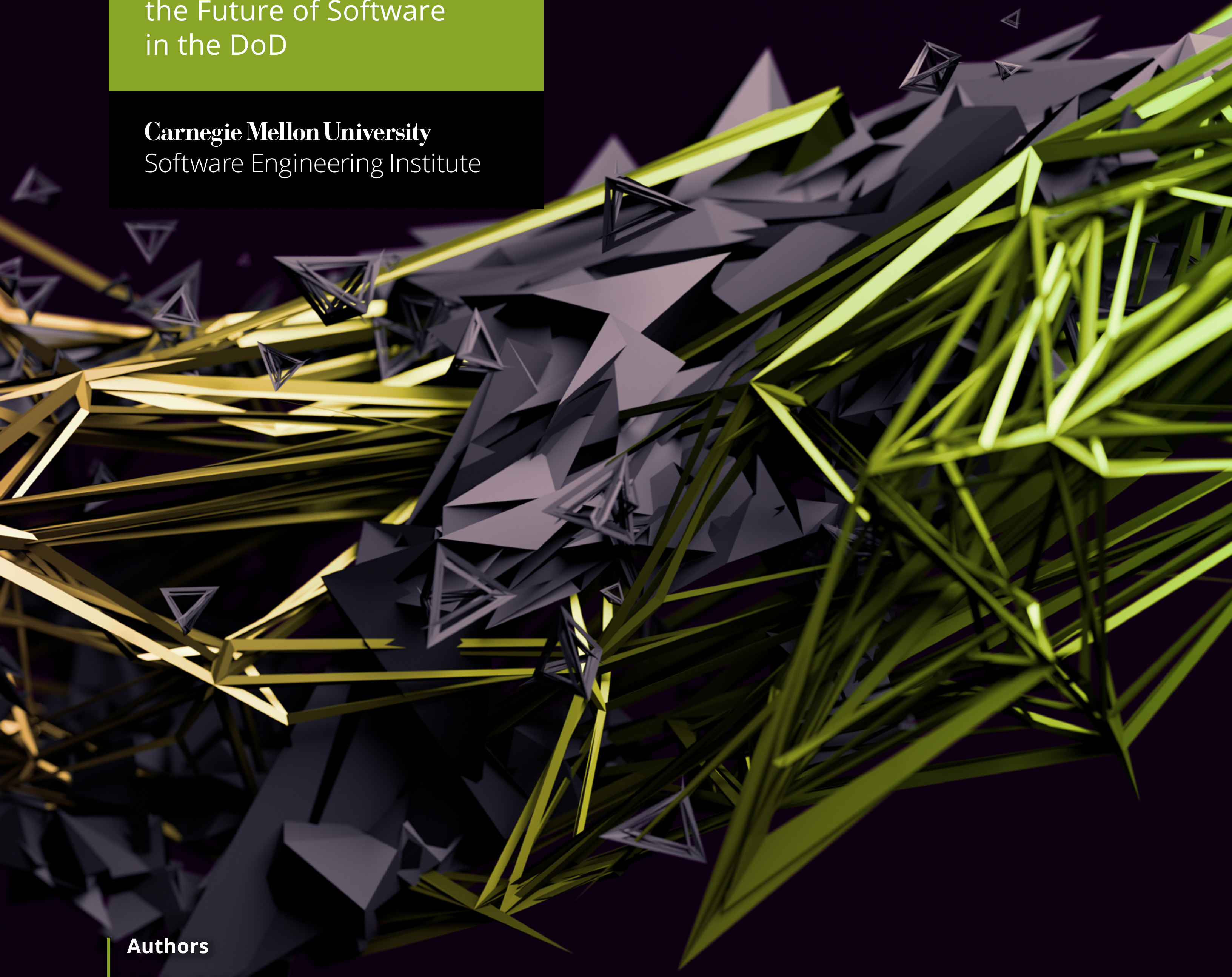
Emerging Technologies

Seven Themes Changing the Future of Software in the DoD

Carnegie Mellon University
Software Engineering Institute



Authors

Michael Abad-Santos

Scott Hissam

Shen Zhang

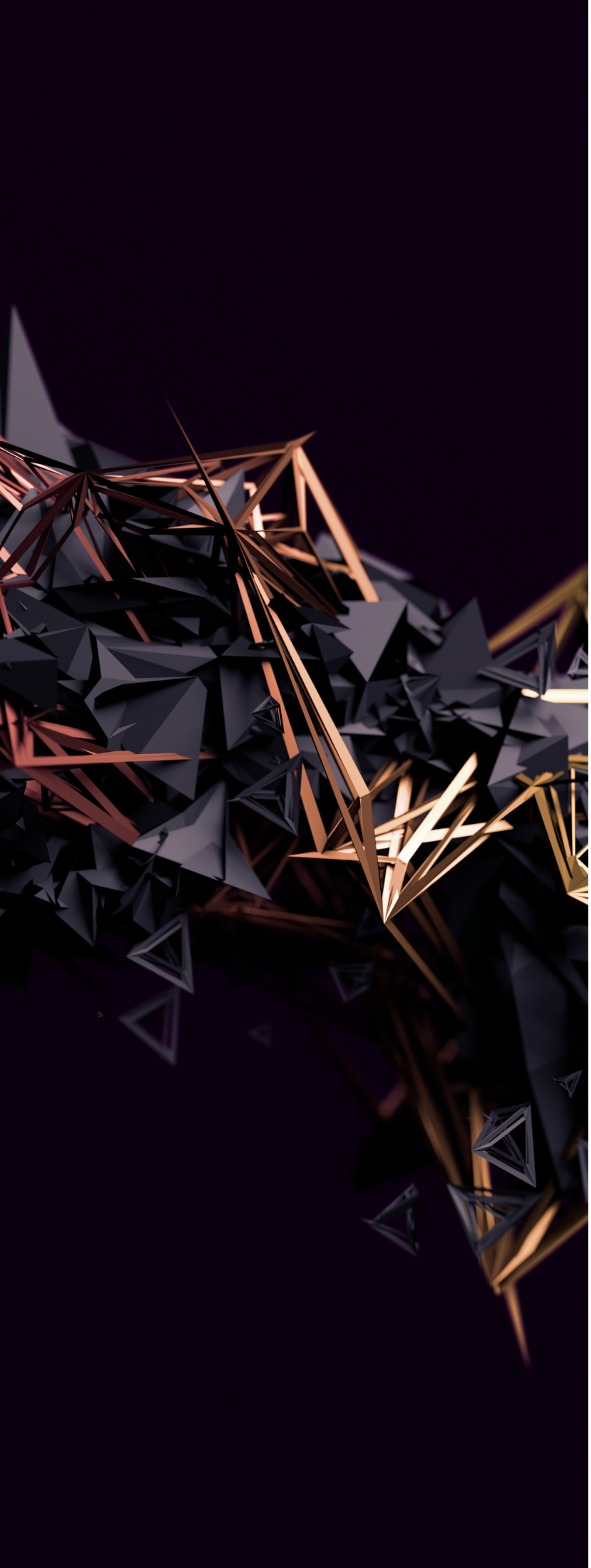


Table of Contents

Acknowledgments

The authors of this report would like to acknowledge the following Software Engineering Institute (SEI) Software Solutions Division (SSD) staff, all of whom provided valuable feedback and input used in this report:

Dionisio De Niz
Technical Director, Assuring Cyber-Physical Systems

Thomas P Evans
Senior Software Architect and Initiative Lead

Charles Holland
Principal Researcher

Mark H Klein
Principal Technical Advisor

Matthew D Milazzo
Senior Program Development Manager

Ipek Ozkaya
Technical Director, Engineering Intelligent Software Systems

Alexis Presti-Simpson
Senior Engagement Manager

David A Scherb
Program Development Manager

Forrest J Shull
Lead for Defense Software Acquisition Policy Research

Robert Stoddard
Initiative Lead, Software Engineering Measurement and Analysis

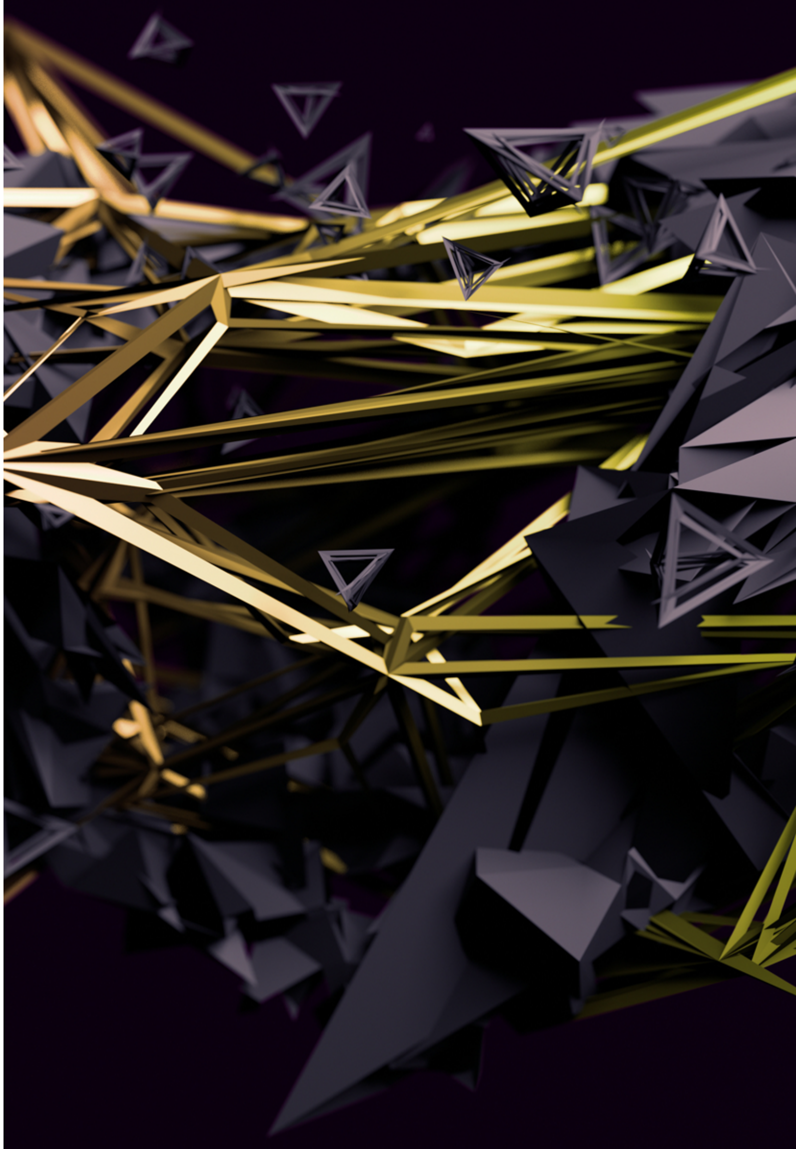
Greg Such
Program Development Manager

Eileen Wrubel
Technical Director, Transforming Software Acquisition Policy and Practice

Hasan Yasar
Technical Director, Continuous Deployment of Capability

We also extend our deepest thanks to SSD leaderships, especially Anita D. Carleton, Director; John E Robert, Deputy Director; and Harold Ennulat, Associate Director, Program Development and Transition, for funding and accepting a new delivery paradigm for this year's study.

