Emerging Technologies 2020: Six Areas of Opportunity August 20, 2020

An SSD-Led Study

Charles Holland

Jake Tanenbaum

Ed Desautels

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

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

Emerging Technologies 2020

Introduction and Overview

Introduction

This briefing highlights the results of a 2020 survey of the emerging technologies landscape to help inform SEI's research strategy and enhance its role as a trusted advisor to DoD.

The six emerging technologies described here hold great promise and in some cases have already attracted the interest of the DoD. By understanding these technologies and their intersection with DoD needs, we can create a research agenda that keeps the SEI on the leading edge and that serves our sponsor's mission.

Agenda

Sources Informing the Emerging Technology Survey

Consensus List of Emerging Technologies

- Advanced Computing
- The Smarter Edge
- Digital Twins
- Artificial Intelligence
- Extended Reality
- Data Privacy, Trust, and Ethics

References and Further Reading

Backup Slides

Emerging Technologies 2020

Sources Informing Our Emerging Technology Survey

Consulting and Related*

Deloitte	10 Breakthrough Technologies 2020
Gartner	Top 10 Strategic Technology Trends for 2020
IDC	FutureScape: Worldwide IT Industry 2020 Predictions
Accenture	Technology Vision 2020
Forbes	The 7 Biggest Technology Trends In 2020 Everyone Must Get Ready For Now

*All sources presented are hyperlinked.

Research Community

MIT Technology Review	10 Breakthrough Technologies 2020
IEEE Computer Society	Top 12 Technology Trends for 2020
Computing Community Consortium	Technical Focus Areas
Networking Information Technology R&D	Program Component Areas

Defense

NATO	Science & Technology Trends 2020-2040
DoD	Digital Modernization Strategy

Other Analysis

Industry Week	Top 10 Technologies to Watch in 2020
World Economic Forum	Top 10 Emerging Technologies 2019
Y Combinator	Requests for Startups
SEI Business Development	Transcripts from discussions

Emerging Technologies 2020

Consensus List of Emerging Technologies

Consensus List of Emerging Technologies

The SEI team developed this list based on a survey of the available literature noted in the previous section. To make its selections, the team applied the following criteria:

- Level of technical interest
- Opportunity for DoD

Significant opportunities for combining multiple technologies exist to multiply capability.

These opportunities present substantial challenges for software engineering.

- Advanced Computing
- The Smarter Edge
- Digital Twins
- Artificial Intelligence
- Extended Reality
- Privacy, Trust, and Ethics

Technology Themes by Source

Technology Theme	MIT Tech. Rev.	NATO	Deloitte	Forbes	Gartner	Industry Week	IDC	Accenture	World Economic Forum	IEEE	Y Combinator	SEI BD	DoD Digital Modern. Strat.
Advanced Computing	Yes					Yes				Yes		Yes	Yes
The Smarter Edge	Yes	Yes			Yes	Yes	Yes			Yes			Yes
Digital Twins		Yes	Yes		Yes					Yes			
AI		Yes		Yes	Yes	Yes	Yes			Yes	Yes	Yes	Yes
Extended Reality		Yes		Yes	Yes	Yes		Yes	Yes		Yes		
Data Privacy, Trust, and Ethics	Yes	Yes	Yes	Yes	Yes	Yes	Yes		Yes	Yes			Yes

Note that source lists were of varying lengths, and in some cases covered scopes far beyond computing/IT.

Emerging Technologies 2020

Consensus List of Emerging Technologies

Advanced Computing

Overview

DoD Interests

- Microelectronics is now the #1 priority for USD (R&E).
- Advanced computing is an important strategy component of the microelectronics push.
- Capabilities plus industrial base issues (trusted foundries, etc.) are key concerns.
- Quantum is another of the USD (R&E) priorities.

Advanced computing is the driver for new capabilities enabled through software.

Background and Trends

Through the mid-2000s, semiconductor advances underpinning Moore's law and Dennard scaling enabled a steady revolution in computing power per core.

This period saw the emergence of multicore chips, GPUs driven by HPC, and video gaming.

In 2011, the National Academy Press Study "The Future of Computing Performance: Game Over or Next Level" described the factors underlying future limitations on growth for single processors based on complementary metal oxide semiconductor (CMOS) technology.

In 2012 and beyond, multi-layer neural networks emerged.

Never forget about power challenges! In 2012, DARPA established the Power Efficiency Revolution for Embedded Computing Technologies (PERFECT) program to research and develop the means to achieve the power efficiency required to enable embedded computing systems.

Emerging Trends in Advanced Computing

Historically, maintenance of the stockpile, cryptography, and challenging scientific problems, such as weather prediction and climate change, have driven federal investment with DoD application.

Recently, there has been a push to exascale (led by DoE for science, Microsoft, and others for AI).

In 2015, the National Strategic Computing Initiative (NSCI) started exascale computing focused on traditional supercomputing plus big data challenges. Exascale machines will arrive soon.

In August 2019, the NSCI Fast Track Action Committee provided an update with a broader vision: Pioneering the Future of Computing.

Today, there is a drive for applications to support COVID vaccine design.

AI: a Key Driver of the Advanced Computing Agenda

AI is driving supercomputing and vice versa.

Jensen Huang, CEO NVIDIA, uses the phrase "Cambrian Explosion" to describe innovation in neural network algorithms AND specialized hardware for implementing them.

Cerebras has developed the Wafer Scale Engine (WSE) that boasts "1.2 trillion transistors, 400,000 processor cores, 18 gigabytes of SRAM, and interconnects capable of moving 100 million billion bits per second." The WSE is designed to enable rapid training of large neural networks.

Microsoft has invested in supercomputing for AI with its Massive AI Supercomputer on Azure. The system features 285k CPU Cores and10k GPUs. Microsoft created it *"for training larger AI models targeting highly complex problems."*

Advances in AI will require new software to run on these systems, opening up new opportunities for software engineering.

Fully Homomorphic Encryption: Privacy Computing

Current art: Information can be encrypted ONLY for transmission and storage.

Fully homomorphic encryption (FHE) makes it possible to analyze or manipulate encrypted data without revealing the data to anyone, a major advance.

FHE builds upon Craig Gentry's seminal 2009 work and other work to date, initially a million times too slow to be practical.

A new DARPA MTO program, Data Protection in Virtualized Environments (DPRIVE) for FHE. DPRIVE's program objective is to design and implement a large word size (1000 bits) hardware accelerator to reduce the computational runtime of FHE algorithms to be only 10 times slower!

IBM has already released a fully homomorphic encryption toolkit for Mac OS and IOS, and its Linux and Android toolkits are on the way.

Quantum Computer Trends

Small-scale quantum computers are emerging using various technologies for qubits by major companies (IBM, Honeywell, Google, Microsoft, etc.) and venture capital-funded activities.

Available on the cloud: This is the Noisy Intermediate Scale Quantum (NISQ) era of up to a few hundred qubits-less than 100 qubits now, which is insufficient for error correction.

The challenge is to show commercial/ economic benefit, with NISQ machines, to enable a virtuous cycle similar to semiconductor technologies over the past 40 years and to demonstrate quantum advantage on problems with value.

Longer-Term Technological Opportunity: Develop a software ecosystem to enable scalable quantum computing.

Quantum Information Science: Enabling a Technological Revolution

Area	Example
Sensing Environments	PNT (alternative to GPS in denied environments)
Information Theory	New materials design
Computing	Cryptanalysis, optimization, ML
Communications	Quantum networking

National Security Relevance

Quantum computers, when they achieve the necessary scale, could be used to break contemporary public key cryptography.

