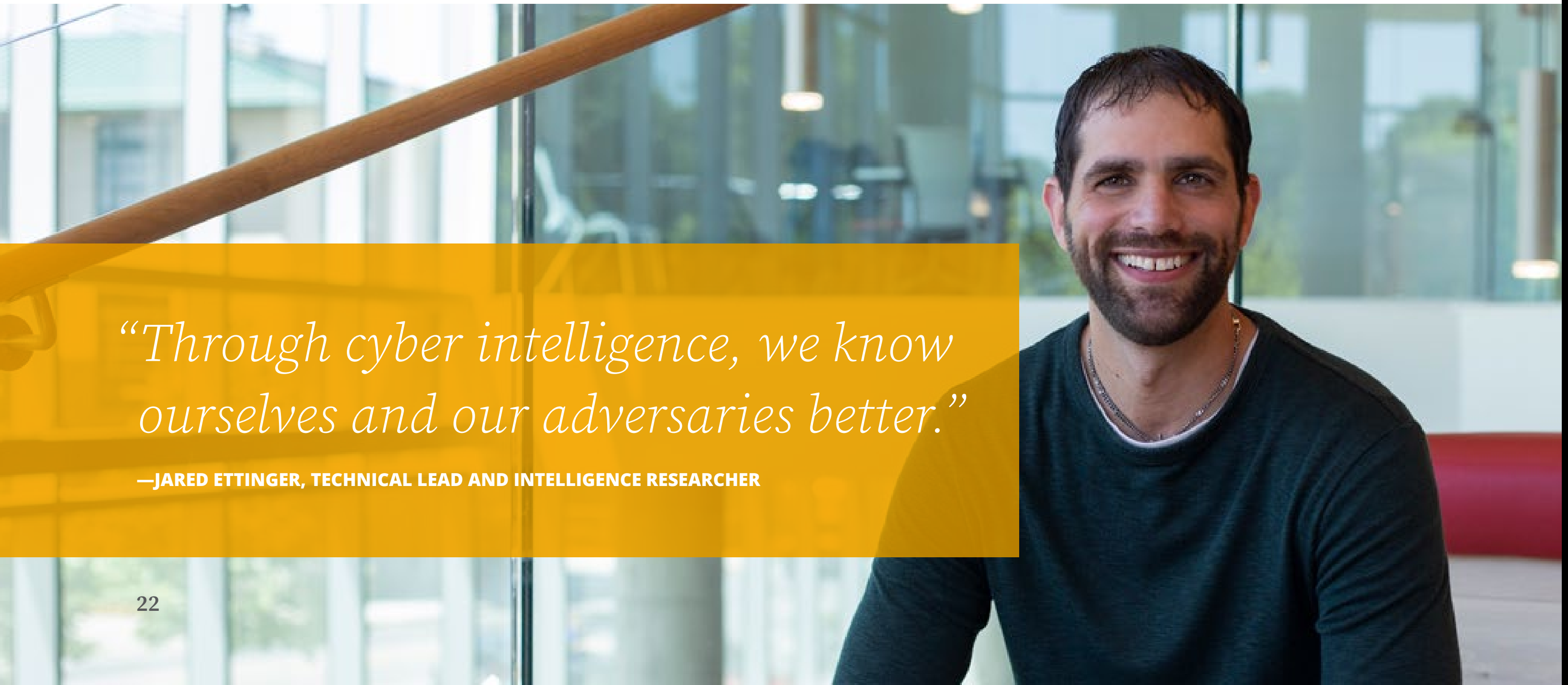
The report also promotes a common cyber intelligence lexicon so everyone can better share information, collaborate, and build trust. "The report defines cyber intelligence as acquiring, processing, analyzing, and disseminating information that identifies, tracks, and predicts threats, risks, and opportunities inside the cyber domain to offer courses of action that enhance decision making," Ettinger explained. "Decision makers use cyber intelligence to protect their organizations' vital interests, including financial reputation, brand, stature, and reputation. Cybersecurity, on the other hand, involves security measures to ensure the inviolability of the confidentiality, integrity, and availability of computer systems and is a critical component of cyber intelligence." Cyber intelligence better positions you to anticipate threats and use that information to efficiently apply security measures and bolster your cybersecurity posture.

Carnegie Mellon University
Software Engineering Institute

Cyber Intelligence Tradecraft Report
The State of Cyber Intelligence Practices in the United States

As Ettinger wrote in the report, "Through cyber intelligence, we know ourselves and our adversaries better. And with that knowledge, we can proactively take steps to better understand risks, protect against threats, and seize opportunities."

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."



"Through cyber intelligence, we know ourselves and our adversaries better."

—JARED ETTINGER, TECHNICAL LEAD AND INTELLIGENCE RESEARCHER

Featured Researcher **Chris May**

Cybersecurity Professionals Flex Their Muscles in SEI-Developed Competition

The SEI has a history of creating innovative cyber workforce development capabilities for the government. In response to 2019's *Executive Order 13870: America's Cybersecurity Workforce*, the Department of Homeland Security (DHS) selected the SEI to orchestrate the inaugural President's Cup Cybersecurity Competition, open to any federal executive branch employee.

The 2018 National Defense Strategy acknowledges cyberspace as a warfighting domain, and many experts believe the first strikes in an international conflict will take place in cyberspace. Though federal departments and agencies rely on cybersecurity to safeguard their systems and information, the need for cybersecurity expertise has outpaced the number of qualified cybersecurity professionals.

Executive Order 13870 addressed this growing demand by calling for, among other things, an annual President's Cup Cybersecurity Competition to be developed to "identify, challenge, and reward the United States Government's best cybersecurity practitioners and teams across offensive and defensive cybersecurity disciplines."

Given only a few months to plan and execute the competition before the executive order's December 31 deadline, SEI team members took just 23 days to draft a comprehensive program plan for the President's Cup, which the White House approved for immediate implementation. Under extreme time constraints, SEI staff also developed 82 hands-on technical challenges for the competition. Using Agile development practices, the SEI team created a fully functional competition platform in only six weeks, collaborating with Carnegie Mellon University's Entertainment Technology Center to incorporate a 3D video game.

"The SEI provided expertise and sound advice to help ensure the President's Cup would be a success."

—HARRY MOURTOS, DHS CISA

More than 1,000 participants and 200 teams from several federal agencies, but with the great majority from the Department of Defense (DoD), registered to compete in the inaugural President's Cup, which was led by the DHS Cybersecurity and Infrastructure Security Agency (CISA). "The Software Engineering Institute cooperated with us in executing the first-ever President's Cup Cybersecurity Competition," said Harry Mourtos of CISA. "The escape room final-round format had never been done before, and it provided a compelling new challenge format that worked well for the eight-hour livestream. The SEI provided expertise and sound advice to help ensure the President's Cup would be a success."

