MPE 2037: Decentralized Autonomous Organizations And Trust Enabling Technologies

TIES
TRUST AND INFORMATION ECO-SYSTEM

USAWC Futures Seminar
COL Troy Alexander
COL Greg Pavlichko
COL Anthony Pollio
LTC Patrick Hofmann
LTC Nicky Shadley

Under the direction of Professor Kris Wheaton

About This Document

The United States Army War College (USAWC) student team Trust and Information Eco-System (TIES) prepared this document as a group Integrated Research Project, which contributed to team members earning a Master of Strategic Studies degree from the USAWC. The research, analysis, and production of this product occurred over 29 weeks from October 2021 – May 2022 as part of the in-residence USAWC Senior Service College program. The team consisted of three U.S. Army Colonels (O-6) and two U.S. Army Lieutenant Colonels (O-5). The team members were LTC Nicky Shadley, LTC Patrick Hofmann, COL Troy Alexander, COL Greg Pavlichko, and COL Anthony Pollio. The team conducted the research under the direction of Professor Kris Wheaton, Professor of Strategic Futures, Center for Strategic Leadership, USAWC.

Requirement

This report answers the questions posed by LTG Laura A. Potter Deputy Chief of Staff G2, Headquarters, Department of the Army (see Annex A). Team TIES collected and analyzed open-source, unclassified, information to produced estimates relevant to LTG Potter's questions:

What technical and process advancements over the next 15 years are likely to enable dynamic information sharing and decision making within a Mission Partner Environment (MPE) despite asymmetries of trust?

- What data formatting, data routing, and trust relationships are required for the future MPE?
- What technology and or process improvements will facilitate multilateral sharing of information in near real-time?
- How is mission partner information protected from indiscreet sharing amongst partners and allies?
- How does this capability utilize future developments in artificial intelligence to solve above stated problems?
- What policy changes are required to enable the future MPE?

Analytic Confidence

This overall estimate is made with moderate analytic confidence. The questions asked were complex, while the timeline was relatively short, due to competing academic requirements of the USAWC core curriculum. Source reliability and corroboration were predominantly moderate to high. However, the analysts were not subject matter experts and worked both individually and collaboratively to research and answer the questions. Theoretical predictions varied, and research sometimes conflicted, specifically with time-based predictions on technical reliability or wide-scale adoption. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Terms of Analytic Probability

Team members used Intelligence Community Directive 203 (see Annex E) to define their terms of analytic probability. Using this scale, team members provided an estimate for each analytic report in this document to forecast the probability that a particular claim would occur.

Source Reliability

Team members noted source reliability as Low (L), Moderate (M), or High (H) for each citation in the report. Each citation is hyperlinked to its source on the internet. Team members determined source reliability using the Trust Scale and Web Site Evaluation Worksheet (see Annex D).

The Team produced this report in both PDF and hard copy formats. Readers are encouraged to use the PDF version, as it provides links to the original source material. Additionally, the team is scheduled to provide a PowerPoint presentation on key findings to LTG Potter and members of her staff on May 9, 2022 (see Annex G).

Report Organization

The Team's key findings are outlined in the next section (see Key Findings). The main body of the report is organized into five sections. Sections one through four contain the individual analytic reports that support the essential attributes of the forecasted 2037 MPE. The four essential attributes are Decentralization (see Section 1), Culturally-Sensitive Mixed Reality (see Section 2), Augmented Intelligence (see Section 3), and Three Factor Trust (see Section 4). Section five contains each team members integrated analytic report. The integrated reports synthesize information from multiple individual analytic reports.

TIES

TRUST AND INFORMATION ECO-SYSTEM

COL Gregory J. Pavlichko
gregory.j.pavlichko.mil@army.mil

COL Troy V. Alexander
troy.v.alexander.mil@army.mil

Anthony F. Pollio Jr.

COL Anthony F. Pollio Jr.
anthony.f.pollio.mil@army.mil

LTC Patrick J. Hofmann
patrick.j.hofmann.mil@army.mil

Nicole Y. Shadley

LTC Nicole Y. Shadley
nicole.y.shadley.mil@army.mil

Key Findings

Research Question

What technical and process advancements over the next 15 years are likely to enable dynamic information sharing and decision making within a Mission Partner Environment (MPE) despite asymmetries of trust?

- *What data formatting, data routing, and trust relationships are required for the future MPE?*
- *What technology and or process improvements will facilitate multilateral sharing of information in near real-time?*
- *How is mission partner information protected from indiscreet sharing amongst partners and allies?*
- *How does this capability utilize future developments in artificial intelligence to solve above stated problems?*
- *What policy changes are required to enable the future MPE?*

Decentralized Autonomous Organizations enhanced by four trust-enabling technologies and four essential attributes are likely to enable the technical and process advancements over the next 15 years to enable dynamic information sharing and decision making within an MPE despite asymmetries of trust.

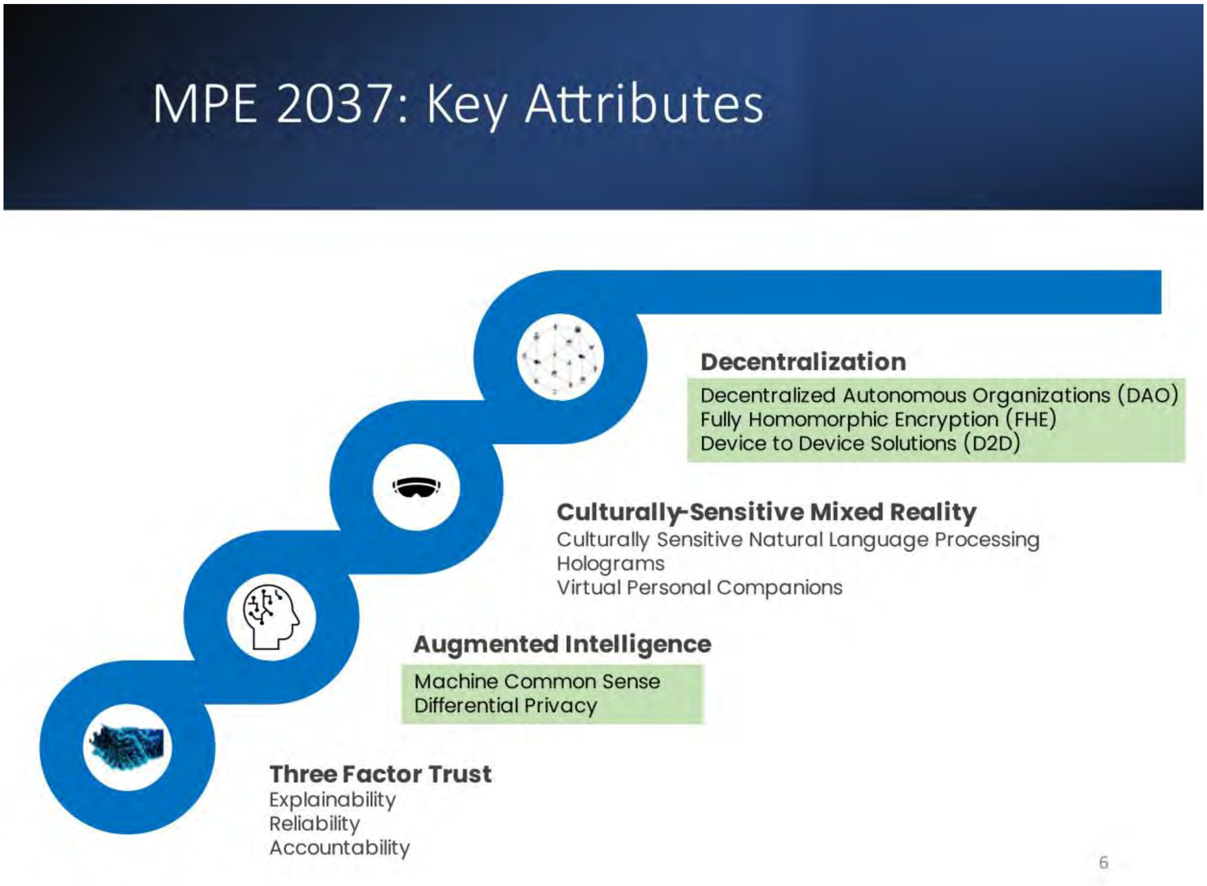
DAOs are enabled by four trust-enabling technologies:

1. Fully Homomorphic Encryption
2. Differential Privacy
3. Machine Common Sense
4. Device to Device Mesh Networks

MPE 2037's essential attributes are:

1. Decentralization
2. Culturally Sensitive Mixed Reality
3. Augmented Intelligence
4. Three Factor Trust

MPE 2037 will likely emerge at the intersection of four essential attributes each supported by at least one key technology and multiple related technologies.



MPE 2037: Key Attributes

Decentralization

Decentralized Autonomous Organizations (DAO)
Fully Homomorphic Encryption (FHE)
Device to Device Solutions (D2D)

Culturally-Sensitive Mixed Reality

Culturally Sensitive Natural Language Processing
Holograms
Virtual Personal Companions

Augmented Intelligence

Machine Common Sense
Differential Privacy

Three Factor Trust

Explainability
Reliability
Accountability

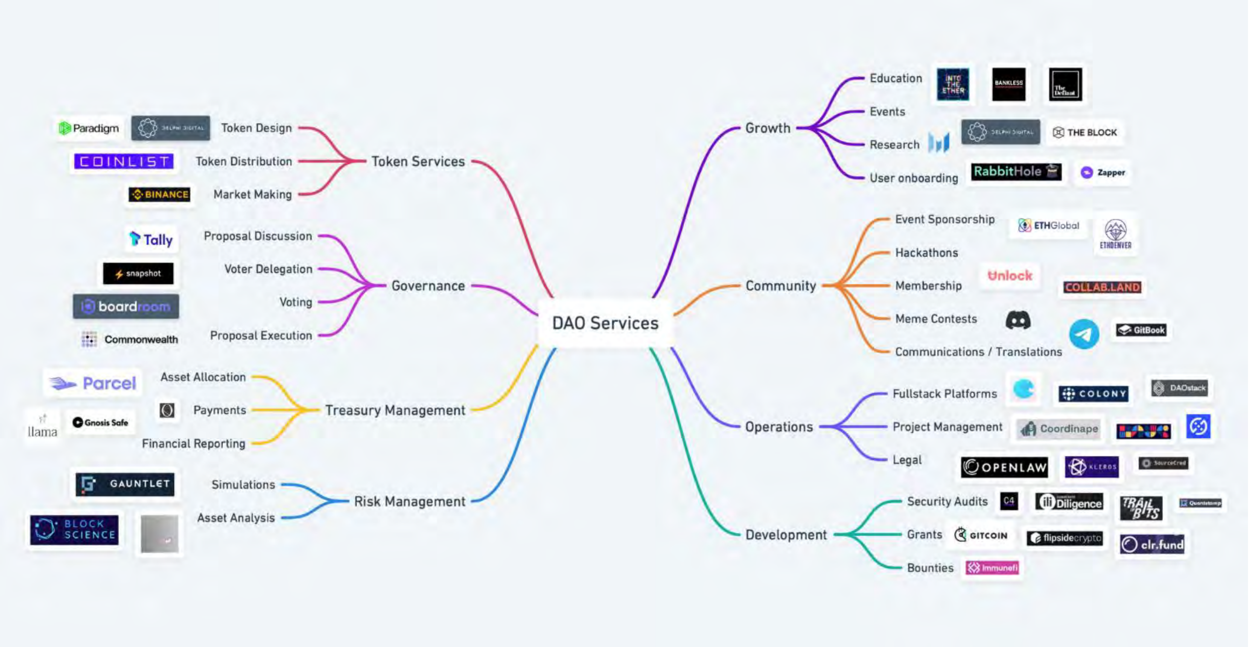
6

Decentralization

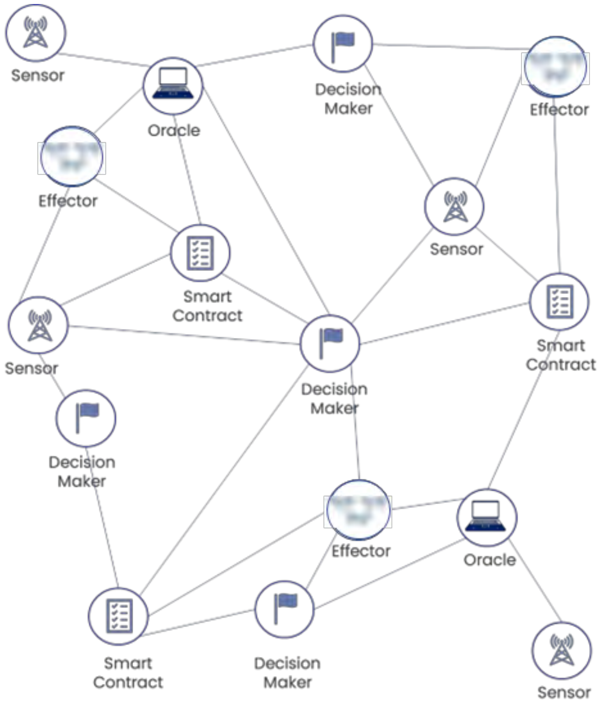
According to over 100 sources, including peer-reviewed academic journals as well as business and industry experts, three emerging technologies, including decentralized autonomous organizations, fully homomorphic encryption, and device to device networks, will likely not only make decentralization possible, but will become the way business and industry operate in the future.

Decentralized Autonomous Organizations (DAOs)

Even though the concept of Decentralized Autonomous Organizations is new, implementation at scale across multiple sectors and government is highly likely by 2037. DAOs are a group of entities that join under a blockchain infrastructure to enforce a set of shared rules to achieve a common goal. Adoption of the DAO methodology will enhance survivability and increase the speed and efficiency of decision making. Private industry, across dozens of sectors, is working to make DAOs viable as a business model.

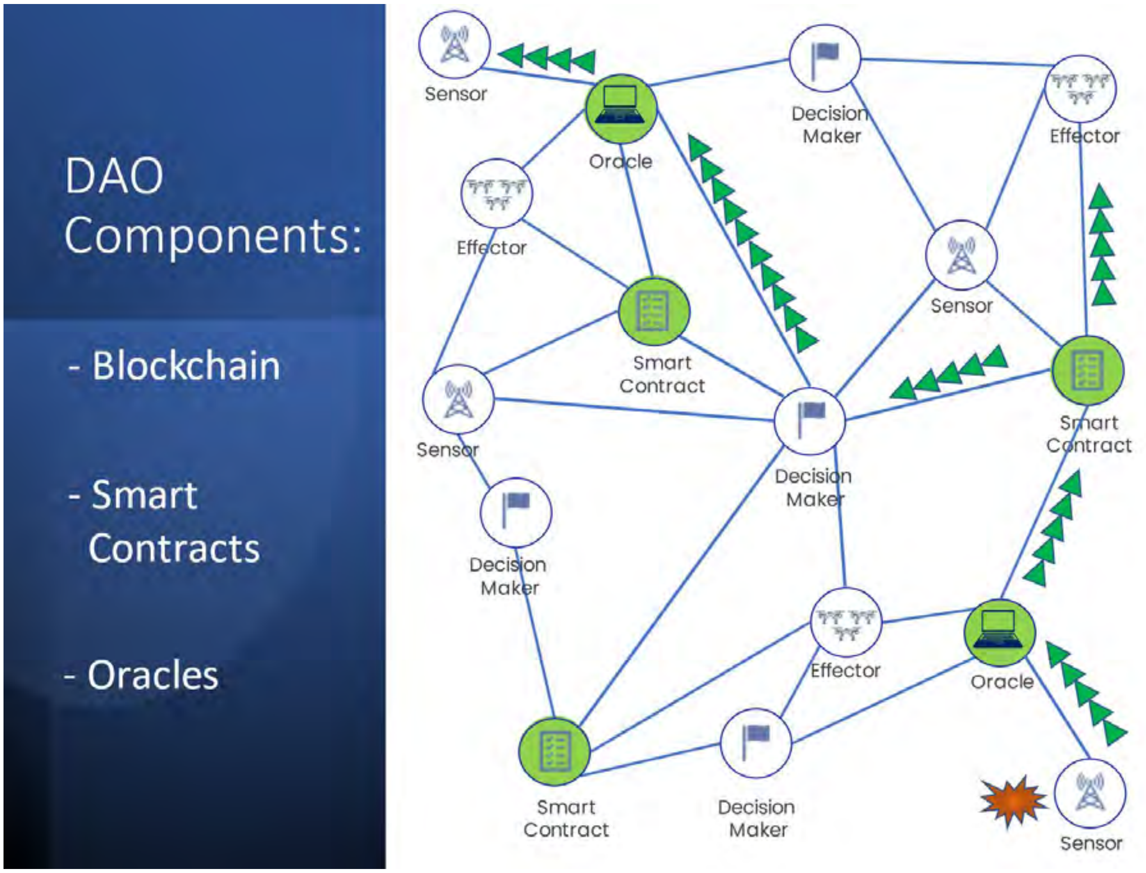


Vitalik Buterin, a co-founder of the cryptocurrency Ethereum, states DAOs are the choice for the crypto industry because they provide simplified and secure transactions through the blockchain, and reduction in bureaucracy due to the use of smart contracts. DAOs also meet the crypto requirement to perform efficient and fast decentralized and secure transactions.



> *In addition, Dr. Weidong Shi, Associate Professor of Computer Science at University of Houston has constructed a DAO model for e-governance applications in government contracting. According to Dr. Shi DAOs could provide transparency, accountability, immutability, and, more importantly, better resource management.*

DAOs are composed of three key components: blockchain, smart contracts, and oracles. The blockchain acts as the ledger that records all transactions within a DAO. A smart contract is the executable component of a DAO. Once specific conditions are satisfied, the smart contract executes the appropriate action.



DAO Components:

- Blockchain
- Smart Contracts
- Oracles

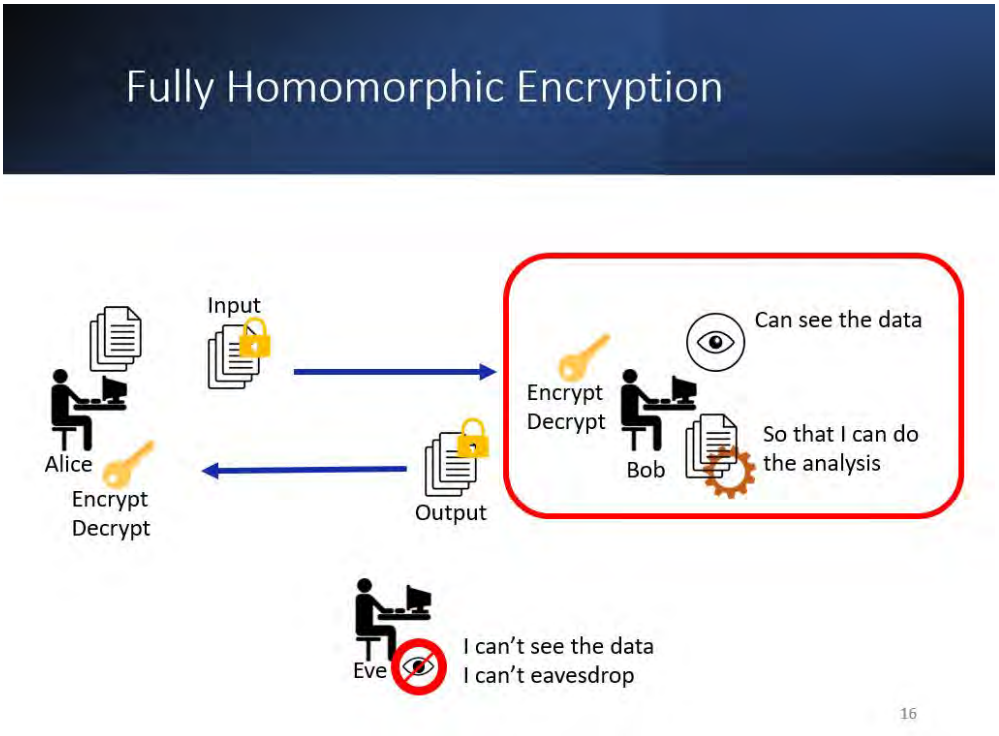
The blockchain records the actions executed by smart contracts so that all members (or at least members with contracted access) can view the results. Oracles are the entry point into and out of the DAO to the World Wide Web. Oracles allow external data inputs into the DAO and allow smart contracts to access existing data sources, legacy systems, and advanced computations.

> *According to Dr. Samer Hassan, associate professor at Harvard University's Berkman Klein Center for Internet and Society, blockchain technology capabilities extend beyond cryptocurrencies and other financial applications. Blockchain enables existing applications to acquire new features, and new distributed applications to emerge.*
>
> *Dr. Hassan also states that in the future, DAOs could be able to autonomously hire people, provide services, gain money for their own aims, own smart property, coordinate with other autonomous software, or facilitate cooperation.*

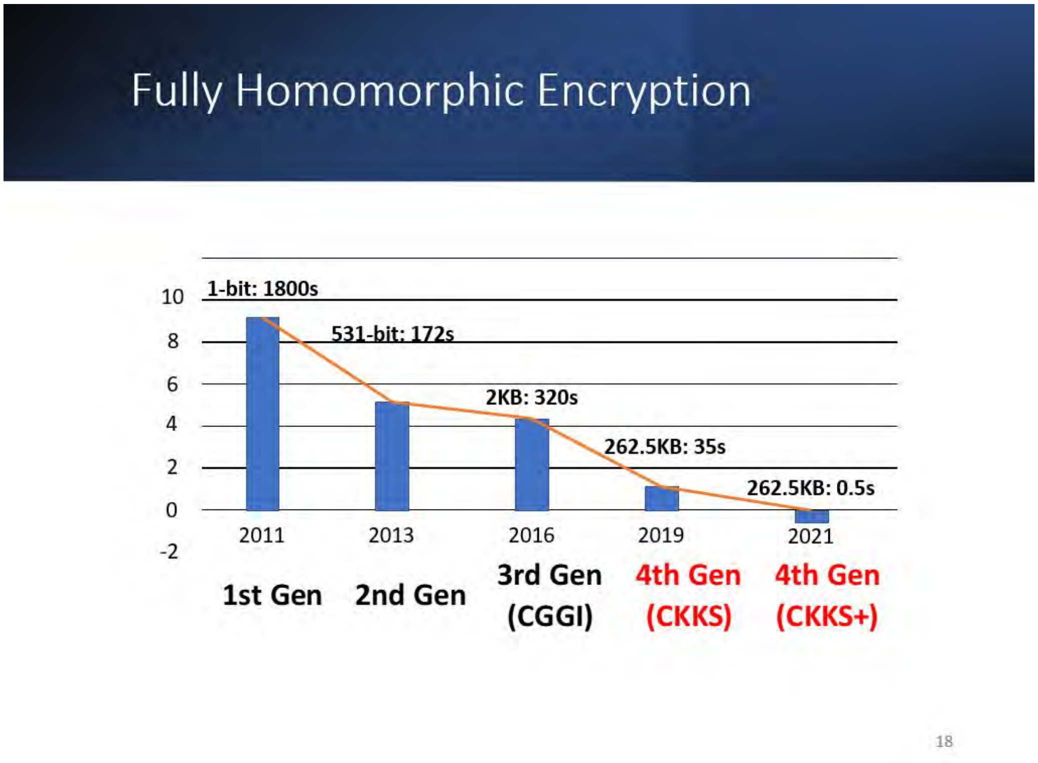
Fully Homomorphic Encryption (FHE)

Even though Fully Homomorphic Encryption is, at this time, a slow cryptographic technique that requires significant processing power, it is highly likely that it will achieve sufficient computational efficiency to operate at scale in the next 15 years. These advances make it likely that FHE will be a component of a secure DAO. FHE is likely to enhance current security protocols and increase trust among members of a DAO.

FHE enables an end-user to run calculations on encrypted data stored in the cloud without requiring the end-user ever to have unencrypted access to encrypted data sets. This cryptographic technique has widespread implications for many industries requiring data privacy and security.


Fully Homomorphic Encryption

Dr. Craig Gentry, the inventor of the FHE protocol, and other academic institutions are iteratively developing more efficient FHE algorithms and techniques. From the first to the 4th generation of FHE, processing time has decreased exponentially. Continued efforts indicate that FHE will mature over time and is highly likely to be scalable by 2037.



Fully Homomorphic Encryption

18

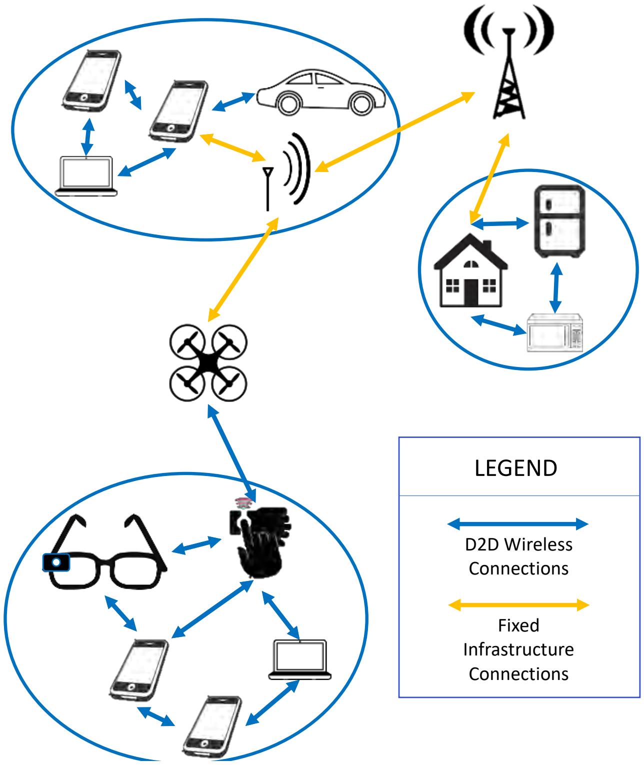
Microsoft hosted a FHE Standardization Conference in 2020 where dozens of experts from around the world, representing government, industry, and academia worked to standardize FHE protocols and libraries. These experts participated in this conference because they all understand that FHE protocol must be standardized for wide implementation.

Likewise, in 2020 DARPA spent $14M dollars to research and develop hardware with the required parameters to scale FHE.

Device to Device Solutions (D2D)

Despite resource and infrastructure limitations, Device-to-device (D2D) solutions, where any device can act as a relay to offload data and improve data transmission rates, are highly likely to contribute to the decentralization attribute of MPE 2037. D2D is device owner agnostic, in that military equipment is not required to achieve the desired capability. D2D will likely extend network capabilities to the tactical edge in remote locations.

D2D



Manos Tentzeris, project lead from Georgia Tech, has produced a small form factor, 5x5 cm, flexible prototype relay that can be attached to any object. This device is scalable and can increase, decrease, and direct bandwidth signals. The next phase in their research is testing the approach outside the lab on large, real-world structures. They are projected to present their findings at the upcoming International Microwave Symposium.

D2D differs from the DOD's concept of cyber-foraging, and Amazon and Xfinity's similar commercial applications in that it will work through all commercially connected mobile, tablet, and smart devices and without purposefully deploying additional nodes to extend the line of sight This technology will expand 6G and beyond capabilities to the most remote areas.

Other technologies likely contribute to the decentralization attribute are Internet of things, network at the edge, edge artificial intelligence, and decentralized self-sovereign identity.

Culturally Sensitive Mixed Reality

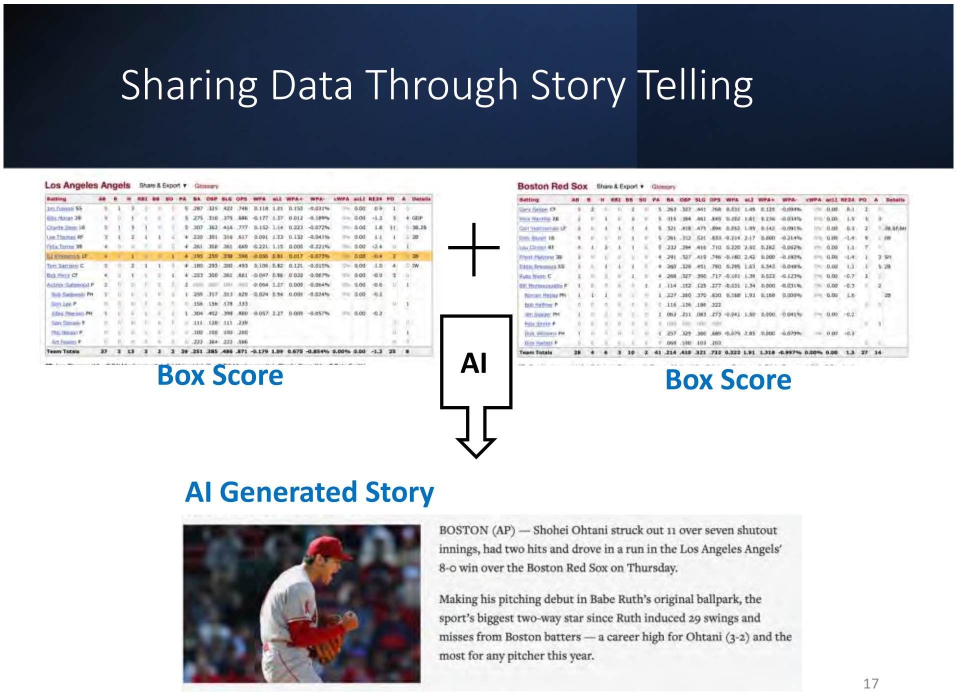
Culturally Sensitive Mixed Reality is the convergence of technology that blends physical and digital worlds to increase the quality of distributed communication and overcomes language and cultural differences. Burgeoning technologies will likely make cultural sensitivity through technology much more common than it is today. Culturally Sensitive Natural Language Processing, Hologram technology, and Virtual Companions, are technical advancements that will likely enable a culturally sensitive, mixed reality MPE by 2037.

Culturally Sensitive Natural Language Processing

Due to commercially available products that use storytelling and data dashboards to communicate data, focused research in the discipline of Deep Learning (DL), and current DARPA research, it is likely that NLP will be culturally sensitive enough to share data through storytelling in multinational environments by 2037. Culturally sensitive NLP will likely reduce miscommunications and increase understanding in a multilingual and multicultural environment.

There are two components of culturally sensitive NLP. The translation component and the storytelling component. Translation is enabled by the advent of deep neural networks and facilitates not only simple language translation but reflects the cultural and linguistic nuance of the translation. The storytelling component uses machine learning to cull large data sets, discover hidden insight and connections, and then communicate this analysis through an AI generated story that is easy to understand.

> *Companies like ClearStory Data use NLP to produce dynamic dashboards that learn and adapt to user inputs to determine the type of information and analysis based on the end-user requirements. News services such as Yahoo Sports and the Associated Press use these services to generate AI written and published analyses on sports and weather.*



Sharing Data Through Story Telling

AI Generated Story

BOSTON (AP) — Shohei Ohtani struck out 11 over seven shutout innings, had two hits and drove in a run in the Los Angeles Angels' 8-0 win over the Boston Red Sox on Thursday.

Making his pitching debut in Babe Ruth's original ballpark, the sport's biggest two-way star since Ruth induced 29 swings and misses from Boston batters — a career high for Ohtani (3-2) and the most for any pitcher this year.

17

> *According to Dr. Mohammad Kamel Daradkeh, an associate professor of Business Analytics and Data Science at University of Dubai, there is a positive correlation between effective data storytelling and better business performance, which is partially mediated by decision-making quality.*

Holograms

Advances in 3D hologram visualization technologies and holographic displays are likely to be adopted for use in MPE 2037. 3D Holograms create personal presences to improve communication by transporting a speaker's body language, facial expressions, and non-verbal cues to a physical location near the other party. It is likely holograms will enable MPE members to make more personal connections and deliver more impactful messages.

> *ARHT Media's CEO Larry O'Reilly envisions hologram technology disrupting the airline and hotel markets for business travelers as large companies and organizations opt for more efficient use of senior leaders' time while saving millions annually on travel expenses.*

> *Recent examples of a strategic leader using holographic technology occurred in late 2020 when the Crown Prince of Dubai made a major speech as a hologram to those in attendance at the World Government Summit. Another occurred in October 2021, when NASA and the European company AEXA Aerospace executed*

> *a 3D tele-medicine visit with an astronaut on the International Space Station by holoporting a doctor into the ISS.*
>
> *Currently this technology is not only expensive but requires an array of large equipment. However, ARHT has already developed a holographic system prototype that can "fit into a couple of duffel bags" while Google's Starline and ARHT seek to make 3D collaboration widely accessible by establishing nodes at multiple fixed locations.*

Virtual Personal Companions

As technologies coalesce and virtual personal companion capacities advance, it is likely that both private and public sectors will leverage Virtual Personal Companions for partner building by 2037. Virtual Personal Companions provide discrete abilities for stakeholders to better understand the nuances of an operating environment and a means for seamless activation of application support for analysis, triaging priorities, and problem-solving. Virtual Personal Companions are programs that understand natural language voice commands, the user environment, and complete tasks for the user.

> *According to the IEEE, the International Congress on Electronics, Electrical Engineering and Computing, has been exploring the standardization of supporting technologies such as Virtual Personal Companions since as early as 2017 to help socially disabled people to enhance interactions.*
>
> *Universities such as Beijing University, The Politecnica Salesiana University in Ecuador, and the University of Central Florida (UCF), are researching the use of virtual personal companions to augment relationship building with autistic children and others that have social disorders.*

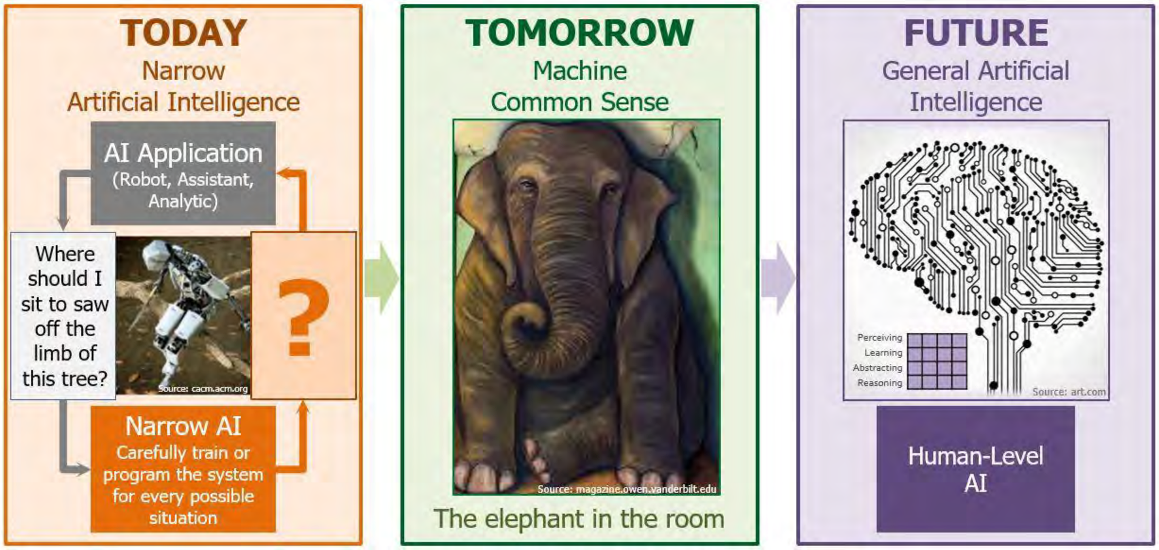
Other technologies likely contribute to the culturally sensitive mixed reality attribute are augmented reality collaboration, convergence of the digital and physical world, and ambient clinical intelligence.

Augmented Intelligence

Augmented intelligence focuses on human-machine interfaces designed to enhance human intelligence rather than to operate independently or replace it. New and emergent technologies such Machine Common Sense and Differential Privacy likely make augmented intelligence viable for use in MPE 2037.

Machine Common Sense

We intuitively know the answer to the question in the below graphic. Although poorly worded, the human brain quickly discerns the correct answer. Conversely, AI struggles with such questions. While the likelihood of true machine consciousness in the next 15 years is remote, current research efforts in academia and business make it likely that Machine Common Sense (MCS) will be realized by 2037 and become a component of MPE 2037. Machine Common Sense is likely to enable networks to learn from unique situations, apply a decision-making model, and communicate with human end users.



According to Mr. David Gunning, a researcher from DARPAs Innovation Information Office, the pursuit of MCS will impact all aspects of AI including sensemaking, reasonableness, human machine collaboration and the transfer of learning. DARPA committed $2B to their Machine Common Sense Program in 2018.

IBM, in collaboration with MIT and Harvard, are researching ways to accelerate the development of AI that exhibits common sense. At the 2021 International Conference on Machine Learning, IBM presented a benchmark to test common sense in AI. The benchmark called, AGENT (Action, Goal, Efficiency, coNstraint, uTility), is structured around four key concepts of core intuitive psychology: goal preferences, action efficiency, unobserved constraints, and cost-reward trade-offs.

Differential Privacy

It is highly likely Digital Privacy will become an overarching approach to protect personal data in the next 15 years due to its expanding use by governments and companies to address legal privacy concerns. Unlike most privacy-preserving tech, differential privacy doesn’t rely on encryption. Instead, “noise” is added to data in a very prescribed, mathematically rigorous way that preserves the properties of the overall data while hiding individual identities.