Today's best estimate on algorithm requirements can be found in Gidney and Ekera's 2019 paper "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits."

NIST leads the major effort to decide on the "quantum resistant algorithms" that will become the standard.

"Crypto-modernization" will be a substantial, decade-long event, and implementation will be a software engineering opportunity.

Must execute modernization now because people are already scraping data, which could enable forensic intelligence efforts using quantum computing.

Emerging Technologies 2020

Consensus List of Emerging Technologies

The Smarter Edge

The Smarter Edge: Overview

Mark Weiser (Xerox PARC) first predicted this concept in his 1988 paper, “Ubiquitous Computing.”

Edge data is captured by new sensors. Key components include

- ubiquitous sensing
- the Internet of things (IoT)

Computer hardware improvements enable more complex, advanced software. Key components include

- fog computing
- cloudlets

The field of analytics has seen innovation in new ways to examine data.

In AI, algorithmic improvements allow a smaller resource footprint. Key components include “tiny AI”—the miniaturization of AI and ML.

Application Drivers: Health, Manufacturing, Predictive Maintenance, Autonomy

The Smarter Edge: Considerations

Smarter Edge Considerations

- Bandwidth
- Latency
- Outages
- Security
- Privacy
- Power awareness

Photo: U.S. Army

Application Drivers: Health, Manufacturing, Predictive Maintenance, Autonomy

Edge Components: Tiny AI

Moving ML to the edge faces the following constraints:

- ultra-low power
- small resource footprint
- minimal library and/or binary dependencies

The inaugural 2019 TinyML Summit attracted 90+ companies.

Karl Pfister, the originator of Smart Dust in the 1990s, was a speaker.

Qualcomm is a company to be watched in this area.

Edge Components: 5G Networks

Represents a combination of improved standards and hardware for mobile networks

Provides greater bandwidth to service the massive growth in IoT

Called a "technology offering promise" in DoD 2019 Modernization Strategy

> *"Key benefits from 5G NR are the ability to deliver fiber-like speeds to end-user devices, improved performance at network cell edge, low latency performance (<2ms radio latency), and greater spectral efficiency."*

Involves security risks

- Major foreign presence in component manufacture
- Untrusted hardware and/or software in the enterprise

What are the software engineering and/or software challenges?

- Inherited vulnerabilities from backward compatibility with older networks

The Other Smart Edge: Space and Swarming Drones

Space

- This scenario is enabled by the emerging potential for low(er) cost satellite constellations of small satellites.
- The DARPA Blackjack concept comprises several DARPA programs. This is one such DoD idea, and there are other commercial endeavors.
- Creating a system of several hundred LEO based satellites to enable hypersonic cruise missile defense will be a significant challenge and undertaking.
- SpaceX: We've launched 32,000 Linux computers into space for Starlink internet.
- Related concept: satellite mega-constellations.

Drones

- Added level of complexity and S&T challenges when devices are numerous and mobile
- Requirement for swarming behavior (the dynamics of the edge devices are important) for the desired functionality

Emerging Technologies 2020

Consensus List of Emerging Technologies

Digital Twins

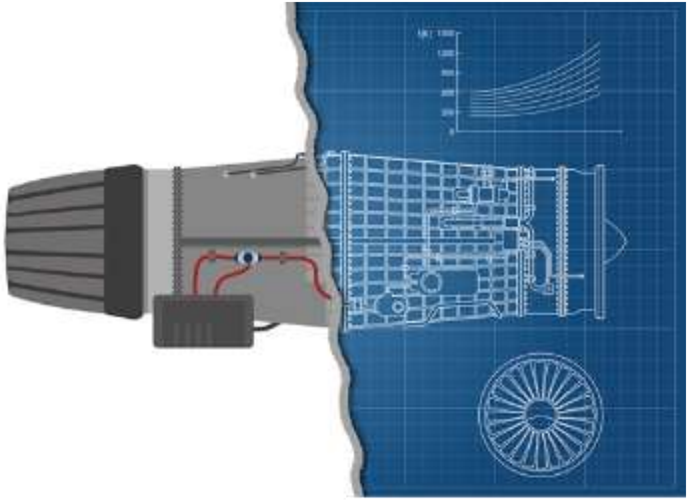
Overview

A “Digital twin” is a digital copy of a physical object or world (with some non-trivial level of fidelity).

Treating a complex object as a point in some queuing model is simulation but not a digital twin.

The digital twin concept is not new, but its importance and roles are expanding. This expansion is driven by a more complete ecosystem, taking advantage of advanced computing, visualization capabilities, real time sensor data, etc.

USD(R&E) recognizes the importance of digital twins in the DOD Digital Engineering Strategy June 2018.



Example Applications

- Data Models: Early work on twins was based only on data models (wanting an authoritative source of data for design and assembly). CAD models would fit here (not a behavioral view).
- Circa 2018, the Singapore National Research Foundation produced Virtual Singapore, a digital model of an entire city used for planning but not for real-time feedback.
- A growing area is in the use of digital twins in enterprise-wide business ops and manufacturing.
- The Structural Simulation Toolkit is a scalable simulation technology using supercomputers to model supercomputers, an interesting niche topic.

Reasoning about Physical Objects

Efforts underway in virtual prototyping are driven by advances in HPC capability and advances in scientific computing algorithms representing complex physics.

This has been underway for decades. DoD HPCMP is a good example of this work area, including the CREATE program led by Doug Post.

Examples include flows over airplane wings and store separation.

Behavioral representation but not a feedback to a real-time twin object. Stockpile stewardship has been the big driver.

Recent Developments

A new trend is the incorporation of real-time feedback data into the digital twin for prediction and/or control.

The digital twins concept informs better global weather modeling (for example, the incorporation of satellite and sonobuoy measurements).

Other recent developments include

- IBM: Farming's digital doubles will help feed a growing population using less resources.
- SEI: Digital Twin Ops Project. (Jerome Hugues)

Challenges and Opportunities

Uncertainty Quantification: The digital twin is never the precise replica of reality. How does one quantify the uncertainty in the prediction?

Multiple digital twins interacting and cooperating

Applying AI/ML techniques on the digital twin model with real time feedback data

Modeling the human in the digital twin model

Modeling physiology and biological processes (Nature)

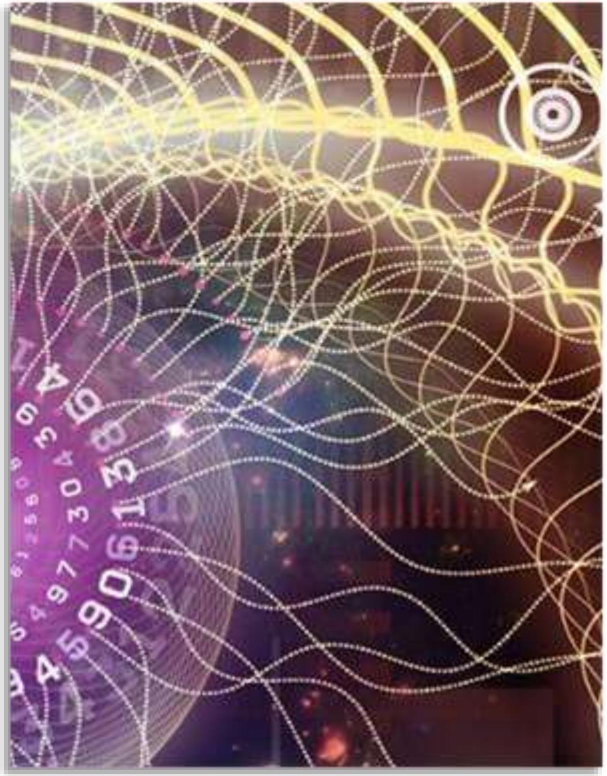
Protecting the data of individuals and enterprises is increasingly important for the successful IT ecosystem.