We also thank the SEI's Technical leadership for their guidance and insight, especially SEI Chief Technology Officer Tom Longstaff and Deputy Chief Technology Officer Roman Danyliw.



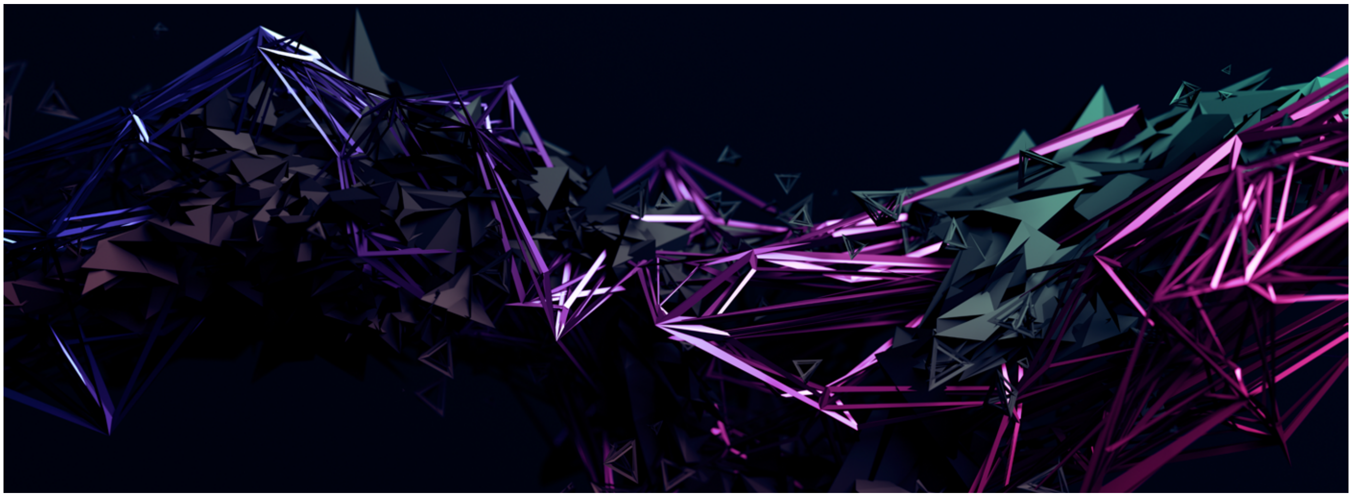
Executive Summary

This report summarizes the SEI's Emerging Technologies Study (ETS), the findings of which are important to the SEI, its DoD sponsors, and the software engineering community. Additionally, this report discusses the Emerging Technology Knowledge Base (ETKB), an internal SEI tool employing a Wikipedia-like structure to codify the data and information gathered during this study. The ETKB enables the identification of relationships among and links between the emerging technology investigated to the overarching goals and objectives of the SEI, its customers, and its sponsors.

This report discusses the following seven emerging technologies, which we have chosen from a purely software engineering perspective (that is, practices and technology). These technologies have evolved in the areas of artificial intelligence and machine learning (AI/ML), cybersecurity, digital transformation, and distributed computing.

The technologies are presented with particular emphasis on the subtopics (and their technology readiness level [TRL]):

- Advanced Computing
- Advanced Materials
- AI/ML
  - Smart Data Curation (very early TRL): Using AI to establish realistic data sets for large-scale testing of software may help address the lack of real-world data sets.
  - AI-Assisted Software Development (mid-level TRL): Some early production tools such as Amazon's Code Whisperer and GitHub's Co-Pilot are now emerging.
- Biotechnology
- Cybersecurity
  - Zero Trust (early to mid-level TRL): While this topic is getting a lot of publicity, the technology to support zero trust principles remains lacking.
- Digital Transformation
  - Smarter Edge (mid- to late-TRL) and Digital Transformation: Deep Data Semantics (early TRL) (likely combined with Advanced Computing's Ubiquitous Computing): Research into these topics is growing and predicted to become more important in emerging technology.
  - Higher Fidelity Model-Based Software Engineering (MBSE) (early TRL): Building on research previously conducted by the SEI and others in the software engineering community (such as the Architecture Analysis and Design Language [AADL], Predictable Assembly from Certifiable Code [PACC], and Adaptive Quality of Service [AQoS]), this work could advance the state of the practice for MBSE. Prior SEI work, such as PACC, may have been before its time: Some of the subject-matter experts we talked to in the fields of low-code/cloud computing and MBSE described a "next-generation" MBSE, in which "models become the software" (i.e., by removing the human-in-the-loop translation of software and system models to running code).
- Distributed Computing
  - Comparing the themes and sub-themes from this year's ETS to those of the prior ETSs, other emerging technologies still prevail, including quantum computing, blockchain, and AI. Interestingly, although still included in this report, some technologies, such as quantum computing, remain more "futuristic," with timelines that are 10 years out. Not surprising, though, are the DoD's most pressing and present concerns about post-quantum cryptography (also known as *quantum-resistant cryptography*), which could invariably compromise traditional (or pre-quantum) cryptographic algorithms.

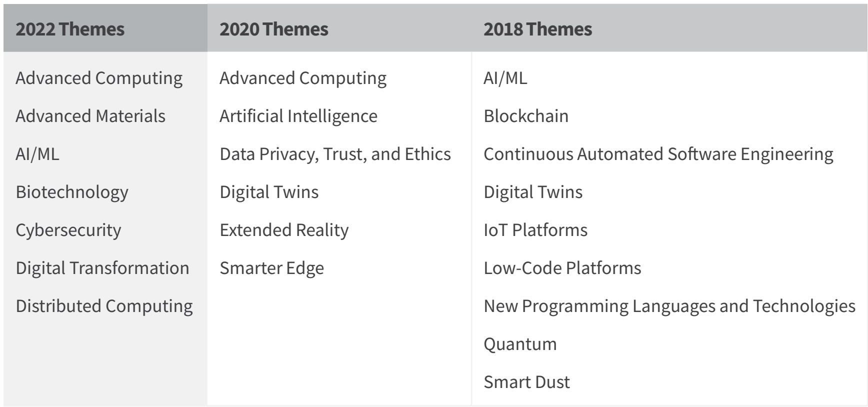


Introduction

THE PURPOSE OF THE EMERGING TECHNOLOGY STUDY (ETS) IS TO ASCERTAIN WHICH EMERGING TECHNOLOGIES ARE BECOMING SIGNIFICANT TO THE SEI, ITS DOD SPONSOR, its customers, and the software engineering community at large. The SEI's contractual line research resources are limited. Consequently, ETSs are intended to focus the SEI's research in areas that will augment our existing capability to provide sound advice and guidance on software engineering technologies and practices and provide direct benefit to the DoD and federal government. Additionally, insights from the ETS also provide opportunities for the SEI to deepen the impact that such emerging technology will have for the broader software engineering community by contributing to the body of knowledge and application of the emerging technology in DoD-relevant settings.

To complement the ETS, we developed a method to codify the data and information gathered during our investigation that employs a knowledge management system to facilitate a continuous approach to tracking emerging technology. We created this Emerging Technology Knowledge Base (ETKB) to explicitly interrelate and link the investigated sources to the overarching goals and objectives of the SEI's customers and sponsor. This approach provides a means to signify, categorically, how such emerging technology "fits" into the SEI's charter as a Federally Funded Research and Development Center (FFRDC). Another key capability of the ETKB is the ability to effectively manage the ever-changing landscape of emerging technology in a continuous manner, thus allowing SEI staff to contribute to the knowledge base as new and relevant ideas arise. It enables traceability of our justification and shifts the paradigm for future studies into one of knowledge management within a structured database.

As with prior studies, this ETS sought input and feedback on emerging technology from all of the directorates within the SEI Software Solutions Division (SSD), its business development team, and the CTO's office. We also consulted sources from academia, government, industry, and a number of existing and new SEI contacts to gather their insight. All of these sources either complemented or confirmed other unclassified and public sources to round out the technology horizon formed from this year's ETS. From those sources, in addition to an extensive literature review, the authors identified a number of themes and sub-themes. We include those themes here alongside the themes generated by the ETS 2018 and ETS 2020 activities for comparison.



2022 Themes	2020 Themes	2018 Themes
Advanced Computing	Advanced Computing	AI/ML
Advanced Materials	Artificial Intelligence	Blockchain
AI/ML	Data Privacy, Trust, and Ethics	Continuous Automated Software Engineering
Biotechnology	Digital Twins	Digital Twins
Cybersecurity	Extended Reality	IoT Platforms
Digital Transformation	Smarter Edge	Low-Code Platforms
Distributed Computing		New Programming Languages and Technologies
		Quantum
		Smart Dust

Figure 1: *ETS Themes from previous years*

Having identified those ETS 2022 themes and sub-themes, we used the ETKB to link related information from our literature review and subject matter expert (SME) interviews to SEI stakeholder-relevant goals and agendas, such as the National Defense Strategy 2018 and the Under Secretary of Defense for Research and Development Critical Technology Areas. They are also linked to SEI work products, including the National Agenda for Software Engineering R&D, past SEI emerging technology scouting activities (2018 and 2020 ETS), and current FY22 SEI Line-funded projects.

This linking is the mechanism underlying the knowledge gleaned from the data and information curated from this year's ETS. It enables relationship analysis that connects the scouting results to SEI stakeholder needs and SEI activities. This approach enables a comprehensive analysis of the associations between the emerging technology codified in the ETKB and how and where those technologies might benefit the SEI's mission in support of its stakeholders.

Enabled by the relationship created through this ETS and the ETKB, our scouting highlighted the greatest number of links to this year's ETS sub-theme of Hyperautomation under the theme Digital Transformation. This might be attributable to the transition in 2022 toward a post-pandemic period. Organizations were motivated (or forced) to do more with less as the traditional workforce morphed into a remote workforce, and as that same workforce dwindled through retirement or the pursuit of new avenues of employment. From hyperautomation we identified direct relationships to Autonomous Operations, a sub-theme under AI/ML. From a DoD mission perspective, we also found a number of links and relationships to Autonomous Operations, most specifically for both Distributed Cyber-Physical Systems (think about unstaffed, autonomous assets on the tactical edge) as well as Cyberwarfare (especially for situation awareness and detection).