The 2019 competition culminated in December with a live, in-person championship round in Arlington, Virginia. Five members of the U.S. Army won the team competition, and a U.S. Air Force cadet was the individual winner. Learn more about the President's Cup Cybersecurity Competition at cisa.gov/presidentscup.

Featured Researcher **Hasan Yasar**

DevSecOps Takes DoD Software Development to the Next Level

The Department of Defense's (DoD's) software acquisition and development functions must be responsive to warfighter needs in order to keep pace with potential adversaries, both in the physical and cyber domains. DoD groups have realized they must move away from slower waterfall development methodologies and adopt modern software development practices, processes, and tools to provide responsive, timely, and secure software capabilities for warfighters at the speed of relevance. The SEI has enabled several DoD organizations facing these issues with a solution: DevSecOps.

"DevSecOps is a software development approach that brings together development and operations with security integral to the methodology," explains Hasan Yasar, the SEI's technical director of continuous deployment of capability.

DevSecOps emphasizes collaboration among stakeholders throughout the software development process, automation of everything that can be automated (including integration, testing, and deployment), monitoring to be able to shift priorities as needed, and infrastructure as code (IaC) for a stable foundation. As much a culture as a methodology, DevSecOps breaks down silos among stakeholders, including IT operations, acquisitions, architects, quality assurance and testers, developers, customers, and security personnel, to adapt to issues and threats more effectively and efficiently.

The SEI has helped the DoD through the challenges of implementing DevSecOps across various systems.

"The SEI was able to assist in removing barriers to adoption, from cultural to architecture and tooling complexity, by being part of DoD teams, building pipelines, selecting toolsets, and providing training, guidance, and implementation support to DoD groups," noted Yasar.

The SEI's DevSecOps work with the DoD aligns with the SEI's vision of leading and advancing software and cybersecurity to solve the nation's toughest problems. In fiscal year 2019, the SEI supported DoD DevSecOps in multiple engagements:

- *DevSecOps training.* Yasar and CMU professors collaborated with the Defense Acquisition University's (DAU's) professors and learning director for software acquisition to develop curricula for the DAU DevSecOps Academy. SEI pilot programs taught DoD acquisition, engineering, and information assurance professionals to work toward continuous authority to operate (ATO) using automated software development practices and modern tool chains. The project gave the DAU a foundation to provide DevSecOps training to DoD personnel at scale.
- *DevSecOps guidance.* The SEI developed DevSecOps architecture guidance for a DoD partner to break a monolithic application into microservices, increasing the speed of capability delivery to the warfighter, enhancing security, and improving the data and information environment to deliver a capability to users in 24 hours. The SEI also developed practices for using DevSecOps on modular/container-based architecture applications. Future modular development is now planned in cycles of 3 weeks instead of 12–18 months.

The SEI is also accelerating the establishment of the U.S. Tenth Fleet Cyber Foundry, allowing the Navy to respond to new cyber threats more rapidly using modern development tools and techniques, including Agile and DevSecOps practices. Reducing a software development cycle from months to weeks or even hours can have a profound impact in a relentlessly challenging cybersecurity environment. Focused on continuously delivering performance as well as speed, the SEI is also working with the first DoD program to have a continuous ATO, setting a gold standard that many programs are working to emulate. By providing DevSecOps training, coaching, architectural guidance, and implementation support, the SEI has enabled DoD organizations to be more agile and adaptive to react more proactively to threats.

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."

> *"DevSecOps is a software development approach that brings together development and operations with security integral to the methodology."*
>
> **—HASAN YASAR, TECHNICAL DIRECTOR, CONTINUOUS DEPLOYMENT OF CAPABILITY**

“Developers shouldn’t have to reinvent the security wheel. They should be free to focus on their mission.”

—TIM CHICK, SYSTEMS TEAM TECHNICAL MANAGER

Featured Researchers **Tim Chick & Aaron Reffett**

Designing Layered Security Architecture for DevSecOps

The Department of Defense (DoD) is implementing DevSecOps—an Agile software development methodology that builds security into every stage of the software lifecycle—across all of its software development efforts. The SEI is advising the DoD on how to implement security within the DevSecOps process. “We want to help applications achieve continuous ATO,” or authority to operate, said Tim Chick, the technical manager of the Systems Team in the SEI’s CERT Division. “It’s a big security challenge.”

Chick is leading his team’s push to create a new security architecture for DevSecOps. The new architecture builds software security requirements into the layers of an application. Containerized applications will inherit their security controls from their application layer. Each layer’s modular security implementation can be swapped out without affecting that of other layers, facilitating software updates. Modules can be reused as needed. To avoid vendor lock-in, security will be implemented with open source components.

“Developers shouldn’t have to reinvent the security wheel,” said Chick. “They should be free to focus on their mission.” Under this modular, layered approach to security, software developers will not need to reimplement security for every module of an application. This approach speeds up software development and delivery, facilitates continuous adaptation and frequent modular upgrades, and improves mission support.

The layered, modular security architecture makes it easier to implement cybersecurity best practices to meet evolving threats. It also facilitates ongoing security compliance and management efforts. Security can be implemented earlier in the development process and customized for each application layer. Software modules will have better access control and improved protection from vulnerabilities and attacks from both external and internal threats. They can also be individually monitored for security compliance, reducing the overall testing burden. This architecture will help applications achieve continuous ATO, better meet mission needs, and further the National Defense Strategy’s approach to cyberspace as a warfighting domain.

Chick’s team is partnering with the U.S. Air Force to design this layered security architecture. The team is currently working on documenting the DevSecOps security model. The resulting document will serve as a guide for DevSecOps development efforts across the DoD.

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for “2019 SEI Year in Review Resources.”

Featured Researchers **Jamie Lord & Tracy Bills**

Building International Cybersecurity Capacity

Cyberattacks pose significant risks to critical infrastructure and strategic industrial sectors throughout the world. Global leaders must mitigate the risks these attacks pose to systems that keep governments and economies functioning. In this global threat environment, there is a growing need for expert teams that can quickly and effectively detect and respond to computer security incidents.

The United States relies on and collaborates with its allies to combat emerging cyber threats. In response to these threats, the U.S. Department of Defense (DoD) cybersecurity strategy mandates improving the cyber capabilities of its allies in regions important to its military and diplomatic strategies.

The SEI supports the DoD's strategic goals, including the 2018 National Defense Strategy's focus on strengthening alliances and attracting new partners, as well as cyberspace as a warfighting domain, by improving international cybersecurity capabilities. To increase the overall U.S. cybersecurity posture, the SEI helps U.S. allies establish computer security incident response teams (CSIRTs). CSIRTs are service organizations responsible for receiving, reviewing, and responding to computer security incident reports and activity. CSIRTs with national responsibility, or national CSIRTs, are designated by a country to protect its cybersecurity.

The SEI helps CSIRTs understand how to

- establish the cybersecurity capabilities they need
- collaborate with the broader community regionally and internationally

As an extension of this capacity building, the SEI also develops and provides incident response training, practical and tabletop exercises, facilitated discussions and workshops, exchanges of best practices, and implementations of cybersecurity roadmaps.