> *According to the January 2020 U.S. Census Bureau Status Report, the Bureau is using differential privacy as the method for the 2020 census disclosure control in public use data products. This represents a radical departure from current practice, where its statistics define the drawing of legislative districts, determine the distribution of federal funds for more than a hundred government programs, and are extensively analyzed by social scientists.*

> *According to collective research by Harvard University's Data Science Initiative, differential privacy has significant application for secure private to public data-sharing. The European Union, United Kingdom, and Australia have adopted or are considering the adoption of differential privacy.*

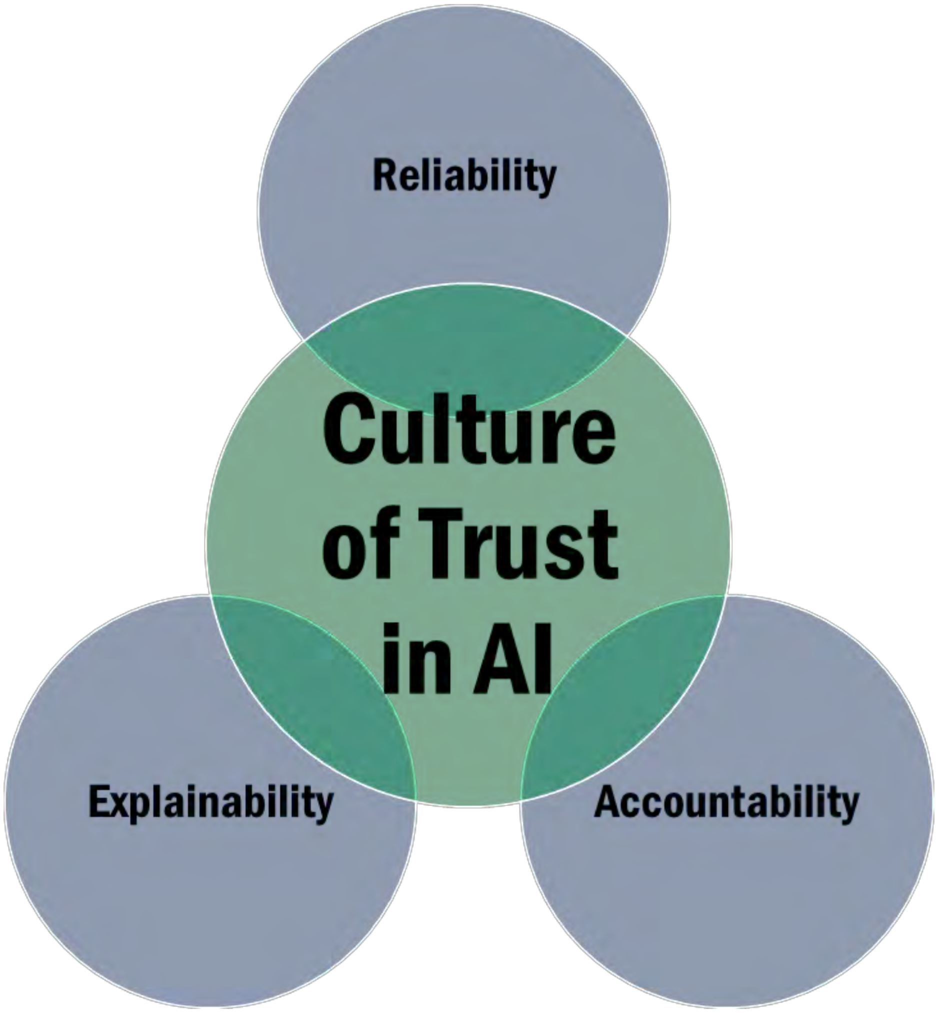
> *According to Mary Theofanos of the National Institute of Standards and Technology's Material Measurement Laboratory, the NIST is seeking to set metrics and measurements of the best algorithms to address concerns that differential privacy may hide some trends or that some of the techniques used could change the data in some way such that it's not reflective of the actual dataset.*

Other technologies likely contribute to the augmented intelligence attribute are quantum computing, analog computing, and automatic machine learning.

Three Factor Trust

It is highly likely that the intersection of three factors will create an organizational culture capable of overcoming distrust in new AI. While the literature identifies numerous factors, three are most applicable for building an organizational culture of trust:

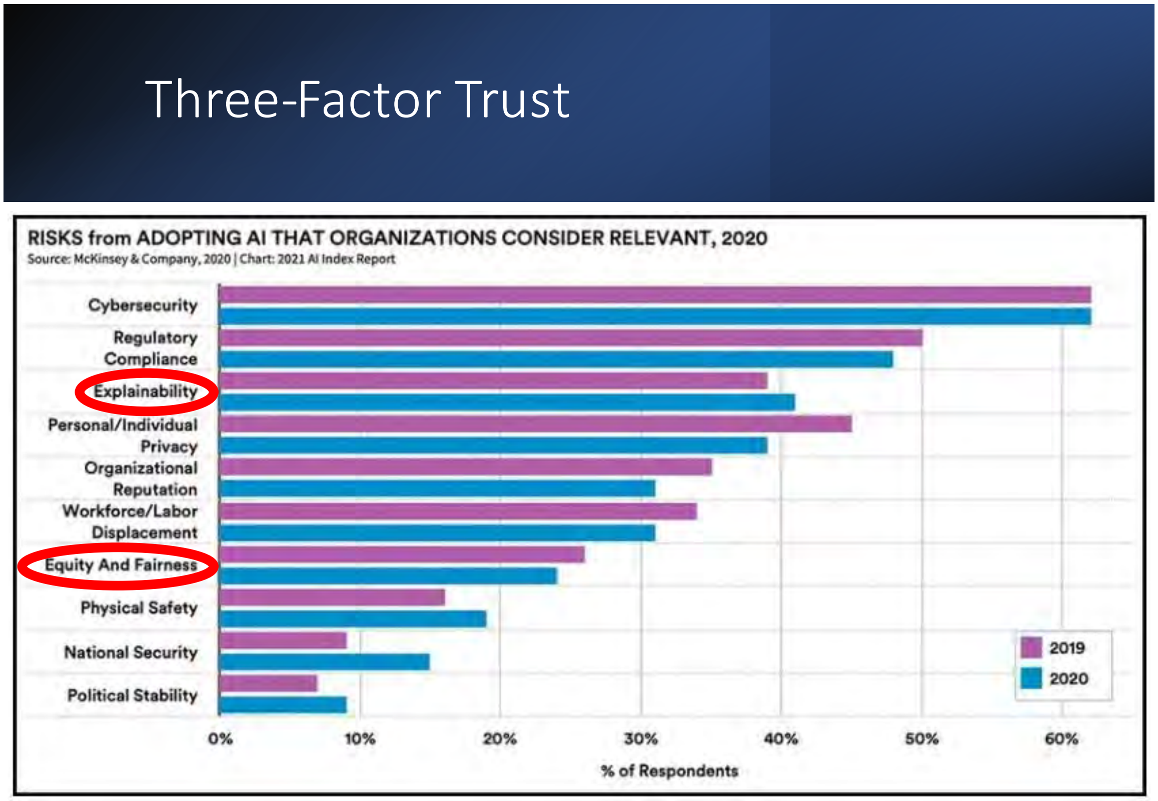
- Explainability
- Reliability
- Accountability



For background on the challenge of distrust in new AI, academic literature and survey data indicate high levels of initial distrust in new AI within commercial companies, especially distrust in new AI decision making technologies.

> *A 2021 ESI ThoughtLab survey of over 1,000 senior executives indicated that 80% of American companies were struggling with low levels of trust in AI and this distrust limited their ability to adopt new technologies.*
>
> *A Harvard study showed that trust and familiarity with AI are directly linked – determined that the most AI-savvy companies with more familiarity using AI had higher confidence in the technologies and were able to more rapidly adopt new AI tech.*

While the literature does not have a consensus on definitions for explainability, reliability, and accountability, and there is some overlap between these terms, a few charts from The Stanford Institute for Human-Centered Artificial Intelligence's annual AI Index help us visualize the challenges these factors address. Here, the AI Index identifies the risks organizations considered most relevant in 2021, showing explainability as well as concepts inherent in reliability and accountability in the top ten risk.



Three-Factor Trust

RISKS from ADOPTING AI THAT ORGANIZATIONS CONSIDER RELEVANT, 2020

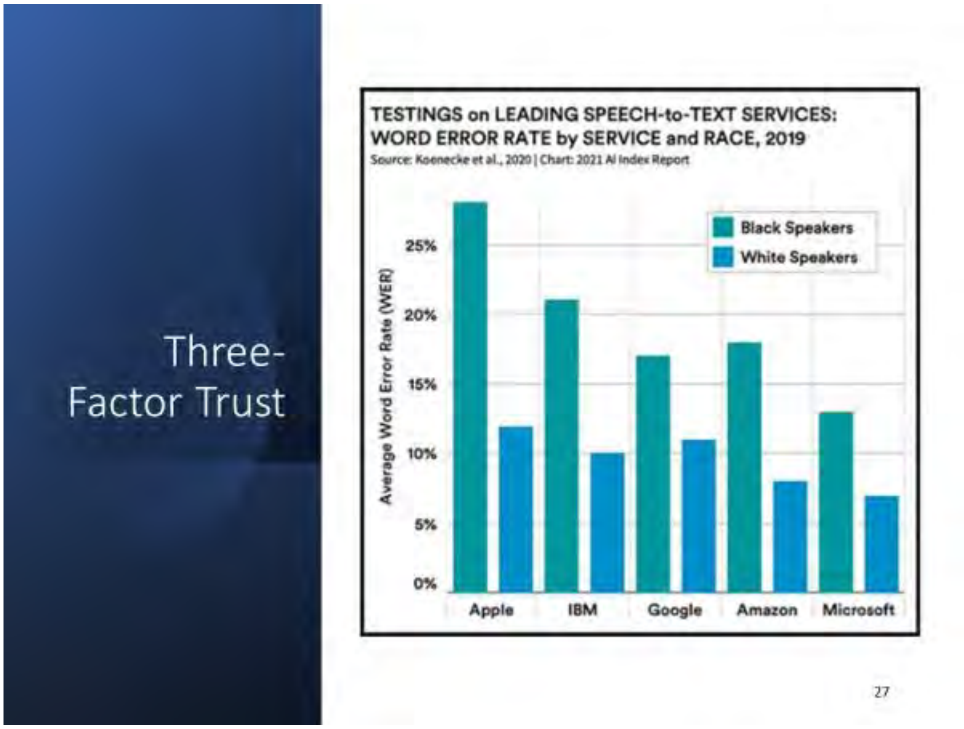
Source: McKinsey & Company, 2020 | Chart: 2021 AI Index Report

26

The first factor of the trust model, Explainability, is a concept that attempts to add transparency to the AI decision-making process. Explainability seeks to overcome distrust in AI resulting from the opaque nature of AI decision making. This is commonly referred to as the black box problem in AI.

> *A December 2021 peer-reviewed article in the Nature Human Behavior Journal shows that, despite the knowledge that AI has proven to outperforming human doctors in clinical diagnoses, patients prefer less reliable human recommendations when they cannot understand how AI algorithms generated their medical recommendations.*

Reliability refers to AI models that deliver consistent recommendations and avoid skewed recommendations resulting from data biases. The chart here from the AI Index illustrates an enduring challenge with culturally-sensitive AI, demonstrating lower reliability for black speakers originating from skewed training data.



Three-Factor Trust

TESTINGS on LEADING SPEECH-to-TEXT SERVICES: WORD ERROR RATE by SERVICE and RACE, 2019

Source: Koenecke et al., 2020 | Chart: 2021 AI Index Report

Brianna Lifshitz from Georgetown argues reliability depends primarily on removing bias from AI algorithms and data sets and recommends additional diversity among developers as a solution. Related research from Cambridge University examines the socio-cultural causes of racial, gender, origin, political, social, and ideological biases unknowingly inputted by human developers based on individual and group backgrounds.

Reliability concerns over AI bias are likely to be intensified when creating AI for use in multicultural and multilingual environments like an MPE 2037 coalition.

Lastly, Accountability integrates moral, legal, and societal values with technological developments during the design process as well as during the training of algorithms. Accountability includes the requirement to justify AI decisions to partners, users and others with whom the AI system interacts. Given that ethics are dependent on the socio-cultural contexts and informed by the values held by programmers, AI accountability in a multinational and multicultural environment, again like MPE 2037, will likely be an increasingly important trust factor.

Accountability also played a role in the previous medical distrust example, as patients were further distrustful of AI medical decisions when patients believed the AI system was less accountable than a human doctor for errors.

> *Researchers at UC Berkley and at the University of Pennsylvania separately demonstrated the ability to improve user trust by giving people control over algorithms. When users were given the freedom to slightly modify an algorithm, they felt more satisfied with it, were more likely to believe it was superior, and more likely to use in in the future.*

Other technologies likely contribute to the three-factor trust attribute are cancelable biometrics, zero trust environments, and confidential computing.

Conclusion

Decentralized Autonomous Organizations enhanced by four trust-enabling technologies and four essential attributes are likely to enable the technical and process advancements over the next 15 years to enable dynamic information sharing and decision making within an MPE despite asymmetries of trust. To achieve the MPE 2037, it is likely that research efforts will be focused on fully homomorphic encryption, differential privacy, machine common sense and device to device mesh networks. It is also likely that these trust enabling technologies along with the other technologies discussed in this report will enable the essential attributes of MPE 2037.

All these technologies are likely to mature by 2037. However, it is likely that unless the U.S. Army creates an organizational culture capable of overcoming distrust in new AI, the Army will not adopt capabilities centered on novel AI applications. If the organizational culture does not change in respect to AI and new technology adoption, operationalization of MPE 2037 is unlikely.

Table of Contents

Section 1: Decentralization

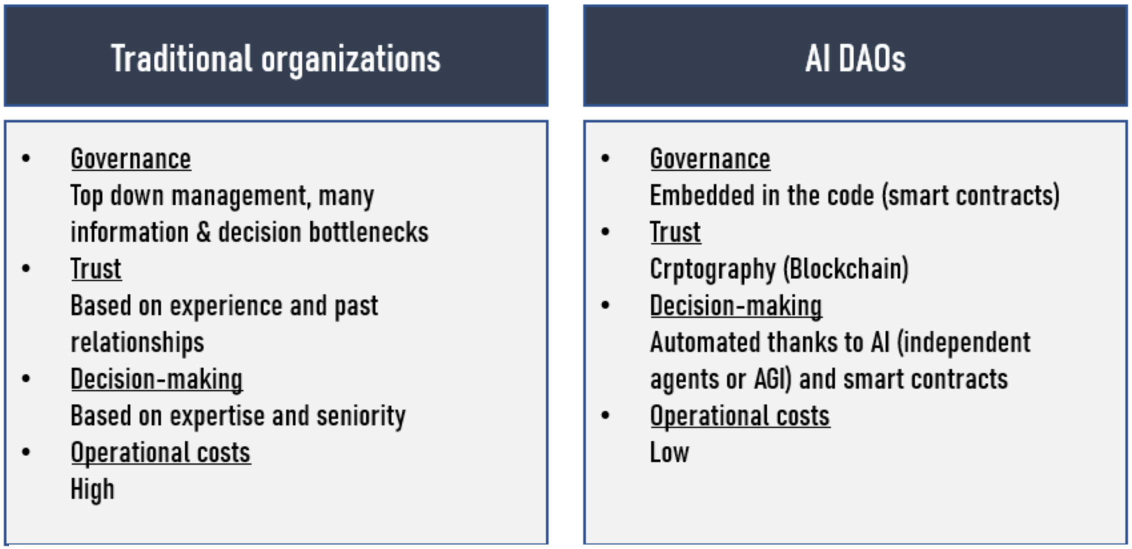
Decentralized Autonomous Organizations Highly Likely An Emerging Paradigm; Executed At Scale Across Multiple Industries By 2037

Executive Summary

Even though the concept of Distributed Autonomous Organizations (DAO) is very nascent, it is highly likely (71-85%) that the DAO model will be implemented at scale across multiple industrial sectors, to include government, by 2037. At its core, a DAO is a group of entities with common goals that join under a blockchain infrastructure that enforces a set of shared rules to achieve a shared goal. Private industry, primarily in the startup and cryptocurrency space, is working to make DAOs viable as a business model. The DAO paradigm has vast potential for almost every type of industry, including making government transactions more decentralized, efficient, and secure.

Discussion

DAOs are novel socio-technical systems that set a new way for online coordination and decision-making. [H] As shown in Figure 1, DAOs operate with a very different structure than traditional organizations. [M] Distributed Autonomous Organizations mediate interactions of members (human or machine) through blockchain applications. [H] The blockchain applications control interactions via a set of rules embedded in the source code. [H] Blockchain is a distributed ledger, a distributed append-only database with a synchronization mechanism. [H] Although most DAOs host blockchain projects or some



Traditional organizations	AI DAOs
• Governance Top down management, many information & decision bottlenecks	• Governance Embedded in the code (smart contracts)
• Trust Based on experience and past relationships	• Trust Crptography (Blockchain)
• Decision-making Based on expertise and seniority	• Decision-making Automated thanks to AI (independent agents or AGI) and smart contracts
• Operational costs High	• Operational costs Low

Figure 1. Traditional vs. DAO Organizations. Click on figure or go to https://towardsdatascience.com/why-building-an-ai-decentralized-autonomous-organization-ai-dao-85d018700e1a

sort of blockchain-based businesses, DAO as a service platform has reduced entry barriers for non-technical users and non-blockchain-related organizations. [H]

Started by a group of programmers in 2016, the first DAO of consequence was aptly named The DAO. At the time, it was the most successful investment crowdfunding effort, representing the cryptocurrency Ethereum. The DAO was essentially a hedge fund where contributors could directly vote on proposed projects. [H] However, due to a coding error, an attacker robbed a large portion of The DAO funds. [H] Despite this setback and risk, private industry has persisted in the effort to create decentralized organizations that operate in the blockchain. [H]

Contrary to popular belief, blockchain governance is often not autonomous, self-governed, or technologically enforced. [H] Governance represents the framework for decision rights, incentives, and accountabilities to encourage desirable behavior. [H] However, the networked nature of blockchain and DAOs makes governance difficult. [H] Regarding blockchain "on-chain" governance, an agreement is often best reached off-line." [H] Blockchain is beginning to blur the distinction between application and infrastructure. More research is required to develop effective governance structures [H] These issues signify that new governance models and mechanisms are likely (56-70%) required for effective adoption and implementation across industries. However, there is limited insight into the governance challenges that these models should address. [H]

Solidity is an object-oriented programming language created specifically by the Ethereum network team for constructing and designing smart contracts on Blockchain platforms. [M] Solidity addresses limitations of Bitcoin's scripting language, like the lack of Turing completeness. [H] Solidity has enabled multiple decentralized applications (Dapps) and the so-called "smart contracts," computational agreements between parties that may be self-executed and self-enforced. [H] A smart contract is a set of promises specified in a digital form, including protocols within which the parties perform on these promises. [H] As illustrated in Figure 2, blockchain provides an ideal platform for executing decentralized smart contracts. Roughly speaking, a smart contract is a piece of program that consists of a set of rules and corresponding operations of related accounts. [H] Smart contracts require an automated program to execute without manual intervention. [H] For a smart contract, if a set of events in the contract is triggered, it will be executed automatically by the decentralized system. [H]

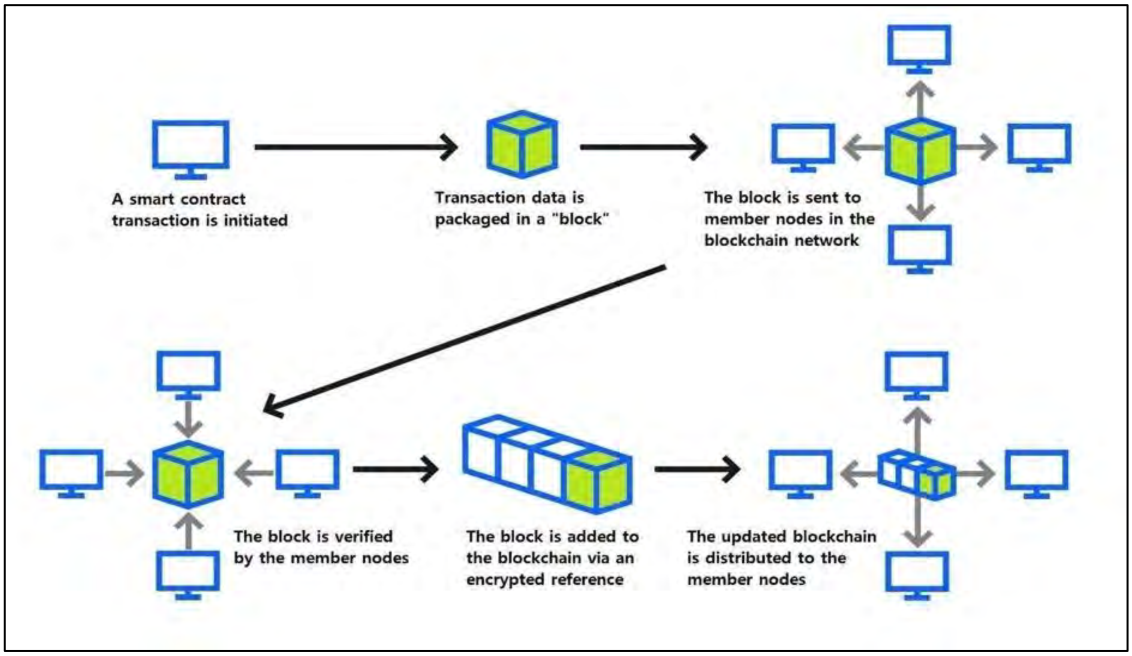

A smart contract transaction is initiated
Transaction data is packaged in a "block"
The block is sent to member nodes in the blockchain network
The block is verified by the member nodes
The block is added to the blockchain via an encrypted reference
The updated blockchain is distributed to the member nodes

Figure 2. How a smart contract transaction is incorporated into a blockchain. Click on figure or go to https://jipel.law.nyu.edu/vol-9-no-1-5-minn/

Compared to traditional forms of organization, DAO offers more security and stability because no one can control the entire organization. [M] Moreover, since DAO runs on decentralized blockchain technology, it can remain autonomous without interference from external factors. [M] In addition, better power distribution makes DAO fairer than traditional resource allocation and decision-making. These advantages have made DAO more and more popular and attracted attention. [M] An example of a successful DAO is Collab.Land. [M] Collab.Land is a discord bot that manages token gated channels and roles.

Collab.Land solves the problem of managing thousands of members with various roles and channel access. [M] These types of efficiencies are why startups are interested in the DAO paradigm. [M] DAO members are empowered to voice their opinion on resources allocation, enabling startups to compete with incumbents on a level playing field. [M] The unique structure and values of DAO complement that of startups, making them a viable option for companies that lack the resources to scale. [M]

A blockchain-based government DAO, appropriately implemented, could provide transparency, accountability, immutability, and, more importantly, better resource management. [H] This system reserves all records for auditing, thus limiting litigation between parties involved and increasing the speed of allocation and execution of smart contracts. As illustrated by Diallo et al, [H] and their description of a eGov DAO to better manage government contacts, the DAO model demonstrates the highly likely (71-85%) potential to help the government save resources, manage more efficiently, and reduce the security risk. [H]

Nevertheless, the DAO paradigm is an emerging field thus still in active development and open for broader research. Thus, it is still too early to assess if it will fulfill its decentralization promise. [H] Governance is a difficult issue and will require academic research and business use cases to determine the best model. With DAO's focus on decentralization, it may be challenging to pinpoint actions on people or companies, resulting in unclear accountabilities. [H] This lack of responsibility and accountability can be problematic in swift decision-making and execution of governance actions. [H] However, decentralized control and autonomy are the significant features of a DAO. [H] DAOs could be empowered to autonomously hire people, provide services, gain money for their aims, own smart property, coordinate with other autonomous software, or facilitate cooperation. [H]

Analytic Confidence

The analytic confidence for this estimate is moderate. However, the sources were very reliable and corroborated one another. There was adequate time, but the analyst worked alone and did not use a structured method. Many of the sources were peer-reviewed academic journal articles, industry websites, and respected periodicals. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Greg Pavlichko

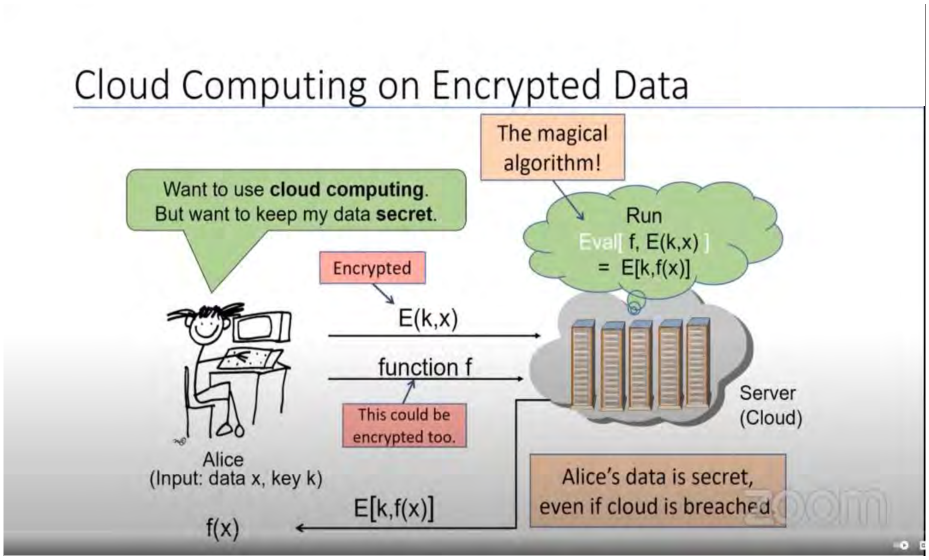
Fully Homomorphic Encryption Highly Likely To Be Computationally Efficient Enough For Use At Scale By U.S. Military By 2037

Executive Summary

Even though Full Homomorphic Encryption (FHE) is at this time a relatively nascent and slow cryptographic technique, by virtue of a logarithmic reduction of computational cost (time & computing power) to FHE operations over the past several years, as well as increased government interest and a concerted academic effort to develop protocol standards, it is highly likely (71-85%) that FHE will achieve sufficient computational efficiency to operate at scale in the next 15 years. FHE is a technique that enables analytics and machine learning (ML) on encrypted data sets without a need to decrypt the data sets. This cryptographic technique has widespread implications for many industries requiring data privacy and security. Efforts by private industry and DARPA to develop novel hardware solutions to support FHE make this technique viable in the next 15 years.

Discussion

Fully Homomorphic Encryption is a cryptographic protocol postulated by Dr. Craig Gentry in 2009. [H] Fully Homomorphic Encryption (FHE) is an encryption scheme that enables analytical functions to execute directly on encrypted data while yielding the same results as if the user executes the functions in plaintext. As Figure 1 illustrates [H], FHE enables an end-user to run calculations on encrypted data stored in the cloud without requiring the end-user ever to have unencrypted access to encrypted data sets. [H]



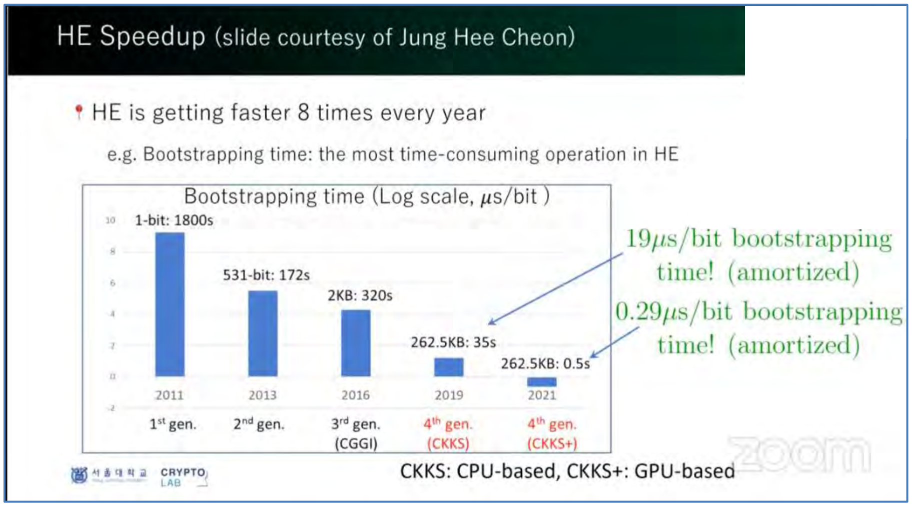
Cloud Computing on Encrypted Data

The magical algorithm!
Want to use **cloud computing**. But want to keep my data **secret**.
Run Eval[f, E(k,x)] = E[k,f(x)]
Encrypted
E(k,x)
function f
This could be encrypted too.
Server (Cloud)
Alice (Input: data x, key k)
Alice's data is secret, even if cloud is breached.
E[k,f(x)]
f(x)
zoom

Figure 3. Representation of FHE- A Decade or So of Fully Homomorphic Encryption. Click on Picture or go to https://www.youtube.com/watch?v=487AjvFW1lk&t=414s

The term homomorphic, meaning the same change, describes how the technique works. FHE cryptography makes the same computational changes in the ciphertext (encrypted data) and the plaintext (unencrypted data). [H]

The most significant drawback to implementing FHE is the computational cost. FHE is time and memory intensive, with basic computations taking hours or days. FHE relies on lattice cryptography, [H] which presents complex mathematical challenges to would-be attackers that require technologies beyond the current state of the art to solve. The challenge with modern lattice-based FHE is the unavoidable noise accumulation with each calculation performed. [H] Each homomorphic computation, generates a certain amount of error that corrupts the encrypted data representation. Once this noise accumulation reaches a certain point, recovering the original underlying plaintext becomes impossible. [H] Computational structures called "bootstrapping" help address this untenable noise accumulation, reducing it to a level that is comparable to the original plaintext but produces massive computational overhead to perform. [H] However, as indicated in Figure 2, [H] FHE is becoming eight times more computationally efficient every year. [H] In July of 2020, IBM conducted several field trials of FHE in the financial sector and demonstrated that FHE is becoming viable at scale. [M]


HE Speedup (slide courtesy of Jung Hee Cheon)

- HE is getting faster 8 times every year

e.g. Bootstrapping time: the most time-consuming operation in HE

CKKS: CPU-based, CKKS+: GPU-based

Figure 4. Logarithmic Increase in FHE Computational Efficiency- A Decade or So of Fully Homomorphic Encryption. Click on Picture or go to https://www.youtube.com/watch?v=487AjvFW1lk&t=414s

The United States government, specifically the Defense Advanced Research Agency (DARPA), has invested resources in further developing FHE to be efficient enough to use at scale. For example, the Data Protection in Virtual Environments (DPRIVE) program seeks to enable FHE computation within a factor of ten of unencrypted computations, enabling data security for all states of data across DoD and commercial applications. [H] To meet this challenge, DARPA is designing and implementing a hardware accelerator for FHE computations that significantly reduces the current computational burden to speed up FHE calculations drastically.

Before FHE is adopted in medical, health, financial, and other sectors to protect data, it will have to be standardized, most likely by multiple standardization bodies and government agencies. [H] An essential part of standardization is broad agreement on security levels for varying parameter sets. [H] Several FHE standardization workshops have occurred, involving government, industry, and academia. [H] There are also several research groups publishing FHE libraries for applications and general use. [H] These efforts are critical to coalescing and developing FHE standards for widespread implementation.

The biggest challenges to scaling FHE are the computational cost and the relative nascency of this innovation. The processing power and memory required to execute FHE calculations do not make this technique scalable for government use at this time. [H] However, DARPA has invested over $14M [H] dollars in researching and developing hardware with the required parameters to scale FHE. In addition, Dr. Gentry and other academic institutions are iteratively developing more efficient lattice algorithms and bootstrapping techniques. [H] These efforts indicate that FHE will mature over time and is highly likely (71-85%) to be scalable by 2037.

Analytic Confidence

The analytic confidence for this estimate is high. Sources were very reliable and corroborated one another. There was adequate time, but the analyst worked alone and did not use a structured method. Many of the sources were peer-reviewed academic journal articles, government .mil websites, and a video by the FHE developer. Given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Greg Pavlichko

Device To Device Solutions Will Highly Likely Make Possible Dynamic 6G And 7G Networks Within The Next Ten Years

Executive Summary

Device-to-device (D2D) solutions will highly likely (80-95%) enable future global deployment of 6G and 7G technologies over the next ten years despite resource and infrastructure limitations. Innovative research in streamlining network capabilities and shared access through multiple devices will highly likely expand wireless capabilities to remote locations.

Discussion

The expectation of future 6G and 7G platforms equates to high data transmission rates with low latency, which facilitates machine learning (ML), artificial intelligence (AI), edge computing, virtual reality (VR), and other capabilities. (see 6G and Beyond). Recent research and development (R&D) efforts in the alternative line of sight (LOS) network expansion capabilities will highly likely ensure the implementation of 6G by 2030. The challenge of maintaining high data rates at the edge or remote locations revolves around the distance the data travels. The use of D2D transmissions or dedicated short-range communications (DSRC) provides one solution to solving the issue of distance without the requirement of a standard network. [M] D2D proves that using other devices as cooperative networks or relays creates a dynamic nonstandard network. [M] (see Figure 1) Using D2D connections "can significantly improve network coverage and spectrum efficiency" and incorporating non-orthogonal multiple access (NOMA) with cooperative full-duplex relaying D2D improves the quality and throughput of connections. [MM] D2D connections are similar to the military's wireless concept of cyber foraging but on a commercial scale and without purposefully deploying additional nodes to extend the LOS. [M]

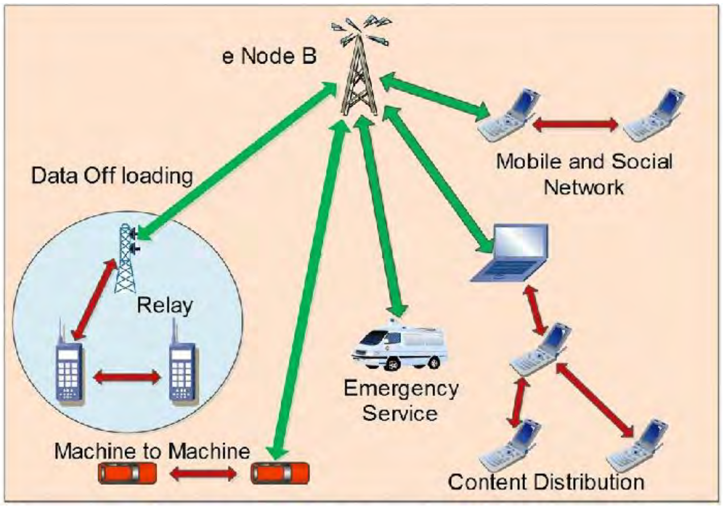


Figure 1. Illustration of device to device communication. [M]

Researchers from Georgia Tech are developing a flexible solution that is scalable, directional, and customizable. This device also accommodates different frequencies and power levels. The technology can be a smart case or set as a tile to adhere to any surface like an unmanned aerial vehicle. The tiles have an antenna array and support multiple-input multiple-output (MIMO) capabilities. They can act as relays by extending a network to the most remote areas while supporting the data-intensive internet of things and virtual reality. This smart tile provides a rapidly deployable solution at a low cost. M

Examination into millimeter wave (mmWave) (see Figure 2) frequencies prove a feasible application with satellite platforms in 6G and beyond communications. M This key enabler provides high-capacity satellite communications to support the increased traffic demands and service requirements. M To resolve the reduced distance of several hundred meters, the researchers proposed using "MIMO and advanced beamforming with very large scale antenna (VLSA)[1]." M

Figure 2. mmWave Communication Demo. Click on the picture or go to: https://youtu.be/sjYh6aNfbsQ to view the video.

Security against vulnerabilities is essential, but challenges always revolve between balancing risks against capabilities and efficiencies. Employing effective countermeasures against potential exploits will highly likely improve trust and confidence in using D2D technologies that will support 6G and beyond networks. Researchers successfully tested the effectiveness of using the Rivest-Shamir-Adleman (RSA)[2] encryption algorithm to secure D2D-aided multicast transmissions by pushing traffic through properly selected nodes that work as heads for D2D clusters. M According to Hailin Cao from Chongqing University, a method in securing satellites to integrated terrestrial networks is using an "intelligent reflecting surface

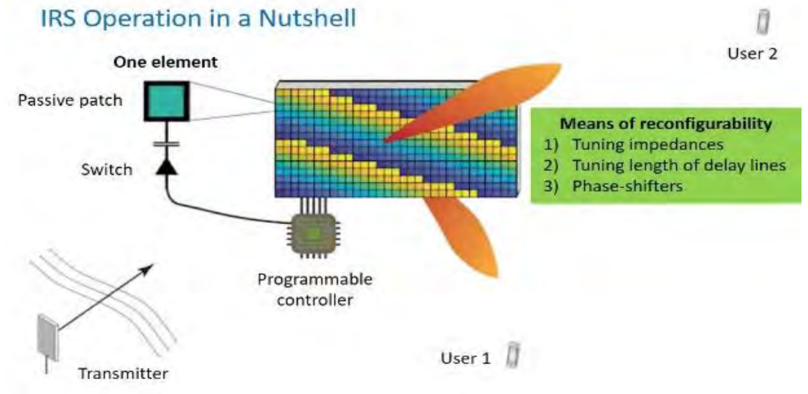


Figure 3. Fundamentals of Intelligence Reflecting Surfaces. Click on the picture, or go to: https://youtu.be/CDt0JNrOKxk to view the video. Source: University of Oulu

[1] Advanced beamforming with very large-scale antenna (VLSA) steers the beam to only the desired direction or user improving the transmission range.