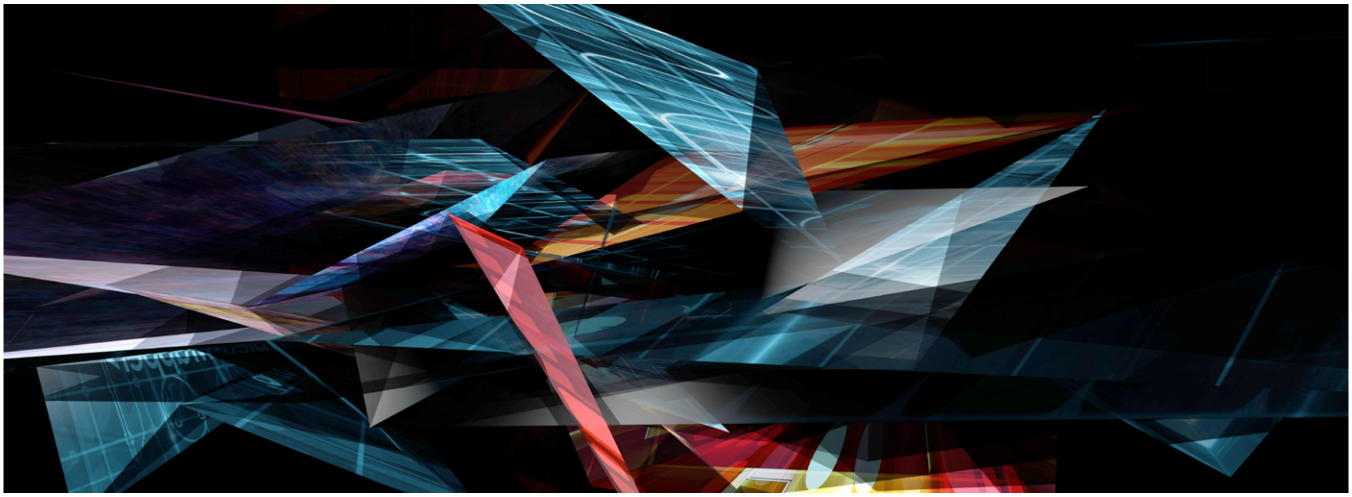
Based on our scouting, the horizon for hyperautomation for business is the next one to five years for cases in which the identified emerging technologies were in the high TRL range (depending on the technology). This means that there may already be techniques that can be adapted or transitioned into the DoD and federal spaces. From a DoD mission perspective, we could not establish concrete timelines or TRLs for hyperautomation that would be applicable. This means that there may be an opportunity to expand the concept of hyperautomation to a DoD mission perspective.

From a purely *software engineering* perspective (that is, practices and technology), the most subjectively interesting emerging technologies are artificial intelligence and machine learning (AI/ML), cybersecurity, digital transformation, and distributed computing, with particular emphasis on the subtopics (and their technology readiness level [TRL] noted:

- Advanced Computing
- Advanced Materials
- AI/ML
  - Smart Data Curation (very early TRL): Using AI to establish realistic data sets for large-scale testing of software may help address the lack of real-world data sets.
  - AI-Assisted Software Development (mid-level TRL): Some early production tools such as Amazon's Code Whisperer and GitHub's Co-Pilot are now emerging.
- Biotechnology
- Cybersecurity
  - Zero Trust (early to mid-level TRL): While this topic is getting a lot of publicity, the technology to support zero trust principles remains lacking.

- Digital Transformation
  - Smarter Edge (mid- to late-TRL) and Digital Transformation: Deep Data Semantics (early TRL) (likely combined with Advanced Computing's Ubiquitous Computing): Research into these topics is growing and predicted to become more important in emerging technology.
  - Higher Fidelity Model-Based Software Engineering (MBSE) (early TRL): Building on research previously conducted by the SEI and others in the software engineering community (such as the Architecture Analysis and Design Language [AADL], Predictable Assembly from Certifiable Code [PACC], and Adaptive Quality of Service [AQoS]), this work could take MBSE to the next level. Prior SEI work, such as PACC, may have been before its time: Some of the subject-matter experts we talked to in the fields of low-code/cloud computing and MBSE described a "next-generation" MBSE, in which "models become the software" (i.e., by removing the human-in-the-loop translation of software and system models to running code).
- Distributed Computing
  - Comparing the themes and sub-themes from this year's ETS to those of the prior ETSs, other emerging technologies still prevail, including quantum computing, blockchain, and AI. Interestingly, although still present in this report, some technologies, such as quantum computing, remain more "futuristic," with timelines that are 10 years out. Not surprising, though, are DoD's most pressing and present concerns about post-quantum cryptography (also known as quantum-resistant cryptography), which could invariably compromise traditional (or pre-quantum) cryptographic algorithms.

The following sections take up these themes and sub-themes in greater detail. The text has been drawn from the ETKB and edited for this report. Internal citations and corresponding entries in the References section correspond to sources consulted in our literature review and interviews with SMEs.



Advanced Computing

WE USE THE TERM ADVANCED COMPUTING TO REFER TO ADVANCES IN COMPUTING POWER THAT ARE ENABLED BY ADVANCES IN COMPUTER HARDWARE, FROM THE CHIP LEVEL TO THE SYSTEM LEVEL. Advanced computing is the driver for new capabilities that are enabled through software. In addition to traditional semiconductor-enabled computing, quantum computing is an important emerging technology that will revolutionize computing.

Exponential Intelligence

Description

Exponential Intelligence is a self-improving AI that is based on a self-induced feedback loop, leading, over time, to a super intelligent AI—an intelligence that would rival and surpass any human cognitive, learning, or planning task.

Generally, this level of cognizance would imply replacement of human actors in key decision-making processes within AI systems.

Significance

In the DoD context, as systems increase in complexity and remote technologies pervade, there is a need to transfer control of automatable systems to computers (for instance, in combat UAVs). In such a context, to meet increasing force multipliers and efficient operators, parts of the operational task would be delegated to sophisticated automation strategies, including AI, until only critical tasks are left for humans. This assumption—operating at the edge of exponential intelligence—cannot be pushed indefinitely into the future.

Supporting Literature

Buchholz, Scott; Bechtel, Mike; & Briggs, Bill (eds). Deloitte Insights: Tech Trends 2022. Deloitte Development LLC. 2022. **www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf**

Quantum Computing

Description

Quantum Computing is a type of non-classical computing that uses quantum bits (based on elementary particles rather than classical binary bits) that exhibit quantum entanglement whose correlation is not explained by classical physics.

Quantum computing has origins in the 1980s when the quantum mechanical model of computers was represented by Turing machines [Benioff 1980]. Since then, additional models, algorithms, and now prototypes have been developed with increasing complexity in applications, number of quantum bits, and computational scale. Of particular importance, quantum computer states are stored as n bits of information, which enables sophisticated algorithms (such as factorization algorithms) to process much faster than the equivalent in classical computers.

This capability has promising applications in cryptography and search problems with very high time complexity.

One of the hallmark challenges of quantum computing is the presence of quantum decoherence, which is the stochastic nature of quantum systems to interact with their surroundings. It requires a level of compute isolation far greater than classical computers.

Significance

In the DoD context, a critical emerging concern is whether today's cryptographic algorithms can be easily broken with quantum computing in the future. (See the section **Post-Quantum Cryptography**.)

Supporting Literature

The White House. *Executive Order on Improving the Nation's Cybersecurity*. May 12, 2021. **www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity**

Gambetta, Jay. Expanding the IBM Quantum roadmap to anticipate the future of quantum-centric supercomputing. May 10, 2022. *IBM Blog*. **research.ibm.com/blog/ibm-quantum-roadmap-2025**

Buchholz, Scott; Bechtel, Mike; & Briggs, Bill (eds). Deloitte Insights: Tech Trends 2022. Deloitte Development LLC. 2022. **www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf**

Ubiquitous Computing

Description

Ubiquitous Computing is the explicit and implicit presence of computational capability: augmenting processes, workflows, and decision making with minimal integration with the computational devices themselves.

This concept has been around for decades [Wikipedia 2022] and, as the name implies, it involves the pervasive use of software in everyday objects beyond traditional computing interfaces, such as a desktop. Ubiquitous computing can be characterized by a number of key features [Friedewald and Raabe 2011]:

- decentralization or modularity of systems
- embedding of hardware and software in everyday objects creates mobile support for highly accessible user information context awareness and adaptation
- automatic recognition and autonomous processing

Significance

In the DoD context, the concept of ubiquitous computing becomes relevant when technologies for individual warfighters evolve to have compute capabilities, such as built-in software in a soldier's accoutrement. The size and scope of this implementation vary greatly, ranging from handheld equipment to the fibers of a soldier's uniform.

By receiving granular data from each warfighter, battle command and management can eventually provide more informed, scenario-specific decisions to soldiers, which will ensure successful engagements, especially in volatile combat missions.

Supporting Literature

Buchholz, Scott; Bechtel, Mike; & Briggs, Bill (eds). Deloitte Insights: Tech Trends 2022. Deloitte Development LLC. 2022. **www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf**

Advanced Materials

ADVANCED MATERIALS, SUCH AS SMART MATERIALS AND NANOMATERIALS, ARE THE FOUNDATION for enabling new capabilities in physical systems by expanding limits in material properties.

Environmental Sciences

Description

Environmental Sciences is the interdisciplinary field encompassing atmospheric science, ecology, environmental chemistry, geosciences, and social sciences.

Significance

In the DoD context, the increase in systems complexity and the pervasiveness of remote technologies drive a need to transfer control of automatable systems to computers. An example of this trend is the combat UAV. To meet increasing force multipliers and efficient operators, parts of the operational task will be delegated to sophisticated automation strategies, including AI, until only critical tasks are left for humans. This assumption—operating at the edge of exponential intelligence—cannot be pushed indefinitely into the future.

Supporting Literature

MIT. 2022: 10 Breakthrough Technologies. *MIT Technology Review*. February 21, 2023 [accessed]. **www.technologyreview.com/2022/02/23/1045416/10-breakthrough-technologies-2022**

Physical Resiliency on the Edge

Description

Physical resiliency on the edge applies to systems that can self-heal, self-repair, and self-maintain to continue their operational objectives with minimal to no materiel logistical support.

For **distributed cyber-physical systems**, mission-critical assets with sensitive software and hardware operate on the tactical edge, which may represent adversarial conditions on the battlefield. Under these conditions, the physical resiliency of the hardware becomes critical, because whether software is running completely locally at the node or receiving data remotely, the associated hardware is necessary to fulfill those tasks.