To support national CSIRTs, the CERT Division of the SEI founded the Forum of Incident Response and Security Teams (FIRST), which evolved into a nonprofit organization led by its international membership. FIRST holds an annual Conference on Computer Security Incident Handling, where the SEI continues to play an active role. At each FIRST Conference, the SEI hosts the Annual Technical Meeting for CSIRTs with National Responsibility (NatCSIRT). The 2019 meeting was held in Edinburgh, Scotland, and drew 125 attendees from 51 countries.

The SEI's international capacity-building work in regions such as sub-Saharan Africa, East Asia and the Pacific, eastern Europe, and the western Balkans emphasizes the need to share cybersecurity information and collaborate with other regional CSIRTs. In 2019, the SEI supported regional events, such as a cybersecurity boot camp in Leon, Spain, for 29 students from 16 countries and a training symposium in Santiago, Chile, for 38 students from 14 countries.

U.S. Government agencies share indicators of compromise—pieces of forensic data that identify potentially malicious activity on a system or network—with partner countries. This sharing of information increases overall global cybersecurity posture. To help partner countries collaborate with the United States, the SEI developed an Incident Response Workshop that helps CSIRT staff members detect, respond to, and mitigate malware. The workshop will be conducted across the globe with an initial focus on the Indo-Pacific region. This modular workshop can be tailored to serve CSIRTs with varying levels of operational expertise and ability.

As the field of incident response continues to adapt to emerging threats, national CSIRTs are expanding the services they provide. To better help national CSIRTs build their capacities, the SEI expanded its work to include support for sector CSIRTs, including critical infrastructure sectors. For example, in the United States and abroad, the SEI is helping financial sector entities implement best practices in information sharing and incident response planning and preparation.

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."

JAMIE LORD, SECURITY OPERATIONS TECHNICAL MANAGER

TRACY BILLS, SENIOR CYBERSECURITY OPERATIONS RESEARCHER

"Just as pervasive, wireless broadband communication did for the Internet of Things, 5G will accelerate and amplify the Internet of Everything."

—GREG SHANNON, CHIEF SCIENTIST, CERT DIVISION

Featured Researcher **Greg Shannon**

5G in DoD Operations: Maximize Value and Minimize Risk

CERT Division Chief Scientist Greg Shannon describes how the SEI can help the Department of Defense solve the challenges of 5G.

5G technology promises dazzling capabilities, and its adoption in the commercial, industrial, and military sectors is certain. However, U.S. manufacturers are not dominating competitors in the development of economical 5G equipment and the investment and roll-out of its infrastructure. Chinese vendors, whom many fear may give state actors privileged access to their equipment, are poised to be the first movers in the worldwide 5G market. Department of Defense (DoD) operations must be prepared for 5G, both to guard against its risks and to gain the most from its many benefits.

Just as 4G LTE enabled mobile video and audio streaming, 5G's high bandwidth, low latency, and constant connectivity will enable a new generation of smart technologies. Autonomous vehicles, automated factories, and augmented reality will finally have a network capable of handling the data these applications require.

DoD capabilities, from everyday logistics to hypersonic weapons systems, will also benefit. Improved edge computing will support maintenance staff and warfighters alike. The volume and delivery speed of data will feed a new generation of artificial intelligence (AI) and machine learning (ML) tools. Yet the DoD will have to manage the risks posed by the presence of 5G on base, off base, and in the field, regardless of who manufactured the equipment or wrote its software.

The DoD's current model of fragmented, bespoke communications networks will, in part, yield to unified, commercially supplied and operated 5G networks. The latest in tactical, wireless mesh networks, a technology the SEI continues to explore in its Future Autonomous Battlespace RF with Integrated Communications (FABRIC) project, will need to coexist with nontactical 5G networks. Commingled military and nonmilitary communications will be carried over infrastructure supplied by international vendors. The leading vendors, which also develop the infrastructure's software, are not from U.S.-allied nations. For the first time, the U.S. will not dominate the standard communications technology.

Whatever 5G control the U.S. may have inside its borders will diminish greatly in overseas operations, where DoD assets will have to interoperate with 5G networks built with even more non-U.S. components, possibly operating in a different spectrum band.

Just as pervasive, wireless broadband communication did for the Internet of Things, 5G will accelerate and amplify the Internet of Everything. Eventually, the low-power transmitters capable of pinging 5G networks, plus consumers' increasing demand for connectivity, will incentivize manufacturers to add 5G capabilities to more and more products. Manufacturers of products from dishwashers to doorknobs will find it cheaper to build 5G connectivity into every item rather than just some. This increased sensorization of products and operations by the private sector presents a security challenge to defense acquisitions, which will need to guard against inadvertently introducing unauthorized, sensorized materiel into restricted DoD environments. Even the desirable increase of authorized, connected devices will increase the DoD's attack surface.