[2] Rivest-Shamir-Adleman (RSA) is a public-key cryptosystem used for secure data transmission. Because it is a slow algorithm, it is not used to encrypt user data. If a large enough key is used, it is difficult to break the encryption.

(IRS[3])”. [M] (see Figure 3) Deploying an IRS near the satellite user to reflect the common-spectrum friendly interference protects the satellite downlink transmission from being eavesdropped.” This strategy minimalizes the signal-to-interference-plus-noise-ratio, ensuring reliable transmission between the terrestrial and satellite locations. [M]

Analytic Confidence

The analytic confidence for this estimate is moderate. Sources were technical and resourced from ongoing research, which corroborated one another. There was adequate time, and the task was not complex. Despite the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LTC Nicole Y. Shadley

[3] The intelligent reflecting surface (IRS) empowers secure cooperative transmission between satellite and terrestrial integrated networks.

Blockchain Tech, Such As Smart Contracts And Proof-Of-Stake Protocol, Will Likely Enable Data Sharing In Low Trust Environments Within The Next 5-10 Years

Executive Summary

Despite the requirement for large amounts of energy resources and resistance from traditional stakeholders that may delay the expanded use of blockchain tech, organizations will likely (55-80%) be able to use blockchain tech to address the challenges of data sharing in low trust environments within the next 5-10 years. The expanded use of blockchain tech will be due to the adoption of the proof-of-stake protocol and the use of smart contracts.

Discussion

The term blockchain tech is most closely associated with cryptocurrencies, such as Bitcoin or Ethereum (see Figure 1). However, organizations can use the same blockchain tech that enables cryptocurrency for other functions, such as management of patient Electronic Health Records (EHR). [H] Additionally, organizations could apply this same technology to address challenges associated with data sharing in other low trust environments, since many of the challenges are similar to managing EHR. [H]

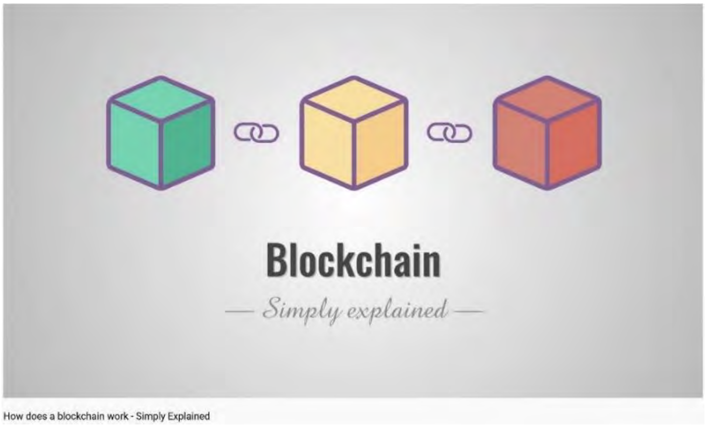


Figure 5. How does a blockchain work. Click on picture or go to: https://www.youtube.com/watch?v=SSo_EIwHSd4 to view video. Source: Simply Explained Channel on YouTube.

Organizations are already exploring Blockchain technology for use in the field of managing EHR. [M] An example is the MIT MedRec project. [H] One of the challenges associated with EHR management is that a single patient may have multiple records that are fragmented in siloed databases across multiple providers. [H] Sharing of EHR files can be impeded by nonstandard data formatting and low trust relationships among the various providers. [H] In this environment, the patient data is centrally managed by the provider, who controls access. Attempts by patients or other providers, such as medical specialists, to access the data can be difficult and time consuming. [H]

To address this challenge, organizations can use blockchain tech to create a private blockchain where only properly vetted entities, patients and providers, can participate in the blockchain. [H] In this example, patient EHR is not stored on the blockchain. Individual providers store the data in highly secured databases that they manage. [H] The participants use the blockchain to create an immutable distributed ledger that validates access to the EHR and records all access requests. [H] For routine EHR events, participants can establish smart contracts[4] that automatically regulate EHR access between individual participants or groups of participants. [H] The patient, the owner of the data, controls access to his/her EHR through the blockchain. The patient can audit the distributed ledger at any time to ensure only authorized entities have accessed his/her EHR. [H]

The U.S. telecom provider Verizon is also exploring the use of blockchain tech to improve transparency and customer trust in their news releases through their Full Transparency initiative. [M] As part of the initiative, Verizon will track all official news releases on a blockchain ledger, which will allow the public to validate that a Verizon press release is legitimate. [M]

One of the issues impacting wider adoption of blockchain tech is the large amount of energy required to execute the consensus mechanism that validates new blocks in the chain. [M] The Bitcoin blockchain uses a popular consensus mechanism called proof-of-work (POW), where miners compete to validate transactions and get rewarded. [M] A Cambridge Centre for Alternative Finance 2021 study estimated the energy required to validate Bitcoin transactions to be 143 terawatt hours, which if ranked against countries by energy use, Bitcoin transactions would be the 30th largest consumer of energy in the world. [M] To mitigate this challenge, organizations could use the existing and more energy efficient proof-of-stake (PoS) consensus mechanism, which uses approximately 90% less energy per transaction. [M]Rather than having multiple miners compete to validate transactions in a race to the finish, the PoS protocol allows miners to stake a small amount of cryptocurrency for a chance to validate a new block on the chain and an algorithm selects a single miner to validate the transaction. [M]

Another impediment to wider adoption of blockchain tech for managing EHR is traditional stakeholder resistance. As outlined in a 2015 Office of the National Coordinator for Health Information Technology (ONC) report, "market conditions create business incentives for some persons and entities to exercise control over electronic health information in ways that unreasonably limit its availability and use." [H] Since this same type of stakeholder resistance will impact an organizations ability to apply blockchain tech to other areas of data sharing in a low trust environment, it will likely take organizations 5-10 years to implement.

[4] A smart contract is a program that controls assets on the blockchain in ways that guarantee predictable behavior. [M]

Analytic Confidence

Analytic confidence in this estimate is moderate. The analyst had adequate time and the task was simple. However, while the reliability of sources on current blockchain tech were moderate to high, the sources related to the timelines for expanded application of blockchain technology were moderate. Although, multiple sources did tend to corroborate each other on the potential future applications of blockchain tech, no sources provided definitive timelines.

Author: COL Anthony Pollio

Advances In Edge Artificial Intelligence While Disconnected From The Cloud Likely To Speed Military Decision Making By 2030

Executive Summary

By 2030, technologically advanced militaries are likely (55-80%) to adapt private sector Edge AI innovations to improve military decision making by improving performance, optimizing, network traffic, and reducing latency. Despite current commitments to a cloud-based architecture, growing adversary interest in contesting the Electromagnetic Spectrum will push militaries to adopt data processing alternatives that provide localized, disconnected solutions.

Discussion

Edge AI is the combination of Edge Computing and Artificial Intelligence to process algorithms locally that enable independent decision making without connecting to the internet or a remote cloud-based server. [H] Edge computing moves data collection, analysis, and processing to the "edge" of the network where the user is located and edge computing brings computing power and data storage to where data is collected. [H] Similarly, Edge AI uses modern Artificial Intelligence capabilities to solve problems without reaching back to a cloud server for processing bringing advanced analytics, machine learning, and intelligent automation to improve decision making. [H]

By 2030, multiple technology companies are likely to incorporate Edge AI to improve performance, optimize network traffic, and reduce latency as 5G and 6G networks become operational (see Figure 1). [M] Verizon is testing data from weather drones on its 5G network with Mobile Edge Computing technology and AI. [M] Moving computing power to the edge of the network where the weather drones operate, "drastically limits

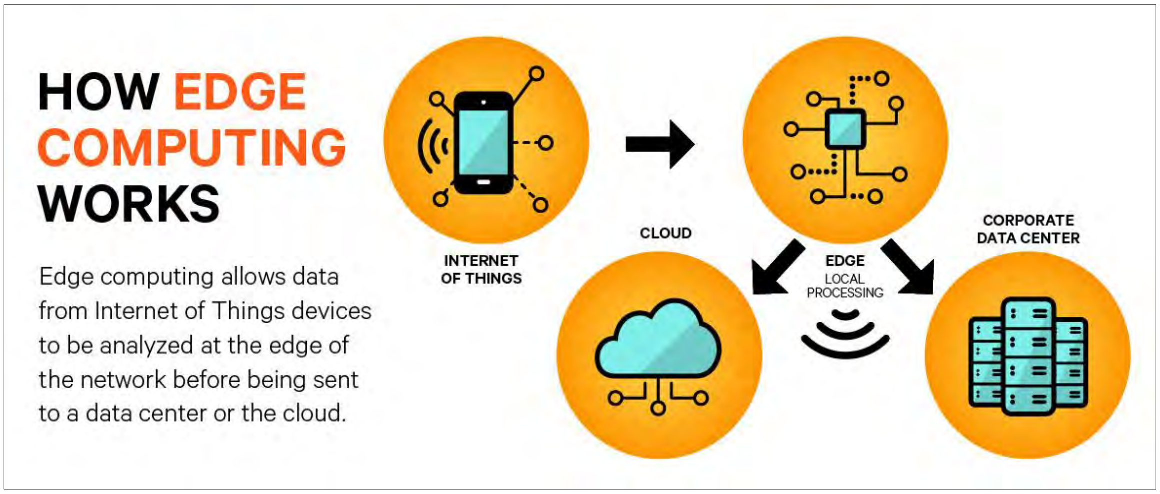

HOW EDGE COMPUTING WORKS
Edge computing allows data from Internet of Things devices to be analyzed at the edge of the network before being sent to a data center or the cloud.
INTERNET OF THINGS
CLOUD
EDGE
LOCAL PROCESSING
CORPORATE DATA CENTER

Figure 1. How Edge Computing Works

latency and makes ambitious applications possible." [M]

Some advanced militaries have already started adapting edge AI technology to support military operations. The Israeli Defense Force (IDF) likely already tested some Edge AI capabilities in the last Gaza clashes, and boasted of waging the "first AI war." [H] The IDF has already begun initial testing of "edge-data architecture" that moves beyond the cloud to forward units to speed data processing and decision making. [H] It is unclear, however, how successful these tests were.

Edge AI adaption for military purposes will have to overcome several challenges, however. In addition to significant latency concerns, current Edge AI computer, memory, and power requirements are too large for deployment in field conditions. [M] Compounding this problem, Edge AI for military application will need the capacity to leverage machine learning to "stitch" multiple inputs in near-real-time to inform decision making. [M]

And even advanced militaries still lag technology companies. Last year, a senior officer from the United Kingdom stated that the commercial industry has surpassed the military's capabilities in Edge Computing and Edge AI noting that, "a processor on a self-driving car has 800 times the power of the most advanced military processor." [H] In September 2021, the U.K. made Edge Computing and AI top priorities for their Strategic Command. [H]

Tesla's Edge AI technology may point to initial solutions to achieve stitching from multiple sensors. Autonomous driving vehicles incorporate significant amounts of Edge AI technology and Tesla is using a single giant neural network known as a "transformer" in each vehicle to receive input from eight cameras simultaneously. [H] Another AI technology with promise for use at the edge in coalition warfighting is GPT-3, which has recently been adapted to function across multiple languages. [H] Machines are beginning to understand differences between languages and have even applied some cultural understanding. [M] For example, a question on the "best" sports team delivered different reasonable answers that differed depending on whether the question was presented in English, German, or French. [M] Apple and Microsoft are also planning to add more AI capabilities to their network edges in an attempt to reduce latency introduced by cloud-based AI and improve security by reducing data movement. [H] As latency and security are major concerns during military operations, similar Edge AI capabilities would likely be adapted for military use.

Some of the expected shifts from cloud-based AI to Edge AI may be representative of no more than an observable cycle in computing. An AI writer at Forbes argues that computing technology has swung between centralization and decentralization many times, and that Edge AI is the latest pendulum swing. [M] If the Forbes writes is correct, militaries are still likely to rely on Edge AI at the forward edge of a battlefield where low-latency and security are primary requirements.

Analytic Confidence

This is a moderate confidence estimate. The reliability of sources is high, information and assessments from multiple sources were consistent, however, theoretical predictions varied and much of the technology remains unproven. And very few sources made predictions on timing for development or adoption of Edge AI capabilities.

Author: LTC Patrick Hofmann

Zero-Trust Security Will Highly Likely Bridge The "Trust Gap" Of Information Sharing By 2035

Executive Summary

Despite implementation costs and maintenance requirements, Zero-Trust (ZT) security is highly likely (80-95%) to be adopted internationally by 2035 due to its flexibility and scalability, the ability for phased implementation, and vendor neutrality. ZT security methodology will highly likely reduce the "trust gap" between entities to enable information sharing.

Discussion

Zero Trust security framework follows a principle of "never trust, always verify." Although John Kindervag[5] of Forrester Research developed this concept in 2011, adoption of the principle had been minimal. [M] This vendor-neutral methodology requires all users, "to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data." [H] Several counties and large corporations are already implementing and using ZT security methodology to secure and safeguard their data. [M] The White House was the first to publish an Executive Order to improve the nation's Cybersecurity posture by adopting

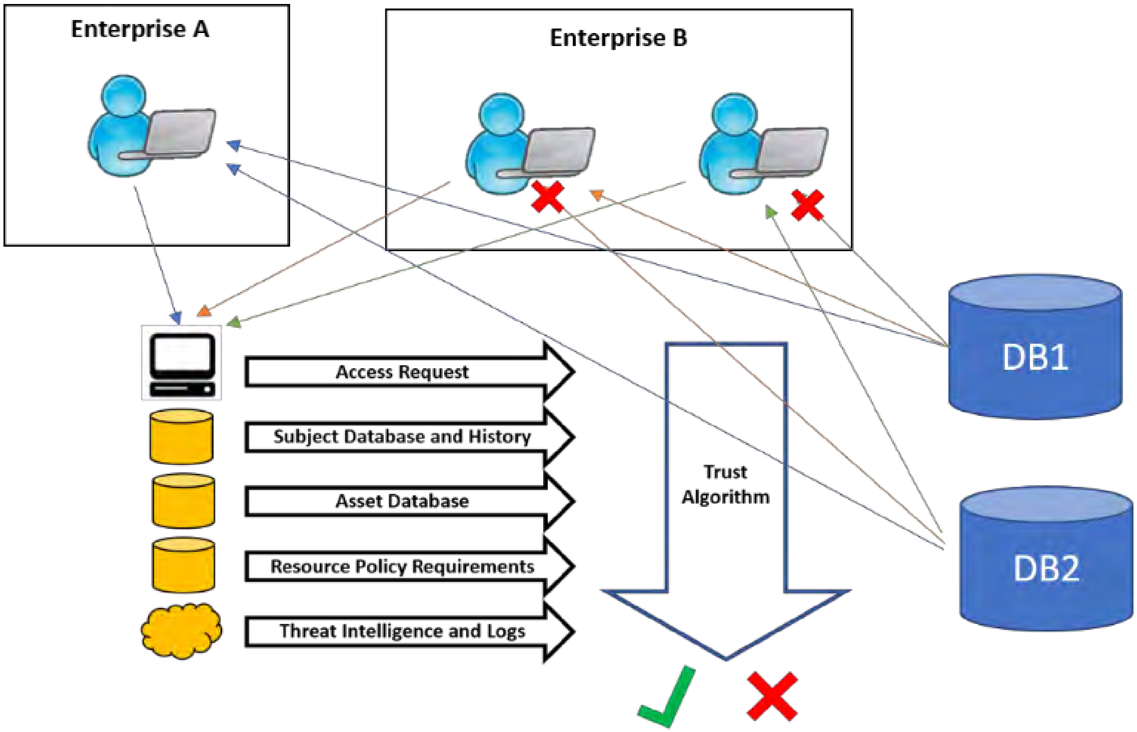

Enterprise A
Enterprise B
Access Request
Subject Database and History
Asset Database
Resource Policy Requirements
Threat Intelligence and Logs
Trust Algorithm
DB1
DB2

Figure 1. Consolidated representation of the ZT algorithm in a cross-enterprise collaborative environment. Click on the picture or go to: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf for additional details. Source: NIST Special Publication 800-217

[5] Field Chief Technology Officer of Palo Alto Networks

ZT architecture. [H] 50% of Australian and New Zealand industries already have ZT projects underway, with 18% across Europe and the Middle East. [M]
COVID-19 forced industry and government organizations to shift to remote or hybrid operations, increasing vulnerabilities to security threats and attacks. [M] Because ZT methodology is not a pre-packaged solution and has a phased approach, organizations are highly likely to invest, innovate, and adopt the security posture. [M] ZT methodology (see Figure 1) is an enhanced security system that can reduce the cyber "trust gap" in data management and privacy through the protection of access endpoints, identities, and other threat vectors. [M] For example, Microsoft Azure, Ivanti's Zero Sign-on, OneLogin Workforce Identity, and Thales SafeNet Trusted Access already have passwordless authentication services to prevent the theft of privileged access credentials. [H] ZT methodology will highly likely be easier to as more vendors develop solutions and options helping to bridge the "trust gap" [H]

The critical importance of implementing and significant benefits of ZT methodology is widely accepted at the top levels of industry and government because data and accesses are partitioned until the appropriate credentials are verified. Depending on backend resources supporting the architecture, ZT can slow the network down, but the risk and costs of a data breach (see Figure 2 and Data-Sharing Mindset) almost certainly outweigh the lag in pulling data. The current challenge revolves around qualified vendors with complete solutions and the lack of trained personnel to build and implement the enhanced security strategy. [M] Public-private partnerships are modernizing and creating dynamic ZT solutions to help overcome scalability, flexibility, and continuity issues. These efforts can resolve talent management concerns within the next 5-10 years. [H] ZT solutions will highly likely be accepted worldwide as more organizations accept the importance of ZT security and invest in advancing technology.

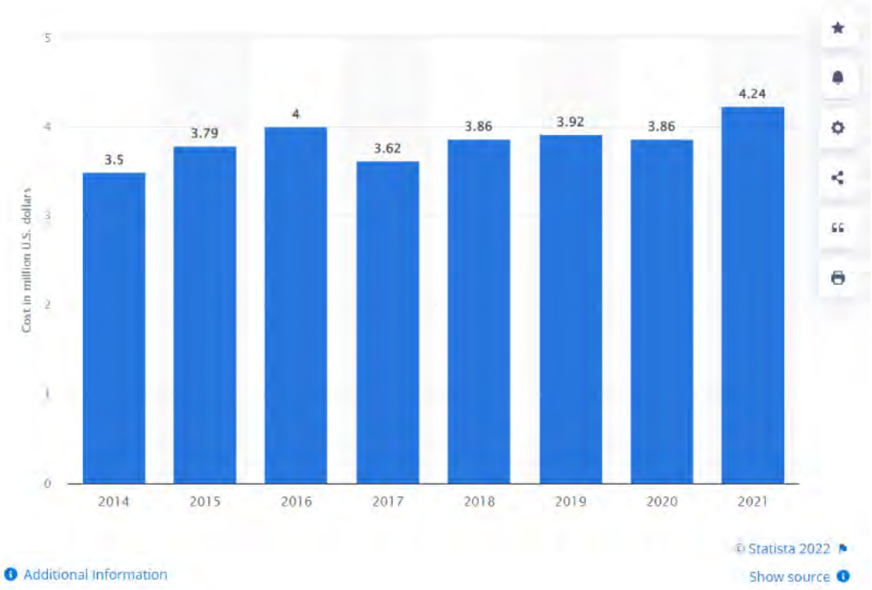


Figure 2. Average costs of data breaches worldwide from 2014 to 2021. Click on the picture or go to: https://www.statista.com/statistics/987474/global-average-cost-data-breach/. Source: Statista

Implementing and maintaining a ZT security environment is likely to face both technical and non-technical challenges. Gary Kinghorn, the Nozomi senior director, stated, “The strategy published today rightly acknowledges that moving toward a zero-trust model is a significant disruption… there is no easy way to just bolt on zero-trust. It will take a lot of work and funding to get there...” H Despite this potential pushback and some countries’ due to minimal emphasis and resourcing of funding and skillsets, industries and countries will need to adopt a ZT methodology to protect against data breaches. Within the U.S. both private and government sectors face severe cybersecurity workforce gaps. The federal government’s IT workforce is aging. In 2020, 15.7% of the IT workforce was over the age of 60, and only 3.2% were under the age of 30. H Building a robust and trained workforce with the technical background needed to protect against emerging cyber threats could take 15 years. A recent independent study conducted by Forrester Consulting reflected more than 75% of security strategy decision-makers emphasized the importance of ZT to combat increasing security threats, 60% are turning to ZT and micro-segmentation[6], and 78% plan to include ZT security operations in the coming year. M PJ Kirner, CTO and co-founder of Illumio, commented, “As we watch threats evolve and breaches become more devastating, the need to implement Zero Trust strategies has never been more urgent…the path to a Zero Trust posture can be broken into bite-sized phases…This incremental approach is a journey that bolsters your security posture to reduce risk and increase cyber resiliency.” H

Analytic Confidence

The analytic confidence for this estimate is moderate. Sources were reliable and tended to corroborate one another. There was adequate time, and the task was not complex. Despite the lengthy time frame of the estimate, this report is not sensitive to change due to new information.

Author: LTC Nicole Y. Shadley

[6] Micro-segmentation is a network security technique that enables security architects to logically divide the data center into distinct security segments down to the individual workload level, and then define security controls and deliver services for each unique segment.

6G and 7G Networks Will Highly Likely Merge The Digital And Physical Worlds Improving Real-Time Analysis By 2035

Executive Summary

The establishment of 6G networks and the research and development (R&D) of 7G capabilities is almost certain (95-99%) to be implemented by 2035 and will highly likely (80-95%) become the conduit supporting the interaction between digital and physical worlds despite the infrastructure upgrade requirements. Terahertz bits per second network capacity enables mass amounts of data to travel in real-time from the sensor to the analyst thus providing enriched analysis and intelligence.

Discussion

Research reveals that generational leaps in mobile technology occur every nine to ten-year cycles. Thus full 6G rollout is almost certain to occur between 2030 and 2035. [MM] To meet the generational timeline, research and development efforts have begun shifting towards future 6G and 7G capabilities. [M] Huawei projects 6G speeds of 8,000,000 megabits per second, equal to downloading 142 hours of high-quality Netflix videos every second. The increase in data rate speeds from 6G will highly likely change how people interact with technology. [M] The digital and physical worlds merge with increased capability and capacity of the network and through the deployment of sensors to capture real-time activities. [M] 6G speeds will boost the ability to support artificial intelligence (AI), more immersive virtual reality (VR) applications, blockchain, [M] high-fidelity mobile holograms, and potential wearable devices and micro-devices mounted on the human body which has many applications. [H]

Figure 6 6G vision for 2030. Click on the picture or go to: https://youtu.be/T6ubRoZCeVw to view the video. Source: University of Oulu

More countries and businesses are shifting focus to 6G. This prioritization and resourcing of 6G technology most likely ensures full implementation by 2035. Erick Ekudden, Ericsson's Chief Technology Officer, and Huawei founder Ren Zhenfei estimate that early commercial deployment of 6G will occur in 2028 and 2029. [M] However, India's new Minister for Communication, Ashwini Vaishnaw, stated, "6G development has already started. That will be seen somewhere in the time frame 2024 or 2023-end." [M] Vietnam [M] and Spain, [M] have shifted priorities and begun investment into 6G research. Two Chinese technology companies have started R&D into 6G. Huawei confirmed collaborative research with Canadian university researchers, and Purple Mountain Laboratories, China Mobile, and Fudan University are also exploring next-generation wireless. [M] Two technology alliances have formed to advance 6G technology. ATIS Next G Alliance [M] is the North American advancement toward 6G and beyond. Next, Generation Mobile Networks (NGMN) Alliance [M] is the other alliance that comprises T-Mobile, China Mobile, Vodafone, and Canada's Bell.

Future innovations and technological advancements need increased speeds, capacity, and capability that both 6G and 7G networks can provide. Artificial intelligence, machine-learning algorithms, cloud services, [M] artificial general intelligence, mind-reading, deep learning, big data analytics, and quantum computing require higher network capacity with low latency. [M] (see figure 2) Cisco's R&D have already begun paving the way to support faster speeds and traffic demands with their Silicon One ASIC chip and the 8201 routers. They have shown "35 percent more bandwidth and 26x less power draw in a smaller, lighter, and low-cost package." [H] Purple Mountain Laboratories has reported wireless transmission speeds of 206.25Gbps in a lab environment, but many countries are researching and developing technologies and submitting patents to deliver 6G. "China is responsible for 40.3 percent of global 6G patent filings, followed by the U.S. with 35.2 percent. Japan with 9.9 percent, Europe with 8.9 percent, and South Korea with 4.2 percent, according to a recent report by Nikkei." [M]

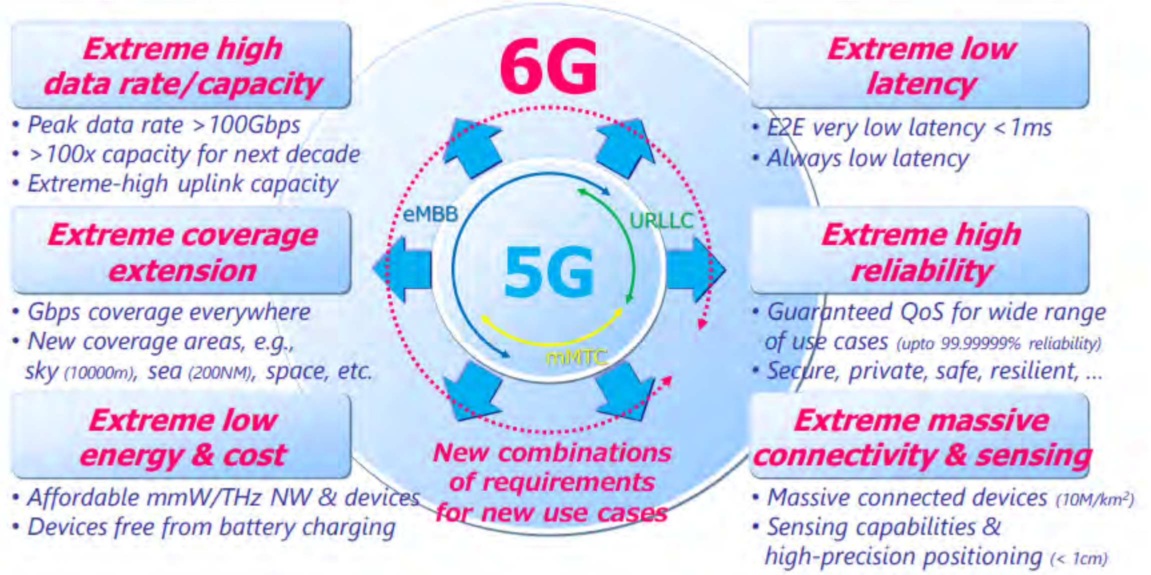

6G
5G
eMBB
URLLC
mMTC
Extreme high data rate/capacity
• Peak data rate >100Gbps
• >100x capacity for next decade
• Extreme-high uplink capacity
Extreme coverage extension
• Gbps coverage everywhere
• New coverage areas, e.g., sky (10000m), sea (200NM), space, etc.
Extreme low energy & cost
• Affordable mmW/THz NW & devices
• Devices free from battery charging
Extreme low latency
• E2E very low latency <1ms
• Always low latency
Extreme high reliability
• Guaranteed QoS for wide range of use cases (upto 99.99999% reliability)
• Secure, private, safe, resilient, ...
Extreme massive connectivity & sensing
• Massive connected devices (10M/km²)
• Sensing capabilities & high-precision positioning (< 1cm)
New combinations of requirements for new use cases

Figure 2 Requirements for 6G wireless technology Click on the picture or go to: https://www.docomo.ne.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_v4.0.pdf for additional information. Source: NTT DOCOMO

6G is estimated to be available as early as 2028 with commercial availability by 2030 and 7G around 2040. [M] The greatest determining factors that dictates the roll out speed of 6G and 7G architecture will be supportable line of sight, development of AI, edge and core computing, and microchips that can support the higher throughput data rates. [M] The U.S. President and Japanese Prime Minister entered into a joint agreement in April 2021 to invest $4.5 billion for the development of 6G and beyond technologies. [M] Partnerships with like-minded countries can open the door for cross pollination of military to industry innovation through organizations like Futures Command.

Although the focus is shifting from 5G to 6G and 7G development, technological advancements have significant hurdles for researchers. Dr Shirvanimoghaddam, an expert in wireless technology at the University of Sydney, stated that 6G would need significant improvements in "material science, computing architecture, chip design, and energy use." [M] Additionally, developments are needed in antenna and duplexing technologies; AI, edge, and cloud computing; and spectrum sharing. This new service is projected to boost global growth and productivity. However, it must remain affordable and efficient to meet the United Nation's Sustainable Goals by 2030. [M] Brave Research Project (see Figure 3) identified the spectrum between 90GHz and 300GHz, which is between millimeter-wave and infrared that offers opportunities for huge bandwidths required to increase data rates and network capacities beyond 5G performance enable achievement of the 1-terahertz bits per second (Tbps) wireless communication. [M] Terahertz and sub-terahertz frequencies are anticipated for 6G and 7G data rates which creates challenges with commercial viability and terahertz communications will be limited to "line of sight" [H] However, developments in low earth orbit and middle earth orbit satellites may enable connections anywhere and everywhere. [M] So, resolving these challenges will highly likely ensure broad deployment of 6G networks while creating a platform for 7G research.

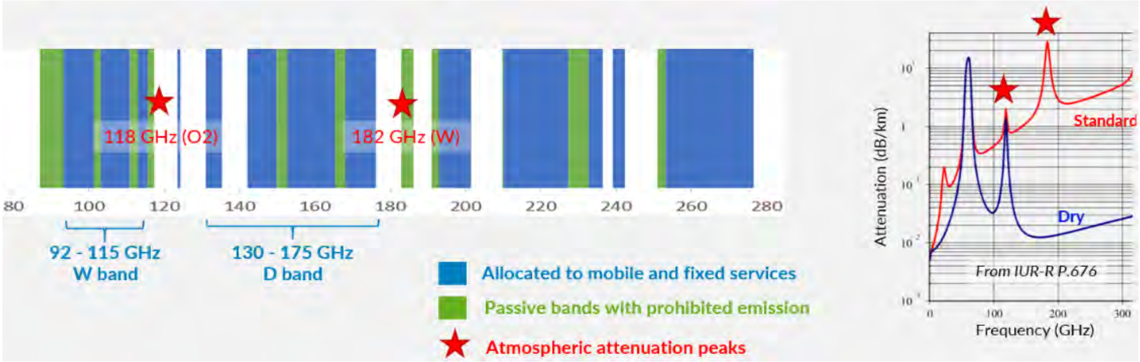


Figure 3 The frequency bands allocated to the fixed and mobile services in the range 90-275 GHz. Click on the picture or go to: http://www.brave-beyond5g.com/index.php/sub-thz/ for additional information. Source: Brave Research Project

Analytic Confidence

The analytic confidence for this estimate is moderate. Sources were reliable and tended to corroborate one another. There was adequate time, and the task was not complex. Despite the lengthy time frame of the estimate, this report is not sensitive to change due to new information.

Author: LTC Nicole Y. Shadley

Initial Fielding Of Quantum Computing Sensor To Decision-Maker Communication Capability Highly Likely By 2037

Executive Summary

Despite the challenges of stabilizing quantum bits (Qubits) quality, scalability, and cost, it is highly likely (71-85%) several large enterprise multi-trans-national companies and state competitors will begin initial trial fielding of secure sensor to decision-maker communication capabilities between 2032-2037.

Due to recent extensive quantum computing developments, China's quantum computing momentum, and quantum computing's discernable magnitude of impact on current information security protocols, the U.S. will highly likely intensify the race toward quantum supremacy.

Discussion

Quantum Computing is rapidly advancing from a scientific concept to a tangible technology actuality, with companies like Microsoft announcing in 2021 the launch of its cloud-based platform which will allow anyone to use quantum hardware tools called Azure Quantum, which boasts "some of the most compelling and diverse quantum resources available." [H] Quantum computers surpass the world's fastest supercomputers and solve complicated problems with tremendous speed [H] with case studies in optimization, [M] chemistry (specifically within energy and utilities),[M] financial services, [M] and logistics. [M]

Figure 7. Members of the IBM Quantum team at work investigating how to control increasingly large systems of qubits for long enough, and with few enough errors, to run the complex calculations required by future quantum applications. Click on picture or go to: https://research.ibm.com/blog/ibm-quantum-roadmap.Source: IBM.com

Quantum computers do this by substituting the binary "bits" of classical computing with something called "qubits," [H] which are the fundamental building block of a quantum computer.

In contrast to the benefits to physics, engineering, enhancing generative datasets for training machine learning algorithms and decrypting data secured with public-key encryption, [H] quantum computing is a complex feat wrought with challenges. [M] Notably, stabilizing qubit quality, scalability, and costs present commercial and government deployment hurdles. [H] Recent research advances address these hurdles (e.g. stabilizing qubit quality, scalability and cost).[H] Qubits are fragile and susceptible to error. [H] Quantum systems are difficult to make because noise and other environmental factors which diminish performance affects qubit stability. [M] Most quantum computers have to be kept to near absolute zero temperatures (0 Kelvin or -459.67 Farenheit). [H]

Present-day, state-of-the-art quantum computers typically suffer roughly one error every 1,000 operations. [H] To account for this error rate, the current approach is to add more and more qubits to reduce the margin of error. Hence, a key milestone to obtain quantum primacy is a 1,000 qubit quantum computer. [M] Many companies are focusing energy and research to achieve this. For example, IBM's roadmap for scaling quantum technology projects increasingly larger and better chips, with a 1,000-qubit chip, IBM Quantum Condor, targeted for the end of 2023 (see Figure 1). Google is investing heavily into error correction to mitigate the requirement for exponentially more qubits, which will increase potential for scalability and reduce costs. [M]

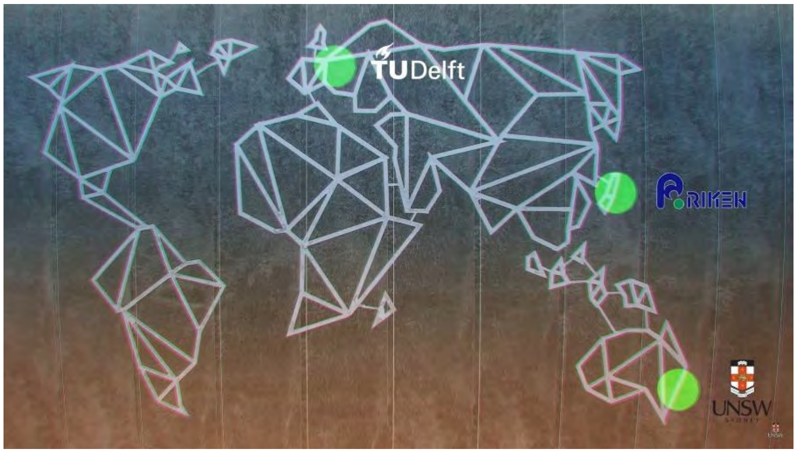


Figure 2. Quantum operations with better than 99% fidelity were also demonstrated in three similar experiments at UNSW, TU Delft and RIKEN, signaling the global maturity of quantum information processing in silicon. Click on picture or go video https://youtu.be/bjLUhg5mKic. Source: ScienceDaily.com

Building fault-tolerant computers above 99% marks a significant breakthrough in quantum computing. [H] Three independent university research programs recently achieved fidelity in quantum computing operations, achieving fault tolerance of less than 1%[7] using silicon embedded with phosphorus atoms via ion implantation, a method used in producing all existing silicon computer chips, [M] allowing their quantum breakthrough to be "compatible with the broader semiconductor industry." (see Figure 2) This demonstrated performance now makes it suitable for scaling up to practical applications. [H]

MIT researchers successfully reduce the size of the qubits in a way that reduces the interference that occurs between neighboring qubits. Addressing both qubit

[7] Delft University of Technology (Netherlands) achieved 1-qubit and 2-qubit fidelities of 99.87 percent and 99.65 percent, respectively.[H] RIKEN (Japan) achieved 1-qubit and 2-qubit fidelities of 99.84 percent and 99.51 percent, respectively.[H] University of New South Wales (UNSW) achieved a 1-qubit operation fidelity of up to 99.95 percent and a 2-qubit fidelity of 99.37 percent.[H]

miniaturization and quality, the MIT team increased the number of superconducting qubits on a device by a factor of 100. [M]

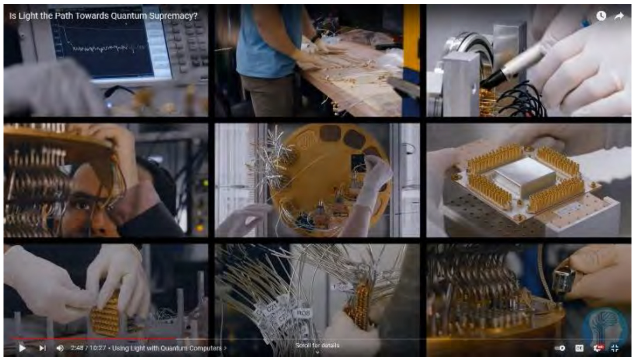
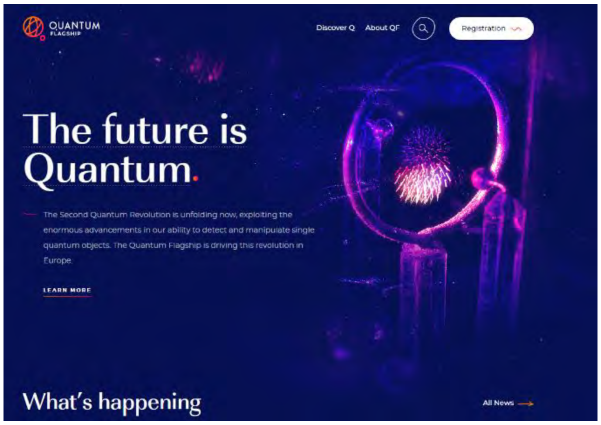

Is Light the Path Towards Quantum Supremacy?
2:48 / 10:27 • Using Light with Quantum Computers >
Scroll for details

Figure 3. Scientists have found a way of using Light/Photonics to massively speed up Quantum Computers on their path to reaching Quantum Supremacy. Click on picture or go video https://youtu.be/ET6gjOXxYsk. Source: AI News

China has made tremendous gains by developing a quantum computer made from photons—particles of light—that has outperformed the world's fastest classical supercomputers. [H] Unlike a traditional computer built from silicon processors, is an elaborate tabletop setup of lasers, mirrors, prisms, and photon detectors. In early 2022, U.S. Department of Energy's (DOE) Argonne National Laboratory and the University of Chicago read out their qubit on demand and then kept the quantum state intact for over five seconds – a new record for this class of devices. [H]

Recent progress in nonlinear optical materials and micro-resonators has brought quantum computing at room temperature into the realm of possibility. Scientists from the National University of Science and Technology MISIS (Russia) and Linköping University (Sweden) together with colleagues from Hungary and U.S. found a way to manufacture stable semiconductor qubits using silicon carbide (SiC). [M] Though a nascent capability, qubits that operate at room temperature, in contrast to the majority of existing analogues, opens up new prospects for creating a quantum scalable computers, ultra-secure communication tunnels, and new quantum internet technologies.