Emerging Technologies 2020

Consensus List of Emerging Technologies

Artificial Intelligence

Artificial Intelligence Landscape



Artificial intelligence is now pervasive, with ramifications for economic and national security and prosperity.

Harnessing AI is on the scale of harnessing the power of electricity.

The Joint Artificial Intelligence Center (JAIC) is the focal point for the DoD’s utilization of AI.

Understanding AI Technology: An overview of artificial intelligence and machine learning technology designed for non-technical managers, officers, and executives. Greg Allen, Chief of Strategy and Communications, JAIC, April 2020 with foreword by General Jack Shanahan.

Two-day JAIC hosted workshop September 9-10, 2020: Transforming the DOD through AI.

Artificial Intelligence Landscape

Worldwide interest: EU through Horizon 2020 and predecessor programs—First International Workshop on Realizing Artificial Intelligence Synergies in Software Engineering (RAISE 2012), Russian and Chinese interest at top government leadership levels.

Academic perspective: Computing Community Consortium (CCC) A 20 Year Community Roadmap for Artificial Intelligence Research in the US (August 2019) led by Yolanda Gil (President of AAAI) and Bart Selman (President Elect of AAAI): Building consensus around research visions and creating funding opportunities to enable them.

A 20-Year Community Roadmap for Artificial Intelligence Research in the US

Industrial commitment: Microsoft, Google, Amazon, Qualcomm, Intel.

Google AI's Jeff Dean: "We want to use AI to augment the abilities of people, to enable us to accomplish more and to allow us to spend more time on our creative endeavors."

New large Microsoft AI for Health initiative led by Peter Lee

Hardware Trends

Advanced computing driving ML progress and applications. Large machines plus specialized architectures

ExtremeTech: Microsoft teamed with Open AI to create one of the world's top performing supercomputers exclusively for training AI large models with billions of parameters.

Google also making supercomputing capabilities available.

Wafer-scale chips and other ASCIs for AI: Enabling training (and re-training) in hours rather than days, just emerging from multiple performers. CEREBRAS wafer scale chip is one example with one of first deployments at Pittsburgh Supercomputing Center.

A different computing problem: AI Computing at the edge. Tiny neural nets.

Software Trends

AI tools empowering moderate to experienced programmers

Microsoft Tools

- Microsoft Deep Coder: Learning to Write Programs
- Code Defect AI

Amazon Code GURU

- Profiler tool helps developers find an application's most expensive lines of code and specific visualizations and recommendations on how to improve code to save money.
- Reviewer tool uses machine learning to identify critical issues and hard-to-find bugs during application development to improve code quality.

OpenAI, a renowned research lab dedicated to AI studies. They recently began offering their powerful text generator as a service. The newest iteration, GPT-3, is even more capable than ever. It's able to generate simple code (e.g., UI) based on human language descriptions.

Autonomous Vehicles in DoD

Air Force Materiel Command: Autonomous vehicles coming to PIRA (2019). Autonomous vehicles make up a 10-vehicle convoy array for an Air Force targeting scenario, freeing up personnel from slow speed, uneven terrain driving.

CCDC Army Research Laboratory: Army researchers augment combat vehicles with AI (2020). It launched a research program to build autonomous systems to execute multi-domain operations. Challenges listed include

- minimizing training time, data
- rugged, non-road environments
- adversarial conditions

Air Force Institute of Technology: Diffusion of Autonomous Vehicles as an Organizational Innovation (2017) examined organizational readiness for autonomous vehicle adoption. “Squadron leadership—especially the commander or commander-equivalent—was found to be a critical enabler for change and innovation.”

Adversarial Machine Learning (AML)

- Adversarial Machine Learning -- Industry Perspectives (Microsoft, 2020): “Based on interviews with 28 organizations, we found that industry **practitioners are not equipped** with tactical and strategic tools to protect, detect and respond to attacks on their Machine Learning (ML) systems.”
- Example attack motivations

Exploratory	Understand details of data, model parameters
Evasion	Force the model to produce an undesired result
Poison	Maliciously transform the training data

- Coming next: Quantum Adversarial Machine Learning

Opportunities

AI as a Service: Provide (give access to your data) get the AI/ML answer. Provides new models of business: (Predictive) maintenance for jet engines (enabling selling jet engines with costs by the hour of use is moving this way)

AI as Automated Assistant for Humans: Decision-making—especially important in the Intelligence Community for rapidly developing and providing documentation, especially in crisis situations.

AI Engineering: Transfer software engineering principles to AI. The SEI has embraced the DoD role for AI engineering; work in progress.

Causal Learning: Deep learning can only predict *what* will happen, with little transparency. Create AI systems that can predict *why* something will happen, through cause and effect.

Emerging Technologies 2020

Consensus List of Emerging Technologies

Extended Reality

Extended Reality Overview

- Comprises virtual reality, augmented reality, and other technologies
- Virtual reality: fully-immersed in a virtual environment requiring some form of headset
- Augmented reality: objects and information are overlaid on your view of the real world.
- Key trends: moving beyond games and entertainment to transforming the way we work, build, create and collaborate
- 5G will enable the spaces in which Extended Reality can function—for example, conducting a VR/AR meeting from a taxi.
- Application areas: Drivers in diverse applications spaces: video games & entertainment, health care, real estate, military, science, education. NASA using to plan future Mars projects.
- Large DoD opportunities in training and simulation, diagnostic repair, and ops.

Applying Extended Reality - Examples

Photo: U.S. Army

Electronic Visualization Laboratory (EVL) at the University of Illinois at Chicago: CAVE Automatic Virtual Environment (CAVE): A science-based facility for visualizing supercomputing data.

DARPA Deep Green (circa 2007): A real-time computation of course of action of action and projection onto wearable glasses.

Games: enabled by GPU advances commoditized the field and have enabled the potential revolution.

Engadget (May 2020): Spatial goes free, aiming to become the Zoom of virtual collaboration. The tool "Spatial" renders an environment (e.g., a conference room) in the cloud for desktop users to minimize resources. Next step for work in the era of COVID?

Opportunities and Challenges

Scalability and interoperability among different AR/VR devices

Realistic Training (in VR). Incorporation, at reduced cost and complexity, of diverse human behaviors/experiences into simulations—especially important for DoD applications.

The Carnegie Mellon University Future Interfaces Group works beyond traditional VR and AR human-computers interfaces—novel sensing and interactive technologies, coupled with machine learning. See for example CMU Prof. Chris Harrison.

DoD focus on Modeling and Simulation for realistic and efficient operational training is located in Orlando.

Photo: U.S. Army

Emerging Technologies 2020

Consensus List of Emerging Technologies

Data Privacy, Trust, and Ethics

Data Privacy, Trust, and Ethics

Data is now a strategic asset.

Data privacy, trust, and ethics concerns are heightened due to advanced computing, AI, the edge, and IoT.