Therefore, these decentralized nodes must be able to tolerate systemic and local faults, and they must offer expedient resolution. Approaches to physical resiliency at the edge include physically hardened physical infrastructure made with novel materials to minimize required intervention or adversarial tampering.

Significance

In the DoD context, as software acquires an ever-more-significant role in combat environments (e.g., realizing computational and algorithmic advantage), the DoD must defend computer systems from external threats. Attackers often seek to damage supporting infrastructure or gain control the lowest hardware abstraction level. By providing physically resilient barriers, defenders will have an overall decreased attack surface, which increases the success of the operating software.

Supporting Literature

StartUs Insights. Top 10 Military Technology Trends & Innovations for 2023. *StartUS Insights*. February 20, 2023 [accessed]. **www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022**

Renewable Energy

Description

Renewable Energy is energy that is sourced, and possibly stored for future use, from natural resources that are replenished at higher rates than they are consumed and therefore are not exhausted on a mission or human time scale.

Sources of renewable energy include wind power, solar power, movement of water, and geothermal heat, all of which are resources that can replenish themselves over time without human intervention. Renewable energy sources—from generation of electricity in utilities to smaller applications for which heat or electricity is required—are growing in popularity. However, one limitation of renewable energy is lack of continuous availability, which is especially important for stable generation of electricity [Wikipedia 2022a].

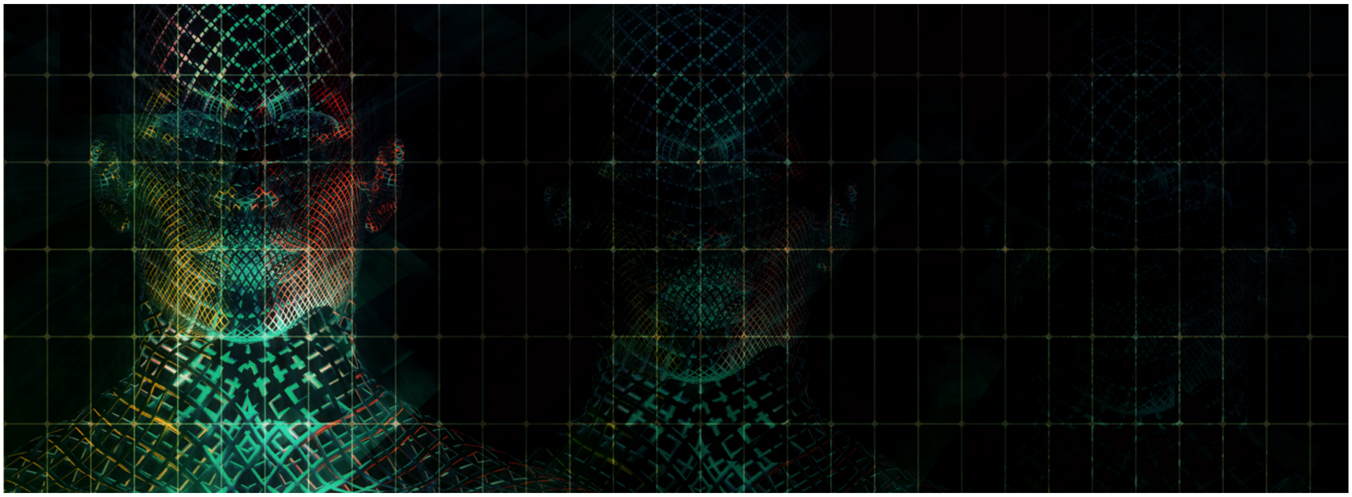
Significance

In the DoD context, renewable energy sources are used to provide alternative methods for delivering operational capabilities to warfighters. Furthermore, reliable, renewable energy sources will help warfighters reduce the dependency on traditional fossil fuels, which may be difficult to transport in adversarial environments.

Supporting Literature

Temple, James. Practical Fusion Reactors. MIT Technology Review 10 Breakthrough Technologies in 2022. February 23, 2022. **www.technologyreview.com/2022/02/23/1044948/practical-fusion-reactors-carbon-free**

Crowhart, Casey. A Long-Lasting Grid Battery. *MIT Technology Review 10 Breakthrough Technologies in 2022*. February 23, 2022. **www.technologyreview.com/2022/02/23/1044962/grid-battery-iron-clean-energy**



AI/ML

ARTIFICIAL INTELLIGENCE (AI) IS THE THEORY AND DEVELOPMENT OF COMPUTER SYSTEMS ABLE TO PERFORM TASKS THAT NORMALLY REQUIRE HUMAN INTELLIGENCE, such as visual perception, speech recognition, decision-making, and translation between languages. Machine learning (ML) is a way of achieving AI.

AI Assisted Software Development

Description

AI-assisted software development uses AI to assist, or otherwise supplant, the human software developer in the production of software code from the comprehension of expressed functional and non-functional requirements and/or specifications.

Significance

As software engineering becomes more complex, the demand to automate less-complex implementations is increasing. Furthermore, common software patterns and implementations are readily available in public domains. These solutions can be leveraged to provide a robust tool set for software engineers that will increase their productivity on more specialized tasks.

Supporting Literature

Amazon AWS. AWS announces Amazon CodeWhisperer (Preview). *Amazon AWS*. June 23, 2022. **aws.amazon.com/about-aws/whats-new/2022/06/aws-announces-amazon-codewhisperer-preview**

GitHub. Your AI pair programmer: GitHub Copilot uses the OpenAI Codex to suggest code and entire functions in real-time, right from your editor. *GitHub*. February 20, 2023 [accessed]. **github.com/features/copilot**

AI Assurance

Description

AI Assurance is a process applied at all stages of the AI engineering lifecycle to ensure that any intelligent system produces outcomes that are valid, verified, data driven, trustworthy, and explainable to a layperson. It also ensures the system is ethical in the context of its deployment, unbiased in its learning, and fair to its users [Batarseh 2021].

Significance

To keep up with the ever-dynamic pace of adversarial threats, mission operators and warfighters will need to comprehend an ever-increasing number of sources of intelligence and sensors to choose the best course of action in real time. Such comprehensiveness can easily overwhelm human cognition. Consequently, decision makers must be able to trust AI in all its forms—autonomous, augmented, and assisted—regardless of whether a system is fully autonomous or there is a human in the loop. Even autonomous systems will interact with other systems and therefore must operate and interact with assured behavior.

Supporting Literature

Rollings, Mike. How to Make Better Business Decisions. *Gartner*. October 20, 2021. **www.gartner.com/smarterwithgartner/how-to-make-better-business-decisions**

den Hamer, Pieter. Top Trends in Decision Intelligence 2022. *Gartner*. October 2021.

Autonomous Operations

Description

Autonomous operations is the capability to continuously operate and carry out mission objectives without (human or human-in-the-loop) intervention in the event of adversarial, unpredictable, or unforeseen situations based solely on internal guidance or control.

Significance

The vastness of all the domains that require the attention of both offensive and defensive operations will require presence in those domains (from deep space to deep under the surface, often in harsh and dangerous environments) to carry out those missions. The ability to carry out missions in such environments not only keeps human resources out of harm's way, but also allows those resources to be employed in those missions where they are needed. To accomplish such resource savings, where autonomous assets are employed, they must be able to operate autonomously.

Supporting Literature

Gartner. 2023 Gartner Top 10 Strategic Technology Trends. Gartner. February 20, 2023 [accessed]. **www.gartner.com/en/information-technology/insights/top-technology-trends**

StartUs Insights. Top 10 Military Technology Trends & Innovations for 2023. *StartUS Insights*. February 20, 2023 [accessed]. **www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022**

Buchholz, Scott; Bechtel, Mike; & Briggs, Bill (eds). Deloitte Insights: Tech Trends 2022. Deloitte Development LLC. 2022. **www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf**

Continuous AI

Description

Continuous AI is the continuous automated lifecycle workflow to (re)design, codify, model/build, train/test, deliver, and update assured AI engineering.

Significance

From its initial conception, AI or an AI system is a human-intensive activity. It involves the initial algorithmic development and adaptation, goal expression and development, the development and maturation of one or more data sets, and (if necessary) the training on those data sets. Through these steps, the AI system evolves and grows at the pace of such human activity. At some point, though, the AI system reaches a critical mass and begins taking over the lifecycle of redesign to deploy with decreasing involvement of human activity, making the AI system self-evolving.

Supporting Literature

AI Engineering, from *Gartner Top Strategic Technology Trends for 2023* [Gartner 2023].

Smart Data Curation

Description

Smart Data Curation uses AI to establish realistic synthetic data sets for testing software at scale, particularly in training AI models that require large data sets, which may be impractical for manual or deterministic methods to rigorously perform.

Significance

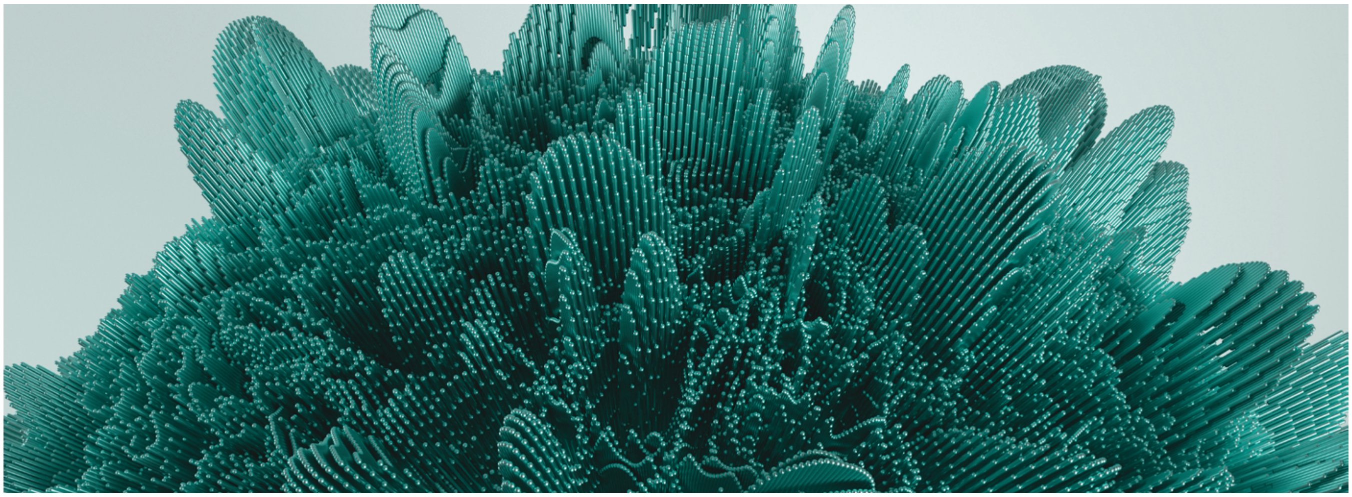
From AI and ML to large-scale data systems, there is a strong demand for realistic data sets that can be used for all forms of testing. This is a challenge for these systems, because often real-world data is not yet available or the use of real-world data is hindered by policy or regulation (e.g., personally identifiable information [PII] or information protected under the Health Insurance Portability and Accountability Act [HIPAA]). And even if real-world data is available, it can be very expensive to collect it in a useful time frame. Other approaches, often human-centric and algorithmic, fall short of effectively altering real-world data (such as to avoid revealing PII or HIPAA data), resulting in negative benefits in testing on data that no longer accurately represents the real world.