Venture capital funding grew by 500% from 2015 to 2020. [M] In conjunction with private-public funding, Canada based company D-Wave is investing over $400 million in R&D. [L] In 2018, the U.S. signed into law a bill initiating the National Quantum Initiative providing an initial inject of $1.2 billion to fund activities promoting quantum information science over a five-year period. [H] The National Institute of Standards and Technology (NIST), the National Science Foundation (NSF), and the Department of Energy (DOE) are collaborating to develop quantum computing projects as part of this initiative. [H] Also, in 2018, Germany's federal government announced a quantum initiative worth €650 million. [L]



The future is Quantum.

The Second Quantum Revolution is unfolding now, exploiting the enormous advancements in our ability to detect and manipulate single quantum objects. The Quantum Flagship is driving this revolution in Europe.

What's happening

Figure 4. EU race toward Quantum Supremacy. The Quantum Flagship is one of the most ambitious long-term research and innovation initiatives of the European Commission Click on picture to learn more go to https://qt.eu Source: EU Quantum Flagship

With initial funding of $10 billion, China is building a National Laboratory of Quantum Information Sciences. [M] The Australian Strategic Policy Institute recommends that the Australian government immediately lay the groundwork for a $3-4 billion [H] investment in quantum technologies.

The European Union's Quantum Flagship [H] also launched in 2018 with an initial budget of €1 billion.(see Figure 4) With a preliminary 10 year duration, the flagship brings together research institutions, academia, industry, enterprises, and policymakers, in a joint and collaborative initiative that seeks to achieve quantum advancements at an unprecedented scale.

Quantum computing is proving effective in sensor-to-decision making, with open computing challenges, such as IBM Grover's algorithm-based design game, where participants using quantum random access memory (qRAM) to learn about implementing complex quantum data structures, [M] demonstrate the combination could solve real-life, complex decision-making problems. Additionally, aviation manufacturers like Airbus are initiated a quantum computing challenge [H] to solve complicated problems in the aviation industry to reduce time taken for processing mathematical problems during the design phase of an aircraft. With quantum computers, reduced processing time up to 4 times was observed. [M]

Analytic Confidence

Analytical confidence in this estimate is moderate. The analyst had adequate time to initially assess, however, quantum technologies are complex and volatile. The sources available on this topic are generally reliable and tended to corroborate on another. The open sources available did tend to present scientifically quantifiable theories, with academic research validating complexities, yet forward thinking narratives by private companies toward success may be biased and shield proprietary information. The analyst collaboration was strong. Furthermore, given the rapidly evolving field, this report is subject to change due to new information.

Author: COL Troy Alexander

Decentralized, Self-Sovereign Identity Systems Highly Likely To Increase Secure, Private Information Sharing Capability For Use At Scale Within 5-10 years

Executive Summary

It is highly likely (71-85%) that Decentralized, Self-Sovereign Identity (DID/SSI)[8] systems will achieve sufficient industry and policy efficiency to operate at scale in the next 5-10 years. DID/SSI provides a means for digital identification without reliance on any external authority, enabling entities to control their identity and data flow during digital interactions while enhancing security and privacy. Despite the challenges of establishing an overarching governance framework for its operation, the market drive to protect privacy is pushing user, industry and government institutions toward advancing a decentralized identity, self-sovereign identity (DID/SSI) systems both for private and public use. DDI/SSI is currently an emerging, unstructured field of research, however, numerous efforts by private industry, public institutions and consortiums such as the World-Wide Web (W3) Decentralized Identifier Working Group, make this technique viable by 2037.

Discussion

Figure 8. The Benefits of Decentralized Identity for your Organization. Click on picture or go to: https://youtu.be/35jP81hxV4Y to view video. Source: MATTR channel on YouTube.

Decentralized identity is frequently used interchangeably and in conjunction with "self-sovereign identity." [M] While there are numerous emergent standards that enable self-sovereign identity (SSI), decentralized identifiers (DID) standards are widely evolving to ensure interoperability. DID/SSI help protect privacy and keep personal data more secure while granting individuals and organizations a platform to own and control digital identity while maintaining privacy. Hence, both individuals and organizations limit risk, can seamlessly audit data, and check clearance credentials to remotely provide access to information. [H] (see Figure 1).

[8] Note, though interchangeable for this document, there are slight nuances between decentralized identity and self-sovereign identity concepts.[M]

a. DIDs are completely under the authority of the user. There is NO central registry, identity provider or certificate authority that gives the receiving entity a "thumbs up" on the validity of the data.

b. SSI is an identity concept where people and businesses store and control their data on their own devices; providing this data when someone needs to validate them. This is all done without relying on a centralized database.

According to the World Wide Web Consortium (W3C), DIDs are a nascent type of identifiers that enables verifiable, decentralized digital identity. [H] A DID refers to any subject (e.g., a person, organization, thing, data model, abstract entity, etc.) as determined by the controller of the DID.

Distinguishable from mainstream, federated identifiers, DIDs are deliberately designed so that they can be separated from centralized registries, identity providers, and certificate authorities. [M] DIDs are categorized into public and private DIDs. [L] Public DIDs are typically suitable when users seek to be publicly identifiable while maintaining credentialled privacy, such as passport management or licensures. [M] Private DIDs creating a protected channel between two or more entities that is inaccessible to others and allows creation of distinct DIDs for diverse relationships for avoiding data correlation. [M]

Digital Identity You Own & Control
A new form of DIGITAL IDENTITY
Present & Verify
Everyday, we carry wallets full of CARDS
No digital equivalent
404 ERROR PAGE NOT FOUND
MY DIGITAL ID
Her new DIGITAL WALLET APP
TRUSTWORTHY
Leverages PROVEN CRYPTOGRAPHIC SYSTEMS
Issue standards-based credentials
Websites and apps can check that they're valid
20% FOR STUDENTS
friction free
Yeah, she's with us!
CONTACT ME!
Identifiers and our personal information
We need digital identifiers that individuals can own independently
Expressing
Exchanging
Verifying
Digitally present & authenticate a set of verifiable credentials
Just like a physical card
DIGITAL CARDS ARE PRIVATE
Easier to STAY IN CONTROL
Unlock a more TRUSTWORTHY INTERNET
Respect privacy for ALL OF US

Figure 2. The Benefits of Decentralized Identity for your Organization. Click on picture or go to: <u>https://youtu.be/Ew-_F-OtDFI</u> to view video. Source: Microsoft Security channel on YouTube.

A decentralized identity approach helps people, organizations, and things interact with each other transparently and securely, in an identity trust fabric. (see Figure 2) People control their own digital identity and credentials. [H] DID/SSI rely on multi-source identification (MSI) processes.

MSI processes are decentralized systems that permit multiple credentials from numerous providers to be brought to bear in a dynamic, scalable manner where trusted authorizations are required for participants in an information workflow. [H] In MSI, there are three players: credential issuers, credential holders, and credential verifiers. [H] Any person or organization can play any or all of the roles. Credential issuers set which credentials are issued, what each credential means, and validate credentialed information input. [H] Credential holders determine what credentials are needed and which to employ in a workflow to prove things about themselves. [H] Credential verifiers determine what credentials to accept and who to trust. [H]

Business and government institutions are rapidly realizing the market value of DID/SSI solutions that outpace established identity managing solutions resulting from a network of trusted identity exchange between organizations and industries. Though nascent and still yet to be proven tested on a large scale, several tests indicate that DID/SSI will ultimately see mass implementation. M

The main challenges to fully scale DID/SSI frameworks revolve around governance. M Specifically identifying interoperability standards, a consistent approach for linking identity addresses back to real world identities and creating an open digital identity landscape M that legitimizes participation.

Several large tech companies are actively collaborating with members of the Decentralized Identity Foundation (DIF), the W3C Credentials Community Group, and the wider identity community. H For example, Microsoft has joined with the Fast Identity Online Alliance (FIDO) and other alliance partners like W3C to help develop safer, more secure, interoperable technologies for authentication that will work with many organizations' DID solutions regardless of the underlying technology. H

Systems such as the decentralized Sovrin Network provide space for decentralized, self-sovereign emergence (see Figure 3). Sovrin a public service utility enabling self-sovereign identity on the Internet so that individuals can collect, hold, and choose which identity credentials —such as a driver's license or employment credential—without relying on individual siloed databases that manage the access to those credentials. H

Demonstrations of services using this technology are already underway. H For example, Kiva is building an identity protocol based on self-sovereign identity for building credit history in Sierra Leone. M Another example is the COVID Credentials Initiative ("CCI"). They are working on a digital certificate based on self-sovereign identity that lets individuals prove they have recovered from the COVID-19, have tested positive for antibodies or have received a vaccination. H The European Union is creating an eIDAS (electronic IDentification, Authentication and trust Service) compatible European Self-Sovereign Identity Framework (ESSIF). H The ESSIF makes use of decentralized identifiers and the European Blockchain Services Infrastructure (EBSI). H

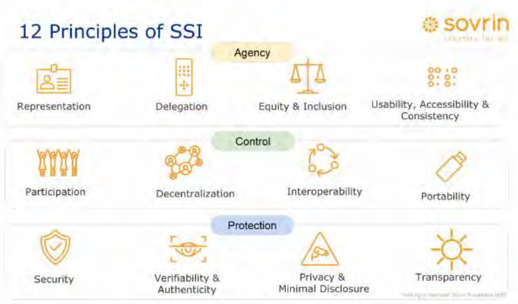


Figure 3. Graphic Representing of Sovrin Networks Self-Sovereign Foundational Principles. Click on picture or go to: https://sovrin.org/principles-of-ssi/ to read more. Source: The Sovrin Foundation.

Decentralized identity is a conceptual shift away from current identity frameworks, yet it can co-exist with the account-based identity model that has existed for decades. H Though DID/SSI systems are still relatively new, it is not a technology that a single company can simply release to the market. It requires both standards as well as collaboration between the private and public sector to have a healthy ecosystem of issuers, holders, and verifiers. [M]

Given the progress of alliances such as FIDO, W3 as well as governmental organizations such as the EU, it is highly likely DID/SSI solutions will reach critical mass adoption, digital experiences. [M] These efforts indicate that DID/SSI will mature over time and highly likely scalable within 5-10 years.

Analytic Confidence

The analytic confidence for this estimate is high. Sources were reliable and corroborated one another. There was adequate time, however, the concepts and variety of DID/SSI are vast and evolving. The analyst worked alone and did not use a structured method. The variety of sources included peer-reviewed academic journal articles, governmental websites, digital alliance associations, and videos by DID/SSI developers. Given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Troy Alexander

Section 2: Culturally-Sensitive Mixed Reality

Advances In Multilingual Neural Machine Translation Systems Likely To Improve Coalition Communications by 2027

Executive Summary

Neural Machine Translation (NMT) capabilities including Natural Language Processing and Machine Translation Quality Estimates are likely (55-80%) to be adopted by 2027 military operational areas where success depends on successful coalition integration. These developments coupled with the Department of Defense's increased focus on building coalitions for competition and conflict make this adoption very likely despite the uncertainty regarding the quality of NMT translations.

Discussion

Neural Machine Translation (NMT) is now the dominant model for machine translation in academic research and commercial use. [H] NMT technology has evolved over the past five years due to increased remote-work demands and was further expedited by the COVID-19 pandemic. This evolution has enabled researchers to incorporate more than two languages at a time when conducting machine translations. [H] Prior machine translation systems often used a "pivot language" for multilingual translations when data for direct bilingual translation did not exist. English became the most used pivot language, essentially serving as a shared third language or "bridge" between the two other languages. [M] English dominated as a pivot language due to the availability of large and well-developed English language data sets. [M]

This translation model, shown in Figure 1 below, demonstrates how machine translation could translate a phrase from Finnish into Greek when no Finnish-to-Greek training data is available. Using pivot translation, the system uses the existing Finnish-to-English engine to translate into English (the pivot) and then use a separate English-to-Greek engine to complete the translation into the target language. [H] Sometimes, more than one pivot is required based on the available language data. Each pivot translation risks introducing of additional errors, most commonly in translation errors that compound as they move through the system, and a loss of context and nuance from the original language. H

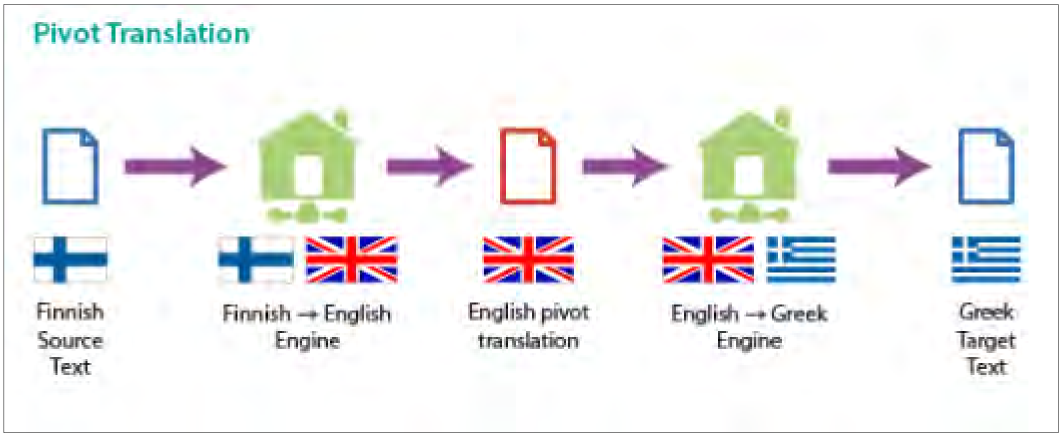


Figure 1. Pivot Translation. Source: CSA Research

Google's Multilingual Neural Machine Translation developed a "zero-shot translation" model that does not use a pivot and is capable of providing "translation between language pairs never seen explicitly by the system." H Unlike pivot translations where the system uses only one language pair at a time for translation, zero-shot models can use multiple language pairs with relevant data at the same time. The result is better than trying to bridge a gap using a single pivot language. While zero-shot translations are generally less accurate than pivot translations, they have the advantage of producing multilingual translations while also eliminating the cascading error problem described above for pivot translations. the directly translates one language into another. H Using the same Finnish-to-Greek example, Figure 2 demonstrates zero-shot translation.

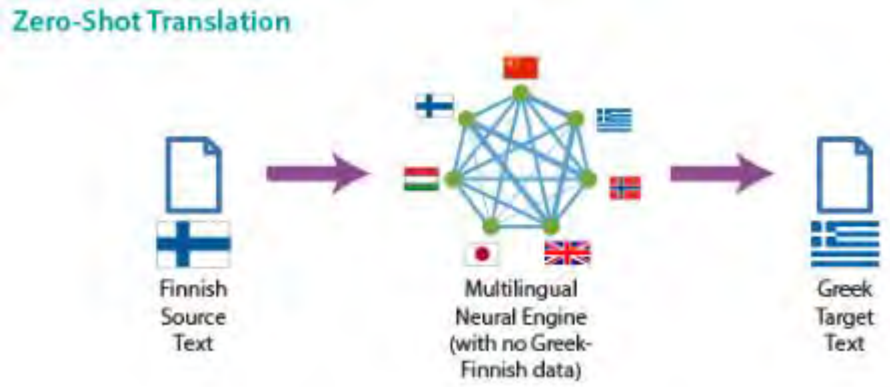


Figure 2. Zero-Shot Translation Model

In multinational and coalition environments, both models present opportunities to improve communication between partners, especially in circumstances where the coalition includes several members with varying languages. Neural Machine Translations and Natural Language Protocols could assist with rapidly disseminating orders and instructions or serve to translate electronic data shared between machines. [H] Opportunities during competition could include development of specific military corpus (vocabulary data) to train algorithms on military-specific language, as well as a focus on expanding the broader corpus now for partners and allies assessed to be most important during a conflict. [M]

Relatedly, several companies are leveraging machine translation to develop real-time “multi-language translation capabilities” for video conference calls. [M] VIDIZMO has developed improved “automatic audio and video redaction through AI” to perform several functions that would be useful in a coalition environment. [M] VIDIZMO’s solution auto-transcribes all video conferences in the original language and produces subtitles and transcripts in multiple languages. Technology is available now from several companies that the DOD could immediately adopt for AI translations of spoken speech into various languages that is available to be watched later, yet this technology is not available in coalition headquarters due to policy restrictions. [M] Going a step further, Apple, Google, Microsoft, and Amazon have all made major investments in real-time language technology that instantly translates any speech into the listener’s language. [M] And, a U.K.-based startup, Papercup, is focusing on improving some speech translation challenges including creating voices that are more human-like, retaining the emotions and pace of the original speaker, as well as capturing the uniqueness of the original speaker’s voice.[H] A combination of all of these technologies would be useful within any diverse coalition command structure.

Even as neural machine translations have improved, many people remain distrustful of the technology and the quality of machine translations. [H] NMT creators built tools called Machine Translation Quality Estimations (MQTE) to provide “scores” to automatic translation that assess the quality of translations with the goal of increasing human trust in their systems. MTQE seeks to address general distrust in new AI for machine translations. See Figure 3 for an example of MQTE scoring.

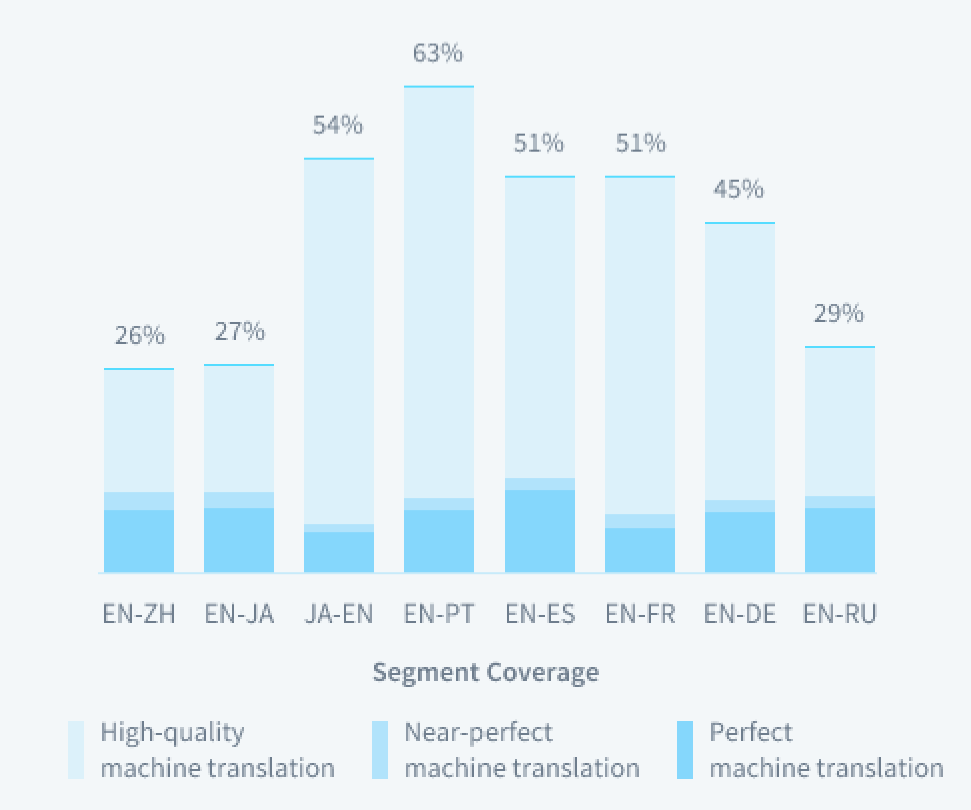


Figure 3. Memsource MQTE Machine Translation Scoring

Analytic Confidence

This is a moderate confidence estimate. The reliability of sources is moderate, information and assessments from multiple sources were consistent, however, theoretical predictions varied and much of the technology is used commercially today. Most sources were industry papers and news articles and not peer-reviewed academic journals. Very few sources made predictions on timing for development or adoption of NMT technology.

Author: LTC Patrick Hofmann

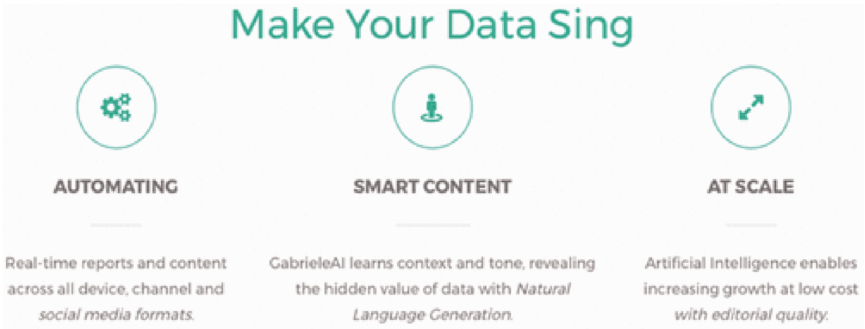
Deep Learning Likely To Enable Natural Language Processing To Be Culturally Sensitive Enough to Share Data Through Storytelling In A Multinational Environment By 2037

Executive Summary

Due to commercially available products that use storytelling and data dashboards to communicate data, focused research in the discipline of Deep Learning (DL), and current DARPA research, it is likely (56-70%) that NLP will be culturally sensitive enough to share data through storytelling in multinational environments by 2037. Even though research indicates that sharing data through storytelling and Natural Language Processing (NLP) is becoming more and more common in everyday technologies, NLP has not displayed cultural sensitivity or and ability to transition easily between different languages. Academia and commercial institutions, however, have developed deep learning techniques that enable software applications to cull large data sets and turn data analysis outputs into written or spoken stories describing the data. Research and advancements in deep learning will likely enable the next logical progression; the devolvement of multilingual, culturally sensitive applications that account for cultural differences in storytelling.

Discussion

Data stories reveal and communicate insights gained from analyzing datasets obtained from the public domain, crowdsourcing, or big data sources. [H] Data storytelling (i.e., the practice of creating data stories) is a structured approach comprising data, visuals, and narratives for communicating insights from data. [H] The object of developing data stories is to give voice to the data to inform, explain, persuade, or engage the target audience. [H] Research indicates a positive correlation between effective data storytelling and better business performance, which is partially mediated by decision-making quality. [H]



Make Your Data Sing

AUTOMATING

Real-time reports and content across all device, channel and *social media formats.*

SMART CONTENT

GabrieleAI learns context and tone, revealing the hidden value of data with *Natural Language Generation.*

AT SCALE

Artificial Intelligence enables increasing growth at low cost *with editorial quality.*

Figure 1. Narrative Story Telling Through Data Construct. Click on Picture or go to https://journals.sagepub.com/doi/epub/10.1177/2053951718756686

Using a construct as seen in Figure 1, [H] companies like Arria NLG, Automated Insights, Narrativa, Narrative Science, and Yseop have developed software services that translate data into human language. [H] These automated NLP techniques promise to 'refine' the raw material by using narratives to sort data and make visible a hierarchy between information that is important and unimportant for what the end-user wants to know. [H] News services such as Yahoo Sports and the Associated Press use these services to generate and publish analyses on sports and weather. [M] Other companies like ClearStory Data use NLP to produce dynamic dashboards that learn and adapt to user inputs to determine the type of information and analysis based on the end-user requirements. [M]

Deep learning, a discipline within the field of artificial intelligence and a subset of machine learning, has increased the capability of traditional NLP. [M] Deep learning uses the human brain's structure as its foundation and uses structured algorithms in layers to create an "artificial neural network" that can learn and make intelligent decisions on its own. [M] Artificial neural networks are a learning system that's far more capable than that of standard machine learning models. [M] As seen in Figure 2, [M] a key advantage of deep learning over traditional machine learning is automatic feature extraction. [M] On the contrary, in conventional machine learning, this task is carried out outside the algorithmic stage. As a result, people, data scientists' teams and not machines, are in charge of analyzing raw data, [M] slowing the process and forfeiting potentially undiscovered analysis.

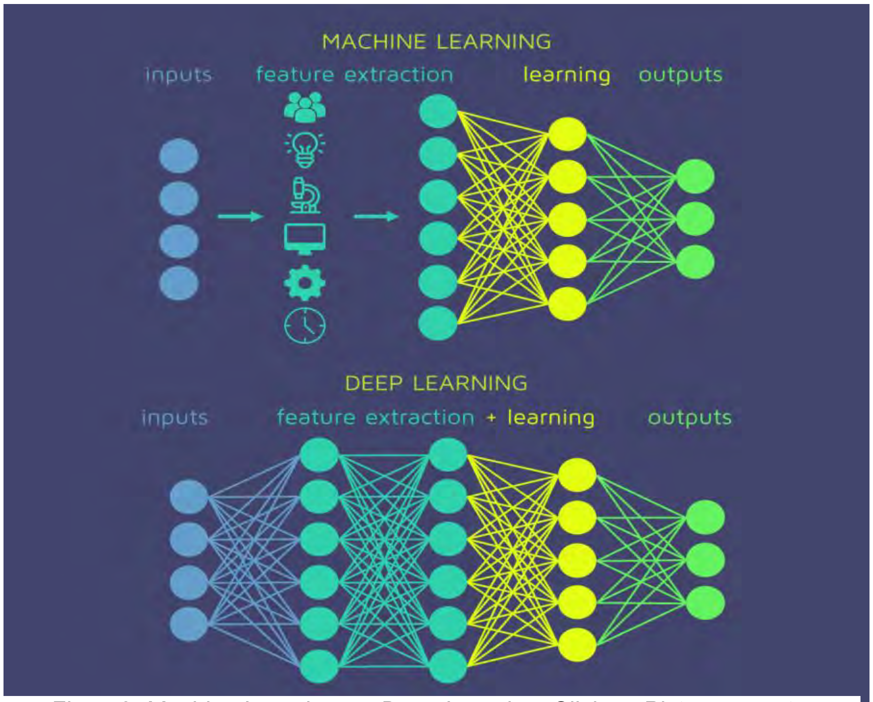


Figure2. Machine Learning vs. Deep Learning. Click on Picture or go to https://quantdare.com/what-is-the-difference-between-deep-learning-and-machine-learning/

DARPA is currently researching cultural sensitivity in NLP. [H] The DARPA Computational Cultural Understanding program (CCU) is seeking to create a language understanding service with the ability to analyze cross-cultural communication more accurately. [H] The goal of this DARPA research is not just to read language, but to understand and interpret cultural cues. [H] Another goal is to develop processing technologies that can recognize, adapt to, and recommend how to operate within the emotional, social, and cultural norms that can differ across societies, languages, and communities. [H] DARPA believes CCU requires a revolution in AI technology, not just an evolution of what already exists. [H] The expected outcome of CCU is a machine learning model that requires minimal-to-no training data in local culture and no labeled data. DARPA expects to infer the meaning of unlabeled discourse behaviors in context. [H]

Advances in NLP using deep learning will be challenging. Deep learning techniques are resource-intensive. Deep learning requires extensive data sets and GPU (Graphical Processing Units) processing as opposed to traditional CPU (Central Processing Units) processing. [M] GPUs are more conducive to artificial neural networks due to many hundreds of cores compared to the 2-4 cores present on a CPU. However, [M] GPUs are more expensive than CPUs and are sensitive to demand and supply chain issues. In addition, neural networks take more time to learn, as learning time is a function of the amount of data and the number of layers in the network. [M] DARPA is researching a revolutionary step in the CCU, and the desired solutions require novel hardware that does not yet exist.

DARPA awarded a three year $10M contract to SRI International in the fall of 2021. [M] SRI International will develop natural language processing that recognizes, adapts to, and recommends how to operate within the emotional, social, and cultural norms that differ across societies, languages, and group affinities. [M] Although there are many companies that provide NLP services for business, research on Computational Cultural Understanding is focused in the defense sector. It is likely (56-70%) that once the DARPA CCU program results in appropriate hardware and software solutions, private industry will become interested in pursuing this technology for implementation in the business sector.

Analytic Confidence

The analytic confidence for this estimate is medium. Sources were generally reliable and corroborated one another. There was adequate time, but the analyst worked alone and did not use a structured method. Many of the sources were peer-reviewed academic journal articles, government, industry, and private company websites. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Greg Pavlichko

Advanced Militaries Likely To Adopted High-Quality Real-time, High Fidelity, Full 3D Body Scan Holoportation To Improve Communication By 2032

Executive Summary

Advances in 3D visualization technologies such as holopresence and holographic displays are likely (55-80%) to be sufficiently advanced for application during military operations by 2032. These technologies will improve two-way communication between individuals and groups by bringing gestures, body language, facial expressions, and realism that were unrealized with 2D architecture. Despite the current high prices, latency, and high-bandwidth constraints, these technologies are likely to rapidly migrate into defense applications.

Discussion

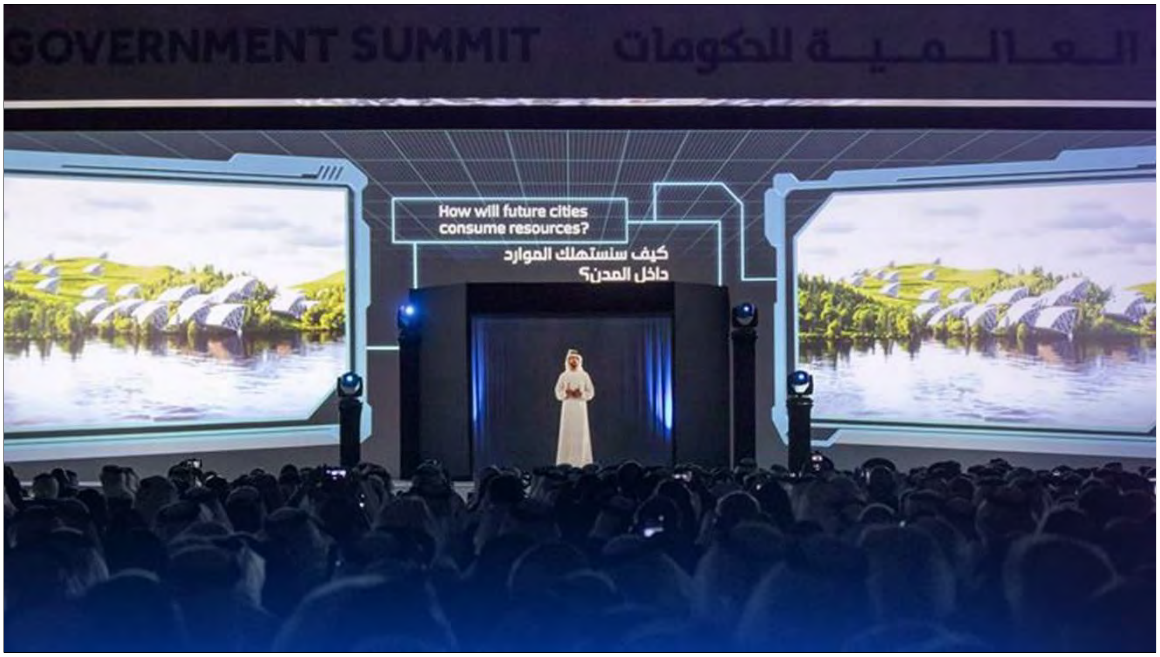


Figure 1. The Crown Prince of Dubai at the World Government Summit. Source: ARHT

The COVID-19 pandemic ushered in a wave of 2D collaboration tools that many people would have found odd before the pandemic. However, consumers rapidly adapted to communicating via video teleconference chats through Zoom, FaceTime, WhatsApp, and other platforms. [M] Several companies are developing the next evolutions in this technology to include 3-dimensional, real-time, full body holograms. [M] Holograms can enable strategic leaders to make more personal connections and deliver more impactful messages while saving time by eliminating the need to travel to see every partner and ally. In 2020, the Crown Prince of Dubai made a major speech as a hologram to the World Government Summit he hosted (see Figure 1). [M]

ARHT Media is a Canadian company that has built a projection system the company calls a “Holopresence” experience. Holopresence uses 4K cameras and compressed data to deliver a “life-sized and lifelike” real-time 3D image and audio with less than a 0.3 second delay. ARHT’s CEO Larry O’Reilly focuses on “creating presence” through body language presentation that including all the speakers’ non-verbal cues including emotions and emphasis. [M] Holopresence works point-to-point, can bring multiple holograms from several distant locations at once, or record presentations or meetings for presentation later. Unlike some of their competitors, AHRT’s Holopresence can be permanently installed in a building or purchased as a portable system that breaks down to fit into “a couple of duffle bags” (see Figure 2). [M]

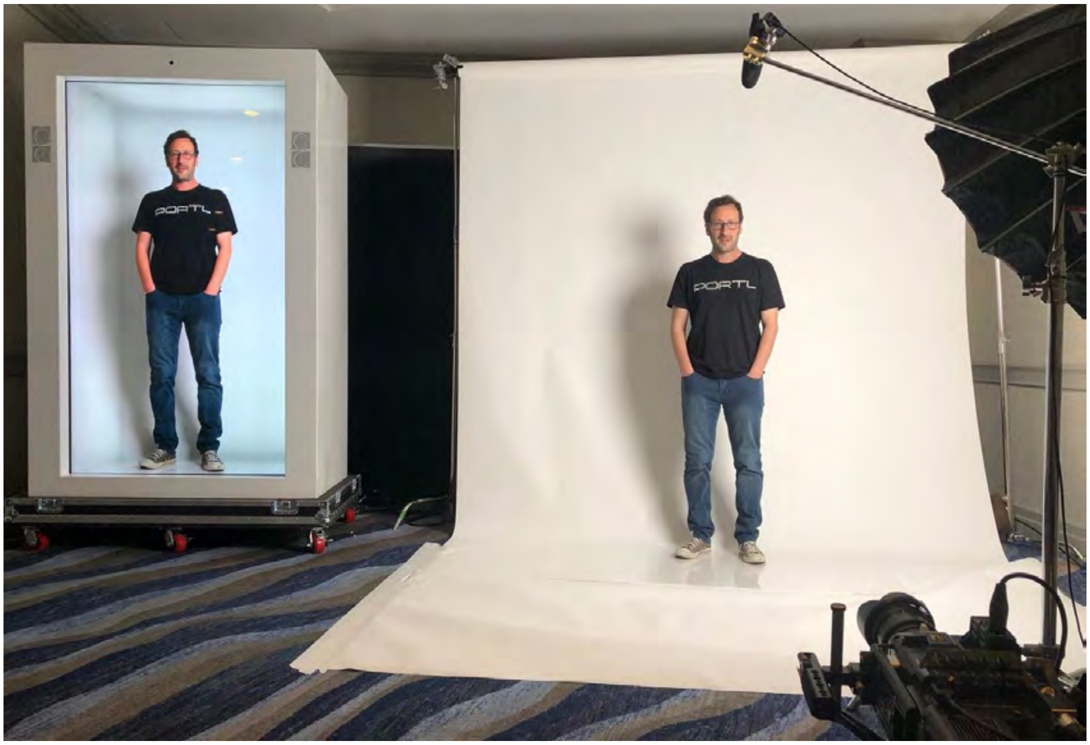


Figure 2. Proto Portl Holopresence

In October 2021, NASA, in collaboration with AEXA Aerospace, projected a hologram from Earth to the International Space Station (ISS). This holoportation occurred as the ISS was traveling 17,500 miles per hour 250 miles away from the individual being holoported on the ground. [H] NASA used Microsoft's HoloLens display device, camera, and AEXA software to conduct the two-way communication between an astronaut and his doctor. This test demonstrates the feasibility of using hologram technology even in remote areas.