Privacy vs. Security:

- Privacy: focuses on the use of personal data.
- Security: focuses on protecting data from malicious attacks and theft.

Differential Privacy

This concept addresses the challenge of publicly sharing data set information about patterns of groups while withholding individual information. It is important for the census, medical analyses, etc.

Differential privacy adds noise to the data in a very prescribed, mathematically rigorous way that preserves the properties of the overall data while hiding individual identities.

NIST published a blogpost to help enterprises and groups with differential privacy on July 27, 2020.

Maintaining Data Confidentiality While In Use

The emerging solutions of trusted execution environments (TEE) and fully homomorphic encryption (FHE) aim to protect data while in use.

They are especially important for AI training data sets that include sensitive personal information, but are also important in a wide range of data environments.

The Confidential Computing Consortium (CCC) is a community focused on securing data using hardware-based TEE technologies and standards.

CCC was established through the Linux Foundation in September 2019.

TEEs provide a level of data integrity, confidentiality, and code integrity.

Fully homomorphic encryption (FHE) is an alternative that can protect data but can't ensure the correct operations are executed.

Blockchain

Blockchain is a distributed ledger technology with roots in Bitcoin.

Blockchain creates pervasive business opportunities by establishing an immutable ledger for recording transactions, tracking assets, building trust, and enabling smart contracts.

Hyperledger Fabric, released through the Linux Foundation has become a leading collaboration mechanism. IBM is making a big push in Blockchain—part of its “5in5” strategy.

Gartner projects practical enterprise applications in the next 3 to 5 years.

The USAF has some embryonic efforts (funded through SBIR) using Hyperledger Fabric for supply chain logistics.

Trust

Trust has many aspects, among which is *confidence* in the data you see (or the output of some AI system).

Explainable AI concerns the ability to understand why the AI made a given decision. Often tradeoffs between accuracy and explainability. Improving explainability also benefits system qualities like fairness, testing, safety, etc.

- Can the AI system explain its answer?
- Can I really have confidence, or is this outcome bias?
- Are there small changes to inputs that would alter the system's predictions?

DARPA launched its Explainable AI (XAI) program in 2017.

Deepfakes (synthesized video, audio, etc.) present misleading or incorrect information.

One perspective on trust in AI: AI is the problem, but it is also the answer to overcoming the misuse of AI systems.

Ethics

"Such is the speed, complexity and ubiquity of innovation today, we need a regulatory process that looks ahead to how emerging technologies could conceivably be weaponized, with holding back the development of these technologies for beneficial ends."

--Anja Kaspersen, former Head Geopolitics and International Security, at the World Economic Forum, Ten Trends for the Future of Warfare (2016).

Ethical considerations are not limited to AI, but rather are becoming increasingly important across the spectrum of emerging technologies.

Ethics

AI built with significant volumes of personal data has the potential to enable great advances in a variety of fields; for instance, healthcare.

Individuals can be persuaded to allow the use of their personal data to create such AI systems if they can be shown the benefit of doing so.

These same individuals will quickly lose trust in, and conceal information from, such systems if they are poorly governed or suffer a breach of private information.

Source: *Deloitte Insights*. Ethical Technology and Trust. January 2020.

Fairness: Are AI systems resulting in unfair outcomes?

- Harms of allocation: resources, services withheld from certain groups
- Harms of representation: propagation of negative stereotypes

Emerging Technologies 2020

References

Advanced Computing References

Goldwasser, Shafi. Cryptography & Machine Learning: What Else? Presented at Crypto 2020. August 17-12, 2020 (virtual conference). https://crypto.iacr.org/2018/slides/goldwasser_iacr_distinguished_lecture.pdf.

Hennessy, John L. and Patterson, David A. "A New Golden Age for Computer Architecture." *Communications of the ACM.* Pages 48-60. February 2019. Vol. 62 No. 2. https://cacm.acm.org/magazines/2019/2/234352-a-new-golden-age-for-computer-architecture/fulltext

Martonosi, Margaret and Roettele, Martin. *Next Steps in Quantum Computing: Computer Science's Role*. Computing Community Consortium. November 2018. https://cra.org/ccc/wp-content/uploads/sites/2/2018/11/Next-Steps-in-Quantum-Computing.pdf.

National Academies of Sciences, Engineering, and Medicine. 2019. *Quantum Computing: Progress and Prospects*. Washington, DC: The National Academies Press. https://doi.org/10.17226/25196.

NIST Computer Security Resource Center. Post-Quantum Cryptography. January 2017. https://csrc.nist.gov/projects/post-quantum-cryptography

Advanced Computing References (cont.)

NIST. 26 Algorithms Advancing to the Post-Quantum Crypto ‘Semifinals’. January 30, 2019. https://www.nist.gov/news-events/news/2019/01/nist-reveals-26-algorithms-advancing-post-quantum-crypto-semifinals

National Science and Technology Council, Committee on Science, Subcommittee on Quantum Information Science. *National Strategic Overview for Quantum Information Science*. September 2018. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Strategic-Overview-for-Quantum-Information-Science.pdf

The Smarter Edge References

Campbell, Mark. “Smart Edge: The Effects of Shifting the Center of Data Gravity Out of the Cloud.” *Computer.* Pages 99-102. Vol. 52. No. 12. Dec. 2019. https://doi.ieeecomputersociety.org/10.1109/MC.2019.2948248

Satyanarayanan, Mahadev. “The Emergence of Edge Computing.” *Computer*. Pages 30-39. Vol. 50. No. 1. Jan. 2017. doi: 10.1109/MC.2017.9. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7807196

Digital Twins References

Alber, M., Buganza Tepole, A., Cannon, W.R. *et al.* “Integrating machine learning and multiscale modeling—perspectives, challenges, and opportunities in the biological, biomedical, and behavioral sciences.” *npj Digit. Med.* **2,** 115 (2019). https://doi.org/10.1038/s41746-019-0193-y

Leopold, George. “Military Enlists Digital Twin Technology to Secure Chips.” *EE Times*. January 2, 2020. https://www.eetimes.com/military-enlists-digital-twin-technology-to-secure-chips/?utm_source=newsletter&utm_campaign=link&utm_medium=EETimesMilAero-20200108#

Mussomeli, Adam; Parrott, Aaron; Umbenhauer, Brian; and Warshaw, Lane. “Digital twins: Bridging the physical and digital.” *Deloitte Insights*. January 15, 2020. (Accessed August 20, 2020). https://www2.deloitte.com/us/en/insights/focus/tech-trends/2020/digital-twin-applications-bridging-the-physical-and-digital.html

Purdy, Mark; Eitel-Porter, Ray; Krüger, Robert; and Deblaere, Thijs. “How Digital Twins Are Reinventing Innovation.” *MIT Sloan Management Review*. January 14, 2020. (Accessed August 20, 2020). https://sloanreview.mit.edu/article/how-digital-twins-are-reinventing-innovation/

Artificial Intelligence References

Amazon. Amazon CodeGuru. (Accessed August 20, 2020). https://aws.amazon.com/codeguru/

Bergstein, Brian. "What AI still can't do". *MIT Technology Review.* February 19, 2020. (Accessed August 21, 2020). https://www.technologyreview.com/2020/02/19/868178/what-ai-still-cant-do/

Kästner, Christian. "Software Engineering for AI-Enabled Systems" (CMU 17-445/645, Summer 2020). https://ckaestne.github.io/seai/S2020/

Kästner, Christian. Software Engineering for AI/ML—An Annotated Bibliography. (Accessed August 20, 2020). https://github.com/ckaestne/seaibib

Ozkaya, Ipek (ed. in chief) and Carleton, Antia (guest editor). The AI Effect: Working at the Intersection of AI and SE. *IEEE Software*. Vol. 37. No. 4. July/August 2020. (Accessed August 20, 2020). https://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=9121610&punumber=52

Marco Polo. The Global AI Talent Tracker. (Accessed August 20, 2020). https://macropolo.org/digital-projects/the-global-ai-talent-tracker/?mod=djemDailyShot&mod=djemDailyShot

Simonite, Tom. "OpenAI's Text Generator Is Going Commercial." June 11, 2020. (Accessed August 20, 2020). https://www.wired.com/story/openai-text-generator-going-commercial/

Artificial Intelligence References (cont.)