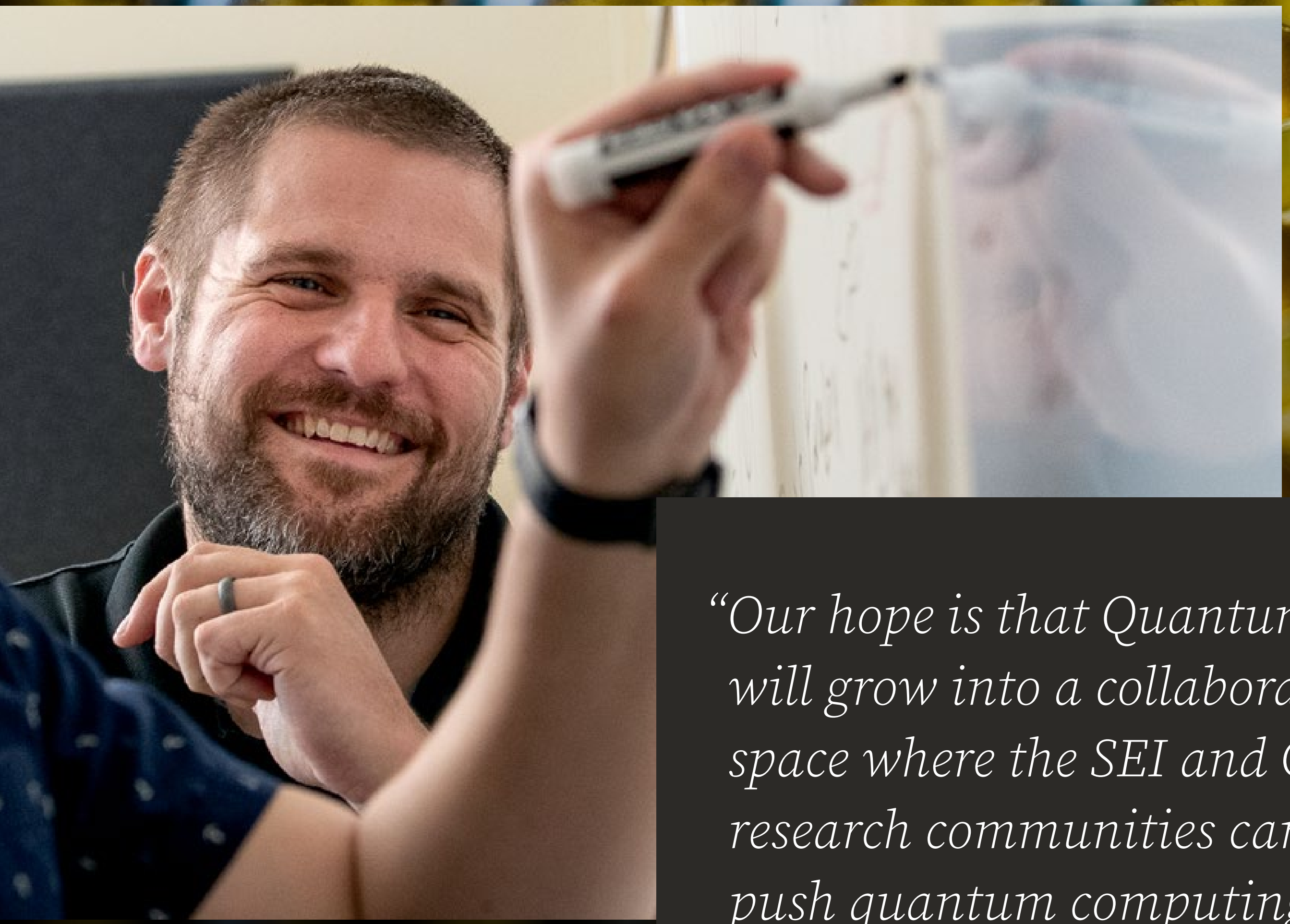
5G is a global, commercial technology. For the DoD to maximize the value and minimize the risk of 5G, it must stay in step with industry.

The SEI stands ready to help the DoD adopt and coexist with 5G:

- *Agile, software-driven acquisition in logistics.* The SEI has an established history of advising the DoD in software acquisition, which will become even more important as 5G inspires more and more software-based products.
- *DevSecOps development environment.* 5G application development within the DoD will require the modern DevSecOps software development techniques of industry to incorporate the desired operational capabilities. The SEI will continue to lend the DoD its expertise at implementing these techniques in the DoD as it scales 5G applications across multiple contexts and programs of record.
- *Risk assessment.* Tools and methods derived from the SEI's CERT Resilience Management Model (RMM) will help the DoD quantify the risk and resilience of base operations impacted by 5G capabilities.
- *Vulnerability discovery and disclosure.* The SEI's CERT Coordination Center (CERT/CC) has strong relationships with IT vendors and security researchers. With so many 5G base stations and other infrastructure—and the software it runs on—beyond direct U.S. influence, the CERT/CC's role in ensuring the quality and coordination of software vulnerability and disclosure will be more critical than ever.
- *AI and ML.* Extracting value from the volume and variety of 5G-enabled data flows will require AI and ML tools. The SEI will help the DoD consider the associated challenges and opportunities, from using sound AI engineering practices to defending against adversarial AI.

5G will become globally pervasive, impacting the DoD in peace and conflict. The SEI advises and demonstrates to the DoD the software and security challenges and opportunities of 5G, ultimately to dominate on the battlefield.

DANIEL JUSTICE, SOFTWARE DEVELOPER



> “Our hope is that Quantum Hub will grow into a collaborative space where the SEI and CMU research communities can push quantum computing research forward.”
>
> —JASON LARKIN, RESEARCH SCIENTIST

Predicting the Future of Quantum Computing

The integrated circuit computing paradigm that powered so many computing breakthroughs over the past five decades is reaching its limit. According to Jason Larkin, a research scientist in the SEI’s Emerging Technology Center, this problem means the complexity of the computing challenges facing the Department of Defense (DoD) is beginning to exceed the capacity of current hardware and software. For example, classical computers could take billions of years to solve the problems involved in verifying and validating complex software systems or developing advanced artificial intelligence (AI).

Quantum computing is a new paradigm that could introduce the next era of computing speed and power and support the development of a new generation of software capabilities. The SEI’s research on quantum computing aims to predict how this emerging technology will evolve in the coming years in an effort to advance the state of research in the field and guide the DoD about when to invest in quantum computing and which forms will most likely meet the DoD’s needs.

“Quantum computers promise greater computing power by leveraging the quantum phenomena of superposition and entanglement to create the fundamental element of quantum computing: the qubit,” explained Larkin. “When measured, they collapse into a one or a zero like classical computers, but their exponential scaling provides unique properties we can leverage to potentially increase computational capacity.”

Quantum technology represents such a potentially significant leap forward in computing that it might impact multiple modernization areas of the 2018 National Defense Strategy, from developing AI for advanced autonomous systems to creating simulations for space warfighting material production. Communications security; precision position, navigation, and timing capabilities; enhanced sensor networks for targeting; and data analysis are other areas where the DoD hopes to benefit from quantum computing.

But first, quantum hardware has to mature out of what researchers call the era of the NISQ, or noisy intermediate scale quantum processing unit. According to Larkin, qubits are “noisy” because they are likely to flip to different states when interacting with each other and their environment. In recent years, quantum computing researchers have found ways to correct for the noise. However, development remains in the early stages, and it is difficult to tell when the hardware will deliver the capabilities that early research promises are possible.

A major goal of the SEI’s research is to predict when quantum computers might demonstrate quantum advantage: when a quantum computer can obtain a solution more quickly, or obtain a better-quality solution, than a classical computer for a problem with practical relevance. The SEI is investigating several algorithms to predict the advent of quantum advantage and its hardware requirements. To help the DoD achieve quantum advantage, Larkin said, the SEI is working with NISQ devices to

- benchmark variational quantum optimization techniques and their ability to tolerate NISQ-era quantum computing units (QPUs)
- improve circuit generation for NISQ-era QPUs
- analyze the hierarchy of the problems of interest and identify which parts can be mapped effectively to QPUs
- address the challenges of scaling up the number of qubits in a quantum computer and predicting quantum advantage
- develop software tools to help data scientists and engineers use quantum computers
- promote quantum-computing literacy in the DoD workforce

Because applied quantum computing is so new, a robust research community has not yet formed around the field. Part of the SEI’s work is to promote greater communication among individuals and institutions to help advance the field, improve education, and hasten the arrival of useful applications. As part of its collaboration with Carnegie Mellon University (CMU) on quantum computing, the SEI has established Quantum Hub (quantum.etchub.xyz/hub/login), a central location for researchers everywhere to collect and share information about leading work. “Our hope is that Quantum Hub will grow into a collaborative space where the SEI and CMU research communities can push quantum computing research forward,” Larkin said.