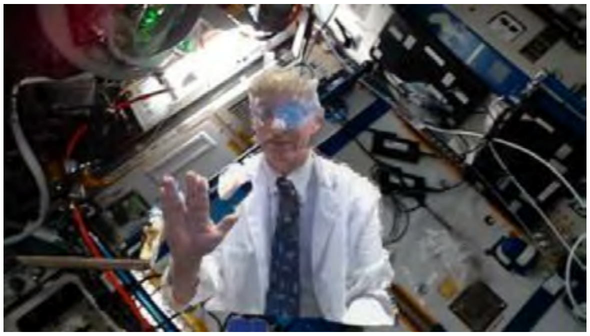


Figure 3. NASA flight surgeon holoportation. Source: ESA

This technology remains expensive, but, as with most new technology, eventually prices will drop for the models. Advances in 5G and edge computing should also enable hologram diffusion by providing "enough compute and bandwidth at an affordable price to support real-time, high fidelity, full 3D body scan teleportation." [M]

Analytic Confidence

This is a moderate confidence estimate. The reliability of sources is moderate, information and assessments from multiple sources were consistent, however, theoretical predictions varied and much of the technology is used commercially today. Most sources were industry papers and news articles and not peer-reviewed academic journals. Very few sources made predictions on timing for development or adoption of holographic technology.

Author: LTC Patrick Hofmann

The Next Evolution Between Machine And Human Communication Is Almost Certain To Occur By 2027

Executive Summary

Despite regulatory, privacy, and security concerns, the convergence of digital and physical worlds is almost certain (95-99%) to occur by 2027. Cutting-edge research and development (R&D) into tactile and alternate physical representations converts how data and information are ingested, processed, and visualized.

Discussion

Recent technological advancements in sensors are shifting the way data is collected. Professor M. Shamim Hossain at King Saud University and his research team published an article, "The shift to 6G communications: vision and requirements" that predicts the tactile internet[9] as the next evolution where machine-to-machine (M2M) and human-to-

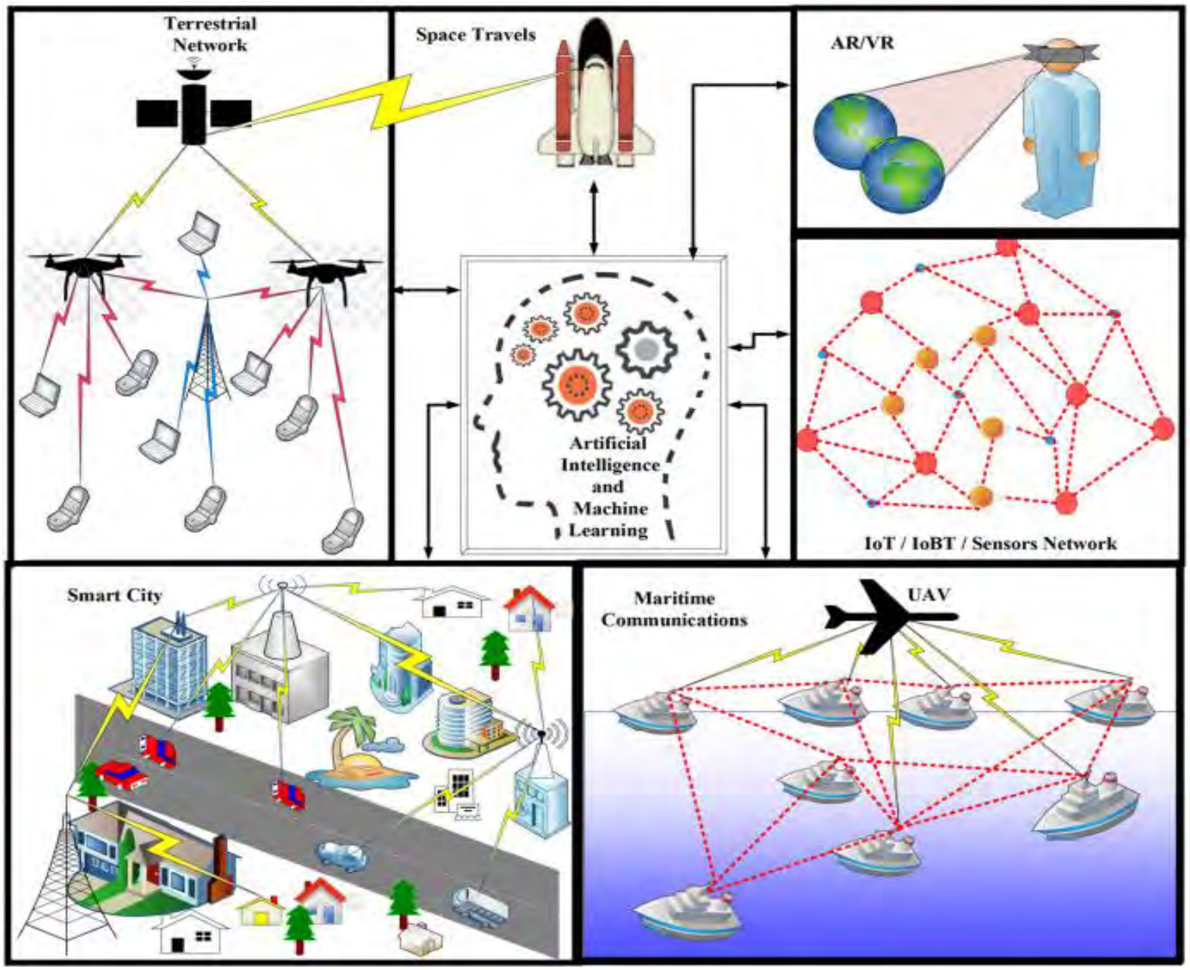


Figure 1. A pictorial overview of the 6G wireless network that covers space-air-ground-sea communications.[M]

[9] The tactile internet is defined as a very low-latency communication system that ensures very low round-trip delay along with high availability, reliability, and security for real-time human-machine interaction-centric applications execution.[H]

machine (H2M) communications will add haptic sensations to data collection and feedback. This tactile internet or "internet of senses" (IoS) enables real-time communication between humans and machines with their environment. M Continued improvements in artificial intelligence (AI), machine learning (ML), and quantum computing will affect how fast the IoS and internet of things (IoT) processes, analyzes, and produces information. IoS, along with 6G and beyond network innovations (see 6G and Beyond), will highly likely provide more enriched analytic information available in alternate physical representations integrated across daily life within the next five years. M (see Figure 1) Extensive and groundbreaking innovative research are exploring promising technologies with brain-machine interfaces limiting physical interactions by providing a direct communication link between the human brain and computers or other external devices. M (see Figure 2)

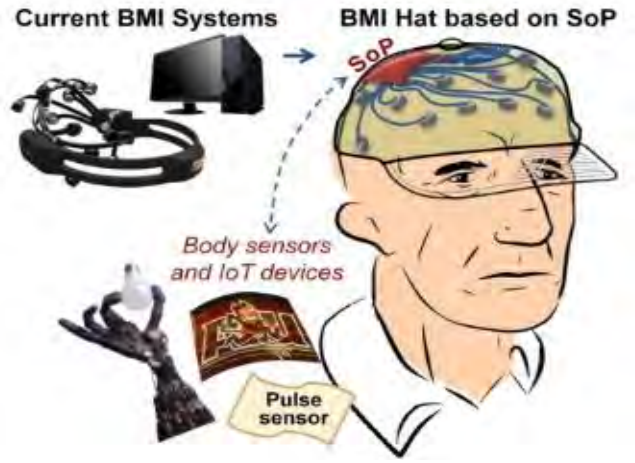


Figure 2. Context-aware control of smart objects via human-machine communications. M

Several technology companies have already engineered solutions that integrate user experiences through haptics. (see Figure 3) Ultraleap[10] designed an immersive experience that allows users to touch and feel what they see in augmented and virtual reality (VR) using ultrasound to project sensations and hand-tracking and mid-air haptic solutions with real-time response. MM Microsoft's solution, AirWave, for immersive experiences provides haptic sensations using air vortex rings similar to a speaker diaphragm. M

Figure 3. Future of Haptics in VR . Click on the picture or go to: https://youtu.be/I5ZI3tAQjzI to view the video. Source: Microsoft

3D hologram projections are also advancing rapidly. Massachusetts Institute of Technology uses AI and

[10] Ultraleap is a merger of Ultrahaptics and Leap Motion tech companies that specialize in immersive technology.

ML to create 3D holograms. The school uses a deep learning-based method to produce holograms efficiently in near real-time. Lead researcher, Liang Shi, believes the new approach (tensor holography)[11] will help deliver commercially available holographic displays within ten years. M Dan Smalley of Brigham Young University and his research team have developed methods to "draw screenless, free-floating objects in space" similar to "a 3D printer for light." Their research creates an environment "where people can interact with holographic-like objects that coexist in their immediate space." M (see Figure 4)

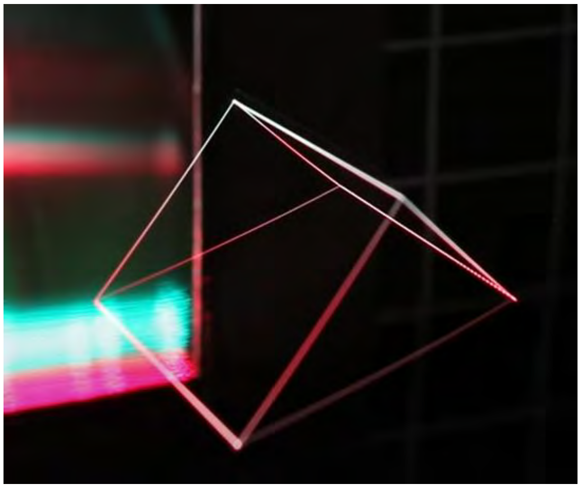


Figure 4. Using lasers to create the displays of science fiction, inspired by Star Wars and Star Trek. Click on the picture or go to: https://youtu.be/N12i_FaHvOU to view the video. Source: Brigham Young University

An additional emerging innovation is Mojo Vision's eye-tracking display-enabled contact lenses. The tech company has been designing this product since 2017, and the current 2022 version is a self-contained display-enabled lens that includes an "accelerometer, gyro, and magnetometer for eye tracking." It can display text, basic graphics, and some illustrations with the help of a custom wireless connection of a neck-worn relay device. The current limitations are power efficiency and short-range wireless connection. M (see Figure 5)

The convergence of the M2H interface will highly likely encounter resistance from regulatory, digital privacy, and data security issues. A Congressional Research Services (CRS) report determined that regulatory authorities and oversight jurisdiction would become unclear as the various technologies converge. H Tech companies like Meta (formerly Facebook), Google, and Twitter gather masses of personal data from users and sell it in bulk to advertisers to make profit. M Data security is also a significant concern (see Data-Sharing

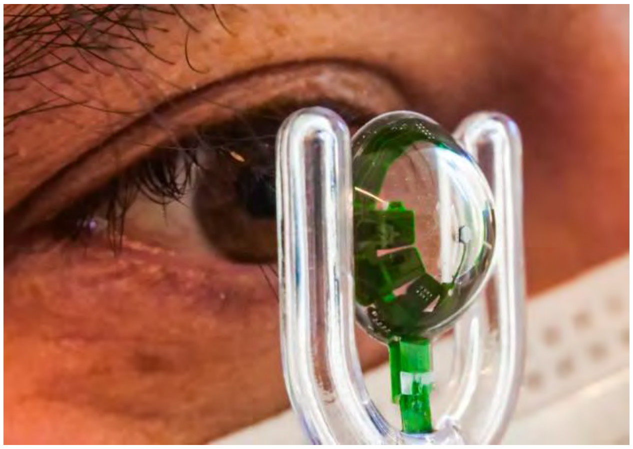


Figure 5 Mojo Vision Sneak Peak. Click on the picture or go to: https://www.cnet.com/videos/mojo-vision-gave-me-a-peek-at-eye-tracking-displays-in-a-contact-lens/ to view the video. Source: Mojo Vision

[11] Tensor Holography synthesizes a 3D hologram with per-pixel depth from a single RGB-D image in real-time.M

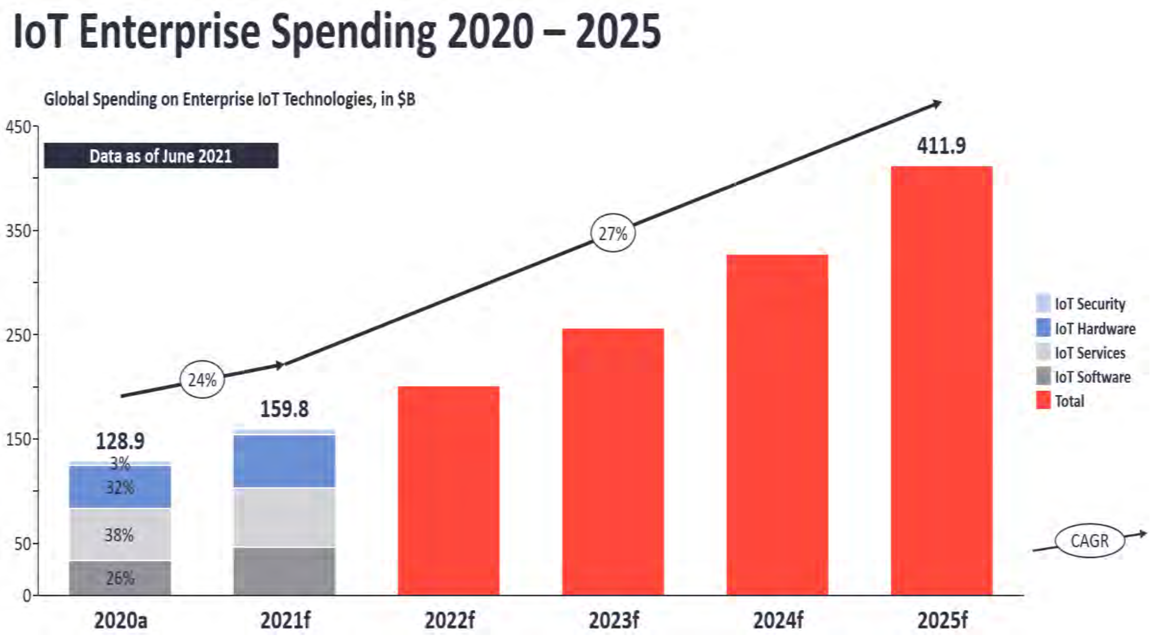


Figure 6 Global IoT spending to grow 24% in 2021 with projection to 2025. Click on the picture or go to: https://iot-analytics.com/2021-global-iot-spending-grow-24-percent/ to view the video. Source: IOT Analytics

Mindset) for example, Oracle suffered a data breach in June 2020 that exposed billions of user records. [H] Converged devices generate and consume large amounts of data and the projected increased IT spending will increase surface areas for cyber-attacks, physical security issues, and data theft. (see Figure 6 for details on current and projected Global IoT spending growth) However, with the appropriate use of AI, ML, and other defensive measures discussed in previous reports, trust and confidence will continue to grow and almost certainly not stop or delay the M2H convergence.

Analytic Confidence

The analytic confidence for this estimate is moderate. Sources were reliable and tended to support one another. There was adequate time, and the task was not complex. Because of the short time frame of the estimate, this report is sensitive to change due to new information.

Author: LTC Nicole Y. Shadley

Within 10-15 Years Expansion of 5G Networks Will Likely Enable Increased Use Of Augmented, Mixed Reality Systems For Virtual Collaboration Eventually Replacing The Cell Phone

Executive Summary

Within 10-15 years, despite current hardware limitations, there will likely (55-80%) be a significant expansion in the use of Augmented Reality (AR) and Mixed Reality (MR) for virtual collaboration and eventually replace the cell phone as the preferred mobile device. The expansion of AR/MR's use for virtual collaboration will be due to the expansion of low latency 5G networks.

Discussion

XR
EXTENDED REALITY
VR VIRTUAL REALITY
AR AUGMENTED REALITY
MR MIXED REALITY
#XR #ExtendedReality #XRViewer
XR - The Future of VR, AR & MR in One Extended Reality

Figure 9. XR - The Future of VR, AR & MR in One Extended Reality. Click on picture or go to: https://www.youtube.com/watch?v=E0QLVj9FJ0A to view video. Source: Science Time Channel on YouTube.

Extended Reality (XR) is the overarching term that encompasses Virtual Reality (VR), AR, and MR (see Figure 1). [M] In VR, the system creates a fully immersive simulated digital environment within which the user can interact. [M] In comparison, AR is designed to enhance the physical world by overlaying virtual digital information onto the real world; it is not designed to create a fully immersive experience. [M] Finally, MR incorporates aspects of VR and AR, where the user can interact with virtual objects in the real world, or an immersive VR environment can be anchored to and replace objects in the real world. [M] The site Finances Online, estimates that the combined AR and VR market was $12 Billion in 2020 and will to grow to approximately $73 Billion by 2024. [M]

Virtual Reality is a better solution for experiences that require a fully immersive, interactive, simulated environment, such as in video gaming. [M] However, extended use of VR systems may create some health risks, such as eyestrain, migraines, motion sickness, and falls. [M] As a result, AR/MR provides a better solution for creating a collaborative environment where a user will need to interact with both the real and virtual worlds for extended periods of time.

More recently, sophisticated AR/MR Head Mounted Displays (HMD) are enabling a wider range of uses for businesses. Two of the most sophisticated AR/MR HMDs available today, designed for business enterprise use, are the Microsoft HoloLens 2 and the Magic Leap 1. [M] One company that is leveraging these new HMDs for virtual collaboration is Spatial, which has created the Spatial AR collaboration workspace application. [M] The Spatial workplace supports numerous devices, including HoloLens 2 and Magic Leap, and enables users to collaborate using a variety of MR collaboration tools.[MM] In addition to existing AR/MR HMDs, several companies have announced new devices that will be released in the next few years, such as Apple's AR/VR device, the Magic Leap 2, and a partnership between Microsoft and Qualcomm to create new lightweight AR glasses. [M]

The U.S. Army's closure of a $22 Billion deal in 2021to purchase AR headsets and services from Microsoft is another example of the expanded use of this technology; the deal includes the purchase of up to $4.2 Billion worth of modified HoloLens 2 headsets. [M] While the Army recently announced delays to fielding the system due to technical issues, these new custom headsets are known as the Integrated Visual Augmentation System (IVAS) and are designed to provide soldiers a digitally enhanced way to collaborate and view the battlefield environment. [MM]

Hardware shortcomings have been an impediment to wider AR/MR technology use. According to Finances Online, the top barrier for adoption is a poor using experience caused by bulky hardware and technical issues. [M] Most current generation HMDs must be connected to a processor unit, which makes them bulky and causes them to consume too much power. [M] However, new 5G networks will help address these hardware issues. Using 5G technology, most of the data processing can be conducted in the cloud and video can be streamed to the HMD using high bandwidth, low latency 5G networks. [M] Offloading the data processing to the cloud will enable HMDs to be smaller, consume less power, and deliver a better user experience, which will increase adoption.

According to Forbes.com, future AR/MR/VR technologies will deliver an improved user experience that will include full-body haptic suits, the ability to use hand gestures, rather than clunky controllers, and eventually result in AR contact lenses. [M] The company Mojo Vision has already developed a prototype AR contact lens that uses a microLED screen, wireless communication, and eye tracking technology to create text overlays for the user. [M] Some analysts believe that AR glasses will eventually replace cell phones as the predominant mobile device of the future. [MM]

Analytic Confidence

Overall analytic confidence in this estimate is moderate. The analyst had adequate time and the task was simple. While several sites provided similar definitions for VR, AR, and MR, it was common for articles to refer to all three categories as a single technology. This was particularly prevalent when articles addressed AR and MR as a single technology, sometimes referring to MR as an extension or evolution of AR. Additionally, forecasts on the direction of hardware development were consistent, but adoption timelines were difficult to predict, since widespread adoption will also depend on developers that will need to create applications for the new hardware.

Author: COL Anthony Pollio

AI Enabled, Decentralized, Personal Companion Technologies Likely To Strengthen Trust And Augment Private Information Sharing Capability By 2037

Executive Summary

Despite challenges of nascent technology developments and privacy concerns, it is likely (55-80%) that Artificial Intelligence (AI) enabled, decentralized, personal companion technologies will proliferate at scale in the next 10-15 years. Personal companions (also referred to as virtual assistants, digital assistants, or AI assistants) provides a means for seamless activation of application support, enabling a user to immediate access a host of programs for analysis and problem solving. Personal companions are programs that understand natural language voice commands, the user environment, and completes tasks for the user. As technologies coalesce and personal companion capacities advance, it is viable by 2037 that both private and public sectors will leverage for partner building. Personal companions will provide discreet abilities for stakeholders to better understand nuances of an operating environment, triage priorities, recall data and historical context, and quickly analyze solutions to establish, build and strengthen trust across multiple parties. All while securing sensitive private information and sharing specific visual information to intended parties as needed, even though others are present.

Discussion

Figure 1. Artificial Intelligence Powered Digital Assistants. Click on picture or go to: https://medium.com/voice-tech-podcast/artificial-intelligence-powered-digital-assistants-1e0bdf108641 to read more. Source: Medium.com

Artificial Intelligence-powered digital assistants are growing in popularity, with names like Apple Siri, Google Assistant, Amazon Alexa, and Microsoft Cortana gaining significant market attention (see Figure 1). [M]

Currently, there are numerous different types of AI virtual assistants ranging from chatbots, voice assistants, AI avatars, to domain-specific virtual assistants. [H] As with portable technological advancements, digital assistance programming concepts are evolving to become “virtual personal companions” who are able to travel with a user to help process vast amounts of information quickly to derive useful insights. [M] Beyond AI, the primary technologies upon which personal companions hinge on include Machine Learning, Cognitive Computing, Text-to-speech, Speech Recognition, Computer Vision, and Augmented Reality. [M]

There are several apps, powered by AI and machine learning (ML), that are normalizing a superior intelligence ‘virtual companion’ which can not only help in day-to-day activities but also play the role of a friend or even emotional health assistant (see Figure 2). [M]

The key technologies behind widening personal companion availability are already in use. [M] Examples of tailored tasks include controlling devices at home, initiating phone calls or text messages, getting answers to questions without having to look up reference materials or getting up-to-date information about several subjects like weather or traffic. [M]

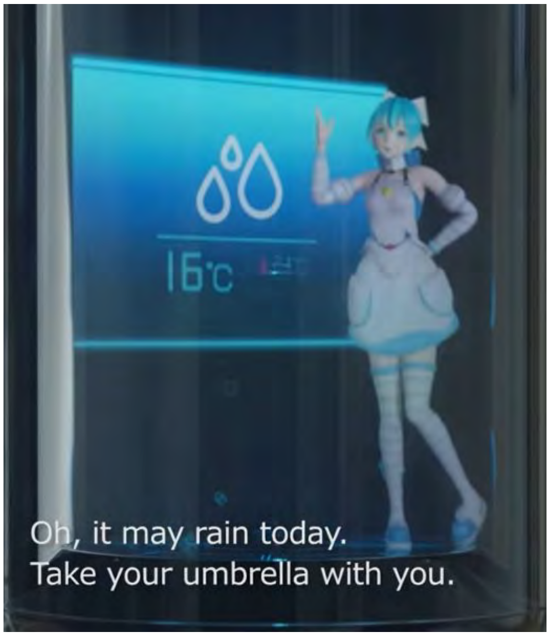


Figure 2. Concept of Personal Companion underway by Gatebox Research Laboratory. Click on picture or go to: https://youtu.be/nkcKaNqfykg to view video. Source: Gatebox Channel on YouTube.

The COVID-19 pandemic and related lockdowns have made the average consumer more willing to interact with businesses in general digitally. [M] Companies are widely integrating AI technologies and end-users utilizing AI assistant technology can be found in the healthcare, telecommunications, travel and hospitality, retail, banking, financial services and insurance sectors. [H] In the healthcare industry alone, research published by MarketsandMarkets [M] projects that the healthcare artificial intelligence market is expected to grow $7.9 billion in 2022 as the industry seeks private, secure methods to improve patient outcomes and reduce healthcare costs. [H] To stay relevant as in-person banking declines, the banking industry is investing in conversational virtual assistant applications that can go beyond a FAQ scenario to handle complete transactions — from changing an address to cancelling a payment and updating a standing order to identifying and resolving a specific need. [M]

Several start-ups are showcasing emergent technologies that incorporate current technology with nascent algorithms that provide emotional [H] and situational awareness analysis to provide near-real time analysis and engagement feedback. For example, start-up companies such as Bluecap has a personal companion that joins meetings and acts as a personal assistant with the capacity of providing secure, encrypted data protection while taking notes, recording calls, and helping a user stay focused on participant behavior, providing an executive summary, key takeaways, and a deep analysis of topics. [M] OneLawAI’s conversational virtual assistant offers legal offices a scalable solution to bolster sales lead generation and provide AI driven legal research to legal teams. [M]

Figure 3. MojoLens contact lens. Click on picture or go to: https://youtu.be/61QNTWE54QU to view video. Source: Mixed Channel on YouTube.

The pandemic has retailers adapting business models as well, seeking interactive, immersive customer experiences [M] that build trust and support sales teams ability to develop relationships. Remarkably, nanotechnology advancements are creating space to take personal companions beyond audio to a portable audio-visual experience using "smart" devices like glasses and contact lenses. [M] InWith and MojoLens are two contact lens companies developing integrated visual assistance. [M] InWith aims to provide the first soft smart contact lens that could deliver real-time information directly to your eyes. [H] MojoLens is on the cusp of developing a hard contact lenses that will quietly provide a user with essential visual data while engaged in events, cultural cues when meeting people, and secure talking points during a presentation, all without holding a device or looking down at a screen (see Figure 3). [M] These types of technologies offer the eventual potential of presenting personal, private 3D AI avatars to give a human touch to virtual interactions. [H]

There are limitations and challenges of AI-based personal companions, specifically with regards to nascent technology developments, privacy and security. [M] Currently, virtual assistants employ a limited amount of intelligence that is configured to meet certain niches (i.e. customer service) and personal companions require incorporation of multiple technologies [M] to provide location-based experiences that are engaging, accurate, real-time and scalable. [L] Controversial data handling policies by companies like Meta (Formerly Facebook) have stoked fears of corporate overreach and privacy concerns after the events of high-profile whistleblower scandals. [M] Consequently, governance initiatives such as the European Union's General Data Protection Regulation (GDPR) [H] are underway that will provide the requirements of privacy and data protection. [H]

Despite these limitations, to facilitate machine-mediated communication, many tech giants (e.g. Google's Siri and Amazon's Alexa) are spending a great deal of time and effort on finding proper sensors that can empower digitized personal companions to interpret our emotion, [M] provide situational analysis, and provide real-time decisions or recommendations based on tailored algorithms to match a user.

Universities are applying resources as well. [H] At Stanford's [H] Open Virtual Assistant Lab (OVAL), [H] researchers are developing methods to decentralize [H] personal companion platforms.

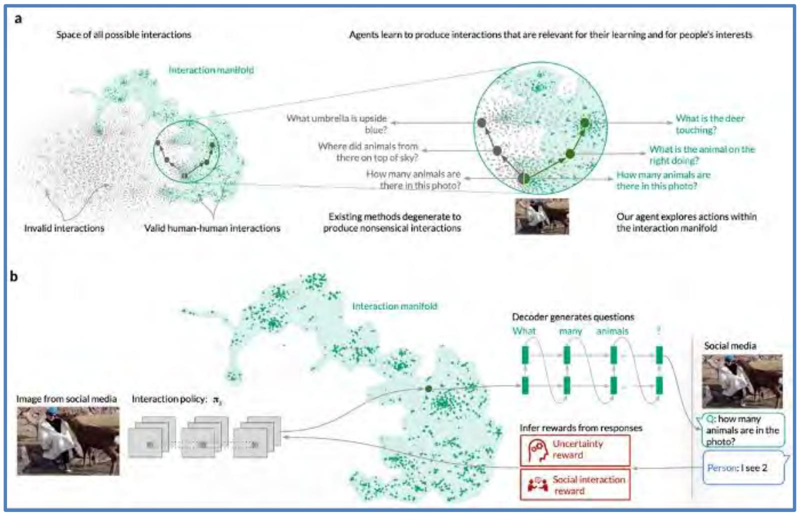

a
Space of all possible interactions
Agents learn to produce interactions that are relevant for their learning and for people's interests
Interaction manifold
What umbrella is upside blue?
Where did animals from there on top of sky?
How many animals are there in this photo?
What is the deer touching?
What is the animal on the right doing?
How many animals are there in this photo?
Invalid interactions
Valid human-human interactions
Existing methods degenerate to produce nonsensical interactions
Our agent explores actions within the interaction manifold
b
Interaction manifold
Decoder generates questions
What
many
animals
?
Social media
Image from social media
Interaction policy: π_θ
Infer rewards from responses
Uncertainty reward
Social interaction reward
Q: how many animals are in the photo?
Person: I see 2

Figure 4. The First Conversational Agent Able to Learn from Open-Ended Human Feedback. Click on picture or go to: https://oval.cs.stanford.edu/ to read more. Source: Stanford Open Virtual Assistant Lab.

Their novel approach aims of dramatically widen the competition and protect privacy and is comparatively inexpensive, since an open-source platform allows numerous users contribute code or skill sets to a shared repository (see Figure 4). [H]

Although personal companion technology providers compete for niche space that is generally tied to a particular device, the variety of these emerging technologies will coalesce. [M] Additionally, nondescript portability [M] will advance to provide users a decentralized means to maintain connection to these intelligent agents any time and place. [M] Hence, allowing users the capacity to leverage real-time system support that perceives its environment, provides personal analytical recommendations, and can take actions that maximize its chance of achieving an operator's goals. [M]

Several indicators ranging from research development and market growth to growing social acceptance since the COVID19 pandemic are driving emergent use of personal companions. [H] Given applicability across multiple industries and the progress of integrating technologies, [H] combined with the nascent capacity to privately provide contextual analysis and advice directly to a user, is likely personal companions will reach scalable adoption in the next 10-15 years. As such, by 2037, personal companions will likely be widely available for military use, providing secure, discreet capacities to better understand nuances [M] of an operating environment, triage priorities, recall data and historical context, and quickly analyze solutions to establish, build and strengthen trust across multiple parties.

Analytic Confidence

The analytic confidence for this estimate is moderate. Sources were reliable and corroborated one another. There was adequate time, however, the concepts and variety of terms associated with personal companions (e.g. virtual assistants, digital assistants, AI assistants, personal avatars, etc.) are vast, inconsistent and evolving. The analyst worked alone and did not use a structured method. The sources varied and included academic journal articles, tech journals, blogs and developer business websites. Given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Troy Alexander

Section 3: Augmented Intelligence

Machine Common Sense Likely To Enable Dynamic, Learning Networks Capable Of Communicating With Users By 2037

Executive Summary

Even though computer scientists and psychologists lack a mathematical model of consciousness and the likelihood of machine consciousness in the next 15 years is remote (1-15%), because of current research efforts in academia and business, it is likely (56-70%) that Machine Common Sense (MCS) will be realized by 2037 and enable networks to learn from unique situations, apply a decision-making model, and communicate with human end users. Academia is researching two MCS paths; mining large-scale data and developing a toddler cognition model. Business research is interested in developing MCS to rely less on bottom-up data and more on top-down reasoning that closely resembles the way humans approach problems and tasks. Achieving MCS will fundamentally change the AI space, allowing AI applications to make decisions under unique environmental conditions, learn from new situations, and communicate naturally with people.

Discussion

True machine consciousness is likely (56-70%) several decades from being realized. A significant obstacle in the pursuit of machine consciousness is both the lack of a universally accepted definition of consciousness and a construct to determine consciousness through behavioral observations. [H] In other words, if we are not able to understand how AI processes information, we will never be able to assess consciousness of AI objectively. [M]

Academic research has thus focused on the more attainable goal of developing machine common sense. Current AI functionality lacks human common sense. Humans do not explicitly express common sense because there is no need to state the obvious. [H] Humans are usually not conscious of the commonsense assumptions that underlie every statement and action. [H] This tacit background knowledge includes intuitive physics, intuitive psychology, and an understanding of the common facts that an average adult possesses. [H] Machines not only lack this basic background knowledge, but the pervasive nature of common sense makes it difficult to articulate and encode in machines. [H]

The two most promising research paradigms are mining data from the world wide web and designing a computational model based on toddler cognition. Mining common sense from massive amounts of data and applying it in intelligent systems, in several respects, appears to be the next frontier in computing. H Developed at Carnegie Melon University, M NELL and NEIL scour the internet 24 hours a day to lean though text and image extraction. As shown in Figure 1, mining data uses the NELL and NEIL data mining techniques to crawl the web constantly. H The inputs to NELL include an initial seed ontology defining hundreds of categories and relations that NELL reads about and 10 to 15 seed examples of each category and relation. H Given these inputs and access to the Web, NELL runs continuously to extract new instances of classes and relations. H The primary drawback to this technique is the lack of flexible, perceptually grounded concept representations, like those found in human cognition. H

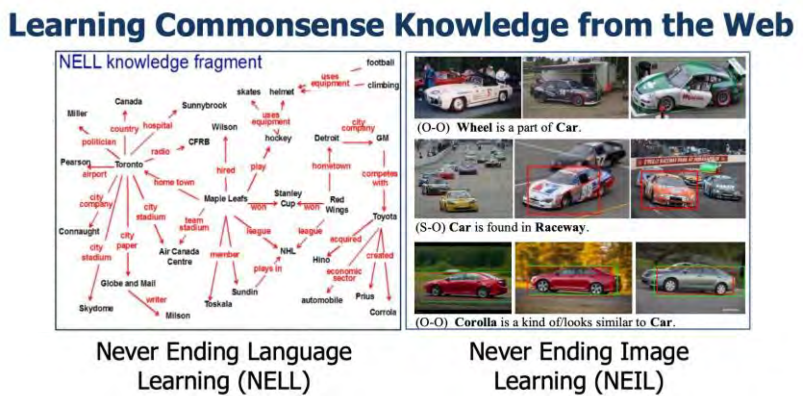
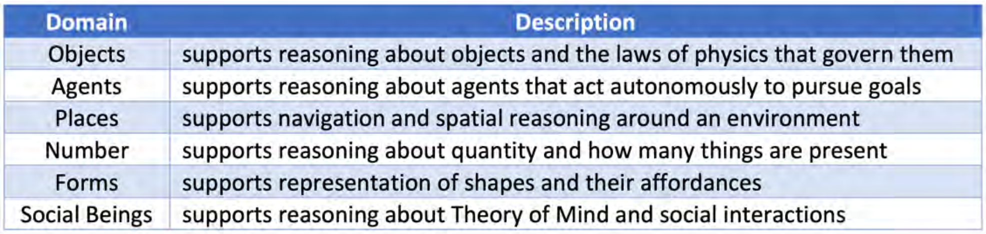


Figure 10: Learning MCS From the Web. Click on figure or got to *https://www.darpa.mil/attachments/Final-MCS-PD-2018-10-18-prog-page.pdf*

The second promising paradigm is modeling childhood cognition. Led by Dr. Elizabeth Spelke at Harvard University, M childhood cognition researchers have years of experimental results that allow them to map children's cognitive capacities. Cognitive development researchers can provide empirical and theoretical guidance for building intelligent machines that think and learn like children. Psychologists have intensively studied children's knowledge in six domains (see Table 1), and some believe that each of these domains constitutes a distinct and relatively autonomous knowledge system. The Theory of Core Knowledge codifies this idea. H Developmental psychologists agree, however, that abilities to reason about objects, agents, places, numbers, geometry, and the



Domain	Description
Objects	supports reasoning about objects and the laws of physics that govern them
Agents	supports reasoning about agents that act autonomously to pursue goals
Places	supports navigation and spatial reasoning around an environment
Number	supports reasoning about quantity and how many things are present
Forms	supports representation of shapes and their affordances
Social Beings	supports reasoning about Theory of Mind and social interactions

Table 1. Theory of Core Knowledge. Click on figure or got to *https://www.darpa.mil/attachments/Final-MCS-PD-2018-10-18-prog-page.pdf*

social world, as described in the Theory of Core Knowledge, emerge early and serve as crucial foundations for later learning. [H]

Over the next 10 years research indicates the paradigm of AI will shift focus from the artificial component of AI to the intelligence component of AI. [M] AI will rely less on bottom-up data and instead on top-down reasoning that more closely resembles the way humans approach problems and tasks. [M] This general reasoning ability will enable broader application of AI, creating opportunities for early business adopters across new and unexpected activities. [M]

The pursuit of MCS will impact all aspects of AI. If either academic, private sector, or government research can produce a viable MCS service, there are four areas where MCS will likely (56-70%) have the most significant impact. The first is sensemaking. MCS will increase AI ability to interpret and understand real-world situations from remote sensors and data. [H] The second is monitoring the reasonableness of machine actions. MCS will enable AI applications to monitor the reasonableness (safety) of an AI application's actions and decisions, even in novel situations. [H] The third is human-machine collaboration. MCS will enable more effective communication and cooperation between machines and humans. [H] The fourth area is transfer learning (adapting to new situations). MCS will provide the foundation for AI to learn new domains and adjust to new conditions without specialized training or programming. [H] Although information regarding the current research efforts of the sensemaking and monitoring reasonableness of machine actions is scarce, it is reasonable that these will follow the solution of human machine collaboration and transfer learning problem sets. Automated machine learning (AutoML) is a research area that is trying to develop AI applications that can select the best algorithms to analyze new data sets without human intervention. The goal of much of the AutoML research is to automate machine learning and bring efficiency to current human-machine collaboration. [H]

The biggest challenge to MCS development is not fully understanding human cognition and how humans develop common sense. [M] Computer scientists must computationally support any unified theory of cognition. In other words, computer scientists will have to create a mathematical model of common sense to impart this characteristic to the machine. [H] However, if AI is ever to reach a machine consciousness, MCS is the steppingstone to that achievement. University of Sussex and Massachusetts Institute of Technology are two universities researching this problem. University of Sussex is building computational models that aim to explain subjective properties of experience in terms of neural mechanisms as well as developing innovative analysis methods based on information theory to derive ‘measures’ of consciousness. [M] Massachusetts Institute of Technology (MIT) Mind Machine Project goal is to reconcile natural intelligence with machine intelligence, and in doing so develop and engineer a class of intelligent machines. [M] MIT is working to develop a software model capable of understanding human social contexts, the signposts that establish these contexts, and the behaviors and conventions associated with them. [M]

Other approaches utilize virtual and augmented reality (VR/AR) to investigate more 'real world' conscious perception, and in particular to understand how perceptions of the body and the self are formed. Overall, our research draws on a wide range of disciplines from philosophy to mathematics to cognitive neuroscience, generating new insights into one of our oldest problems.