Dawson, Caitlin. "Glimpsing into the Future of AI: A Conversation with Yolanda Gil." USCViterbi. September 18, 2019. (Accessed August 20, 2020). https://viterbischool.usc.edu/news/2019/09/glimpsing-into-the-future-of-ai-a-conversation-with-yolanda-gil/

Ning, Emma. "Microsoft open sources breakthrough optimizations for transformer inference on GPU and CPU." Microsoft Open Source Blog. January 21, 2020. (Accessed August 20, 2020).* https://cloudblogs.microsoft.com/opensource/2020/01/21/microsoft-onnx-open-source-optimizations-transformer-inference-gpu-cpu/

Vincent, Brandi. "Legislation launched in early June received new attention and support this week." NextGov. July 2, 2020. (Accessed August 20, 2020). https://www.nextgov.com/emerging-tech/2020/07/congress-inches-closer-creating-national-cloud-ai-research/166624/

Vincent, James. "OpenAI's latest breakthrough is astonishingly powerful, but still fighting its flaws. The Verge. Jul 30, 2020. (Accessed August 21, 2020). https://www.theverge.com/21346343/gpt-3-explainer-openai-examples-errors-agi-potential

* "One of the most popular deep learning models used for natural language processing is BERT (Bidirectional Encoder Representations from Transformers)."

Extended Reality References

Bayern, Macy. “Advancements in AR and VR have set the stage for mixed reality. Here's what to expect, according to industry experts.” TechRepublic. January 31, 2020. (Accessed August 20, 2020). https://www.techrepublic.com/article/10-mixed-reality-trends-to-expect-in-2020/

Bohemia Interactive Simulations (BISim). (Accessed August 20, 2020). http://www.bisimulation.com

Carnegie Mellon University. Future Interfaces Group. (Accessed August 20, 2020.) http://www.figlab.com/

Evans, Jon. “Magic Leap’s $2.6 billion bait and switch.” TechCrunch. April 26, 2020. (Accessed August 20, 2020). https://techcrunch.com/2020/04/26/tragic-leap/?guccounter=1

Hodicky, Jan. (ed.). *Modelling and Simulation for Autonomous Systems: Second International Workshop, MESAS 2015, Prague, Czech Republic, April 29-30, 2015, Revised Selected Papers*. Springer International Publishing, 2015.

Lange, Katie. “Virtual, Augmented Reality Are Moving Warfighting Forward.” Inside DoD. February 10, 2020. (Accessed August 20, 2020). https://www.defense.gov/Explore/Inside-DOD/Blog/Article/2079205/how-virtual-augmented-reality-are-moving-warfighting-forward/

Extended Reality References (cont.)

Marr, Bernard. “What Is Extended Reality Technology? A Simple Explanation For Anyone.” Forbes. Augst 12, 2019. (Accessed August 20, 2020.) https://www.forbes.com/sites/bernardmarr/2019/08/12/what-is-extended-reality-technology-a-simple-explanation-for-anyone/#5c1669d37249

Schmalstieg, Dieter and Höllerer, Tobias. *Augmented Reality: Principles and Practice*. O'Reilly Media, Inc. Boston, 2020. https://learning.oreilly.com/library/view/augmented-reality-principles/9780133153217/cover.html

University of Wyoming. Shell 3D Virtualization Center. (Accessed August 20, 2020). https://www.uwyo.edu/ser/visualization-center/

Visbox, Inc. CAVE Automatic Virtual Environment. (Accessed August 20, 2020). http://www.visbox.com/products/cave/

Visbox, Inc. Immersive 3D Applications. (Accessed August 20, 2020). http://www.visbox.com/applications/immersive-3d/

Privacy, Ethics, and Trust in Technology References

Ethical Use of (Disruptive) Technology

Bannister, Catherine and Golden, Deborah. “Ethical technology and trust: Applying your company’s values to technology, people, and processes.” Deloitte Insights. January 15, 2020. (Accessed August 20, 2020). https://www2.deloitte.com/us/en/insights/focus/tech-trends/2020/ethical-technology-and-brand-trust.html

Barber, Gregory and Molteni, Megan. “Google Is Slurping Up Health Data—and It Looks Totally Legal.” Wired. November 11, 2019. (Accessed August 20, 2020). https://www.wired.com/story/google-is-slurping-up-health-dataand-it-looks-totally-legal/

Murphy, Timothy; Garg, Swati; Sniderman, Brenna; and Buckley, Natasha. “Ethical technology use in the Fourth Industrial Revolution CEO leadership needed.” Deloitte Insights. July 15, 2019. (Accessed August 20, 2020). https://www2.deloitte.com/us/en/insights/focus/industry-4-0/ethical-technology-use-fourth-industrial-revolution.html

Privacy, Ethics, and Trust in Technology References (cont.)

Differential Privacy

Dwork, Cynthia. “A firm foundation for private data analysis.” *Communications of the ACM* Pages 86-95. Vol. 54. No. 1. January 2011. https://dl.acm.org/doi/pdf/10.1145/1866739.1866758

Hassan, M. U., M. H. Rehmani and J. Chen. “Differential Privacy Techniques for Cyber Physical Systems: A Survey.” *IEEE Communications Surveys & Tutorials 22* (2020). Pages 746-789. doi: 10.1109/COMST.2019.2944748. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8854247&tag=1

Deepfakes

Chesney, Bobby, and Citron, Danielle Keates. “Deep fakes: a looming challenge for privacy, democracy, and national security.” 107 *California Law Review* 1753. 2019. https://scholarship.law.bu.edu/faculty_scholarship/640/

Tolosana, Ruben, et al. “Deepfakes and beyond: A survey of face manipulation and fake detection.” *arXiv preprint arXiv:2001.00179.* June 18, 2020. https://arxiv.org/pdf/2001.00179.pdf

Privacy, Ethics, and Trust in Technology References

Others

Wheatly, Mike. “Accenture, AMD, Facebook and Nvidia sign up to advance ‘Confidential Computing.’” SiliconANGLE. June 29, 2020. (Accessed August 20, 2020). https://siliconangle.com/2020/06/29/accenture-amd-facebook-nvidia-sign-advance-confidential-computing/

Kozyrkov, Cassie. “Focus on decisions, not outcomes!” Medium. May 17, 2020. (Accessed August 21, 2020). https://towardsdatascience.com/focus-on-decisions-not-outcomes-bf6e99cf5e4f

Emerging Technologies 2020

Conclusion

We Want to Hear from You

This briefing presents our vision of the current state of six key emerging technologies.

We invite the SEI research community to review and comment on this presentation. We encourage any ideas for improving the briefing for a wider audience.