Supporting Literature

Gartner. 2023 Gartner Top 10 Strategic Technology Trends. Gartner. February 20, 2023 [accessed]. **www.gartner.com/en/information-technology/insights/top-technology-trends**

StartUs Insights. Top 10 Military Technology Trends & Innovations for 2023. *StartUS Insights*. February 20, 2023 [accessed]. **www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022**

Heaven, Will Douglas. Synthetic Data for All. *MIT Technology Review 10 Breakthrough Technologies in 2022*. February 23, 2022. **www.technologyreview.com/2022/02/23/1044965/ai-synthetic-data-2**



Biotechnology

BIOTECHNOLOGY IS THE INTEGRATION OF NATURAL SCIENCES AND ENGINEERING SCIENCES to achieve the application of organisms, cells, parts thereof, and molecular analogues for products and services [IUPAC 2014].

Advanced Bioinformatics

Description

Advanced Bioinformatics is the use of computing technology to collect, store, and analyze genetic sequences to research and solve diseases and improve medical care. This domain of science pushes the envelope of computational limits, storage, and data sharing.

As biological datasets become larger and more complex, there is a need to develop software tools that leverage recent developments in AI/ML to perform analysis. Such analysis is heightened by post-pandemic drivers.

Significance

In the DoD context, the ability to respond to pandemics and analyze large sets of population data will be critical in combating potential biological attacks.

Supporting Literature

Hamzelou, Jessica. Aging Clocks. *MIT Technology Review 10 Breakthrough Technologies in 2022*. February 23, 2022. **www.technologyreview.com/2022/04/15/1050019/aging-clocks**

Regalato, Antonio. A Pill for Covid. *MIT Technology Review 10 Breakthrough Technologies in 2022*. February 23, 2022. **www.technologyreview.com/2022/02/23/1044936/covid-19-pill-pandemic**

Heaven, Will Douglas. AI for Protein Folding. *MIT Technology Review 10 Breakthrough Technologies in 2022*. February 23, 2022. **www.technologyreview.com/2022/02/23/1044957/ai-protein-folding-deepmind**

Piore, Adam. Malaria Vaccine. *MIT Technology Review 10 Breakthrough Technologies in 2022*. February 23, 2022. **www.technologyreview.com/2022/02/23/1044969/malaria-vaccine**

Biometric Privacy

Description

Biometric Privacy is the means necessary to protect the collection, transmission, storage, use, and destruction of biologically unique information or metrics (e.g., fingerprints, facial images, and retina images) that are used to identify specific individuals (e.g., PII).

These techniques are essential to enabling secure access for individuals in ways that do not rely on traditional mechanisms, such as text passwords.

This unique set of information becomes harder to tamper with while allowing for interoperability between U.S. government agencies.

Significance

In the DoD context, the need for biometrics to ensure secure access to data within and between organizations supporting operational missions has grown.

Supporting Literature

Honan, Matt. The End of Passwords. *MIT Technology Review 10 Breakthrough Technologies in 2022*. February 23, 2022. **www.technologyreview.com/2022/02/23/1044953/password-login-cybersecurity**

Genomics

Description

Genomics is a field of biology concerned with the structure, function, evolution, and mapping of genomes. It often requires large data sets and advanced computational capability (e.g., AI/ML) to understand the collective characterization of genes (e.g., how specific genes contribute to complex diseases).

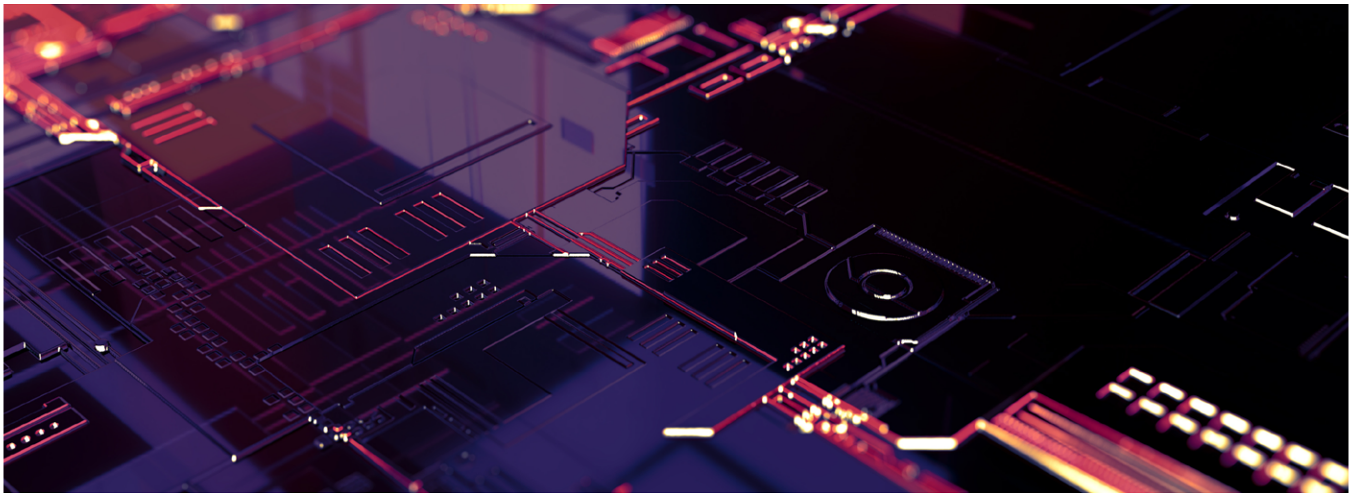
The codification of genomic data lends itself to many applications, including genetically targeted medicine, synthetic biology, and large-scale genetic analysis [Wikipedia 2022b].

Significance

In the DoD context, as a major consumer of medical services and needs, the U.S. military is a prime target for genomic technologies that may improve medical statuses or treat medical conditions for military personnel [MITRE 2010]. This includes using personal genomic data as well as understanding the computational requirements for handling such data.

Supporting Literature

Regalato, Antonio. Covid Variant Tracking. MIT Technology Review 10 Breakthrough Technologies in 2022. February 23, 2022. **www.technologyreview.com/2022/02/23/1044975/covid-19-variant-tracking-scientists**



Cybersecurity

CYBERSECURITY IS THE ART OF PROTECTING NETWORKS, DEVICES, AND DATA FROM UNAUTHORIZED ACCESS OR CRIMINAL USE and the practice of ensuring confidentiality, integrity, and availability of information.

Cyberwarfare

Description

Cyberwarfare is the use of cyberattacks against an enemy state to cause harm comparable to actual warfare, disrupt vital computer systems, or both. Some intended outcomes are espionage, sabotage, propaganda, manipulation, or economic warfare [Wikipedia 2022c].

With the emergence of cyber as a warfare domain and the increasing value of data, nation states and non-nation actors are turning to cyberattacks and defenses to engage in hostile activities. Statistics from DataProt indicate the breadth and gravity of this trend [Cveticanin 2022].

- Cybercrime statistics reveal that as many as 64% of companies across the globe have experienced some sort of hacking attacks.
- Cyberwarfare statistics show that 26.3% of all cyber warfare strikes are directed towards the United States.
- Cyberattack statistics show that 20% of global organizations consider cyber espionage to be their number-one threat. Cyber warfare statistics indicate that as many as 35% of all politically motivated cyberattacks have links to China or Russia.
- Statistics on cyber warfare reveal that about 11% of all cyberattacks are espionage related.

Cyberwarfare capabilities can be organized into offensive and defensive operations. Offensive capabilities include the attack on hostile computer systems with the intent of violating the opposing system’s confidentiality, integrity, or availability. Defensive capabilities include provisioning of preventive and protective measures to dissuade or stop cyberattacks.

Significance

In the DoD context, cyberwarfare will become a key component of warfighting in the future, as evidenced by the expansive capabilities of the U.S. Cyber Command.

Supporting Literature

StartUs Insights. Top 10 Military Technology Trends & Innovations for 2023. *StartUS Insights*. February 20, 2023 [accessed]. **www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022**

Post-Quantum Cryptography

Description

Post-quantum cryptography, also known as quantum-resistant cryptography, aims to develop cryptographic systems that are secure against classical and non-classical (quantum) computations.

As quantum computing evolves, there is a serious concern that the underlying mathematical problems, which most cryptographic algorithms rely on, can be solved with a quantum computer in the future. These mathematical problems include integer factorization and discrete logarithms [Bernstein 2009]. The security of these algorithms hinges on their extreme time complexities, which prevents classical computers from brute-forcing the decryption in any reasonable amount of time.

Significance

In the DoD context, every piece of sensitive or classified data is encrypted using various encryption algorithms. However, because not every one of these encryption algorithms is quantum resistant, hostile actors can capture this data for future exploitation when quantum computers become available. Therefore, the immediate development of quantum-resistant algorithms will be critical in securing our information now and in the future.

Supporting Literature

National Institute of Standards and Technology. Post-Quantum Cryptography. *NIST Information Technology Laboratory, Computer Security Resource Center*. July 5, 2022. **csrc.nist.gov/projects/post-quantum-cryptography**

Zero Knowledge Proofs

Description

Zero-knowledge proofs, also known as a zero-knowledge protocol, are a method by which one party can prove to another party that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true [Wikipedia 2022d].

Significance

In the DoD context, zero-knowledge proofs are essential in transmitting authenticity for highly sensitive systems, where the exposure of any auxiliary information could have serious or grave consequences.

Supporting Literature

Gartner. 2023 Gartner Top 10 Strategic Technology Trends. Gartner. February 20, 2023 [accessed]. **www.gartner.com/en/information-technology/insights/top-technology-trends**

Willemsen, Bart; Krikken, Ramon; & Horvath, Mark. Privacy Enhancing Computation. *Top Strategic Technology Trends for 2022*. Gartner. October 18, 2021. **www.gartner.com/en/documents/4006926**

On the topic of neuromorphic computing for AI/ML, General Dynamics' Tim Gilday offered this observation to the authors[1]:

> “Neuromorphic computing is the use of very-large-scale integration (VLSI) systems containing electronic analog circuits to mimic neuro-biological architectures present in the nervous system. A neuromorphic computer/chip is any device that uses physical artificial neurons (made from silicon) to do computations. As data sets become increasingly large, neuromorphic computing/engineering will be necessary to effectively process data in order to make it usable.”