Today's artificial intelligence systems are overly sensitive and fragile. The development of machine common sense would allow researchers to apply AI technology beyond the current boundaries of niche environments. [M] Not only must researchers realize MCS on the way to true machine consciousness, but it is also likely to happen in the next 15 years. [M] Without common sense attributes, machines are limited in their ability to perform basic human tasks such as rational decision-making under unique environmental conditions, learning from new situations, and communicating naturally with people. [H]

Analytic Confidence

The analytic confidence for this estimate is moderate. However, the sources were very reliable and corroborated one another. There was adequate time, but the analyst worked alone and did not use a structured method. Many sources were peer-reviewed academic journal articles, government .mil websites, and respected business periodicals. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Greg Pavlichko

Differential Privacy Highly Likely To Provide Data-Anonymity Enabling Secure and Private Collaboration Across Organizational Boundaries Within 5-10 Years

Executive Summary

Despite policy concerns that implementation of differential privacy would create an overly restrictive standard for data research and that the technique could change data so that it's not reflective of the actual dataset, it is highly likely (71-85%) that differential privacy will become a principal mainstream, modernized approach of cybersecurity to protect personal data at scale in the next 15 years. Differential privacy is a technique that adds noise to data in a very prescribed, mathematically rigorous way that preserves the properties of the overall data while hiding individual identities. This privacy preservation technique has widespread implications for many industries requiring data privacy and security. Efforts by private industry and the US Census Bureau to incorporate this novel solution make this technique viable in the next 15 years.

Discussion

First developed in 2006 by Cynthia Dwork, Frank McSherry, Kobbi Nissim and Adam Smith, differential privacy (also known as "epsilon indistinguishability") [M] seeks to guarantee privacy of data sources. Irrespective of the decision whether to participate, differential privacy gleans applicable information potential data source without direct traceability. [H]

Differential privacy can be thought of as a technique that an algorithm uses for maintaining an individual's privacy. [H] It does this by effectively adding "noise" to data-sets, so that it is impossible to reverse engineer it. [H] (see Figure 1)

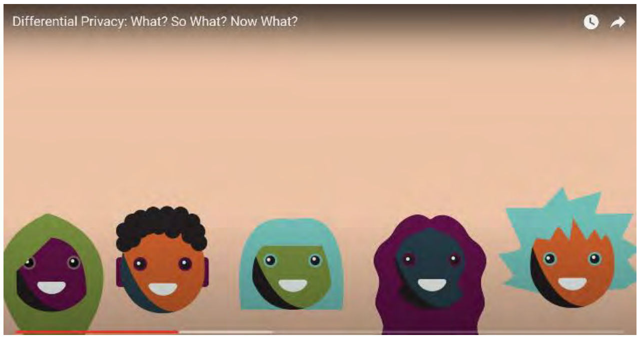


Figure 1. Differential Privacy: What? So What? Now What? Click on picture or go to: https://youtu.be/NRf6sUk1bv0 to view video. Source: UC Berkeley Center for Long-Term Cybersecurity on YouTube.

This differential privacy gives participants (and nonparticipants) in the database a form of plausible deniability: they could always deny that their data was used or even that they participated (or did not participate), and an observer would have almost no evidence either way. [H]

The U.S. Census Bureau is using differential privacy as the method for the 2020 census disclosure control in public use data products, which represents a radical departure from current practice. [H] Differential privacy allows the Bureau to legally guarantee household privacy while using statistics for drawing legislative districts, determining the distribution of federal funds for government programs, and sharing extensively with social scientists. [H]

The European Union [H] and Australia, [H] have adopted or are considering the adoption of differential privacy. The EU is reviewing differential privacy as an emerging standard for companies to ensure privacy when using, storing, and processing data about people. The goal is to give people more control over what companies know about them and standardize those practices across Europe. [H] The Australian Bureau of Statistics is also currently exploring differential privacy methods and synthetic data methods as potential additions to augment their methods of ensuring protecting privacy and secrecy of data providers. [H]

The National Institute of Standards and Technology is reviewing measurements to establish the best algorithms to address concerns that differential privacy may hide some trends or that some of the techniques used could change the data in some way such that it's not reflective of the actual dataset. [H] (see Figure 2)

Figure 2. What is Differential Privacy? Click on picture or go to: https://www.nist.gov/video/what-differential-privacy to view video. Source: NIST.gov

Differential privacy gives the processor significantly more freedom by transforming personal data into aggregate data, allowing a work around to use less restrictive laws governing aggregate data than the laws governing personal data.

Analytic Confidence

The analytic confidence for this estimate is high. Sources were very reliable and corroborated one another. There was adequate time, but the analyst worked alone and did not use a structured method. Many of the sources were peer-reviewed academic journal articles, government .mil websites, and videos by the differential privacy developers. Given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Troy Alexander

Technologically Advanced Militaries Likely To Integrate AI-Driven Ambient Clinical Intelligence Technologies To Augment The Internet Of Military Things By 2027

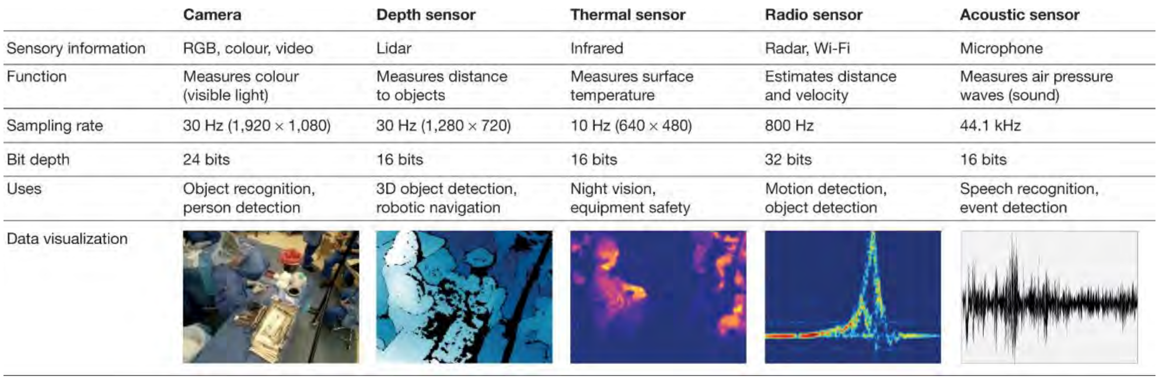
Executive Summary

By 2027, technologically advanced militaries are likely (55-85%) to integrate technological advances in AI-driven Ambient Clinical Intelligence (ACI) to augment the Internet of Military Things (IOMT). ACI leverages contactless sensors embedded in health-care settings to collect data AI machine learning algorithms then processes to make recommendations to clinicians to improve decision making and reduce administrative burdens. Despite persistent patient mistrust in AI generated medical recommendations, ACI has potential for military adaption to improve interrogations, interviews, tactical questioning, detainee monitoring, report writing, and record keeping.

Discussion

Ambient Clinical Intelligence (ACI) builds upon Ambient Intelligence (AmI), defined as sensor networks, pervasive computing, and artificial intelligence that create electronic environments sensitive and responsive to the presence of people. These electronic environments provide continuous and unobtrusive monitoring and understanding of actions in physical environments. [H] ACI involves using contactless sensors and contact-based wearable devices embedded in health-care settings to collect data – including imaging data of physical spaces, audio data, or body temperature - coupled with machine learning algorithms to efficiently and effectively interpret this data (see Figure 1). [H] The COVID-19 pandemic accelerated pushes for ACI development due to the additional demand on an already strained healthcare industry resulting in increased documentation burdens, worsened clinician burnout rates, and additional labor shortages. [M]

For voice-base AI audio sensors, ACI developed by Nuance is capable now of capturing and contextualizing multi-party conversations ambiently and distinguishing between the



	Camera	Depth sensor	Thermal sensor	Radio sensor	Acoustic sensor
Sensory information	RGB, colour, video	Lidar	Infrared	Radar, Wi-Fi	Microphone
Function	Measures colour (visible light)	Measures distance to objects	Measures surface temperature	Estimates distance and velocity	Measures air pressure waves (sound)
Sampling rate	30 Hz (1,920 × 1,080)	30 Hz (1,280 × 720)	10 Hz (640 × 480)	800 Hz	44.1 kHz
Bit depth	24 bits	16 bits	16 bits	32 bits	16 bits
Uses	Object recognition, person detection	3D object detection, robotic navigation	Night vision, equipment safety	Motion detection, object detection	Speech recognition, event detection
Data visualization					

Figure 1. Examples of sensor data collection for ambient clinical intelligence

provider, patient, and others - staff, family members - engaging in the conversation. [H] This technology reduces the amount of time doctors spend on administrative tasks such as documenting encounters and frees them to focus on developing care protocols and caring for a greater number of patients. ACI is replacing human medical scribes healthcare providers currently use to create a record of each doctor-patient encounter. And, ACI systems can rapidly and cheaply scale up to meet increasing need, unlike human scribes. [M] Ambient Clinical Intelligence advances during the past two years have moved beyond simple capture of doctor-patient discussions to immediate generation of accurate clinical notes that are properly formatted for direct input into the patient's Electronic Health Record (EHR) (see Figure 2). [H] Army developers could similarly program AI to rapidly create meeting notes, records, and reports that are currently compiled by hand and created by manually by individuals.

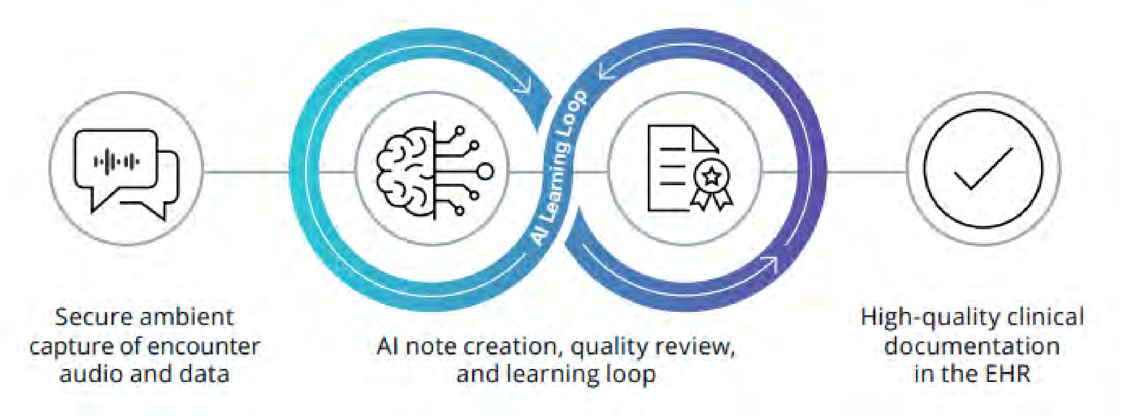

AI Learning Loop
Secure ambient capture of encounter audio and data
AI note creation, quality review, and learning loop
High-quality clinical documentation in the EHR

Figure 2. Examples of Electronic Health Record

Data scientists, researchers, and AI developers are also working to add sensory and signal data to samples of patient voice interactions to detect disease, injury, mental illness, and other insights about the individual. [M] ACI devices are also capable of providing immediate recommendations to support doctor decision making during the exam based on an immediate review of the patient's medical history and analysis of the data collected during the encounter. [H] These technologies have direct applicability in military healthcare settings, including during detainee operations. ACI could assisted interrogators by providing near real-time analysis of detainee biometrics and reporting history to identify consistencies or inconsistencies.

Google and care.ai recently formed a partnership to leverage self-driving car technology to create "Self-Aware Rooms" for monitoring patients in healthcare settings. They seek to "prevent avoidable falls, protocol breaches medical errors, and improve staff efficiency." [M] Each Self-Aware Room is equipped with ambient sensors that combine a machine learning platform and a library of human behavioral data with Google's Edge technology. The Edge AI enables the sensor to monitor behavior and send predictive alerts to the staff that the partnership claims can "monitor, predict, and infer behaviors using billions of data points in real-time." [M] This technology could also be applied in military settings where persistent observations of humans is desired, including detention areas. Ambient clinical intelligence technology could also be leveraged to provide oversight in sensitive areas to prevent abuses like those at Abu Ghraib that could have strategic implications. [M]

Google Health initiatives have progressed their AI ACI on a related healthcare problem – data that often requires manual review because it is complex, unstructured, and unorganized. Google Health leverages advances in natural language processing (NLP) AI to understand the context in which medical notes are written. Using a vocabulary of tens of thousands of medical conditions, Google organizes unstructured data by algorithmically analyzing medical notes. Importantly, sources can be inputted as incomplete sentences, shorthand, or include misspelled words. [M] Amazon's Transcribe Medical seeks to provide similar services to improve efficiency in healthcare. [M] These ACI initiatives, coupled with edge computing, could assist with real-time sorting, categorizing, and understanding captured material following capture and site exploitation. [H]

Analytic Confidence

This is a moderate confidence estimate. The reliability of sources is moderate, information and assessments from multiple sources were consistent, however, theoretical predictions varied and much of the technology remains unproven. Most sources were industry papers and news articles and not peer-reviewed academic journals. And very few sources made predictions on timing for development or adoption of ACI technology.

Author: LTC Patrick Hofmann

Automated Machine Learning Highly Likely To Expand AI Proliferation To Include Widespread Use In Military By 2037

Executive Summary

Despite Automated Machine Learning (AutoML) only recently becoming a focus of research as a derivative of deep learning, a lack of fully functional end products, and a lack of trust in AutoML end to end pipelines, by virtue of automated machine learning reducing human involvement in the development of machine learning algorithms, the development and identification of four important process engines, and reducing barriers to entry, it is highly likely (71%-85%) that AutoML will expand AI proliferation across multiple sectors to include the military by the year 2037. AutoML is a subfield of deep learning where the AI optimizes the machine learning models with little or no human in the loop. AutoML reduces the need for data scientists, increasing availability of artificial intelligence and machine learning to sectors and industries that do not have a high density of previously required skillsets.

Discussion

Automated machine learning is a relatively new field of research, a subset of deep learning, that is driven by both academic and industry interest. [H] AutoML research is focused on how to improve computer vision, data mining and natural language processing. [H] As shown in Figure 1, AutoML designed to automate methods for model selection or hyper parameter optimization. [H] AutoML significantly improves the efficiency of Machine Learning and has achieved considerable successes in recent years.

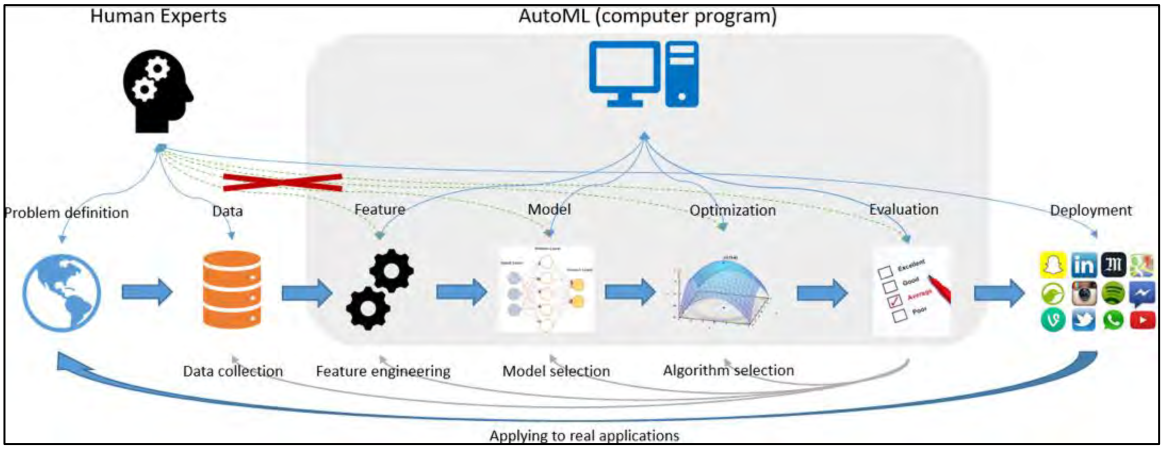


Figure 11This picture shows a typical pipeline of machine learning application, and how AutoML can get involved in the pipeline and minimize participation of humans. Click on figure or got to- https://arxiv.org/pdf/1810.13306.pdf?ref=https://githubhelp.co

AutoML is currently divided into two classes of quality and functionality. The first class is fully functional existing in the research/ academic sector. [H] The other quality type is AutoML produced in the commercial sector, partially functional but producing appropriate end products. [H] Since the results from fully automated products show inconsistency, public users have largely used only semi-automated products. [H] A fully automated industry-standard product with user friendly interface is still missing in this domain. [H]

Not much research exists about user trust in AutoML systems and products. [H] Trust is defined as a willingness to deploy a model produced using automated methods. [H] AutoML pipelines are not unfirmly transparent from end to end, reducing trust in the capability. However, initial academic research indicates that transparency in all steps of the process is critical to achieving trust. AutoML designers and system builders need to present the pipeline steps and decisions made in each of those steps along with the model generation process. [H] This rationale implies AutoML users demand higher transparency from AutoML systems. [H]

As shown in Figure 2, a typical AutoML system will contain four important components overseeing four important tasks of the automated workflow, however in a more commercial oriented system there can be more than these four components. The important components that were identified are [H] the preprocessing engine, the feature engine, the predictor engine, and the model selection and ensemble engine. The preprocessing engine cleans and transforms the data so that subsequent parts of the workflow run smoothly. [H] The feature engine preforms the important process of identifying and engineering the features of the dataset. This includes feature extraction, feature selection, dimensionality reduction, linear manifold transformations, and clustering for unsupervised learnings. [H] The most important component of an AutoML system is the predictor engine. The predictor engine creates the machine learning model to be trained and evaluated in the automated process. [H] The ultimate goal of this engine is to find the best candidates of hyperparameters and learning algorithms to be passed to the next engine. [H] Lastly, the model selection and ensemble engine choose the best prediction algorithm from a pool of candidates from the predictor engine. [H]

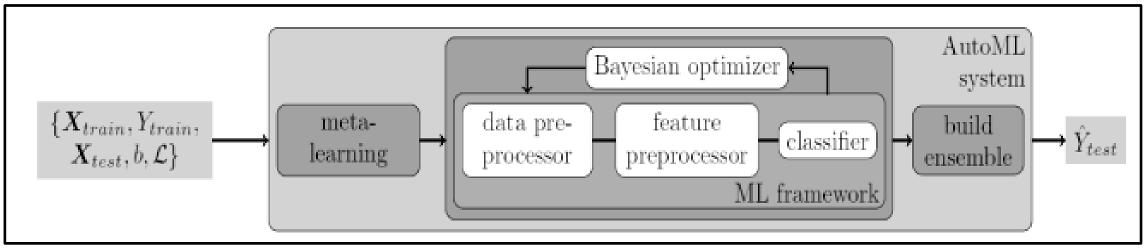


Figure 12 Typical Design of an AutoML system. Click on figure or go to- http://dlib.iit.ac.lk/xmlui/bitstream/handle/123456789/416/Naga.pdf?sequence=1&isAllowed=y

Designing an effective learning model is often tedious and only done well by experts with deep knowledge of machine learning algorithms and domain expertise. [H] AutoML, AI methods generate and optimize machine learning models by automatically engineering features, selecting models, and optimizing hyperparameters. [H] The automatically searched architectures have been used in tasks such as object detection and image classification and have achieved unexpected competitive performances on these filed. [H] The continued automation of the data science field is a catalyst for AutoML adoption and in certain instances, these automated methods produce better results than people. [H] Given the current shortage of data scientists in the profession, automated techniques hold much promise for either improving the productivity of current data scientists or replacing them outright, thus reducing the barrier to entry for many sectors. [H]

Although the goal of AutoML research is complete automation of the machine learning process, this has proved to be very challenging task even after the current technological advancements. [H] In the future, more researchers will focus on this area to design more efficient algorithms and accelerate their applications to solve real-world issues. [H] Moreover, the increasing requirement of hardware for strong computing power could also be the research emphasis in both academic and industry field. [H] However, if academic and industry research maintains its current level of interest and some of the fundamental issues discussed above are solved, it is highly likely (71%-85%) that AutoML will expand AI proliferation across military applications by the year 2037.

Analytic Confidence

The analytic confidence for this estimate is moderate. Sources were very reliable and corroborated one another. There was adequate time, but the analyst worked alone and did not use a structured method. Many of the sources were peer-reviewed academic journal articles and industry websites. However, given the nascency of this field of research and given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Gregory J. Pavlichko

Within 5-10 Years Internet Of Things Technology Will Likely Provide Organizations Ability To Monitor, Control Increasingly Complex Operating Environments In Real-Time

Executive Summary

Over the next 5-10 years, despite the security concerns and the challenges of analyzing the large amounts of data associated with current Internet of Things (IoT) systems, the use of IoT technology will continue to expand and likely (55-80%) provide organizations the ability to monitor and control increasingly complex operating environments in real-time. This expansion will be due to the rapid improvement in Artificial Intelligence (AI), specifically Deep Learning Neural Networks (DNN) and analog computing.

Discussion

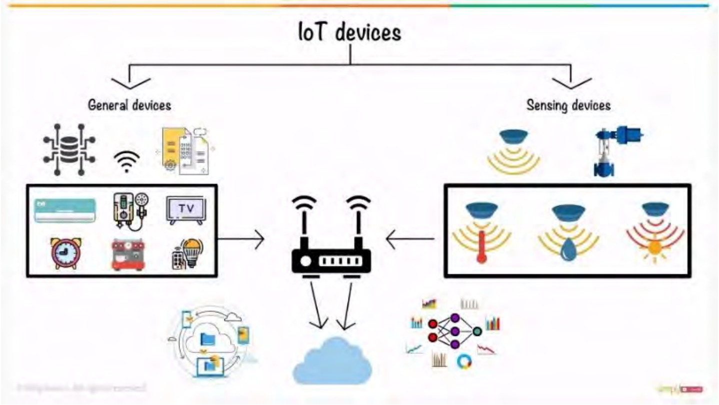


Figure 13. IoT Explained in 6 Minutes | How IoT Works. Click on picture or go to: https://www.youtube.com/watch?v=6mBO2vqLv38 to view video. Source: Simplilearn channel on YouTube.

The term IoT (see Figure 1) is used to describe the billions of devices across the globe that are connected to the internet. [M] IoT Analytics estmated that the number of IoT devices reached 12.3 billion in 2021 and will expand to 27 billion by 2027. [M] According to Statistica.com, estimated spending on IoT technology worldwide in 2020 was $749 billion US dollars. Furthermore, Statistica.com estimates that global spending will increase to $1.1 trillion by 2023. [M] Additionally, a report by the International Data Corporation estimates that discreet manufacturing, process manufacturing, and transportation will account for 33% of spending, while the consumer market, such as smart homes and connected cars, will account for another 16.8%. [M]

A basic IoT system consists of IoT devices, such as sensors or microcontrollers, an IoT hub or gateway that transfers the data to and from the devices, and a system to analyze data and make decisions. [M] A human or AI can conduct the data analysis and make decisions, which can be done at the edge or in the cloud. [M] A simple example of an IoT system is a smart home.

A smart home is an IoT system that uses sensors, devices, and smart appliances in the home to collect data and enable the homeowner to analyze smart home data and control the system of devices using a mobile phone or computer. [M] The system typically connects devices using the homes Wi-Fi network, and the homeowner can control the smart home from any location in the world using a mobile phone. While the homeowner controls the overall smart home system, increasingly sophisticated smart appliances can also act autonomously. [M] For example, a smart fridge can automatically reorder groceries and a smart thermostat can turn-on the heat based on the homeowner's location that can be monitored through the homeowner's mobile phone. [M] As IoT devices become more sophisticated, they will allow users to monitor and control increasingly complex operating environments. Advances in AI DNN and analog computing will drive the development of the increasingly sophisticated IoT smart devices that will be able to increase the speed of AI calculations at reduced energy consumption at the edge and in the cloud (see Narrow AI and Analog Computing).

A challenge that impacts the expanded use of IoT tech in complex operating environments is the large amounts of data collected by the sensors, which needs to be collected, stored, and analyzed. [M] As a result, advancements in the use of AI to analyze large amounts of data will be critical to the expanded use of IoT in increasingly complex operating environments. In the area of autonomous vehicles, the company Tesla is already doing this.

Tesla has been able to combine sophisticated AI and IoT technology to create the autopilot feature for its electric vehicles where it uses 24 sensors and cameras to monitor the car and surrounding environment combined with an advanced AI system to analyze data and control the vehicle in real-time. [M] However, while Tesla has one of the most sophisticated autopilot features available in a commercial vehicle, it still requires the driver to stay alert and be prepared to take control. [M] The ability to process the large amounts of real-time information from the IoT vehicle sensors to control the vehicle would not be possible without Telsa's sophisticated AI system. [M] In order to replicate this sophisticated IoT system in other areas, organizations must develop equally sophisticated AI tailored to their unique complex operating environment.

Another challenge that impacts expanded use of IoT systems is security. With the rapid expansion of the types and numbers of IoT devices, most device makers have focused on creating cheap, intelligent devices that meet customer demands with little consideration for security of the devices. [M] An example where the security problems inherent in many IoT devices manifested itself is the Mirai botnet Distributed Denial of Service (DDoS) attack that targeted companies, such as Etsy, Github, Netflix, Shopify, and Twitter, among others. [M] The attackers exploited inherent security vulnerabilities in IoT devices to create a large botnet to conduct the DDoS attack. [M] The importance of security will increase as IoT systems are used in more complex operating environments, such as the control of traffic and medical devices, where a security incident could cause significant damage or loss of life. Therefore, inherent security vulnerabilities will need to be addressed before IoT systems can expand significantly in complex operating environments. To address the security challenge, device makers need to build devices with security built-in from the beginning of product development, ensure systems can be upgraded to patch vulnerabilities that may surface, ensure devices use strong encryption, and avoid setting default passwords for devices. [M]

Analytic Confidence

The analytic confidence for this estimate is moderate. Sources were reliable and tended to corroborate one another. There was adequate time, and the task was not complex. Despite the lengthy time frame of the estimate, this report is not sensitive to change due to new information.

Author: COL Anthony Pollio

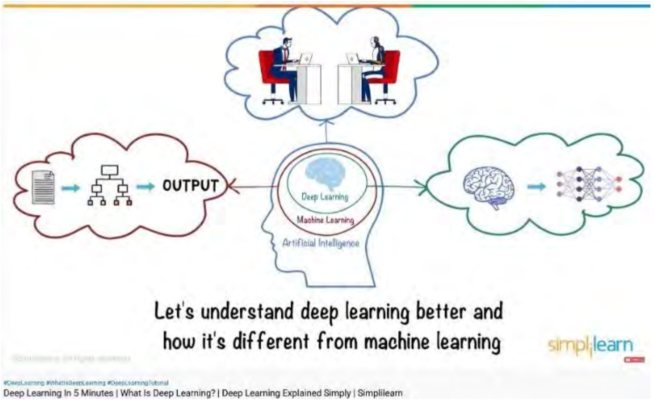
Within 10-15 Years Advancements In Neural Network Architectures Will Likely Enable Rapid Improvements In Deep Learning To Conduct “Narrow” AI Predictive Analysis

Executive Summary

Within 10-15 years, despite the ethical concerns associated with Artificial Intelligence (AI), there will likely (55-80%) be a significant improvement in narrow AI’s ability to conduct predictive analysis. AI’s improvement in these areas will be due to its ability to leverage increasingly large data sets generated by the Internet of Things (IoT) and the use of increasingly sophisticated Deep Learning (DL) neural network architectures.

Discussion

The National Institute of Standards and Technology defines AI as “software and/or hardware that can learn to solve complex problems, make predictions or undertake tasks that require human-like sensing (such as vision, speech, and touch), perception, cognition, planning, learning, communication, or physical action.” [H] At the top level, there are two broad categories of AI. General AI, also known as strong AI, refers to the ability to operate across a wide range of tasks; while narrow AI, also known as weak AI, is tailored to perform a specific function. [H] Many AI experts believe that general AI systems are decades away. In a 2019 survey, 32 AI researchers were asked when general AI would surpass the level of human congnition, known as the singularity; 41% predicted it would occur betweem 2036-2100 and 38% predicted it would occur after 2100 or it would never occur. [M]



Let's understand deep learning better and how it's different from machine learning

#DeepLearning #WhatIsDeepLearning #DeepLearningTutorial
Deep Learning In 5 Minutes | What Is Deep Learning? | Deep Learning Explained Simply | Simplilearn

Figure 14 Deep Learning in 5 Minutes. Click on picture or go to: https://www.youtube.com/watch?v=6M5VXKLf4D4 to view video. Source: Simplilearn Channel on YouTube.

While general AI may not be available for decades, the field of narrow AI continues to make significant progress. Within narrow AI, one area of progress is DL, which is a subset of machine learning (see Figure 1). Deep learning uses unsupervised neural networks to analyze large data sets of unlabeled, unstructured data to provide predictive analysis. [M] In reference to DL, neural networks are a series of algorithms used to identify relationships in data sets by simulating how the human brain’s neural networks operate. [M] The development of new neural network architectures is one reason there will likely be a significant improvement in AI’s ability to conduct predictive analysis in the next 5-10 years. An example of this is the DeepMind AlphaFold project's recent application of new neural network architectures to accurately predict 3D models of protein structures for approximately 100 million known proteins to atomic accuracy, which is a problem that scientists have been trying to solve for 50 years. [HH]

DeepMind is also using a further evolution of the AlphaFold neural network technology as part of their MuZero project, which is designed to play games like Go, Chess, and Atari. [H] However, in late 2020, the US Air Force was able to build an AI system using MuZero to create an AI co-pilot on a U-2S aircraft that included tactical navigation responsibilities for the plane. [H] This demonstrates that these new neural networks can be applied to a wider range of applications, if the large amounts of data required to train them exists.

Since DL relies on large data sets to train the neural networks to perform a particular function, another driving factor for the rapid improvement of DL in the next 10-15 years is the significant increase in data collection across a wide range of areas driven by IoT technologies. [M] As the IoT begins to generate large data sets for a wider variety of operational environments, it will likely enable organizations to apply new DL neural network architectures to a wider array of challenges (see IoT).

Ethical concerns, such as privacy and bias, are two issues that may drive government oversight that impacts improvements in AI predictive analysis. With no government oversight, organizations are beginning to use AI predictive analysis systems to make decisions relating to health care, creditworthiness, criminal justice, and employment, which can have a significant impact on people's lives. [M] In the area of bias, the concern is that biased data will cause the AI system to skew results that may cause inequities or discrimination in decision making. [H] Privacy concerns revolve around the increasing ability of organizations to collect and analyze personal information that could impact individual rights and privacy. [M]

Analytic Confidence

Overall analytic confidence in this estimate is moderate. The analyst had adequate time and the task was simple. The analyst has high confidence in the evaluation of DL and neural network technologies. However, the analyst confidence in the timeline is moderate. The development timeline will depend on how quickly organizations can adapt neural network architectures to new operational environments that will require access to large datasets that may need to be developed. The timeline may also be impacted by future government legislation to mitigate ethical concerns.

Author: COL Anthony Pollio

Within 5-15 Years Advancements In Analog Computing Will Likely Enable Faster AI Computing At Reduced Costs And Energy Consumption

Executive Summary

Within 5-15 years, despite their lack of precision and susceptibility to electromagnetic noise in the environment, analog computing will likely (55-80%) enable faster Artificial Intelligence (AI) computing at reduced costs and energy consumption. Analog computing's ability to enable these improvements will be due to the development of hybrid analog/digital solutions powering Deep Neural Networks (DNN).

Discussion

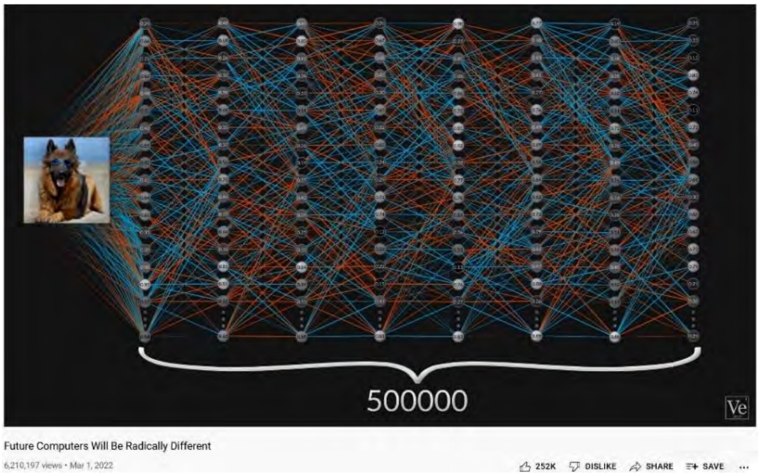

500000
Ve
Future Computers Will Be Radically Different
6,210,197 views • Mar 1, 2022
252K
DISLIKE
SHARE
SAVE

Figure 15. Future Computers Will Be Radically Different. Click on picture or go to: https://www.youtube.com/watch?v=GVsUOuSjvcg to view video. Source: Veritasium Channel on YouTube.

A digital computer "performs calculations and logical operations with quantities and logical operations represented as digits, usually in the binary number system." [H] Most of today's computers are digital. However, there are also analog computers, which predate digital computers. An analog computer uses numerical data that is represented by measurable continuous physical variables, such as voltage, temperature, or current. [H] An early example of an analog computer is the tide-predicting machine developed by William Thomson in 1872. Thompson realized that many astronomical variables effected the tide and developed a mechanical device that simulated these variables to accurately depict tidal conditions. [H] Some observers believe that analog computing is better suited for specific applications, such as completing complex matrix multiplication calculations for AI DNN, where analog systems can complete calculations much faster with significantly less energy consumption (see Figure 1).

One challenge with a traditional digital computer is that it has a compute section and a memory bank; moving data back and forth between the sections significantly increases the time and energy required to complete the larger number of calculations required for AI DNN systems.[MM] As opposed to a digital computer, an analog computer can complete the large number of matrix mathematical calculations in parallel and directly in system memory, which makes it faster and more energy efficient.[MM] One drawback to analog computing is that it is susceptible to electromagnetic noise in the environment that can impact the precision of the calculations. [M]

Mythic is one of the few companies that is applying analog compute-in-memory technology to power DNNs that are faster and more energy efficient for edge AI applications, such as video security, commercial drones, and manufacturing product inspection.[MM] The Mythic solution overcomes the analog computing noise problem by creating a digital/analog hybrid system that converts data from analog to digital at certain steps in the process to prevent the signal from becoming distorted to a point where it may impact the accuracy of the calculations.[MM] Additionally, since the large number of matrix multiplications required in DNNs do not require a high degree of accuracy, Mythic's analog computer chips provide an acceptable level of precision. [M]

Princeton University and IBM are also exploring the use of analog computing to power DNN. In partnership with academic institutions in the U.S., Europe, and Asia, IBM is researching analog in-memory computing for DNN systems, such as natural-language processesing, that the company believes will provide a hundredfold performance improvement over current state-of-the-art digial accelerators and consume significantly less power. [M] While Princeton University has designed a new in-memory analog computing chip that is noise tolerant, can be integrated into existing digital systems, and will enable edge DNN systems for self-driving vehicles, image recognition, and language translation. [M]

While Mythic has fielded a commercial version of their analog computing system, most organizations pursuing analog computing for DNN are still in the research and development phase. The 5-15 years estimate is based on the S-curve model used to describe technology adoption, which when applied to previous innovations indicates that it typically takes approximately 5-15 years to move from the early adopter phase to the saturation phase. [M]

Analytic Confidence

Overall analytic confidence in this estimate is moderate. The analyst had adequate time and the task was simple. The analyst confidence in the timeline is moderate. The development timeline will depend on how quickly organizations can move the technology from research and development to commercially available products.