You can access the briefing here: [wiki link]

Please provide any feedback you have by commenting on the wiki page [TBD].

Emerging Technologies 2020

Backup Slides

Per-Source Emerging Tech Lists

MIT Technology Review	NATO	Deloitte	Forbes	Gartner	Industry Week	IDC	Accenture	World Economic Forum	IEEE	Y Combinator	SEI BD	DoD Digital Modernization Strategy
Hyper-Personalized Medicine	Autonomy	Ethical tech / trust	AI as a Service	Hyperautomation / digital twin	5G Network	Digital Transformation and Innovation	The I in Experience	Bioplastics for a Circular Economy	Edge Computing	A.I.	AI/ML	AI/ML
Digital Money	Humanistic Intelligence	Finance and the future of IT	5G Network	Multi-experience (AR, VR)	Drones	Cloud Technology	Humanistic Intelligence	Social Robots	Non-volatile Memory	Bio	Quantum Computing	Knowledge Analytics
Anti-Aging Drugs	Knowledge Analytics	Digital twin	Autonomous Driving	Democratization	Wearables	Edge Computing	Beta Burden	Tiny Lenses for Miniature Devices	Digital Twins	Carbon Removal Technologies	Software is never done	Evergreen IT Approaches
AI-Discovered Molecules	Trusted Communications	Human experience platforms	Personalized and Preventive Medicine	Human augmentation	3D Printing and Additive Manufacturing	Continuous Deployment	Robotics	Disordered Proteins as Drug Targets	AI and critical systems	Cellular Agriculture and Clean Meat	Cloud Technology	DevSecOps
Satellite Mega-Constellations	Synergistic Systems	Architecture awakens	Computer Vision	Transparency and traceability	Edge Computing	Cloud-native Development	Democratized S&T	Smarter Fertilizers Can Reduce Environmental Contamination	Practical delivery drones	Response to COVID-19	AI verification / assurance / transparency	Hyper-Converged Infrastructure (HCI)
Quantum Computing	Edge Computing		Extended Reality	Empowered edge/IoT	Blockchain	AI/ML		Collaborative Telepresence	Additive manufacturing	Energy	Self-healing systems	Serverless, or Event-Driven, Computing
Tiny AI	Ubiquitous Sensing		Blockchain Technology	Distributed cloud	Quantum Computing	Privacy, ethics, trust in tech		Advanced Food Tracking and Packaging	Cognitive skills for robots	Enterprise Software		Software Defined Networking (SDN)
Differential Privacy	Decentralized Production			Autonomous things	Industrial Internet of Things	Developer Ecosystem		Safer Nuclear Reactors	AI/ML applied to cybersecurity	Financial Services		Block Chain Cybersecurity Shield
Climate Change Attribution	Democratized S&T			Practical blockchain	Robotics and Automation	New inter-industry links		DNA Data Storage	Legal related implications to reflect security and privacy	Healthcare		Cryptographic Modernization
Unhackable Internet	Digital Twin			AI security	AI/ML			Utility-Scale Storage of Renewable Energy	Adversarial Machine Learning	Improving Memory		Quantum Computing

Emerging Technologies 2020

Recycle Bin

Deepfakes: Scenarios

“Soldiers could be shown murdering innocent civilians in a war zone, precipitating waves of violence and even strategic harms to a war effort…

A fake video might portray an Israeli official doing or saying something so inflammatory as to cause riots in neighboring countries, potentially disrupting diplomatic ties or sparking a wave of violence…

A fake video might depict emergency officials "announcing“ an impending missile strike on Los Angeles or an emergent pandemic in New York City, provoking panic and worse.

” (Chesney, 2019)

Deepfakes: Details

“The free access to large-scale public databases, together with the fast progress of deep learning techniques, in particular Generative Adversarial Networks, have led to the generation of very realistic fake content with its corresponding implications towards society in this era of fake news.” (Tolosana, 2020)

Common Techniques:

1. Face Synthesis
2. Identity Swap
3. Attribute Manipulation
4. Expression Swap

Deepfakes: Detection

- Currently easy to detect with time, full context, but slower than social media speed
- Longer videos -> more data -> easier to detect
- Deepfake tech continuously improving
- Using metadata: steganography, RGB, infrared, posting context

Ethical use of (disruptive) technology

“Leaders rated “societal impact” (including income inequality, diversity, and the environment) as the No.1 factor in assessing their organization’s annual performance, ahead of financial performance” (Deloitte, 2020)

- Biased data/algorithmic bias - connections to ML
- Data Privacy
- Disabled accessibility – connections to Veterans Affairs
- Explainable AI
- New Regulation
  - European Union’s General Data Protection Regulation
  - California’s Consumer Privacy Act

Ethical use of (disruptive) technology: Scenario

“For example, data analytics, AI, and machine learning can help researchers and clinicians predict chronic disease risk and arrange early interventions, monitor patient symptoms and receive alerts if interventions are needed, estimate patient costs more accurately, reduce unnecessary care, and allocate personnel and resources more efficiently. When patients understand these benefits, they’re generally willing to share their personal and health information with care providers. But their trust could diminish—or vanish—if weak data security or governance protocols were to result in a data breach or unauthorized use of private health information. This could cause patients to conceal information from care professionals, lose confidence in diagnoses, or ignore treatment recommendations.” (Deloitte, 2020)

Sources

Differential Privacy

M. U. Hassan, M. H. Rehmani and J. Chen, "Differential Privacy Techniques for Cyber Physical Systems: A Survey," in IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 746-789, Firstquarter 2020, doi: 10.1109/COMST.2019.2944748.

Dwork, Cynthia. "A firm foundation for private data analysis." *Communications of the ACM* 54.1 (2011): 86-95.

Deepfakes

Tolosana, Ruben, et al. "Deepfakes and beyond: A survey of face manipulation and fake detection." *arXiv preprint arXiv:2001.00179* (2020).

Chesney, Bobby, and Danielle Citron. "Deep fakes: a looming challenge for privacy, democracy, and national security." *Calif. L. Rev.* 107 (2019): 1753.

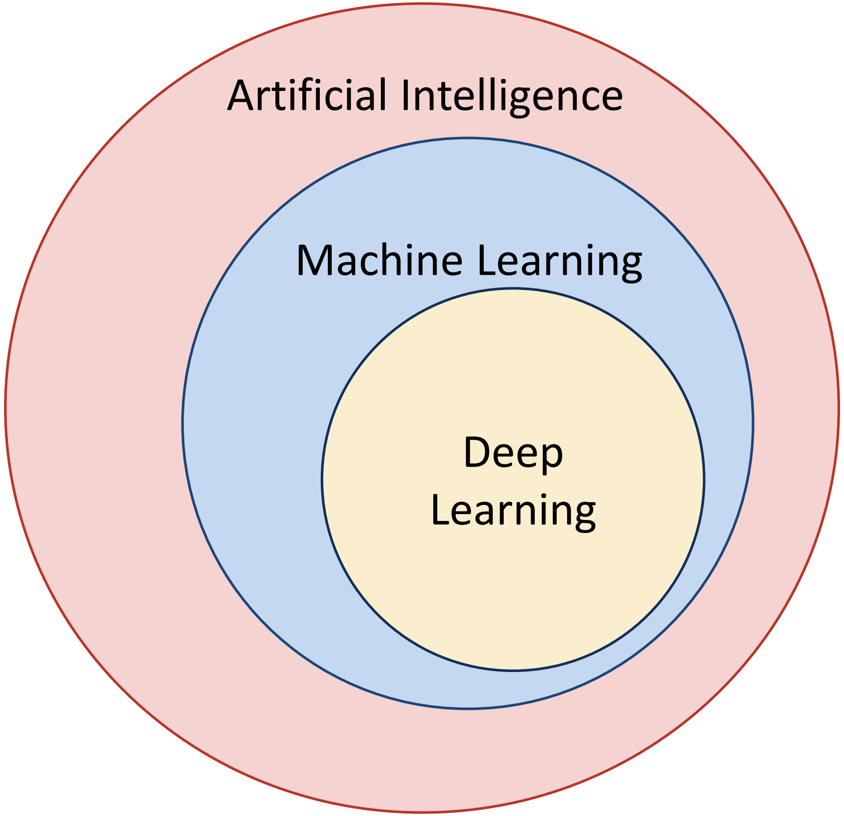
Contemporary Examples

- Ultrasounds
- Hearing aids
- Games (e.g. Pokemon Go) [incorporate into notes of previous slide]