Zero Trust

Description

Zero trust is a design pattern that, for information security, delivers access to information only after the strong validation of user identity, device integrity, environments, geolocation, and least-privilege authorization (which continuously validates every stage of access [or touch point] for digital assets).

The zero trust security model moves away from the risks associated with perimeter-based security by requiring authentication and authorization of every subject, asset, and workflow within an organization's information technology network or system. The approach is a set of organizational practices, not a piece of technology. A zero trust architecture is an enterprise cybersecurity plan that incorporates zero trust tenets into components specified by National Institute of Standards and Technology (NIST) Special Publication 800-207 [NIST 2020].

[1] Tim Gilday, emerging technology senior director, General Dynamics. Interview: June 7, 2022.

Significance

In the DoD context, there is a mandate to adopt zero trust architecture, which includes developing a plan and modernizing processes. Doing so will ensure higher protection against malicious cyberattacks from our nation's adversaries.

Supporting Literature

National Institute of Standards and Technology. Zero Trust Architecture. *NIST Information Technology Laboratory, Computer Security Resource Center*. August 2020. **csrc.nist.gov/publications/detail/sp/800-207/final**

The White House. *Executive Order on Improving the Nation's Cybersecurity*. May 12, 2021. **www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity**

The Cybersecurity & Infrastructure Security Agency. Executive Order on Improving the Nation's Cybersecurity. February 23, 2023 [accessed]. **www.cisa.gov/executive-order-improving-nations-cybersecurity**

Gartner. 2023 Gartner Top 10 Strategic Technology Trends. Gartner. February 20, 2023 [accessed]. **www.gartner.com/en/information-technology/insights/top-technology-trends**

Buchholz, Scott; Bechtel, Mike; & Briggs, Bill (eds). Deloitte Insights: Tech Trends 2022. Deloitte Development LLC. 2022. **www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf**

In an interview with the authors on the topic of Zero Trust Plug and Play, BridgeComm's Michael Abad-Santos offered the following comment[2]:

> “Zero Trust Universal Plug and Play is a form of composition formalisms where semantics of data used within a system are deterministic, where the properties of the components and their inter-connections are analyzable for a variety of relevant quality attributes (including security), and are applied to all endpoints, assets, actors, and data in the system.”

In an interview with the authors on the topic of the All Domain Military Internet of Everything, Abad-Santos explained the concept as follows:

> “The All Domain Military Internet of Everything (ADMIoE) is an envisioned, future DoD construct that enables joint communication, data sharing, and unified technologies across multiple military platforms and assets to deliver maximum software capabilities to warfighters at every level.”

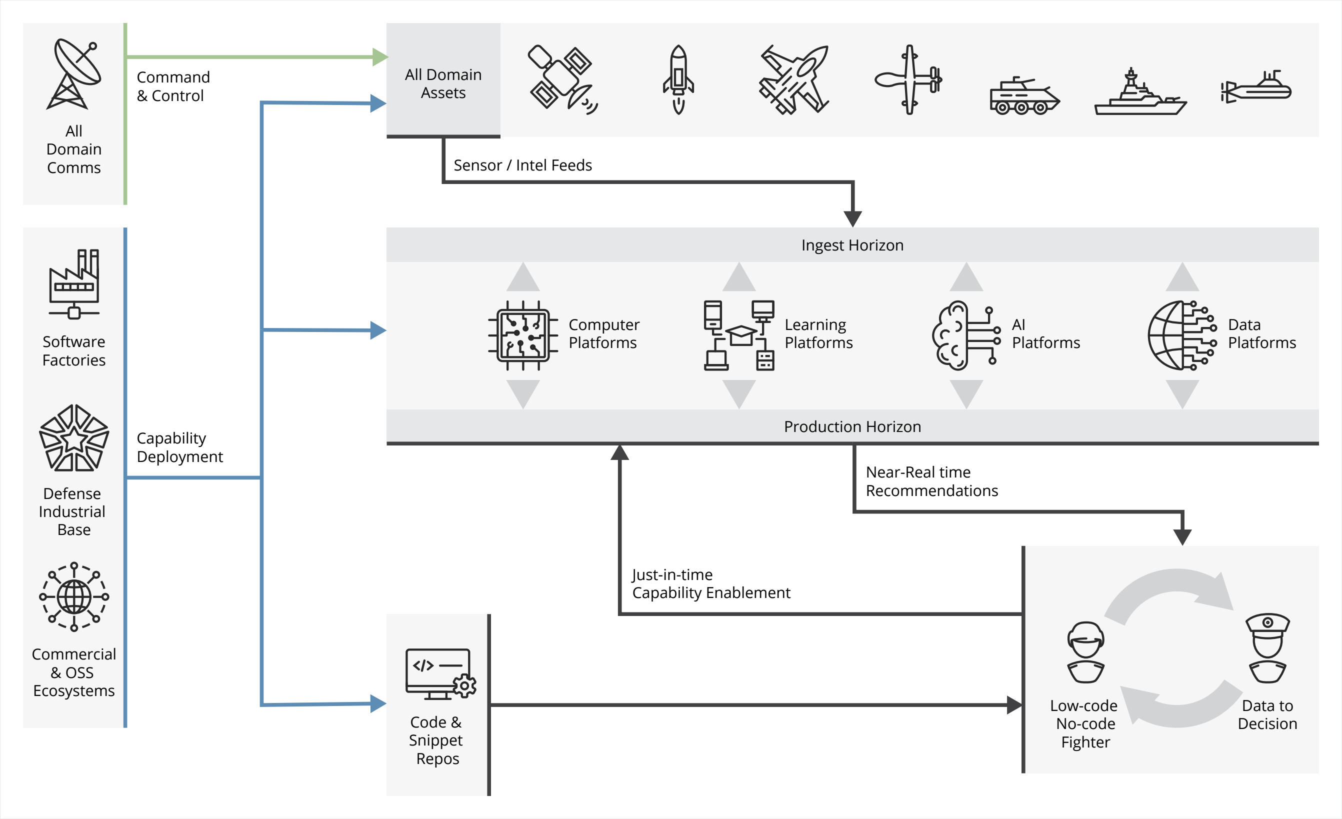
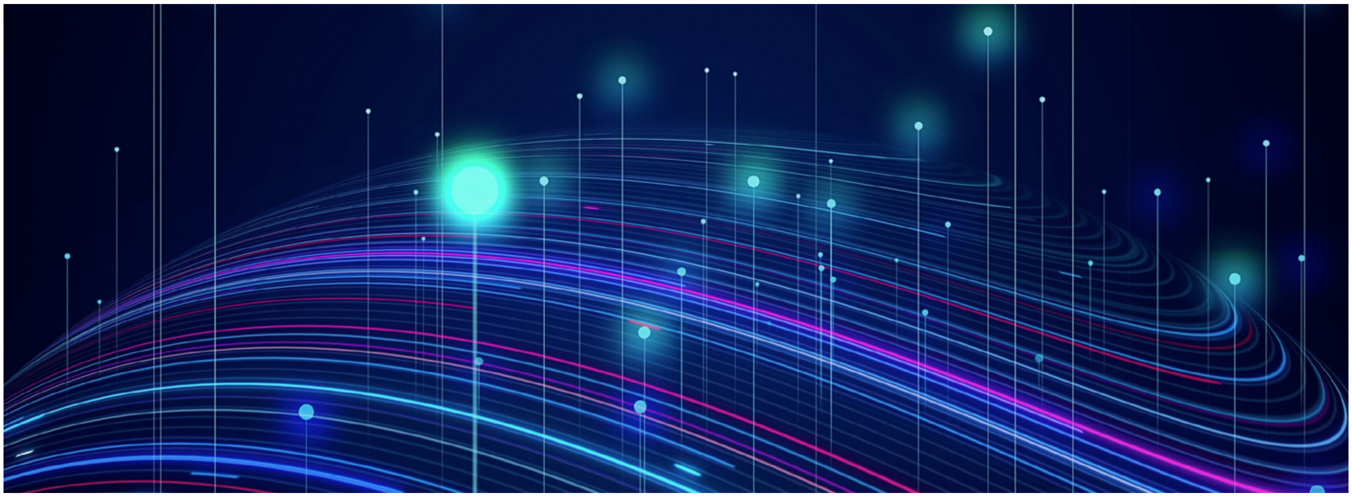


Figure 2: *The All Domain Military Internet of Everything (ADMIoE)*

[2] Michael Abad-Santos, chief executive officer, BridgeComm. Interview with authors.



Digital Transformation

DIGITAL TRANSFORMATION REFERS TO A PROCESS OF ADOPTION OF DIGITAL TOOLS AND METHODS BY AN ORGANIZATION, typically that organization that has either not been including the digital factor as part of its core activities or has not kept up with the pace of change in digital technologies.

Deep Data Semantics

Description

Deep data semantics is the fundamental cross-domain and cross-mission understanding of data element(s) and the ability to interoperate. This concept includes autonomous and non-self-governing systems, semantically beyond the physical and/or bit level and syntax level, and systems in which errors must be reconciled using human intelligence.

Significance

Systems that need to operate and coordinate activities to accomplish missions, often in a distributed manner, must be able to understand not only their own role in the mission but also the roles of other systems. Beyond the communications mechanisms and the medium(s) used to communicate those roles, they must understand the actual mission-level data and properties that are communicated (e.g., objectives, priorities, assets, and policies). For a known or planned constellation of autonomous, semi-autonomous, and manual systems, such an understanding can be programmed in; true ad hoc group collaboration can only be achieved when such deep understanding can be understood without pre-planning.

Supporting Literature

Defense Advanced Research Projects Agency. Creating Cross-Domain Kill Webs in Real Time. DARPA. September 18, 2020. **www.darpa.mil/news-events/2020-09-18a**

In an interview with the authors, the SEI's Hasan Yasar had the following to say on the topic[3]:

> “Real Time Automated IV&V is the tools and methodologies that can be implemented in the DSO pipeline for automation of IV&V activities at scale. Embedded systems present challenges. As systems become more complex the models will be more abstract resulting in more difficultly in creating high fidelity models. Code needs to bring (or carry) evidence that it is correct (e.g., proof-carrying code) which needs to bring IV&V into the model itself.”