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for “2019 SEI Year in Review Resources.”

Featured Researchers **Matt Butkovic & Matt Trevors**

Maturity Model Certification to Improve Cybersecurity in the DoD Supply Chain

Adversaries exploiting the trusted supply chain in the Defense Industrial Base (DIB) exfiltrate tens of billions of dollars of intellectual property and controlled unclassified information annually. One of the primary culprits for much of this theft is poor cybersecurity posture.

To combat this weakness, the Department of Defense (DoD) Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) turned to the SEI's expertise in maturity models and measurement to create the Cybersecurity Maturity Model Certification (CMMC). The program will help improve security in the supply chain and enable the DoD to make risk-informed decisions when it shares information with DIB contractors. Additionally, it will facilitate the rigorous measurement of cybersecurity capabilities and create justified confidence in DIB partners. Better DIB supply chain security will impact multiple modernization capabilities of the 2018 National Defense Strategy.

"Uncompromised security is invaluable to our nation. The new [CMMC] cybersecurity standards will eliminate the current disparate, scattered requirements and get everyone on a level playing field to ensure we work together collaboratively," Katie Arrington, chief information security officer for the assistant secretary of defense for acquisition, told the Charleston Defense Contractors Association's 2019 conference.

The SEI built the initial versions of the CMMC in collaboration with Johns Hopkins University Applied Physics Laboratory, a university affiliated research center, in 2019. The full model was released in January 2020, and pilot testing will occur in the first half of the year. The SEI, in support of OUSD(A&S), will work with the CMMC Accreditation Body, after it is formally established in early 2020, to assist with future implementation of the cybersecurity maturity model.

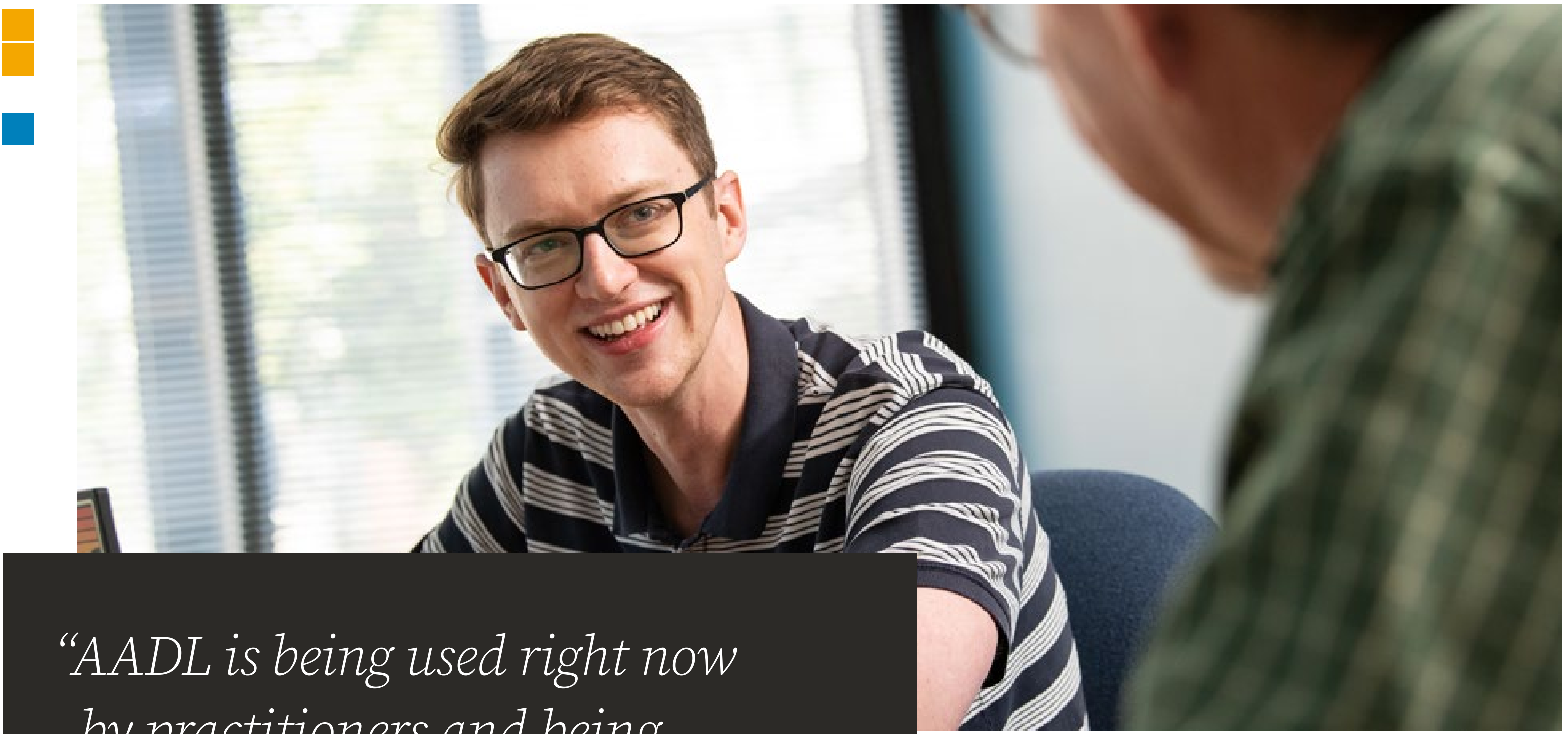
"We've designed the CMMC program based on the solid foundation of long-validated SEI and industry cybersecurity concepts," explained Matthew Butkovic, technical director of cyber risk and resilience at the SEI. "And, we've put at the forefront the needs and resources of all companies that make up the DIB, so that even small businesses can achieve a necessary baseline of maturity and help strengthen the security of the entire supply chain."

To learn more about the CMMC, visit www.acq.osd.mil/cmmc/.

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."

> *"The new [CMMC] cybersecurity standards will eliminate the current disparate, scattered requirements and get everyone on a level playing field to ensure we work together collaboratively."*
>
> —KATIE ARRINGTON, OUSD(A&S) CHIEF INFORMATION SECURITY OFFICER

Photo: U.S. Navy



> *"AADL is being used right now by practitioners and being transitioned to Future Vertical Lift programs."*
>
> **—SAM PROCTER, SENIOR ARCHITECTURE RESEARCHER**

Photo: U.S. Army

Featured Researcher **Sam Procter**

AADL's Research-to-Practice Pipeline Supports the Army Futures Command

Modernizing the U.S. Army can be daunting when every piece of new technology must be exhaustively verified and validated to ensure the safety, security, and mission-critical support of warfighters. "We need agile processes applied to our systems in the future to get the capability to the soldier where they can fight the fight," noted Alex Boydston, project engineer for the U.S. Army Futures Command. "Doing that in an area where you've got to certify and qualify and make it so that it's airworthy is rather challenging." The Army Futures Command, which focuses on Army modernization, partnered with the SEI to create a better approach to building critical embedded systems through the use of the Architecture Analysis and Design Language (AADL) and the SEI's Open Source AADL Tool Environment (OSATE).