Future Extended Reality Applications

- Richer integration with electroencephalogram (EEG) devices, allowing connection to brain
- Active reading assistance
- Social computing
- Hard-to-perceive devices – espionage applications?

AI vs ML



Non-ML AI Possibilities

- Intelligent architectures
- “Systems that have the ability to assess their own performance and set their own goals for learning."

AI/ML: New Developments

- CMU's Martial Hebert: "look at AI very broadly, from the physical layers (sensors), to software, to the ML algorithms, to human interactions and the social sciences“
- How do we design for resource-limited AI, with limited amounts of data/power?

Software Engineering and AI/ML

Different Interpretations…

- Building better models
- Developing better ML frameworks
- Using ML to enable better software engineering
- Applying software engineering to AI-enabled systems

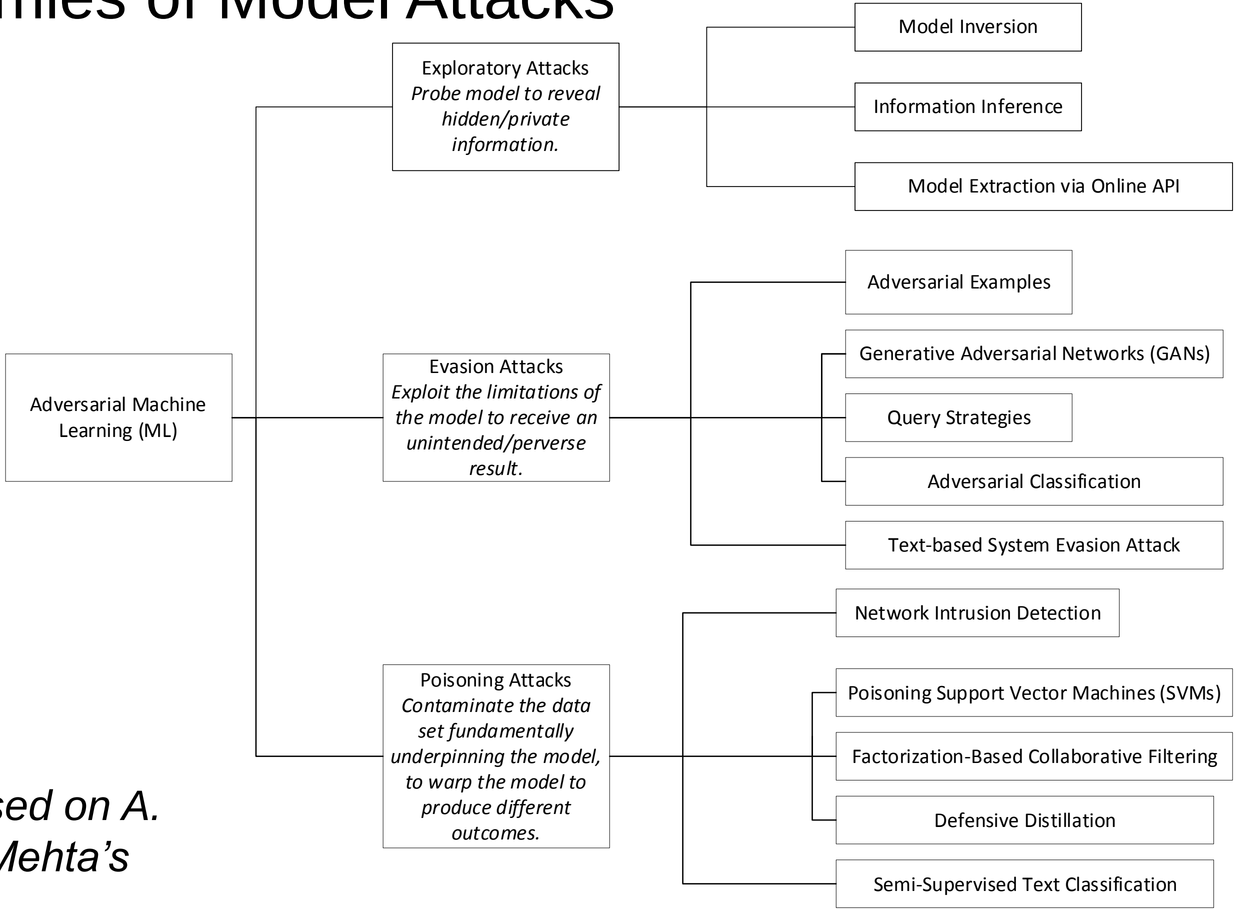
Using ML to Enable Better Software Engineering

- Example applications
  - Code search
  - Code completion
  - Program auto-repair
  - Log analysis
  - Bug detection