Extended Reality

Description

Extended reality includes various computer-assisted and computer-aided forms of augmented reality (superimposition of information on the real world) and virtual reality (simulation and facsimile

[3] Hasan Yasar, SEI, Technical Director, Continuous Deployment of Capability Software Solutions Division. Interview with the authors.

environments) into a unified human–machine interactive interface (HMI) through the use of computer and wearable technology.

By increasing the fidelity and interactivity of HMIs, extended reality enables users to engage in activities that would otherwise be too costly, inaccessible, or physically challenging. This is especially important in safety-critical systems, where software training ensures appropriate operational responses to potential threats to human life.

Significance

In the DoD context, many combat systems are becoming more software intensive. Extended reality provides a medium in which to safely train new operators in the operational intricacies to ensure that our military capabilities can match those of our enemies.

Supporting Literature

StartUs Insights. Top 10 Military Technology Trends & Innovations for 2023. StartUS Insights. February 20, 2023 [accessed]. **www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022**

Higher Fidelity MBSE

Description

Higher fidelity machine-based systems engineering (MBSE) is the lossless capability and quality attribute transformation of software, systems, and systems-of-systems models to their operational (i.e., running) transformation without the need for an engineer in the loop to perform that transformation—the model becomes the system.

Significance

MBSE is a comprehensive approach to software and system-level understanding that comprehends not only a number of stakeholder views but also views for understanding the behavior, composition, and interaction of the software system. The challenge in MBSE is to bring all those views into an operational system, because translating them into systems, subsystems, components, functions, and eventually code requires human activity and results in loss of information due to expediency (e.g., cost over time), inexpressible quality attributes (e.g., must be secure), or untranslatable concepts (e.g., mission assurance).

Supporting Literature

In an interview with the authors, the SEI's Dionisio De Niz offered the following comment on the topic of lossless model representation[4]:

> “Lossless Model Representation is a formalization of the semantics of the requirements, design, implementation, and deployment and execution environments that faithfully exhibits and conforms to the nuance plaguing MBSE. For example, programming languages are lossy in the translation from the human form code/representation to the deployment environment (e.g., processor branch prediction, memory cache prediction, network effects, etc.).”

Hyperautomation

Description

Hyperautomation is a conglomeration of disparate computer technologies (e.g., natural-language processing, AI/ML, optical character recognition, and process models) to automate as many business and information technology (IT) processes as possible.

As organizations become more complex and have remote operational requirements, they need to automate more business processes. When the level of adoption reaches a large scale, comprising multiple tools to enable intelligent automation, it becomes hyperautomation [Gambetta 2022]. It empowers businesses to operate in a distributed capacity and make better decisions to remain competitive.

Significance

In the DoD context, many systems are either legacy in technology or manual in operation. Hyperautomation reduces the burden to support these systems, allowing more efficient use of human efforts.

Supporting Literature

Gartner. 2023 Gartner Top 10 Strategic Technology Trends. *Gartner*. February 20, 2023 [accessed]. **www.gartner.com/en/information-technology/insights/top-technology-trends**

Groombridge, David; Downes, Stuart; Harvey, Tony; & Manjunath, Bhat. Top Trends in Distributed Enterprise 2022. Gartner. October 2021.

[4] Dionisio De Niz, SEI, Technical Director, Assuring CyberPhysical Systems Software Solutions Division. Interview with the authors.

IBM. Data Fabric Architecture. IBM. February 21, 2023 [accessed]. **www.ibm.com/data-fabric**.

Buchholz, Scott; Bechtel, Mike; & Briggs, Bill (eds). Deloitte Insights: Tech Trends 2022. Deloitte Development LLC. 2022. **www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf**

Low-Code Development

Description

Low-code development is a development environment used to create application software through a graphical user interface. A low-code platform may produce entirely operational applications or require additional coding for specific situations [Wikipedia 2022e].

Significance

When current warfighting capabilities cannot keep pace with evolving threats or the ever-changing environment, a warfighter can search, compose, or cobble, interface with, and employ from available code or snippet repositories to create new just-in-time capability to augment or supplant existing lagging capabilities to better support the day's mission and decisions. The warfighter need not deeply understand how the technology is developed and can focus on the operational need.

Supporting Literature

Gartner. 2023 Gartner Top 10 Strategic Technology Trends. Gartner. February 20, 2023 [accessed]. **www.gartner.com/en/information-technology/insights/top-technology-trends**

Natis, Yefim. Top Trends in Composable Applications 2022. Gartner. October 2021.

Smarter Edge

Description

Smarter Edge is an alternative architecture to cloud and on-premises (i.e., large data centers) computing because it shifts much of the computing burden to local edge devices instead of centralized data centers, which incorporates more autonomy and tighter integration with the data-to-decision paradigm.

Significance

Assets at the tactical edge are continuously processing, sometimes in real time, to situational awareness and intelligence feeds that are relevant for the asset's mission. The ability to operate on this edge, in an environment of poor connectivity and logistical support, requires more autonomy and the compute capability to make better decisions while at the same time contributing to the overall mission (also, potentially, in real time). This seemingly paradoxical dichotomy requires those assets to operate in a smarter manner and more like human assets.

Supporting Literature

StartUs Insights. Top 10 Military Technology Trends & Innovations for 2023. *StartUS Insights*. February 20, 2023 [accessed]. **www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022**

Distributed Computing

A DISTRIBUTED COMPUTER SYSTEM CONSISTS OF MULTIPLE SOFTWARE COMPONENTS THAT ARE ON MULTIPLE COMPUTERS BUT RUN AS A SINGLE SYSTEM. The computers in a distributed system can be physically close and connected by a local network, or they can be geographically distant and connected by a wide-area network. A distributed system can consist of any number of possible configurations, such as mainframes, personal computers, workstations, minicomputers, and so on. The goal of distributed computing is to make such a network work as a single computer.

Blockchain Validation

Description

Blockchain validation provides the assurance that processes and components in blockchain technologies satisfy the technical needs of external or higher order applications that depend on the blockchain technology.

Blockchain is a cryptographic approach in which the underlying units of data are securely linked in a digital ledger, resulting in incrementally secure transactions. To leverage this technology beyond the commonly associated cryptocurrencies, there must be mechanisms to validate the underlying transactions. An example of how these transactions can be jeopardized is a 51% attack, in which a single entity controls the majority of nodes that generate the ledger (which is a reason why blockchain is best used in decentralized applications).

Significance

In the DoD context, blockchain is a promising tool for capturing cyber and physical assets, either as part of the supply chain or in active inventory. To provide added value, it must first be validated against the traditional asset management tools for storing this information in a secure, efficient, and accessible manner.

Supporting Literature

StartUs Insights. Top 10 Military Technology Trends & Innovations for 2023. StartUS Insights. February 20, 2023 [accessed]. **https://www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022**

Buchholz, Scott; Bechtel, Mike; & Briggs, Bill (eds). Deloitte Insights: Tech Trends 2022. Deloitte Development LLC. 2022. **https://www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf**

Blockchain Verification

Description

Blockchain verification is the process of verifying that the information contained within the blockchain is correct, because the credentials used when the information was recorded to the blockchain are themselves in the blockchain. Since the blockchain is public, anyone can verify its authenticity.

Blockchain is a cryptographic approach in which the underlying units of data are securely linked in a digital ledger, resulting in incrementally secure transactions. An essential component to this process is the consensus (which includes the proof of work or proof of stake that embodies the work) that each node must work. Because there is no universal standard for consensus, it is imperative that applications perform due diligence in understanding the type of work necessary with each block. For example, some proof-of-work functions may not be quantum resistant (see Post-Quantum Cryptography), which means that future quantum systems could operate with a massive advantage.

Significance

In the DoD context, blockchain is a promising tool for capturing cyber and physical assets, either as part of the supply chain or in active inventory. To assure blockchain use, the determination of each block with respect to asset properties must be fully understood and traced. This verification, when visible, will enable continuous auditing of assets.

Supporting Literature

Roberts, Siobahn. Proof of stake. *MIT Technology Review*. February 23, 2022. **https://www.technologyreview.com/2022/02/23/1044960/proof-of-stake-cryptocurrency**

Cloud Native Development

Description

Cloud-native development is an approach to application development that takes advantage of a specific cloud hosting technology to achieve great performance and cost at the expense of not being cloud technology agnostic.

For organizations to leverage cloud computing environments, they must modernize many legacy software systems, which may include the use of containers or microservices. Doing so creates more loosely coupled systems that can support rapid changes.

Significance

In the DoD context, the proliferation of modern software factories in cloud environments, such as Platform One, is increasing to meet DevSecOps requirements [Air Force 2023]. Many legacy systems, especially avionics platforms and hardware-in-the-loop systems, must have their software architecture re- examined and modernized.

Supporting Literature

Gartner. 2023 Gartner Top 10 Strategic Technology Trends. Gartner. February 20, 2023 [accessed]. **https://www.gartner.com/en/information-technology/insights/top-technology-trends**

Buchholz, Scott; Bechtel, Mike; & Briggs, Bill (eds). Deloitte Insights: Tech Trends 2022. Deloitte Development LLC. 2022. **https://www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf**

Distributed Cyber Physical Systems

Description

Distributed cyber-physical systems are complex integrations of computation, communication, and (mechatronic) control over a physical system or a collection of physical systems that are not necessarily co-located. Hence, they are spacefaring or geographically distributed.

These decentralized systems are necessary in a variety of applications, such as

- renewable energy
- space applications
- swarm robotics

In these systems, each node must be independently capable of securing its data against hostile actors as well as providing hardened capabilities to serve its remote network.

Significance

In the DoD context, as autonomous systems such as unmanned aerial vehicles (UAVs) and satellites become more prevalent, these systems must be developed using processes and protocols to ensure safe and resilient operation.

Supporting Literature

In an interview with the authors about zero knowledge recovery, the SEI's Dionisio De Niz said the following[5]:

> “Zero knowledge recovery is the need (or challenge) to recover from a bad situation in an autonomous system without ever knowing what that bad situation is in advance – the concept is parallel to zero knowledge proof.”

[5] Dionisio De Niz, SEI, Technical Director, Assuring CyberPhysical Systems Software Solutions Division. Interview with the authors.

References

URLs are valid as of the publication date of this document.