"It's very difficult to integrate software and hardware and get that right," stated Boydston. AADL helped get it right in a recent Army project in which multiple contractors designed, developed, and integrated components in a research and development mission system. Early in system architecture development, one of the contractors discovered potential integration problems due to throughput and latency issues. With standard development methods, these performance issues would not have been discovered until system integration. Through AADL and OSATE analyses, problems that would have arisen upon component integration were detected and addressed early in development. In this case, AADL has turned the risks associated with embedded software and hardware integration into an opportunity to integrate and repair earlier in development to avoid schedule delays and increased cost.

Developed as SAE International standard AS5506 under SEI technical leadership, and first published 15 years ago, AADL is an industry-adopted modeling language that represents the architecture of large-scale, software-intensive embedded systems. OSATE allows users to define a model of their embedded computing system and integrate all the parts virtually. Once virtually integrated, "We have analysis capabilities that can tell you if you are running into issues like timing issues or failures issues up front," explained the SEI's Peter Feiler, technical lead of the AADL standardization efforts. "Eighty percent of embedded software system issues are currently discovered post unit-test, and their correction consumes fifty percent or more of the total system development cost." AADL introduces the capability to find and fix embedded system integration problems earlier, significantly reducing the cost of fixes after software and hardware are developed.

"AADL is being used right now by practitioners and being transitioned to Future Vertical Lift programs," noted Sam Procter, senior architecture researcher in the Software Solutions Division of the SEI, referring to one of the U.S. Army's Big Six modernization priorities. Both researchers and DoD system developers use the AADL language and associated tools, reducing the costs of reimplementing theoretical concepts and retraining engineers, as well as detecting defects early to reduce cost and effort during implementation, testing, and operations. It also allows the DoD to develop, test, iterate, and integrate mission-critical technology more quickly to support warfighters in the field, a pipeline that can advance multiple modernization capabilities of the 2018 National Defense Strategy. Procter added, "Really, this work is about transitioning research to practice."

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."

Managing Technical Debt for Modern Software Development

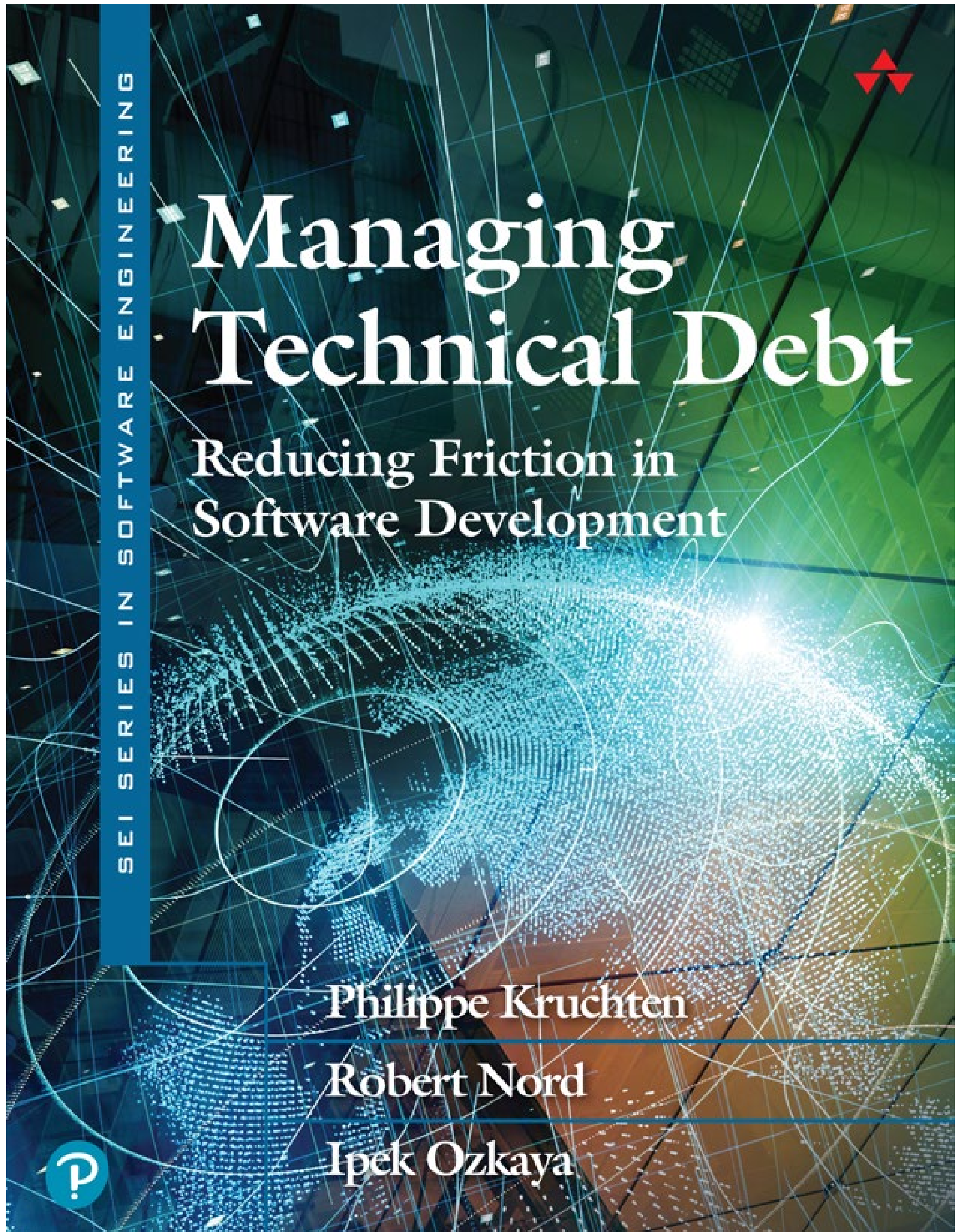
The U.S. Department of Defense (DoD) must constantly manage the dual challenges of budget constraints and the need to accelerate capability delivery. These challenges have encouraged the DoD to adopt incremental approaches to software development and shift from the acquisition of new systems to the more cost-effective evolution and sustainment of existing systems. Accumulated design and implementation decisions made for expediency, without due consideration for sustainment and evolution, often result in systems that become prohibitively expensive to maintain or extend.

Choosing short-term, easy solutions is a pervasive practice in software engineering that can result in technical debt: design or implementation constructs that are expedient in the short term but that make a future change costly or impossible.

Technical debt conceptualizes the tradeoff between the short-term benefits of rapid delivery and the long-term value of developing a software system that is easy to evolve, modify, repair, and sustain. Like financial debt, technical debt can be a burden, or it can be an investment strategy that speeds up development when backed by a plan to repay the debt.