Applying Software Engineering to AI-enabled Systems

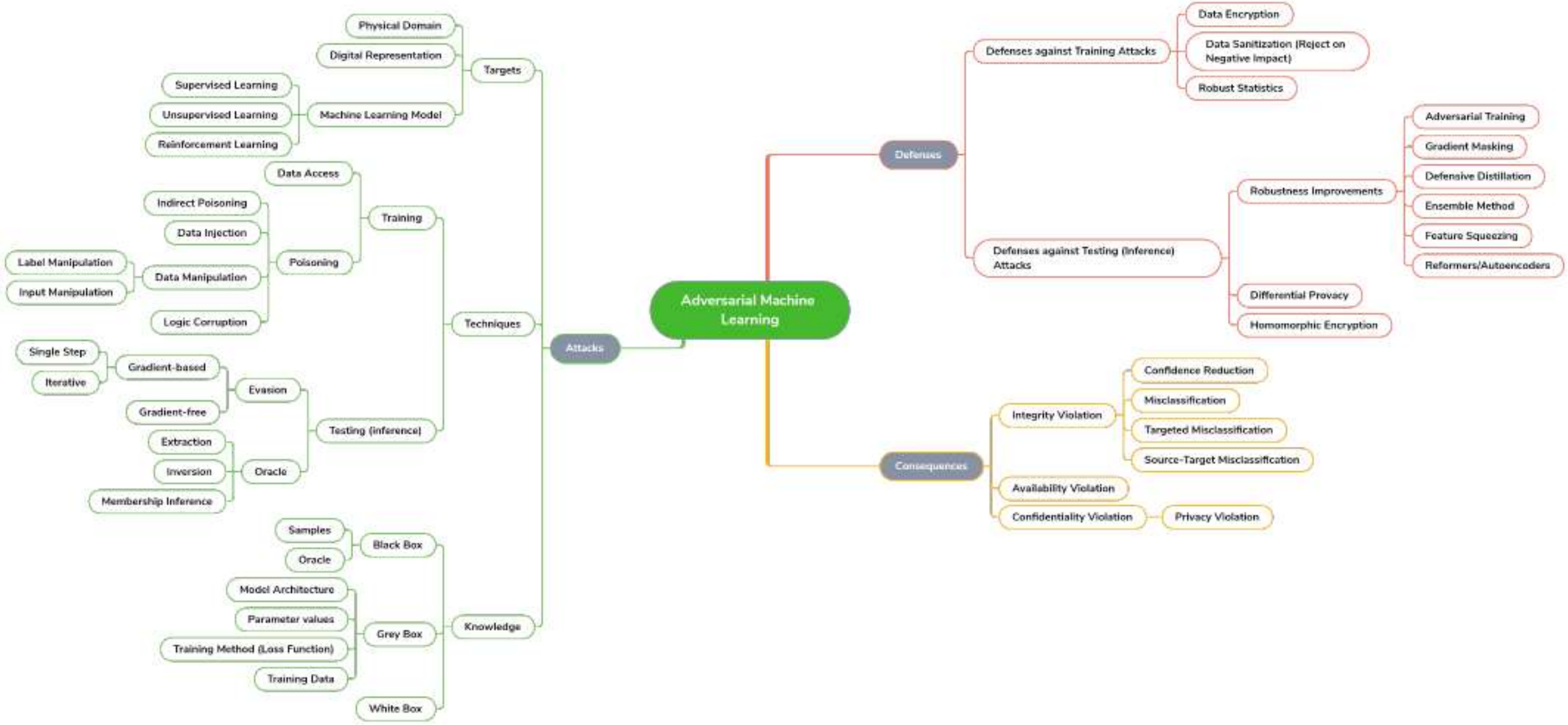
- CMU Professor Christian Kastner's "Software Engineering for AI-Enabled Systems" (course | annotated bibliography)
- IEEE Software: The AI Effect (Editor-in-Chief: Ipek Ozkaya, Guest Editor: Anita Carleton)

Taxonomies of Model Attacks



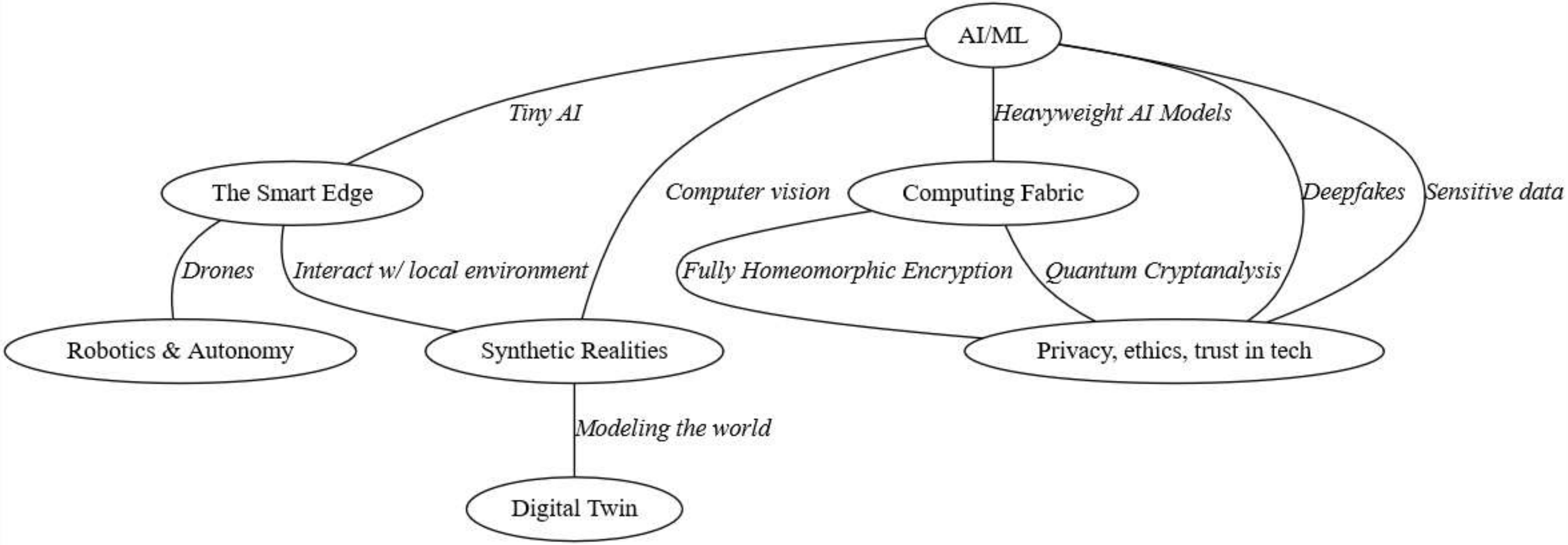
Adaptation, based on A. Kumar and S. Mehta's paper.

NIST Taxonomy of Adversarial Attacks



275

Relationships Between Concepts (WIP)



Advanced Computing:

HPC: Microsoft's Massive AI Supercomputer on Azure: 285k CPU Cores, 10k GPUs

> *This supercomputer system, among the top 5 in the world, is intended for training larger AI models targeting highly complex problems and is, Microsoft said in a blog, "a first step toward making the next generation of very large AI models and the infrastructure needed to train them available as a platform for other organizations and developers to build upon."*
>
> *Turing Natural Language Generation (T-NLG) is a 17 billion-parameter (each one loosely equivalent to a synaptic connection in the human brain) language model that, according to Microsoft, performs tasks such as writing assistance and answering reader questions.*

Considerations

For each of the six emerging technologies discussed in this presentation, we will address questions such as

- What is the technology?
- What is the history and current status of the technology?
- Who are the major players in this technology?
- What are the opportunities and risks for DoD?
- Has DoD taken a policy and/or technical position on the technology?
- Is the technology make or buy?
- What is the opportunity for SEI?

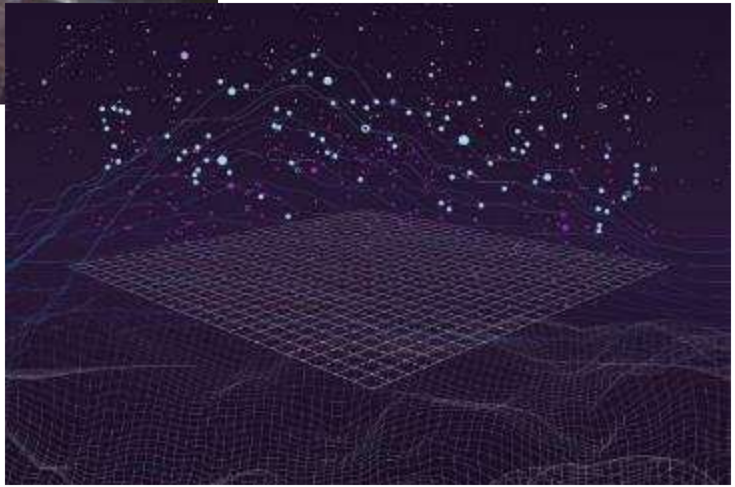
Images

Images

Images IoT

Images Privacy and Ethics

Images Quantum



Images Blockchain

Images Low Code platforms

Images Digital Twin