[Abhari 2012]
Abhari, A. J. et al. Scaffold: *Quantum Programming Language*. TR-934-12. Princeton University. 2012. **www.cs.princeton.edu/research/techreps/TR-934-12**

[Air Force 2023]
United States Air Force. Platform One. United States Air Force, Office of the Chief Software Officer. February 21, 2023 [accessed]. **software.af.mil/team/platformone**

[Amazon 2022]
Amazon AWS. AWS announces Amazon CodeWhisperer (Preview). Amazon AWS. June 23, 2022. **aws.amazon.com/about-aws/whats-new/2022/06/aws-announces-amazon-codewhisperer-preview**

[Batarseh 2021]
Batarseh, F.A.; Freeman, L.; & Huang, C.H. A survey on artificial intelligence assurance. Journal of Big Data. Volume 8. Number 60. April 2021. **journalofbigdata.springeropen.com/articles/10.1186/s40537-021-00445-7**

[Benioff 1980]
Benioff, Paul. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. Pages 563–591. Journal of Statistical Physics. Volume 22. Issue 5, May 1980

[Bernstein 2009]
Bernstein, Daniel J. Introduction to post-quantum cryptography. In Post-Quantum Cryptography. Bernstein, D.J.; Buchmann, J.; & Dahmen, E. [editors]. Springer-Verlag. Pages 1–14. 2009. **www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf**

[CISA 2021]
The Cybersecurity & Infrastructure Security Agency. Executive Order on Improving the Nation's Cybersecurity. February 23, 2023 [accessed]. **www.cisa.gov/executive-order-improving-nations-cybersecurity**

[Cveticanin 2022]
Cveticanin, Nikolina. The Largest Battlefield in History – 30 Cyber Warfare Statistics. DataProt. November 2, 2022. **dataprot.net/statistics/cyber-warfare-statistics**

[DARPA 2020]
Defense Advanced Research Projects Agency. Creating Cross-Domain Kill Webs in Real Time. DARPA. September 18, 2020. **www.darpa.mil/news-events/2020-09-18a**

[Deloitte 2022]
Buchholz, Scott; Bechtel, Mike; & Briggs, Bill (eds). Deloitte Insights: Tech Trends 2022. Deloitte Development LLC. 2022. **www2.deloitte.com/content/dam/insights/articles/US164706_Tech-trends-2022/DI_Tech-trends-2022.pdf**

[den Hamer 2021]
den Hamer, Pieter. Top Trends in Decision Intelligence 2022. Gartner. October 2021.

[Friedewald and Raabe 2011]
Friedewald, Michael & Raabe, Oliver. Ubiquitous computing: An overview of technology impacts. Pages 55–65. Telematics & Informatics. Volume 28. Issue 2. 2011. **www.sciencedirect.com/science/article/pii/S0736585310000547#b0020**

[Gambetta 2022]
Gambetta, Jay. Expanding the IBM Quantum roadmap to anticipate the future of quantum-centric supercomputing. May 10, 2022. IBM Blog. **research.ibm.com/blog/ibm-quantum-roadmap-2025**

[Gartner 2023]
Gartner. 2023 Gartner Top 10 Strategic Technology Trends. Gartner. February 20, 2023 [accessed]. **www.gartner.com/en/information-technology/insights/top-technology-trends**

[GitHub 2023]
GitHub. Your AI pair programmer: GitHub Copilot uses the OpenAI Codex to suggest code and entire functions in real-time, right from your editor. GitHub. February 20, 2023 [accessed]. **github.com/features/copilot**

[Groombridge et al. 2021]
Groombridge, David; Downes, Stuart; Harvey, Tony; & Manjunath, Bhat. Top Trends in Distributed Enterprise 2022. Gartner. October 2021.

[IBM 2023]
IBM. Data Fabric Architecture. IBM. February 21, 2023 [accessed]. **www.ibm.com/data-fabric**

[IUPAC 2014]
International Union of Pure and Applied Chemistry. Biotechnology. IUPAC Gold Book. February 24, 2014. **goldbook.iupac.org/terms/view/B00666**

[MIT 2022]
MIT. 2022: 10 Breakthrough Technologies. MIT Technology Review. February 21, 2023 [accessed]. **www.technologyreview.com/2022/02/23/1045416/10-breakthrough-technologies-2022**

[MITRE 2010]
The MITRE Corporation, JASON Programming Office. The $100 Genome: Implications for the DoD. JSR-10-100. The MITRE Corporation. December 2010. **irp.fas.org/agency/dod/jason/hundred.pdf**

[Natis 2021]
Natis, Yefim. Top Trends in Composable Applications 2022. Gartner. October 2021.

[NIST 2020]
National Institute of Standards and Technology. Zero Trust Architecture. NIST Information Technology Laboratory, Computer Security Resource Center. August 2020. **csrc.nist.gov/publications/detail/sp/800-207/final**

[NIST 2022]
National Institute of Standards and Technology. Post-Quantum Cryptography. NIST Information Technology Laboratory, Computer Security Resource Center. July 5, 2022. **csrc.nist.gov/projects/post-quantum-cryptography**

[Roberts 2022]
Roberts, Siobahn. Proof of stake. MIT Technology Review. February 23, 2022. **www.technologyreview.com/2022/02/23/1044960/proof-of-stake-cryptocurrency**

[Rollings 2021]
Rollings, Mike. How to Make Better Business Decisions. Gartner. October 20, 2021. **www.gartner.com/smarterwithgartner/how-to-make-better-business-decisions**

[StartUS 2022]
StartUs Insights. Top 10 Military Technology Trends & Innovations for 2023. StartUS Insights. February 20, 2023 [accessed]. **www.startus-insights.com/innovators-guide/top-10-military-technology-trends-2022**

[Temple and Crownhart 2022]
Temple, James & Crownhart, Casey. Carbon removal factory. MIT Technology Review. February 23, 2022. **www.technologyreview.com/2022/02/23/1044972/carbon-removal-factory-climate-change**

[White House 2021]
The White House. Executive Order on Improving the Nation's Cybersecurity. May 12, 2021. **www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity**

[White House 2022]
The White House. Executive Order on Enhancing the National Quantum Initiative Advisory Committee. May 04, 2022. **www.whitehouse.gov/briefing-room/presidential-actions/2022/05/04/executive-order-on-enhancing-the-national-quantum-initiative-advisory-committee**

[Wikipedia 2022]
Wikipedia. Ubiquitous Computing. Wikipedia. February 20, 2023 [accessed]. **en.wikipedia.org/wiki/Ubiquitous_computing**

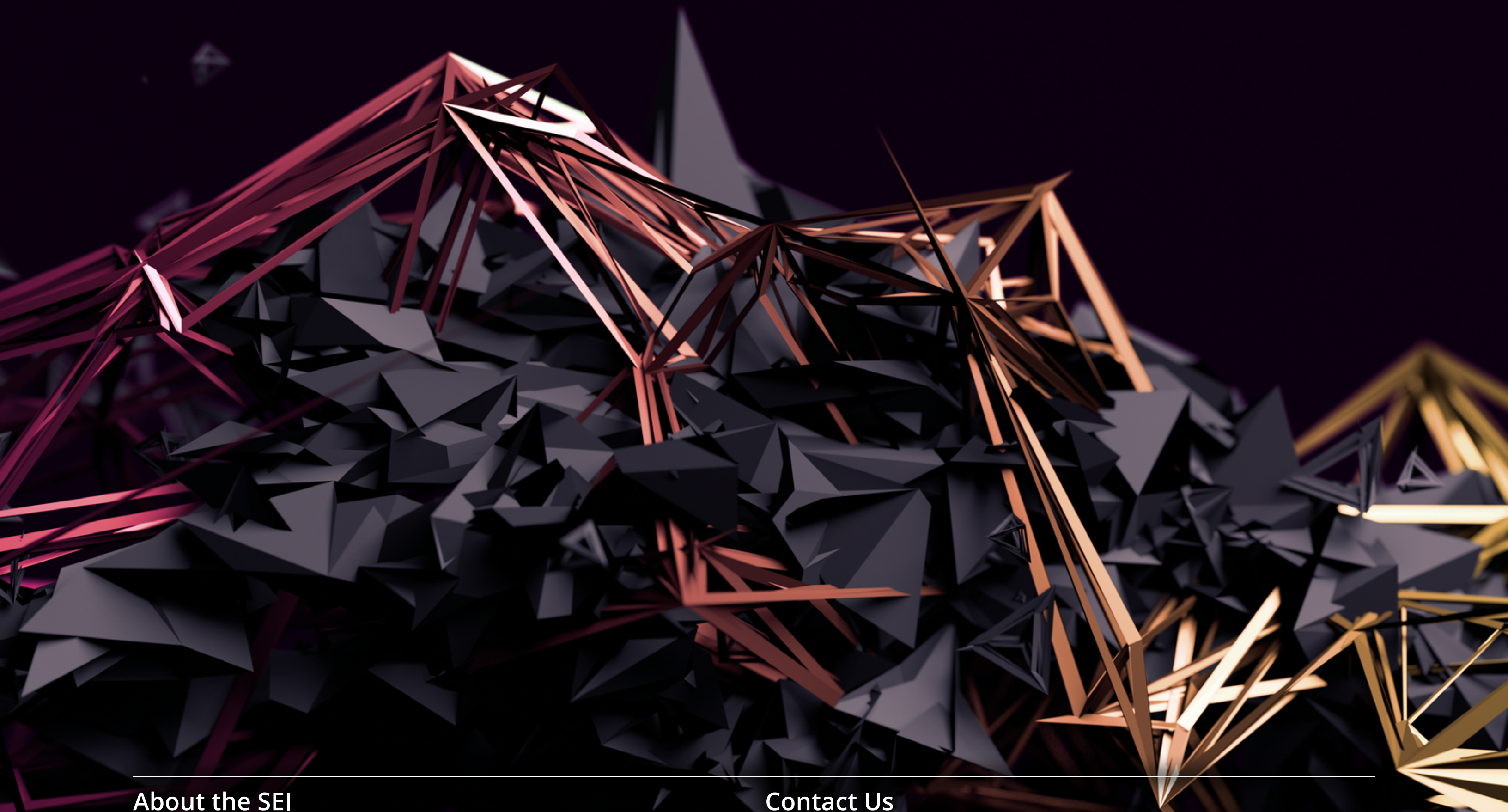
[Wikipedia 2022a]
Wikipedia. Renewable energy. Wikipedia. February 20, 2023 [accessed]. **en.wikipedia.org/wiki/Renewable_energy**

[Wikipedia 2022b]
Wikipedia. Genomics. Wikipedia. [February 21, 2023 [accessed]. **en.wikipedia.org/wiki/Genomics**.

[Wikipedia 2022c]
Wikipedia. Cyberwarfare. Wikipedia. [February 21, 2023 [accessed]. **en.wikipedia.org/wiki/Cyberwarfare**

[Wikipedia 2022d]
Wikipedia. Zero-knowledge proof. Wikipedia. [February 21, 2023 [accessed]. **en.wikipedia.org/wiki/Zero-knowledge_proof**

[Wikipedia 2022e]
Wikipedia. Low-code development platform. Wikipedia. [February 21, 2023 [accessed]. **en.wikipedia.org/wiki/Low-code_development_platform**.



About the SEI

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

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu

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

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

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

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

DM23-0683