Actively managing technical debt can help organizations control the cost of change. While technical debt can have dire consequences, an organization that borrows or leverages time and effort that is repaid in the future can realize greater returns than if it had remained debt free. This dual nature of technical debt—both good and bad—makes dealing with it confusing.

A 2015 SEI survey of industry, defense contractors, and government development and sustainment projects indicated that though technical debt is a long-standing problem in software development, the development community lacks a cohesive approach to it. A new book, *Managing Technical Debt: Reducing Friction in Software Development* in the SEI Series in Software Engineering, fills that gap by formalizing the principles and practices for managing technical debt, on par with practices such as requirements engineering, software architecture, design, and testing. The book was written by Philippe Kruchten, a professor of software engineering at the University of British Columbia in Vancouver, and senior members of the SEI's technical staff Robert Nord and Ipek Ozkaya.

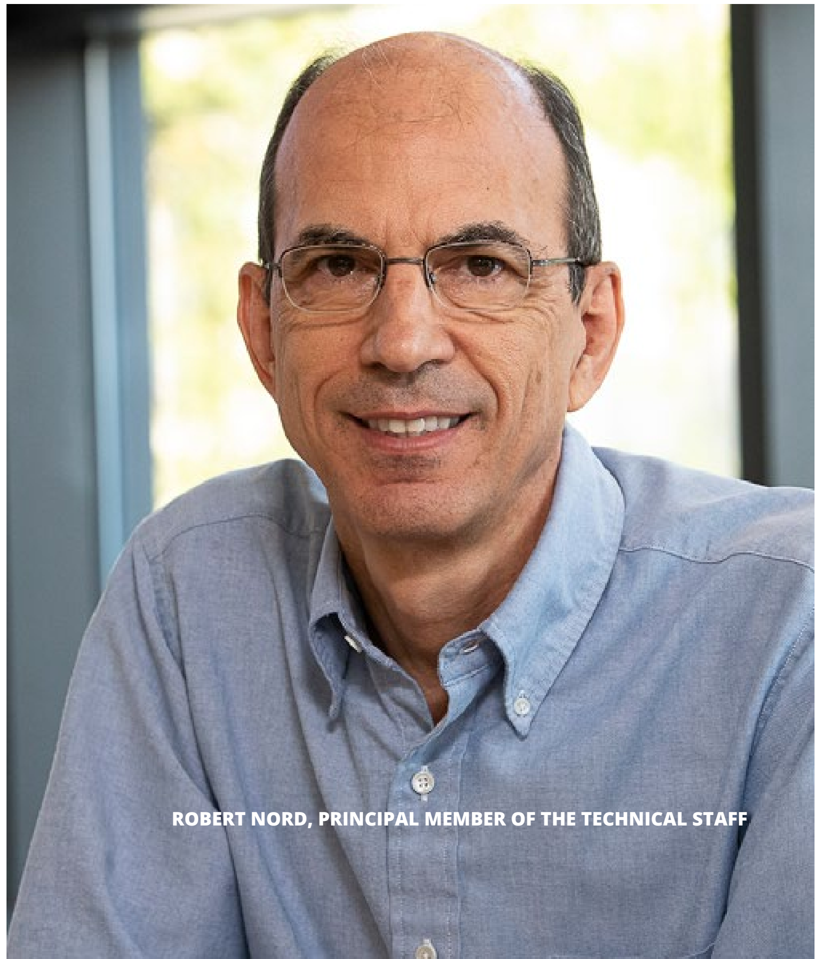

SEI SERIES IN SOFTWARE ENGINEERING
Managing Technical Debt
Reducing Friction in Software Development
Philippe Kruchten
Robert Nord
Ipek Ozkaya
P

The SEI also offers a course called "Managing Technical Debt of Software" and was instrumental in establishing the international TechDebt Conference, co-located with the International Conference on Software Engineering (ICSE), to provide a forum for practitioners and researchers to share emerging practices. Technical debt is increasingly recognized as a core software engineering practice for ensuring that systems are built and sustained within their business, mission, budget, and quality needs.

Currently, the SEI is helping organizations establish management practices for technical debt and advancing ways to automate software architecture and technical debt analysis through software analytics. The work combines techniques from machine learning, refactoring, code analysis, and data mining to describe technical debt items that identify problematic design issues. In addition, the SEI is building automated techniques that can help avoid software design issues that may result in technical debt.

According to the Defense Industrial Base's software acquisition and practices study, "The current approach to software development ... takes too long, is too expensive, and exposes warfighters to unacceptable risk by delaying their access to tools they need to ensure mission success." Streamlining rapid, iterative approaches to software development and fielding, while driving budget discipline and affordability, will put short-term and long-term goals in constant tension. Managing the technical debt from those choices can help the DoD modernize many of the software-driven capabilities outlined in the 2018 National Defense Strategy, from the artificial intelligence and machine learning underpinning advanced autonomous systems to the software components enabling resilient and agile logistical support for the warfighter.

To learn more about this and other topics discussed in the *Year in Review*, visit resources.sei.cmu.edu and search for "2019 SEI Year in Review Resources."



ROBERT NORD, PRINCIPAL MEMBER OF THE TECHNICAL STAFF

IPEK OZKAYA, TECHNICAL DIRECTOR, ENGINEERING INTELLIGENT SOFTWARE SYSTEMS

Carnegie Mellon University Leadership

Farnam Jahanian
President

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

J. Michael McQuade
Vice President, Research

SEI Executive Leadership

From left to right:
Sandra Brown, SEI General Counsel;
Bobbie Stempfley, Director, CERT Division;
Roman Danyliw, Deputy Chief Technology Officer

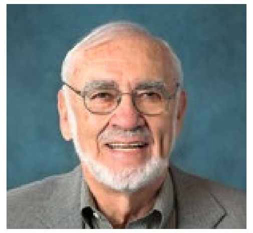
Anita Carleton, Director, Software Solutions Division;
Paul Nielsen, Director and Chief Executive Officer;
Heidi Magnelia, Chief Financial Officer;
Tom Longstaff, Chief Technology Officer

David Thompson, Deputy Director and Chief Operating Officer; Mary Catherine Ward, Chief Strategy Officer; Matt Gaston, Director, Emerging Technology Center

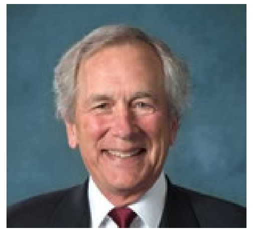
Board of Visitors

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.