Author: COL Anthony Pollio

Section 4: Three Factor Trust

Artificial Intelligence And Machine Learning Will Highly Likely Create A Data-Sharing Mindset By 2030

Executive Summary

Regardless of continuous attempts to breach and manipulate data, supervised and unsupervised Artificial Intelligence models will highly likely (80-95%) increase the trustworthiness and confidence in datasets. However, growing a robust technical workforce to support a coalition data-sharing system will highly likely take eight to ten years which will promote a data-sharing mindset.

Discussion

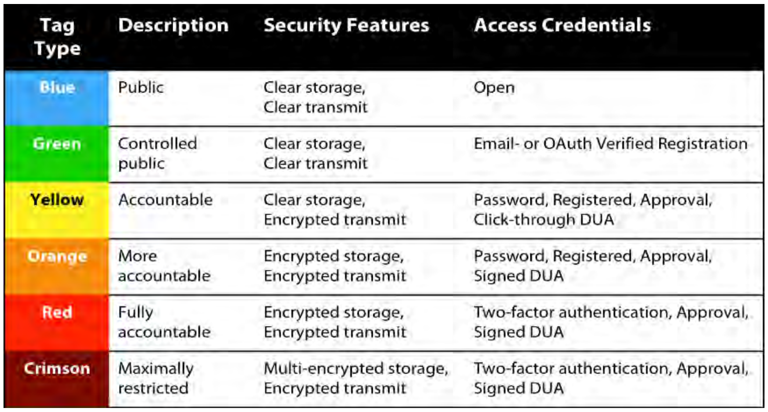
According to Lydia Clougherty Jones, senior research director in Gartner’s Data and Analytics Group, a data-sharing mindset is critical because “when you share data, you’re able to generate more robust analytics and…demonstrate and drive more value…Data plays an enormous role in driving better relationships with employees and better relationships with customers.” These improved relationships could easily translate to industry, allies, and partnerships. [M]

Cost of a Data Breach Report 2021

IBM

Figure 1. Cost of a Data Breach Report 2021, click on the picture or go to https://mediacenter.ibm.com/id/1_br28czad. Source: IBM.com.

Psychologically industries and governments are risk-averse to place their trust and confidence in other organizations’ ability to protect their data and are afraid of the consequences of incorrect data being shared. [M] One reason contributing to reluctance in sharing data is that it could lead to a costly data breach. In 2020, IBM and Ponemon Institute published a report on the insights from 537 data breaches: worldwide resulting in $3.86 million lost and $8.64 million per incident, specifically for the U.S. The report also stated that the average time to contain a breach took 280 days once discovered. The report explains that AI, automation, and a ZT approach can reduce losses from a breach. [H] (see Figure 1; 2021 update statistics) Additionally, the authors of *Sharing Sensitive Data with Confidence* explained how the employment of datatags would also provide the



Tag Type	Description	Security Features	Access Credentials
Blue	Public	Clear storage, Clear transmit	Open
Green	Controlled public	Clear storage, Clear transmit	Email- or OAuth Verified Registration
Yellow	Accountable	Clear storage, Encrypted transmit	Password, Registered, Approval, Click-through DUA
Orange	More accountable	Encrypted storage, Encrypted transmit	Password, Registered, Approval, Signed DUA
Red	Fully accountable	Encrypted storage, Encrypted transmit	Two-factor authentication, Approval, Signed DUA
Crimson	Maximally restricted	Multi-encrypted storage, Encrypted transmit	Two-factor authentication, Approval, Signed DUA

Figure 2. Definitions for each of six ordered Blue to Crimson sample datatags., click on the picture or go to https://techscience.org/a/2015101601/. Source: Technology Science

added security and access features for sensitive data that requires restrictive sharing. (see Figure 2) Datatags reduce the complexity of data-sharing regulations and policies through tags by enabling AI to sift appropriate and legally releasable information. [H] Therefore, advances and implementation of AI, ML, ZT, datatags, and other monitoring tools with human validation will highly likely increase confidence and trust encouraging acceptance and participation in a coalition data sharing system.

The financial and healthcare industries lead the world in data sharing through established and enforced regulations and policies to establish transparency, trust, and confidence in the data and systems that store and process the information. [M] According to Lydia Clougherty Jones, "Data sharing is the way to optimize higher-relevant data, generating more robust data and analytics to solve business challenges (see Figure 3) and meet enterprise goals. [M]

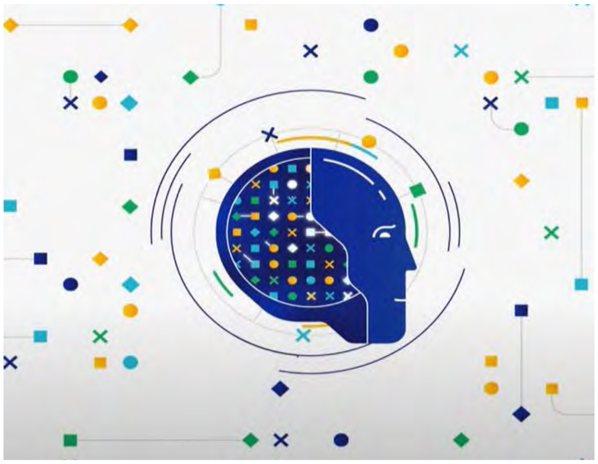


Figure 3. Visa's A.I for Payment Authorization and Fraud Detection. Click on the picture or go to: https://youtu.be/96k0sncyoXA to view the video. Source: usa.visa.com

This logic applies to governmental organizations and their need to share data. Financial and health industries use Artificial Intelligence (AI) systems and Machine Learning (ML) algorithms to detect malicious behavior and signs of data manipulation. [M] Discussion of AI use in the financial industry started in April 2011 with little momentum and took seven to ten years to adopt. [M] In December 2018, the Treasury Department and federal banking regulators encouraged the use of AI fraud detection to prevent anti-money laundering. [M] As the government and industry invest in AI and ML technologies to detect and prevent data manipulation and breaches, it will highly likely improve trust and confidence in global data sharing.

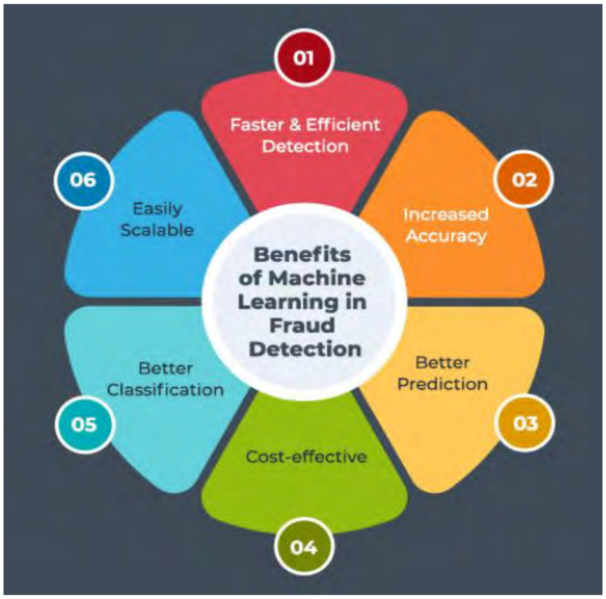


Figure 4. Benefits of using Machine Learning and AI in Preventing Frauds. Click on the picture or go to https://www.analyticssteps.com/blogs/how-ai-used-fraud-detection. Source: analyticsteps.com

During a telephonic interview with the Discover Financial Director AML Compliance FIU, Darci Cavanaugh commented on leveraging AI systems to create efficiencies saving time and money by increasing the speed of validation and security while reducing risk (see Figure 4). However, she stated that the AI requires periodic testing and human feedback to confirm proper operation. To be successful, she recommends establishing a coalition design group to identify requirements.[H] (For complete interview notes, see Annex C) In addition, Peter Millar, Director, Technology Application ACL Services Ltd stated "continuous monitoring with analytics (see Figure 5) in all operations" is critical. [M]

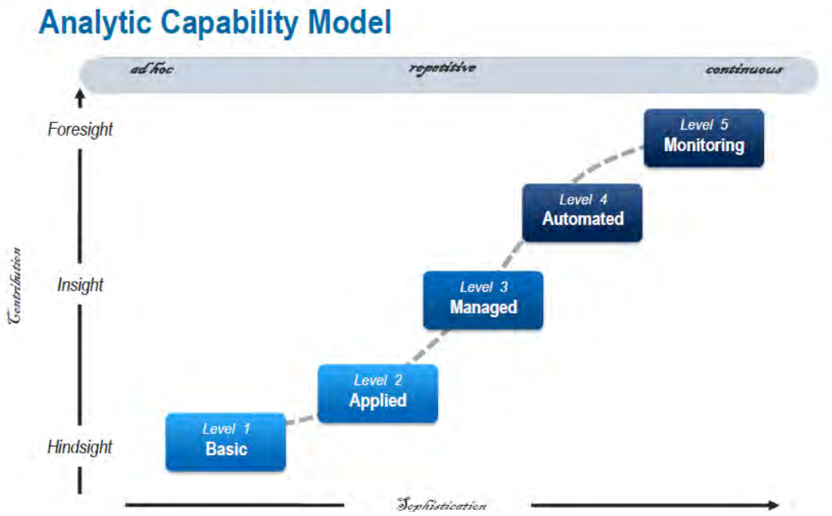


Figure 5. Data Analytic Capability Model for Fraud Detection. For full presentation, click on the picture or go to Great Expectations: How to Detect and Prevent Fraud Using Data Analysis. Source: ACL Services

COVID 19 drove Biobanks to develop data-sharing solutions connecting laboratory scientists, researchers, doctors, and data scientists in a standardized, collaborative, and virtual ecosystem called Laboratory Information Management System (LIMS). LIMS facilitated the "discovery and validation of disease markers and therapeutic strategies," proving existing trust and confidence in data sharing. [M]

Sharing data creates vulnerabilities where malicious insiders abuse privileged access to manipulate critical data. Discovering and tracking data manipulation is difficult and erodes trust and confidence for those who could provide better quality and various data types. Without various inject points, analyzed information is limited. Methods to protect against manipulation are endpoint detection, response tools, tracking real-time changes to files, integrity monitoring tools, and Zero Trust (ZT) methodology. [M]

Analytic Confidence

The analytic confidence for this estimate is moderate. Sources ranging from 2015 to 2022 were reliable and tended to corroborate. The interview with Darci Cavanaugh discussed methods currently used by Discover Financial Institute, which aligns with the research. There was adequate time, and the task was not complex. Despite the lengthy time frame of the estimate, this report is not sensitive to change due to new information.

Author: LTC Nicole Y. Shadley

There Is Roughly An Even Chance Enduring Distrust In Artificial Intelligence Systems Will Cause Large Organizations To Adopt Explainable AI Principles While Integrating New AI Technologies

Executive Summary

The rapid advances in artificial intelligence capabilities and presence in people's daily lives has not yet resulted in widespread trust of AI systems. There is a roughly even chance (45-55%) that organizations using advanced AI will also have to implement Explainable AI (XAI) technical and process approaches to reduce distrust in new AI systems. Despite current reservations regarding biases and opaque decision making, trust in AI is likely to build when Explainable AI and Ethical AI concepts are built into the model.

Discussion

Even as Artificial Intelligence becomes more ubiquitous in daily life, low levels of trust in the technology remain. In one study, less than 30 percent of respondents felt comfortable with businesses using AI when interacting with them. [M] While in another study, 67% of CEOs reported they do not have high trust in AI recommendations for their business. [M] In a Deloitte survey, 67% of executives reported they were not comfortable using data from their companies' advanced analytics systems. [H]

In the medical field, AI has proven to be cheaper while outperforming human clinicians, however, patients do not fully trust the AI-generated recommendations. [H] For important decisions like healthcare, studies showed that people did not trust AI recommendations because patients did not understand how AI algorithms generated their medical recommendations and patients did not believe there was the same level of accountability for AI if a recommendation was wrong. [H]

The Oxford Internet Institute wrote that "distrust in AI could be the biggest dividing force in society." To remedy this, they developed three recommendations to improve people's trust in AI. First, people need more hands-on experience with AI in everyday life. [M] Second, the institute recommends regularly releasing top-level insight into how algorithms make decisions believing this understanding will alleviate enduring distrust. Third, the institute's research showed that people who had some additional control to modify algorithms were more trusting of the AI results. [H] Providing this control could also build trust.

In a 2022 Harvard Business Review article, "Overcoming the C-Suite's Distrust of AI," Andy Thurai and Joe McKendrick recommend four focus areas and actions to increase executive confidence in AI. [M] They recommend creating reliable AI models that deliver consistent insights and recommendations, avoiding data biases that skew recommendations, making sure AI decisions are ethical and moral, and understanding AI well enough to explain the decisions. Several of these recommendations depend on quality data inputs to ensure the algorithms are trained free from human biases. Investing in developing quality synthetic data [M] and data debiasing tools can support these goals. [M]

Brianna Lifshitz's research published in the Georgetown Security Studies Review makes a similar argument to build trust by removing bias from AI. Lifshitz argues this problem has broader national security implications by eroding trust in public institutions. She makes three technical and policy recommendations. First, Lifshitz recommends reworking algorithms and training data similar to other authors referenced in this article. Second, she also emphasizes more explainability, which is covered in the next paragraph. Lastly, Lifshitz recommends promoting intersectional hiring to improve workplace diversity and the resulting social change will reflect in the algorithms. [M] Her research shows a "diversity crisis" in AI – only 2.5% of Google's workers are black while Microsoft and Facebook are both at 4%. [M]

Explainable AI (XAI) is a concept that attempts to purposefully design AI to add transparency to decision making. [M] DARPA describes this as, "the ability to explain [AI systems] rationale, characterize their strengths and weaknesses, and convey an understanding of how they will behave in the future with the ultimate objective of producing explainable models that people can trust. [H] Figure 1 below illustrates opaque AI and XAI models.

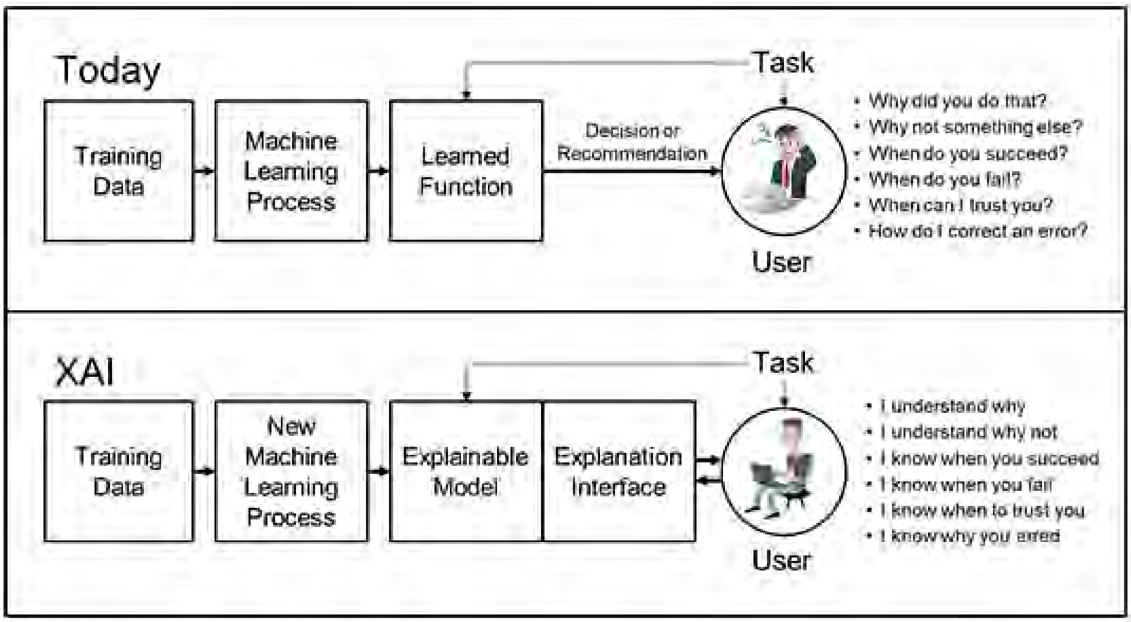


Figure 1. XAI Concept. Source: DARPA.

Relatedly, Deloitte recommends six “Dimension of Trustworthy AI” specifically for AI in government, including 1. Fair and impartial AI, 2. Transparent and explainable AI, 3. Responsible and accountable AI, 4. Safe and Secure AI, 5. Privacy focused AI, and 6. Robust and reliable AI.[H] These recommendations specifically for government application are well-nested with the broader AI recommendations covered previously.

Analytic Confidence

This is a moderate confidence estimate. The reliability of sources is moderate, information and assessments from multiple sources were consistent, however, theoretical predictions varied, and the research is sometimes conflicting. Most sources were industry papers and news articles and not peer-reviewed academic journals. Very few sources made predictions on duration for culture changes or assessed effectiveness after implementation.

Author: LTC Patrick Hofmann

Cancelable Multimodal Biometrics Based On Deep Learning Likely To Improve Scalable, Dialable Rapid Mission Partner Data Sharing By 2030

Executive Summary

Technologically advanced militaries are likely (55-80%) to incorporate cancelable, multimodal biometric systems based on deep learning to achieve rapid, versatile, and dialable[12] compartmentalized information access by 2030. Advancements in artificial intelligence and machine learning increase security concerns of privacy and protection of personal data. Cancelable biometrics management is equivalent to key or pin code management in information security. If a key or pin is compromised, it can be replaced. Cancelable biometrics allows the algorithms associated with a subject's biometric template to be replaced if compromised. Despite challenges of rapid cancelable biometric registration prior to authentication access, recent rapid advancement of biometric technologies for personal authentication, cancelable biometric templates will likely be implemented to mitigate challenges such as theft, spillage, and counterfeiting.

Discussion

Numerous types of biometrics are generally known, and their authentication application and their uses are expanding exponentially; however, biometric authentication has vulnerability drawbacks in the form of leakage or theft. M Proposals such as "cancelable biometrics"[13] are emerging as solutions to secure biometric patterns (see Figure 1). H

Figure 1. Univ. at Buffalo Cancelable Biometric Project seek solutions to secure biometric patterns. Click on picture or go to: https://www.buffalo.edu/cubs/research/projects/cancelable-biometrics.html to read more. Source: Univ. at Buffalo Center for Unified Biometrics and Sensors.

Cancelable biometrics researchers H are aiming at methods to take a biometric image and distort or transform the template in such a manner that it becomes too difficult to obtain the original biometric image from the distorted one (see Figure 2). Additionally, a significant characteristic of a cancelable biometric image is that it can be reissued if compromised. H Should compromise occur, the cancelable biometric feature distortion characteristics are replicable with the original biometrics get mapped to a new template, and subsequently used.

[12] Diable refers to leveling up and down clearance access in near real-time, ranging across Confidential, Secret, Top Secret, etc.

[13] The neologism "cancelable biometrics" describes the deliberate, systematically repeatable distortion of biometric features to protect sensitive user-specific data.

Figure 2. How secure is Biometric Authentication Technology and Biometric Data? Click on picture or go to: https://youtu.be/ZPG3XQhZVII?t=524 to view video. Source: DW Shift channel on YouTube.

Both academic and developer consensus is that cancelable biometric systems must possess four distinctive characteristics: diversity, reusability or revocability, non-invertibility and performance. [H] Diversity suggests that "no same cancelable features can be used across various applications, therefore a large number of protected templates from same biometric feature is required." [M] Reusability/Revocability is the direct revocation and reissuance of cancelable biometric authentication in the event of compromise. Non-invertibility(unlinkability) of template computation is required to prevent unauthorized recovery of original biometric data. Lastly, cancelable biometrics performance formulation should not deteriorate the recognition procedures of a subject. [M]

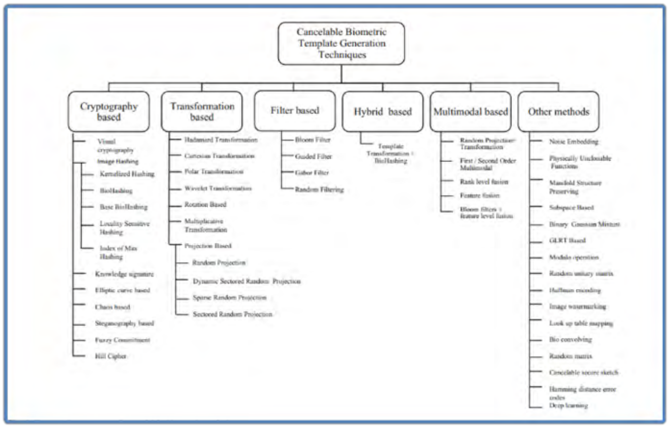


Figure 3. Cancelable Biometric Template Generation Techniques. Click on picture or go to: https://www.researchgate.net/publication/336386976_Cancelable_Biometrics_a_comprehensive_survey to read more. Source: India's National Institute of Technology (NIT).

There are mainly six overarching cancelable biometrics template generation methods. Five that broadly contain approaches with a sixth generally considered for nascent approaches (see Figure 3).

First, there are cryptography-based methods. These methods employ cryptography algorithms for cancelable biometric templates generation. [M] Next, there is "non-invertible transformation" methods. This scheme is one of the earliest methods for generating cancelable biometric templates. In this process, the original biometric templates are morphed by applying different transformations, or minute changes. Typically used with fingerprints, this technique is challenging as a small change in minutiae position of the original fingerprint can lead to a large deviation in minutiae position after transformation. [M]

The third is a filter-based method. Cancelable biometric filters are complex and typically use a “Bloom filter” [M] process. Bloom filter is a space efficient probabilistic data structure representing a set to support membership queries. A challenge is Bloom filter based transformation of any binary feature vector is that it generates irreversible cancelable biometric templates. [M]

Next is a hybrid approach. Hybrid methods merge two or more techniques typically subsequently to create a cancelable biometric template (e.g. cryptography and filter methods). Fifth, multimodal biometrics join several biometric traits with various feature extraction algorithms to produce a layered secure template. Multimodality is achieved by an incorporation of multiple biometric attributes (e.g. combining iris, face, and fingerprint biometrics of same user for identity recognition). The chief advantage of a multimodal biometric system is its reliability, accuracy, security and protectability. [H]

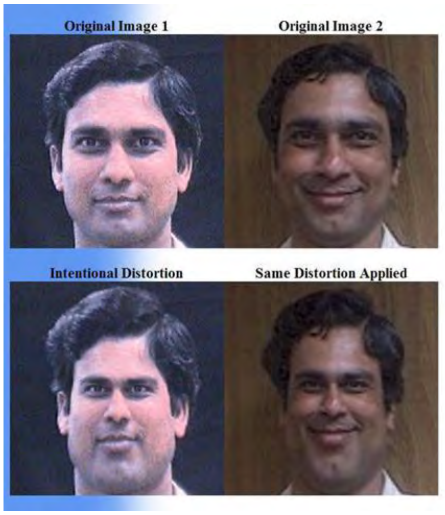


Figure 4. IBM Image of enhancing security and privacy in biometrics-based authentication systems. Click on picture or go to: https://researcher.watson.ibm.com/researcher/view_group_subpage.php?id=1914 to read more.
Source: IBM Research

Other methods are emerging such as: Bio-Hashing (incorporates physical tokens, smart card, USB token, etc.); [H] Bio-Convolving (a non-invertible transforming based approach); Salting Method (an artificial pattern of pure random noise or synthetic pattern are mixed in original binary iris image for generating a cancelable biometric template); and deep learning. [H]

Cancelable biometrics based on deep learning is a nascent, [M] yet effective method and is the latest concept introduced in the field of cancelable biometric template generation methods. Research indicates it will be a secure, multi-biometric system that uses deep neural networks and error-correction coding. [H] Cancelable biometrics using deep learning demonstrates high authentication accuracy, biometric template security and cancelability, fast response times, and cost efficiency are the merits of the presented cancelable biometric system. [H]

Biometric authentication work usually seeks to connect only original biometric templates with commonly used biometric traits (face, iris, and fingerprints); as cancelable biometrics capabilities continue to advance, it is viable for organizations to incorporate its use into system access measures. Several large companies, notably IBM, [H] are increasingly promoting the concept and research of cancelable biometrics (see Figure 4).

[M] The aim is to answer the need for biometrics database privacy such that it can withstand malicious attacks and fast matching of a biometric against a large database of stored biometric readings. [H]

Numerous international universities [H] and government agencies like the National Institute of Technology (NIST) [H] have all taken interest in cancelable biometrics. Hence, this increased focus on cancelable biometrics, driving by emergent artificial intelligence (AI) techniques, particularly deep learning-based, [H] that threaten the future of template protection, [H] will lead advanced militaries to seek cancelable biometric protections.

Analytic Confidence

This is a moderate confidence estimate. The reliability of sources is high, information and assessments from multiple sources were consistent, however, dominant cancelable biometric methodology predictions varied. Despite much of the technology research, resourcing from business is relatively underwhelming and very few sources made overt predictions on timing for incorporation of such capabilities.

Author: COL Troy Alexander

Confidential Computing Will Highly Likely Provide A Data-Protective Environment While Data Is At Rest, In Transit, And In Use, Enabling Secure Collaboration Across Organization Boundaries Within 5-10 Years

Executive Summary

It is highly likely (71-85%) that Confidential Computing will gain broad cross-industry traction to operate at scale in the next 5-10 years. Confidential Computing extends the baseline security guarantees of data encryption at while data is at *rest, in transit*, and in *use.* Despite the lack of a standardized confidential computing frameworks to govern network providers, the business opportunity is extensive. Confidential Computing's potential to address pervasive data security, privacy, and ownership control concerns alongside will drive large IT consortiums to normalize innovative solutions across the enterprise. Confidential Computing has broad applicability across many industries including healthcare, finance, internet of things (IoT), and government. Consortiums such as the Confidential Computing Consortium (CCC), with members including Google, IBM, Intel, Microsoft, and Oracle among others, make adoption of Confidential Computing innovations viable between 2027 and 2032.

Discussion

Cloud data centers and edge computing attacks have significantly increased due to industrialized hacking while most security control implementations are not coherent or consistent to protect data. [H] Confidential computing (see Figure 1) development is an emerging concept in the space of protecting data in use [H] and in early 2022 recognized by the IEEE[14] Computer Society as one of sixteen most significant technology areas emerging. [H]

CONFIDENTIAL COMPUTING
can be used to protect any sensitive or regulated application or data

Figure 16. Promotional Video: What is Confidential Computing? Click on picture or go to: https://youtu.be/Jl2W6G9xfqw to view video. Source: Fortanix channel on YouTube.

In computing, data exists in three states: in transit, at rest, and in use. Data traversing the network is "in transit," data in storage is "at rest," and data being processed is "in use." [H] As computing moves to span multiple environments, from on-premise networks to public

[14] Institute of Electrical and Electronics Engineers https://www.ieee.org/ asserts it is the world's largest technical professional organization dedicated to advancing technology. IEEE is a 501c professional association for electronic engineering and electrical engineering with its corporate office in New York City and its operations center in Piscataway, New Jersey. It was formed in 1963 from the amalgamation of the American Institute of Electrical Engineers and the Institute of Radio Engineers.

cloud to edge, organizations are increasing seeking data protection controls safeguard sensitive data wherever that data resides. M

Several use cases are underway, H including financial institutional use, autonomous vehicles, mechanical engineering, securing healthcare data. In medicine, using Confidential computing, patients' privacy is protected, and hospitals or other data owners remain in control of their valuable data as data is pushed and pulled from other institutions. In 2021, Germany implemented confidential computing-based healthcare applications with its "E-Rezept" (electronic prescription), an infrastructure system that handles drug prescriptions within the German national healthcare system. M

Confidential Computing is the protection of data in use by performing computation in a hardware-based Trusted Execution Environment (TEE). H Separated from a main operating system, a TEE ensures that data is stored, processed and protected in a secure environment. M A TEE is defined by the CCC as an environment that provides a level of assurance of the following three properties: data confidentiality, data integrity, and code integrity. H Data confidentiality means that those unauthorized entities cannot view data while it is in use within the TEE. H Data integrity ensures unauthorized entities cannot add, remove, or alter data while it is in use. H Code integrity requires that unauthorized entities cannot add, remove, or alter code executing in the TEE. H Current conventional computing provides ways to encrypt data at rest and while in transit, nonetheless, confidential computing protects the confidentiality and integrity of your data while it is in use. M

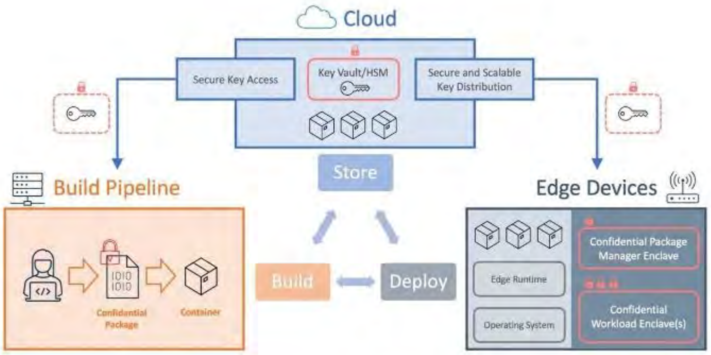


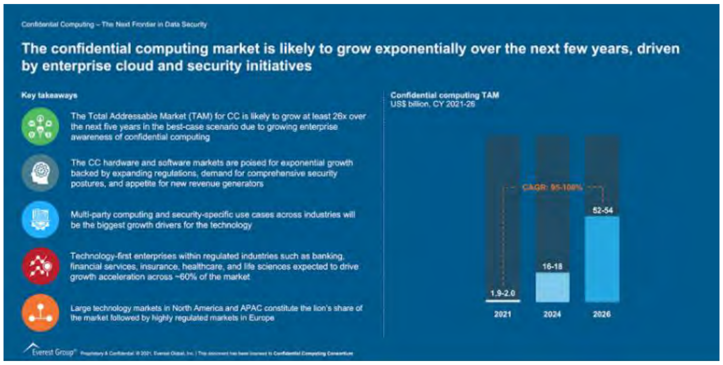
Figure 2. Example Modular solution for Edge/IoT confidential computing Graphic Representing. Click on picture or go to: https://community.arm.com/arm-community-blogs/b/infrastructure-solutions-blog/posts/confidential-computing-brings-secure-data-processing-to-the-edge to read more. Source: The Arm Community.

Confidential computing technology enables multiparty analytics in cases where the data owner might want to share a portion of a dataset while protecting the rest from view (see Figure 2). M

Industries are incorporating confidential computing systems for the protection of items such as Health Insurance Portability and Accountability Act (HIPAA) information, financial data, container data and code integrity, and running algorithms on encrypted datasets from multiple sources. M Protecting highly regulated industries, such as financial services and healthcare, M have led the way in advancing confidential computing innovation. [M] As confidential computing framework implementation protects privacy and data, organizations can collaborate and work with external stakeholders without disclosing intellectual property or other data that they want to keep safe. [M] Notably, the Department of Homeland Security is conducting a confidential computing proof of concept to share intelligence about threats, cyber vulnerabilities and exploits across the public-private-sector enterprise. [H]

The hurdle to scaling confidential computing is setting industry implementation standards. [M] Currently, network and hardware providers offer their own proprietary solutions that may be incompatible with other provider software and hardware systems. [H] This fragmentation increases the vulnerability surface and multiplies the development and testing costs to support multiple clouds. [H] Additionally, lack of standardization erodes validating attestation chains of trust, challenges enforcing policy controls around enclave deployment and use, and seamless lifecycle management. [H]

Though IEEE[15] Computer Society interest in confidential computing is relatively recent, entities like the CCC bring together hardware vendors, cloud providers, and software developers to accelerate the adoption of confidential computing and define TEE technologies and standards. [M] Founding Members of the CCC include: Alibaba, Arm, Google Cloud, Baidu, ByteDance, decentriq, Fortanix, Huawei, Intel, Kindite, Microsoft, Oasis Labs, Oracle, Red Hat, Swisscom, Tencent and VMware. [M] Others, like IBM have been investing in Confidential Computing technologies for over a decade. [H] Additionally, market predictions, such as those provided by strategic IT research company Everest Group (also known as Everest Global), assert that the confidential computing market grows at a compound annual growth rate (CAGR) of 90%-95% in the most aggressive scenario, and 40%-45% even in the most conservative scenario till 2026. [M] Growing availability of confidential computing will continue to expand exponentially given the vast resources, collaboration, proof of concepts initiatives and market indicators. [M]



Confidential Computing – The Next Frontier in Data Security

The confidential computing market is likely to grow exponentially over the next few years, driven by enterprise cloud and security initiatives

Key takeaways

- The Total Addressable Market (TAM) for CC is likely to grow at least 26x over the next five years in the best-case scenario due to growing enterprise awareness of confidential computing
- The CC hardware and software markets are poised for exponential growth backed by expanding regulations, demand for comprehensive security postures, and appetite for new revenue generators
- Multi-party computing and security-specific use cases across industries will be the biggest growth drivers for the technology
- Technology-first enterprises within regulated industries such as banking, financial services, insurance, healthcare, and life sciences expected to drive growth acceleration across ~60% of the market
- Large technology markets in North America and APAC constitute the lion's share of the market followed by highly regulated markets in Europe

Everest Group® Proprietary & Confidential © 2021, Everest Global, Inc. | This document has been licensed to Confidential Computing Consortium

Figure 3. Trends in Confidential Computing. Click on picture or go to: https://youtu.be/ZVSTVBdr82k?t=636 to view video.
Source: Confidential Computing Consortium channel on YouTube.

[15] Institute of Electrical and Electronics Engineers https://www.ieee.org/ asserts it is the world's largest technical professional organization dedicated to advancing technology. IEEE is a 501c professional association for electronic engineering and electrical engineering with its corporate office in New York City and its operations center in Piscataway, New Jersey. It was formed in 1963 from the amalgamation of the American Institute of Electrical Engineers and the Institute of Radio Engineers.

Analytic Confidence

The analytic confidence for this estimate is high. Sources were reliable and corroborated one another. There was adequate time, however, the projections were mostly from industries that may financially benefit from the promotion of the evolving concepts. The analyst worked alone and did not use a structured method. The variety of sources included peer-reviewed academic journal articles, governmental websites, digital alliance associations, and videos by confidential computing developers.

Author: COL Troy Alexander

Section 5: Integrated Reports

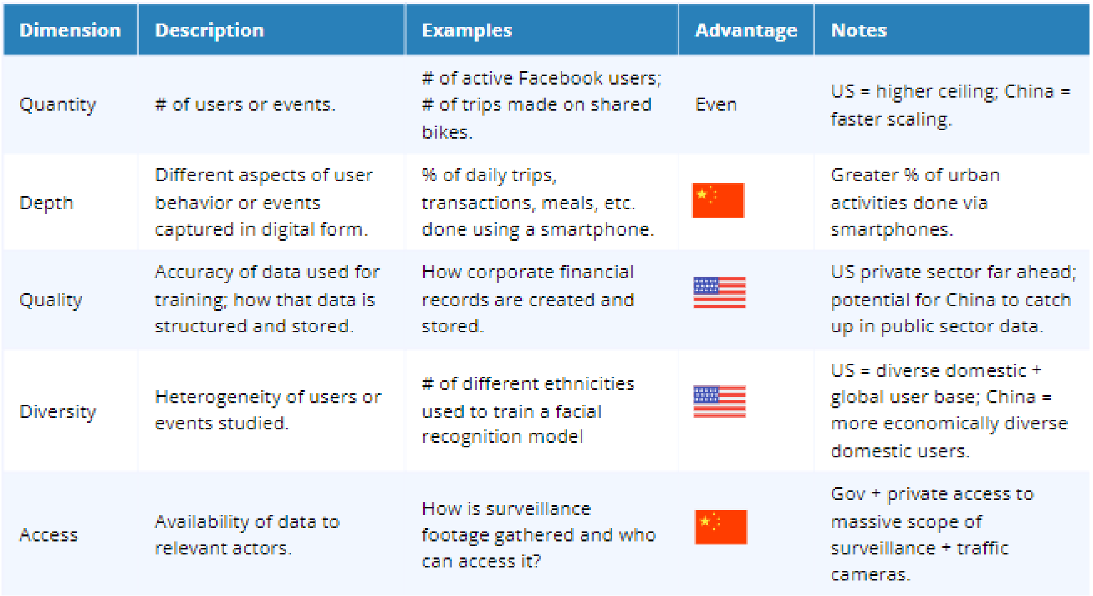
Converging Technological Advancements Will Likely Reduce Asymmetry Of Trust Enabling A Connected Mission Partner Environment Between 2028-2037

Executive Summary

Despite continued privacy and potential data breach concerns, projected network advances and technological innovations will likely (55-80%) reduce asymmetry of trust, creating an enriched and inclusive mission partner environment (MPE). Improvements in artificial intelligence (AI), machine learning (ML), zero-trust (ZT), and blockchain will increase confidence in data management, encouraging ally and partner collaboration in the MPE.