Barry W. Boehm
TRW Professor of Software Engineering, University of Southern California; Director, University of Southern California Center for Software Engineering



Gilbert F. Decker
Consultant; former President and CEO, Penn Central Federal Systems Company; former President and CEO of Acurex Corporation; former Assistant Secretary of the Army/Research, Development, and Acquisition



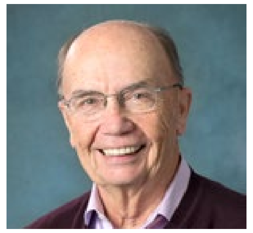
Philip Dowd
Private investor; former Senior Vice President, SunGard Data Systems; Trustee, Carnegie Mellon University

John M. Gilligan
President, Gilligan Group; former Senior Vice President and Director, Defense Sector of SRA International; former CIO for the Department of Energy

Elizabeth A. Hight
Former Vice President of the Cybersecurity Solutions Group, Hewlett Packard Enterprise Services; former Rear Admiral, U.S. Navy; former Vice Director of the Defense Information Systems Agency

Tom Love
Chief Executive Officer, ShouldersCorp; Founder of Object Technology Group within IBM Consulting

Alan J. McLaughlin
Chair, Board of Visitors; Consultant; Former Assistant Director, MIT Lincoln Laboratory



Donald Stitzenberg
President, CBA Associates; Trustee, Carnegie Mellon University; former Executive Director of Clinical Biostatistics at Merck; Member, New Jersey Bar Association

SEI Leadership

DIRECTOR'S OFFICE

Paul Nielsen
Director and Chief Executive Officer

David Thompson
Deputy Director and Chief Operating Officer

Tom Longstaff
Chief Technology Officer

Roman Danyliw
Deputy Chief Technology Officer

SOFTWARE SOLUTIONS DIVISION

Anita Carleton
Director

John E. Robert
Deputy Director

Charles Holland
Chief Scientist

EMERGING TECHNOLOGY CENTER

Matt Gaston
Director

Brenda Penderville
Deputy Director (Acting)

CERT DIVISION

Bobbie Stempfley
Director

Bill Wilson
Deputy Director

Greg Shannon
Chief Scientist

FINANCIAL & BUS. SERVICES

Heidi Magnelia
Chief Financial Officer

STRATEGIC INITIATIVES

Mary Catherine Ward
Chief Strategy Officer

SEI LEGAL

Sandra Brown
SEI General Counsel

Copyright

Credits

Manager, Communication Services
William Thomas

Manager, Corporate & Technical Communications
Janet Rex

Manager, Public Relations
Richard Lynch

Manager, Communication Design
Cat Zaccardi

Editor-in-Chief
Paul Ruggiero

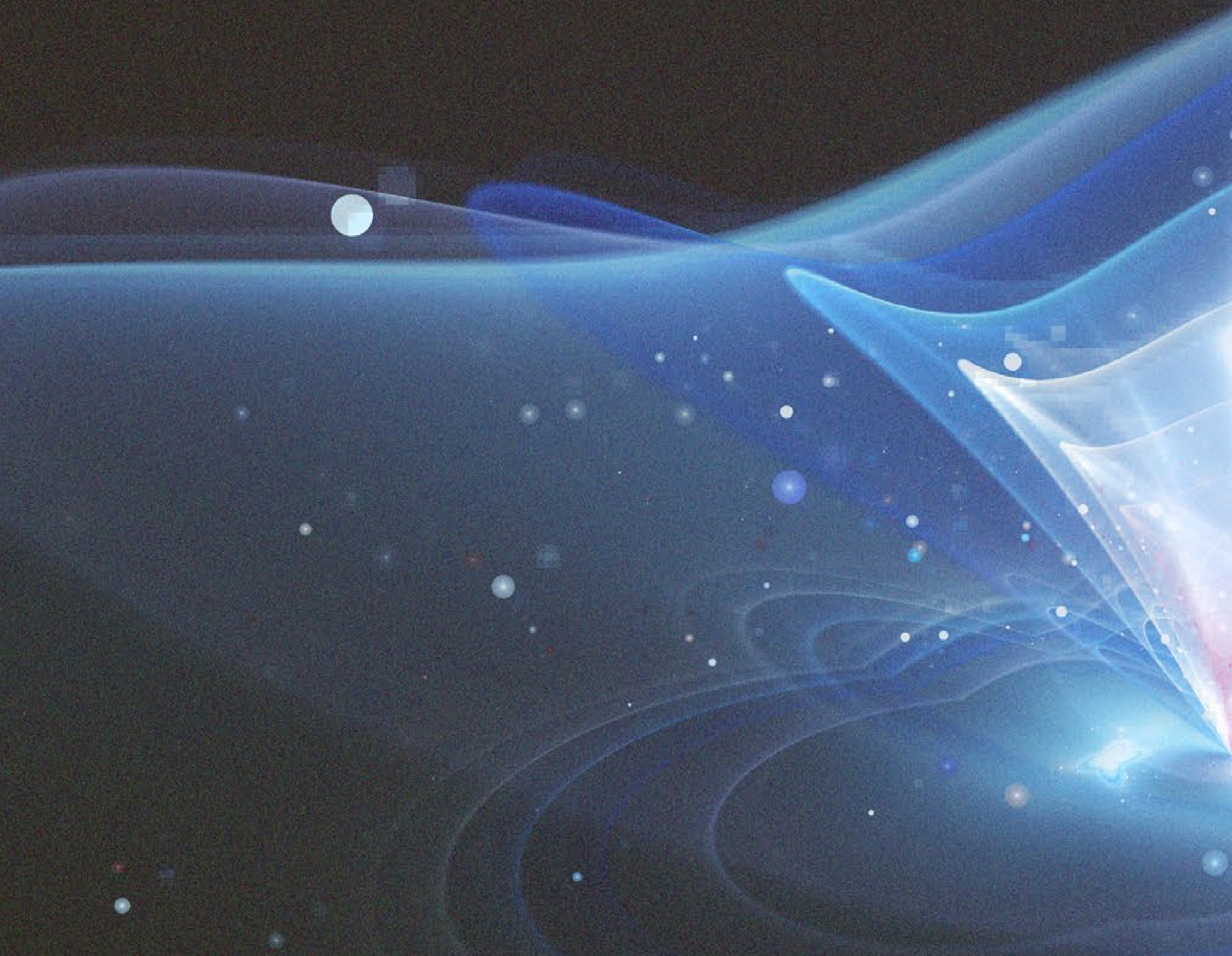
Editorial
Hollen Barmer
Ed Desautels
Claire Dixon
Patricia Flinn
Lope Lopez
John Morley
Sheela Nath
Nancy Ott
William Pollak
Sandy Shrum
Barbara White

Design
Christopher Baum

Illustration
Kurt Hess

Digital Production
Mike Duda

Photography
Alexandrea Van Deusen
David Biber
Tim Kaulen, CMU



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

SEI Washington, DC
NRECA Building, Suite 200
4301 Wilson Boulevard
Arlington, VA 22203

SEI Boston, MA
10 Maguire Road
Lexington, MA 02421

SEI Los Angeles, CA
2401 East El Segundo Boulevard
El Segundo, CA 90245

SEI Patuxent River, MD
23076 Three Notch Road
Suite 201
California, MD 20619