Discussion

Creating an enriched MPE depends on the number of participants and the variety of data inputs. [H] Privacy and potential data breach concerns drive the reluctance to share information. (see Data-Sharing Mindset) Kevin Zheng Zhou[16], a Professor from The University of Hong Kong, and his research team conducted a study on trust asymmetry surveying 134 international buy-supplier relationships in China. The survey validated that trust asymmetry causes negative influences on exchange performance. [M] Using ZT methodology (see Zero-Trust Security) and blockchain (see Blockchain) technology will likely increase confidence in digital trust[17] , encouraging support for increased data sharing in a MPE as early as 2030.



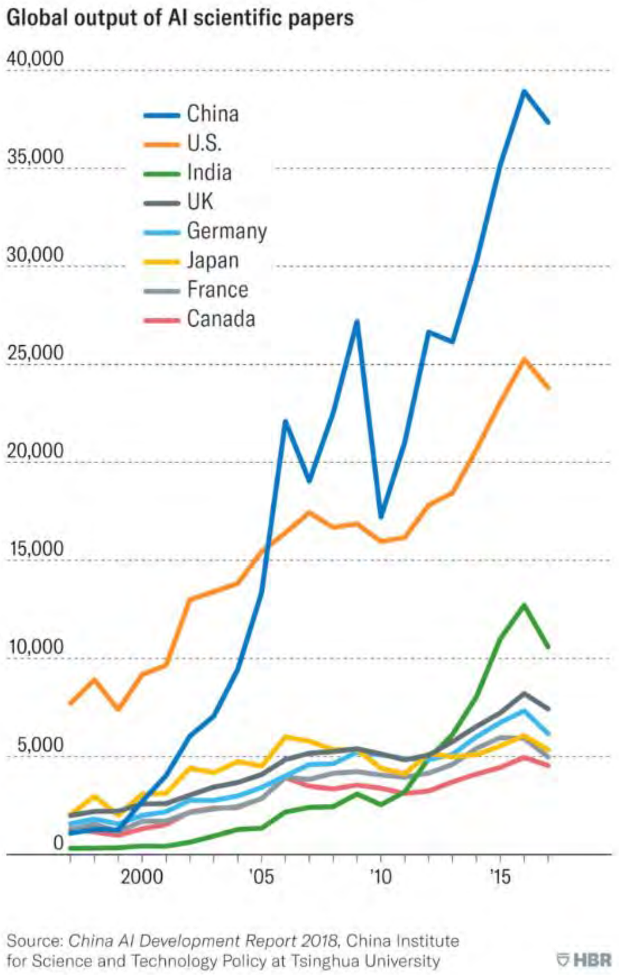
Dimension	Description	Examples	Advantage	Notes
Quantity	# of users or events.	# of active Facebook users; # of trips made on shared bikes.	Even	US = higher ceiling; China = faster scaling.
Depth	Different aspects of user behavior or events captured in digital form.	% of daily trips, transactions, meals, etc. done using a smartphone.	🇨🇳	Greater % of urban activities done via smartphones.
Quality	Accuracy of data used for training; how that data is structured and stored.	How corporate financial records are created and stored.	🇺🇸	US private sector far ahead; potential for China to catch up in public sector data.
Diversity	Heterogeneity of users or events studied.	# of different ethnicities used to train a facial recognition model	🇺🇸	US = diverse domestic + global user base; China = more economically diverse domestic users.
Access	Availability of data to relevant actors.	How is surveillance footage gathered and who can access it?	🇨🇳	Gov + private access to massive scope of surveillance + traffic cameras.

Figure 17. The Five Dimensions of Data in China and the U.S. [M] *Source: Marco Poloan*

[16] Chang-Jiang Scholar Chair Professor and Professor of Management and Strategy

[17] Digital trust is the confidence users have in the ability of people, technology and processes to create a secure digital world.[H]

A data-enriched environment promotes greater refinement and more effective AI algorithms through ML. China’s use of massive amounts of data (see Figure 1) fuels advancements in AI, which outpaced the U.S. (see Figure 2) from “facial recognition, autonomous vehicles, and machine translation.” [M] Transparency in the use of AI is crucial in building the trust of emerging technologies. (see Explainable AI) As more allies and partners share data, ML and deep learning (DL) digestion of the information will highly likely (80-95%) produce enriched intelligence and more impressive AI innovations to protect against incorrect sharing of data and breaches or manipulation by 2030. (see Data-Sharing Mindset)



Source: *China AI Development Report 2018*, China Institute for Science and Technology Policy at Tsinghua University

Figure 2. Global Output of AI scientific Papers. [M]
Source: Harvard Business Review

The evolution in data speeds and capacity that 6G and beyond is projected to provide will increase the attack vectors for vulnerabilities in which the development of ML and AI can combat. (see 6G and Beyond) However, using a combination of humans and machines in parallel and as a check and balance will highly likely reduce the increased risks and develop trust and confidence in the technology. (see Data-Sharing Mindset).

The development of 6G and beyond fixed infrastructures and device-to-device wireless mesh networks will expand data injection and collaborative points. (see 6G and Beyond and Device to Device Solution) Emerging network connections will provide the processing power needed for AI analysis of the massive amounts of data from the internet of things and the internet of sensors to include processing at the edge. (see Machine and Human Communication)

A 2021 study from the University of Florida researched emerging combinations of AI and immersive technologies such as extended reality (XR) in scholarly articles. The convergence of these two different technologies promotes growing collaborative environments between machines and humans. It creates cross-development opportunities that generate enriched information in real-time. This collaborative process gives decision-makers more informed options for creating effects, specifically in "medical training, autonomous cars, and robotics, armed forces training, advanced visualization, conferring intelligence, and interpreting XR-generated data." [M] (see Figure 3)

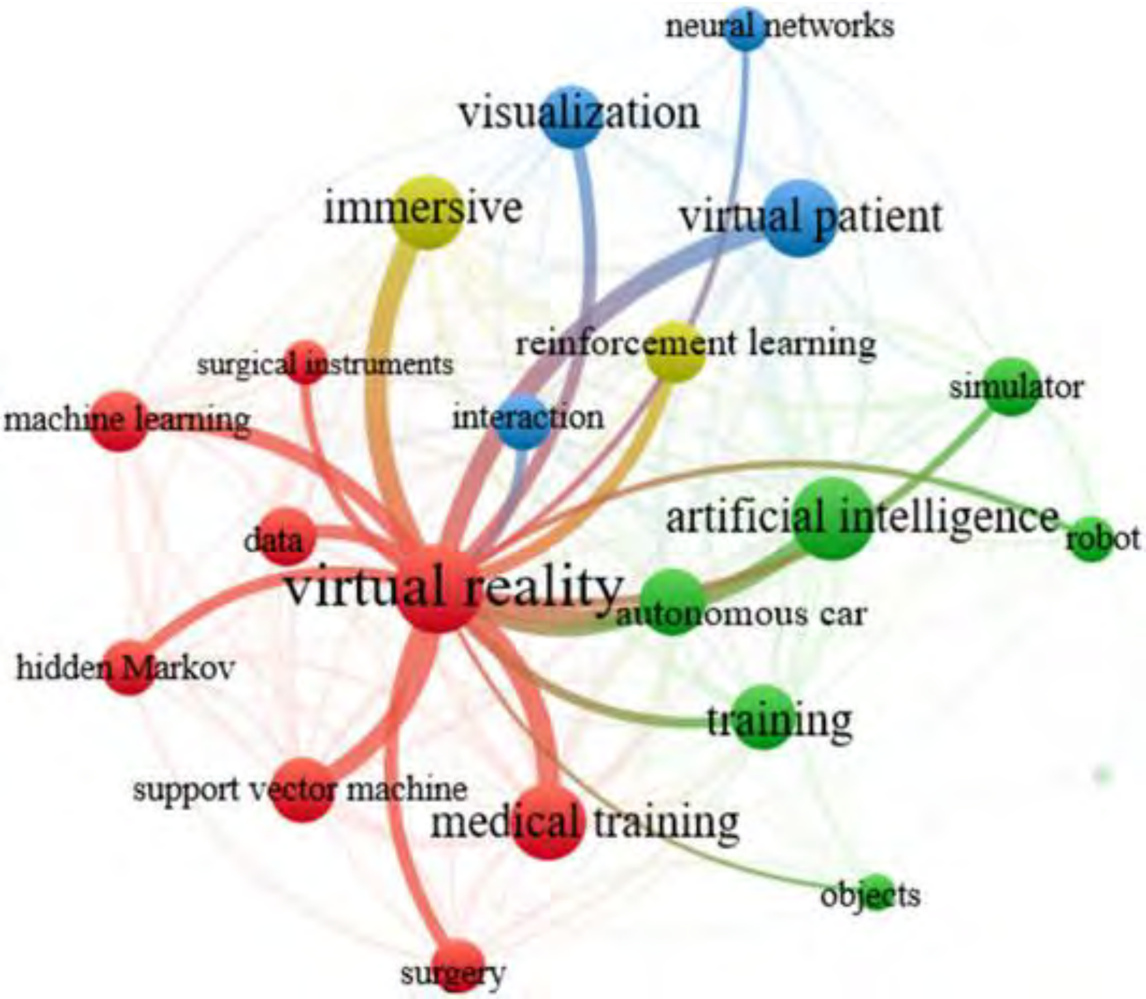


Figure 3. Map of co-occurring terms in various articles. Most occurring terms in relation to virtual reality are AI, training, virtual patient, immersive, and visualization. [M] *Source: Frontiers in Virtual Reality*

Analytic Confidence

The analytic confidence for this estimate is moderate. Sources were reliable and tended to corroborate one another. There was adequate time, and the task was not complex. Despite the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LTC Nicole Y. Shadley

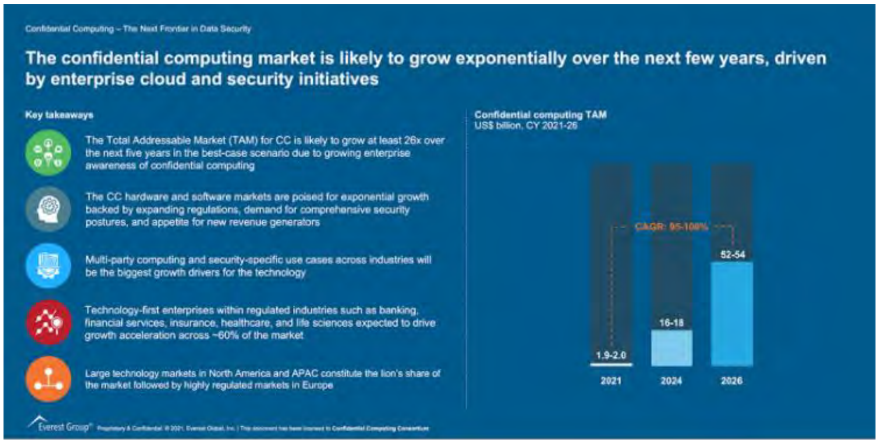
By 2037, Powerful Privacy-Preserving Tech Will Highly Likely Shepherd New Era of Data-Sharing, Enabling Decision Makers To Analyze Intelligence, Dynamically Build Trust, Gain Strategic Decision Advantage

Executive Summary

Despite the vulnerability of data and underdeveloped governance concerns, a new era of data sharing will highly likely (71-85%) emerge due to rapid advances in technologies and privacy-preserving initiatives. In the next 10-15 years, a coalescence of “data-sensors to decision-making” platforms and nascent governance models, notably Confidential Computing, Blockchain, AI/Edge-AI, Fully Homomorphic Encryption (FHE), and 6G/7G networks, will provide the capacity to keep data safe and secure to build trust in dynamic situations and gain a strategic decision point advantage.

Discussion

Fueled partly by the COVID19 pandemic and industrialized hacking, [H] data-privacy concerns spanning multiple industries are driving secure information sharing market activity. Accordingly, as data-privacy business value ascends, corresponding innovations in Confidential Computing, Blockchain, AI/Edge-AI, Fully Homomorphic Encryption (FHE), and 6G/7G networks provide organizations exponentially data-sharing capacities that build collaborative trust in decision making.



Confidential Computing – The Next Frontier in Data Security

The confidential computing market is likely to grow exponentially over the next few years, driven by enterprise cloud and security initiatives

Key takeaways

- The Total Addressable Market (TAM) for CC is likely to grow at least 26x over the next five years in the best-case scenario due to growing enterprise awareness of confidential computing
- The CC hardware and software markets are poised for exponential growth backed by expanding regulations, demand for comprehensive security postures, and appetite for new revenue generators
- Multi-party computing and security-specific use cases across industries will be the biggest growth drivers for the technology
- Technology-first enterprises within regulated industries such as banking, financial services, insurance, healthcare, and life sciences expected to drive growth acceleration across ~60% of the market
- Large technology markets in North America and APAC constitute the lion's share of the market followed by highly regulated markets in Europe

Everest Group® Proprietary & Confidential. © 2021, Everest Global, Inc. | This document has been licensed to Confidential Computing Consortium

Figure 1. The Benefits of Decentralized Identity for your Organization. Click on picture or go to: https://youtu.be/Ew-_F-OtDFI to view video. Source: Microsoft Security channel on YouTube.

Numerous market indicators confirm the acceleration of tech, governance, authentication, and virtual environment initiatives to ensure private and secure data sharing. (see Figure 1) Market predictions, such as those provided by strategic IT research company Everest Group, assert that the Confidential Computing market growth at a compound annual growth rate (CAGR) of 90%-95% in the most aggressive scenario, and 40%-45% even in the most conservative scenario till 2026. [M] (see Confidential Computing)

CONFIDENTIAL
COMPUTING
can be used to protect any sensitive or regulated application or data

Figure 2. Promotional Video: What is Confidential Computing?
Click on picture or go to: https://youtu.be/Jl2W6G9xfqw to view video.
Source: Fortanix channel on YouTube.

The Institute of Electrical and Electronics Engineers (IEEE) [H] Computer Society recognizes Confidential Computing (see Figure 2) development as one of the most significant technology areas emerging [H] in the space of protecting data. [H] (see Confidential Computing)
Confidential computing incorporates encryption technologies like blockchain and FHE. [H] Consortiums, such as the Confidential Computing Consortium (CCC) are standardizing confidential computing frameworks to govern network providers, hardware vendors, cloud providers, and software developers. CCC aims to accelerate the adoption of confidential computing [M] and define associated hardware-based Trusted Execution Environment(TEE) [H] technology standards. (see Confidential Computing)

Rapid advances in blockchain technology and emerging concepts for its employment, such as the proof-of-stake protocol and the use of smart contracts, will likely enable organizations to use blockchain tech to address the challenges of data sharing in low trust environments. [H] (see Blockchain)

Full Homomorphic Encryption (FHE) will achieve sufficient computational efficiency to operate at a scale that enables analytics and machine learning (ML) on encrypted data sets without a need to decrypt the data sets. [H] (see FHE) The combination of Edge Computing and Artificial Intelligence to process algorithms locally will improve performance, optimize network traffic, and reduce latency to enable independent decision making without connecting to the internet or a remote cloud-based server. [H] (see Edge AI)

The establishment of 6G networks (see Figure 3) and the research and development of 7G capabilities will highly likely (71-85%) increase network capacity through the deployment of sensors to capture real-time activities, [M] and boost support of artificial intelligence (AI), immersive virtual and augmented reality (VR/AR) applications, blockchain, M and potential wearable devices and micro-devices. H (see 6G and Beyond)

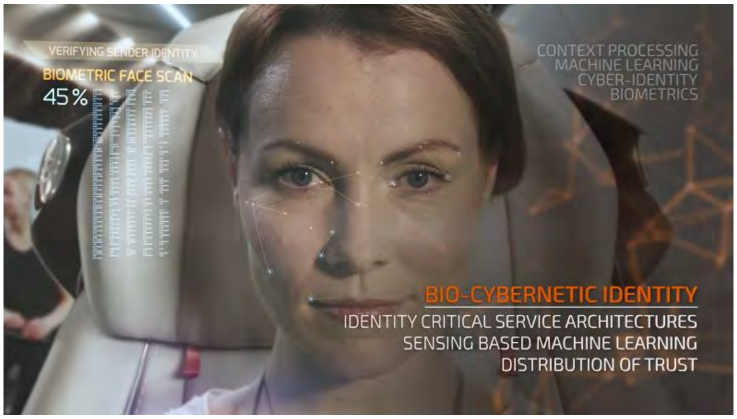


Figure 3. 6G vision for 2030. Click on the picture, or go to: https://youtu.be/T6ubRoZCeVw to view the video.
Source: University of Oulu

The confidence of data privacy standardized technologies will lay the foundation M for novel socio-technical systems, like Distributed Autonomous Organizations (DAO).[18] DAO models, will be implemented at scale across multiple public-private organizations and set new conventions for online coordination and decision-making. H (see DAO)

By 2030, multiple technology companies are likely to incorporate the above frameworks to improve performance, optimize network traffic, and reduce latency. M Business and government institutions integrating these insights early will help affect implementation, standardization, and scalability.

Analytic Confidence

The analytic confidence for this estimate is moderate. Sources were reliable and corroborated one another. There was adequate time, however, several technologies and concepts are nascent while others require further fusing. The analyst worked alone and did not use a structured method, however, did incorporate information provided by peer future analytical assessments. The variety of sources included peer-reviewed academic journal articles, governmental websites, digital alliance associations, and videos by confidential computing developers.

Author: COL Troy Alexander

[18] At its core, a DAOs is a group of entities with common goals that join under a blockchain infrastructure that enforces a set of shared rules to achieve a shared goal. (See SFAR Distributed Autonomous Organizations by COL Gregory Pavlichko)

Artificial Intelligence Enabled Advances In Edge Computing, Natural Language Processing, And Mixed Reality Likely To Enable Multilateral And Multilingual Dynamic Information Sharing Within US-Led Coalitions By 2037

Executive Summary

Due to 6G+ network architecture improvements and reduced costs, coupling edge computing, machine translation, and holography capabilities with blockchain data management technology is likely to enable technologically advanced militaries to create information sharing systems that are dynamic, redundant, and secure by 2037 despite concerns over transparency and biases in AI algorithms.

Discussion

The rapid adoption of new technology has resulted in AI's pervasive presence in commercial settings and in individuals' everyday lives, and is fueling the potential for further adaption into technologically advanced militaries, including the U.S., China, and Russia. [HH] Furthering this trend, the COVID-19 pandemic and increased remote connection demands ushered in a surge of technical collaboration tools that were unavailable at scale prior to the pandemic. [M] And, as the U.S., China, and Russia begin a new era of "Great Power Competition," each nation will need modern methods for connecting with allies and partners. [M]

The U.S. Department of Defense has identified harnessing AI-enabled capabilities as key to maintaining cohesion with allies and partners to prevail on future battlefields. [H] The People's Liberation Army (PLA) has invested in big data analytics and AI to improve capabilities (see Figure 1). [H] And, while the Russian Army has struggled greatly in its war in Ukraine, Russia has sought to create a technologically advanced and autonomous combat capabilities. [M] There are several key technologies likely to advance successfully information sharing across military coalitions within the next 15 years. These include collaborative technologies that help people connect and build trust in other people, technologies that increase trust in data and network security, and recommendations for maximizing human trust in new AI systems through transparency and debiasing to ensure rapid adoption and integration. [M]

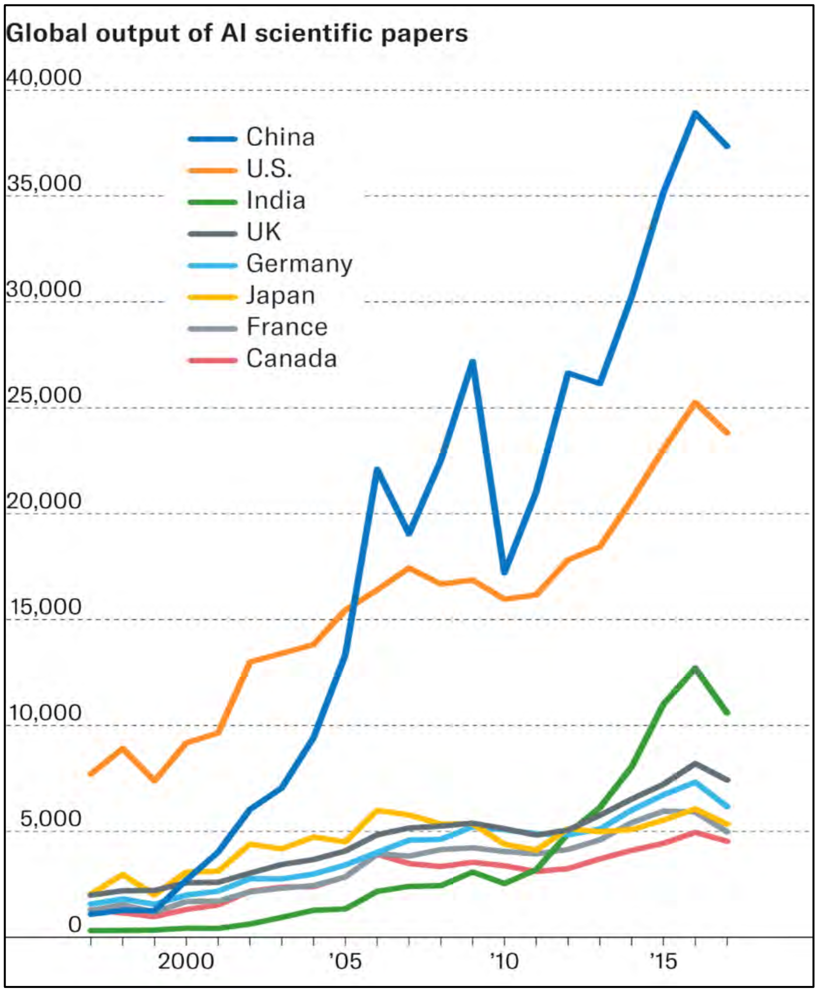


Figure 1. Where New AI Research Comes From. Source: China AI Development Report 2018, China Institute for Science and Technology Policy at Tsinghua University.

The U.S. Army Multi-Domain Operations concept emphasizes decentralized mission command where dispersed operations with allied and partnered forces are central to success on the future battlefield. [H] This concept will drive the military to seek new tools for building trust in other people through in-depth collaboration without physical co-location. One evolution of augmented reality is likely to enable more effective collaboration through holograms (see Holoportation). Advances in 3-dimensional, real-time, full body visualization such as holopresence and holographic displays enable strategic leaders to make more personal connections and deliver impactful messages while eliminating the time, expense, and physical stress resulting from travel. [M] Holographic technology remains expensive and requires large bandwith but, as with most new technology, eventually prices will drop and separate advances in 5G+ and edge computing are also expected to support real-time, high fidelity, full 3D body scan teleportation through their increased computational and bandwidth capacities. [M]

Coupling a holographic presence with separate advances in Machine Translation and Natural Language Processing enable further deepen personal connections through new technology. Large investments by numerous major technology companies has resulted in relatively mature machine translation technology for real-time, multi-language translation of any speech into the listeners' languages (see Neural Machine Translation). [M] For deeper context, DARPA is developing processing technologies that make recommendations for communicating within the emotional, social, and cultural norms that can differ across societies, languages, and communities (see Data Sharing Through Story Telling). [H] When strengthening relationships with allies and partners, nations can improve cross-cultural NLP integration through the development of a shared corpus (vocabulary) to train algorithms on military-specific language, as well as a focus on expanding the broader corpus for partner and allied countries assessed to be most important during a conflict. [M]

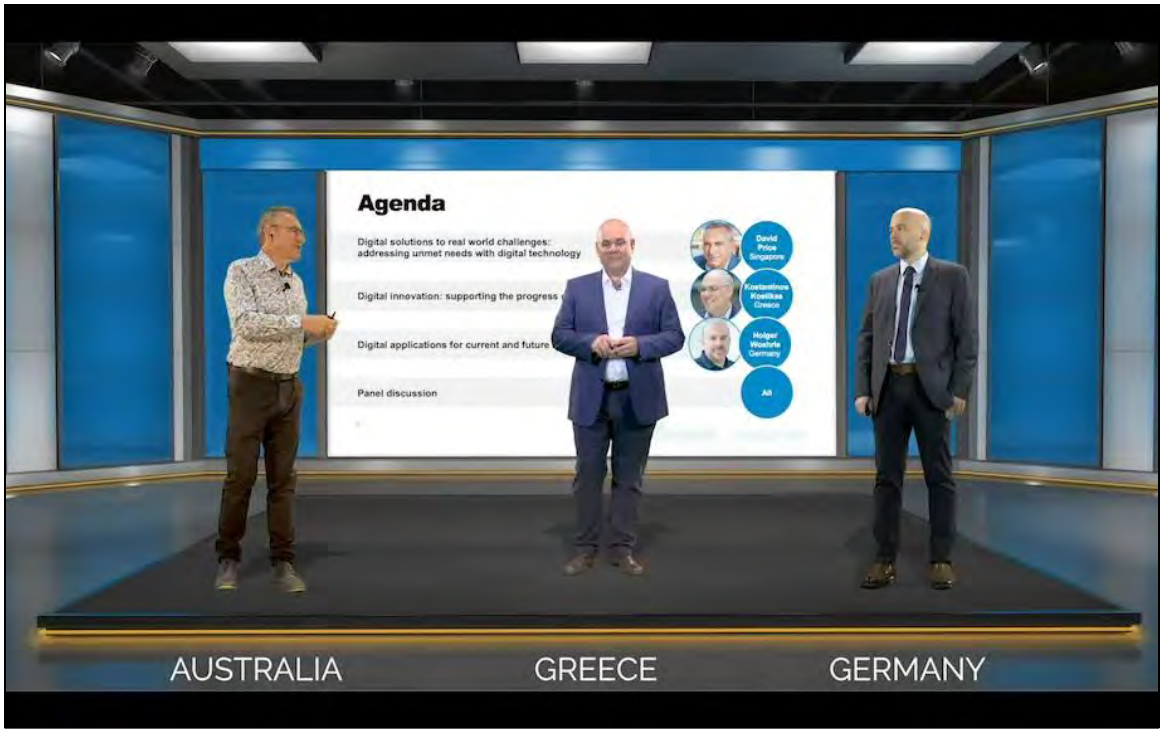

Agenda
Digital solutions to real world challenges: addressing unmet needs with digital technology
Digital innovation: supporting the progress
Digital applications for current and future
Panel discussion
David Price Singapore
Kostantinos Kostikas Greece
Holger Woehrle Germany
All
AUSTRALIA
GREECE
GERMANY

Figure 2. ARHT Media remote work demonstration. Source: ARHT Media.

Other AI-driven advances focus on technology will build trust in data and networks. By 2030, Edge AI deployments are likely to improve military decision making by increasing performance, optimizing, network traffic, and reducing latency – especially as 5G and 6G networks become operational (see Edge AI). [M] Edge computing moves data collection, analysis, and processing to the "edge" of the network where the user is located and edge AI brings neural machine computing power and data storage to where data is collected. [H]

The Israeli Defense Force (IDF) began initial testing of "edge-data architecture" that moves from the cloud to forward units to speed data processing and decision making, likely already tested some Edge AI capabilities in the last Gaza clashes. [H] Further Edge AI adaption for military purposes will have to overcome several challenges, however. In addition to significant latency concerns, Edge AI computer, memory, and power requirements are too large for deployment in field conditions. [M] Compounding this problem, Edge AI for military application will need the capacity to leverage machine learning to "stitch" multiple inputs in near-real-time to reliably inform military decision making. [M] The establishment of 6G+ networks by 2035 will provide the backbone necessary for edge AI by delivering terahertz bits per second network capacity (see 6G and Beyond). [M] The high quantities of data necessary for Edge AI are likely to be secured through vendor neutral Zero-Trust protocols likely to be adopted broadly by 2035 (see Zero-Trust Security). [M]

These rapid AI-enabled advances will not result in military advantage unless humans trust the systems sufficiently to ensure their rapid incorporation. Even as AI becomes ubiquitous in daily life, multiple studies reveal low levels of initial trust in new AI technologies (see Distrust in New AI). [HM] For important decisions, like those involved in healthcare, patients do not fully trust AI-generated recommendations despite evidence that AI outperforms human clinicians at reduced cost. [H] The literature revealed two highly relevant concepts to improve AI adaptation for military operations – explainability, and reliability. Explainable AI emphasized creation of algorithms that are transparent and enable human users to understand how the AI arrived at a decision or recommendation. [H] Reliability is the creation of AI systems whose results are consistent and, for some models, include a "score" or "estimate" of how confident the AI is in its recommendation. [M] Incorporating these insights early when developing AI for military purposes will help ensure successful implementation and speed adoption.

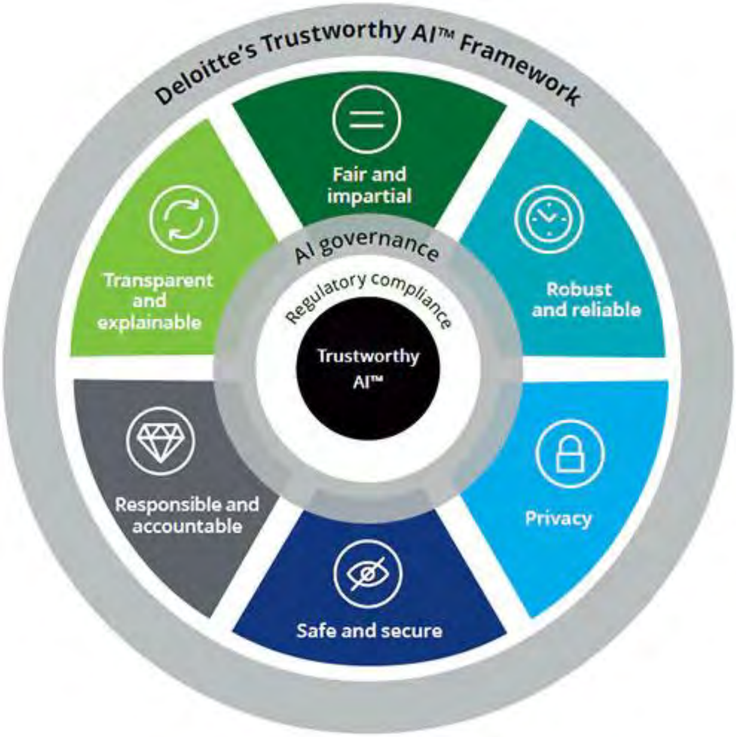


Figure 3. Trustworthy AI Framework. Source: Deloitte.

Analytic Confidence

This is a moderate confidence estimate. The reliability of sources is moderate and information and assessments from multiple sources were generally consistent. However, theoretical predictions varied, and research is sometimes conflicting, specifically with time-based predictions on technical reliability or wide-scale adoption. Most sources were industry papers and news articles and not peer-reviewed academic journals.

Author: LTC Patrick Hofmann

Convergence of Decentralized Autonomous Organizations And Trust Enabling Technologies Likely To Become Foundation For Next Generation Mission Partner Environment by 2037

Executive Summary

The convergence of a variety of emerging technologies such as automated machine learning (AutoML), machine common sense (MCS), fully homomorphic encryption (FHE), blockchain, and decentralized autonomous organizations (DAO), makes it likely (56-70%) that the first military to adopt these technologies to develop a mission partner environment capability will have a marked advantage over their adversaries. The required technologies will likely mature enough to be used at scale by 2037. Despite an enterprise-level culture of risk aversion and asymmetry of trust that will initially prevent widespread acceptance of these capabilities, the private sector will continue developing and improving these technologies and providing successful use cases.

Discussion

The convergence of multiple emerging technologies will likely result in a collaborative and dynamic mission partner environment by 2037. Technologies such as AutoML, MCS, FHE, blockchain, and DAOs provide the pieces and parts to achieve the desired MPE capability. This new paradigm will allow true, real-time collaboration between allies and partners. In addition, new technologies can increase trust between allies and partners and enable policy changes to increase sharing and collaboration of classified or sensitive information.

AutoML research focuses on improving computer vision, data mining, and natural language processing. [H] Auto ML has significantly improved the efficiency of Machine Learning without human data scientist intervention. [H] Once MCS has realized it is likely that AI will exhibit the ability of rational decision-making under unique environmental conditions, learning from new situations, and communicating naturally with people. [H] The convergence of AutoML and MCS will likely produce an MPE that can learn more efficient ways to teach itself how to train on new datasets without human programmers. It will also be able to identify emerging issues with the network and communicate these to end-users. These two technologies will likely produce dynamic artificial intelligence that will be the AI layer backbone of the MPE.

The convergence of FHE and blockchain technologies will likely provide the security required to share data with allies and partners in an asymmetry of trust environment. FHE encryption enables analytical functions to execute directly on encrypted data while yielding the same results as if the user performs the tasks in plaintext. [H] This allows for a repository of encrypted data that can be processed without decrypting data, thus expanding the data available to users. The other component of the security layer is blockchain technology. Because the essential concepts in blockchain technology are decentralization, no single computer or organization can own the chain (see Blockchain). Instead, it is a distributed ledger via the nodes connected to the chain. Nodes can be any electronic device that maintains copies of the blockchain and keeps the network functioning. [M] The convergence of FHE and blockchain will provide the security layer of the MPE, enabling secure sharing amongst allies and partners.

DAOs are novel socio-technical systems that set a new way for online coordination and decision-making. [H] Distributed Autonomous Organizations mediate interactions of members (human or machine) through blockchain applications and smart contracts. [H] A DAO is a form of governance affected by smart contracts that execute agreed-upon protocols (rules) without human intervention. The blockchain applications control interactions via regulations embedded in the source code, and [H] agreed-upon protocols enable smart contract execution without human intervention across the DAO. [M] Although DAO is a recent model, it is likely that by 2037 there will be enough use cases in private industry to make the DAO paradigm viable for an MPE.

As illustrated in figure 1, by 2037, all these emerging technologies will likely be mature enough to aggregate into a collaborative and dynamic MPE. Adoption of these technologies will reduce the culture of risk aversion and asymmetry of trust. These technologies will enable trust in how those the U.S. shares data with use the data and protect data sources. As the data becomes more secure and the AI layer works to parse data to the appropriate users, the speed at which collaboration occurs will increase. The potential speed and accuracy of data sharing and real-time collaboration will be required to implement the future Joint and Army operating concepts successfully.

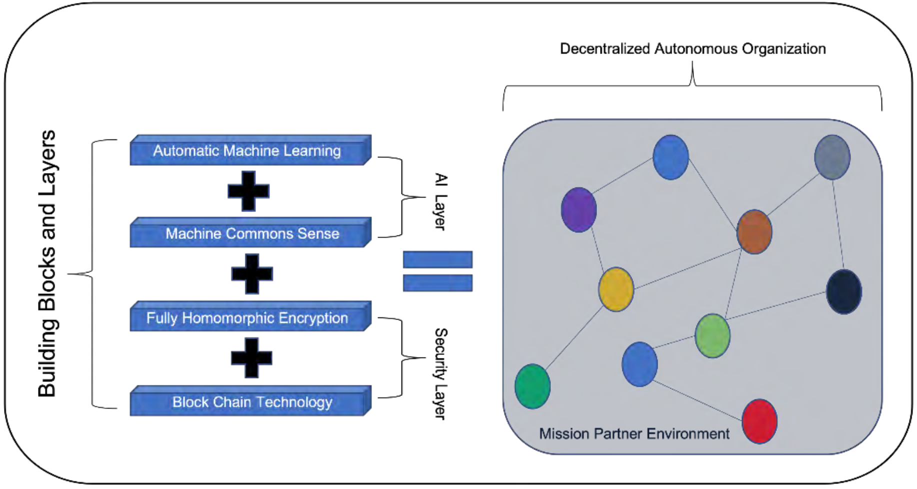

Building Blocks and Layers
Automatic Machine Learning
Machine Commons Sense
Fully Homomorphic Encryption
Block Chain Technology
AI Layer
Security Layer
Decentralized Autonomous Organization
Mission Partner Environment

Figure 18. Illustration of Aggregation of Converging Technologies to Enable an MPE Based on a DAO Model.

Analytic Confidence

The analytic confidence for this estimate is moderate. However, the sources were very reliable and corroborated one another. There was adequate time, but the analyst worked alone and did not use a structured method. Many sources were peer-reviewed academic journal articles, industry websites, and respected periodicals. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Greg Pavlichko

IoT, Blockchain, AR/MR, And AI Will Likely Enable A 2037 MPE That Goes Beyond Data Sharing To Full Collaboration With Partners

Executive Summary

By the year 2037, despite the challenge of being able to operate in a contested future cyberspace domain, the creative combination of technologies including blockchain, Internet of Things (IoT), Artificial Intelligence (AI) Deep Learning (DL) neural networks, and Augmented Reality (AR)/Mixed Reality (MR), will likely (55-80%) enable a Mission Partner Environment (MPE) that provides significantly enhanced data sharing and full collaboration between the U.S. military and its partners. The U.S. military and its partners will be able to combine these technologies to create a 2037 MPE due to the adoption of next generation network technologies.

Discussion

The DOD Instruction 8110.01 defines the MPE as “the operating framework enabling command and control (C2) and information sharing for planning and execution across the full range of military operations … [that] provides the ability for DoD and M[ission] P[artners] to exchange information with all participants within a specific partnership or coalition.” [H] The Department of the Army Deputy Chief of Staff G2 has noted that the MPE in 2037 must enable dynamic information sharing and decision making, despite asymmetries of trust (see Annex A).

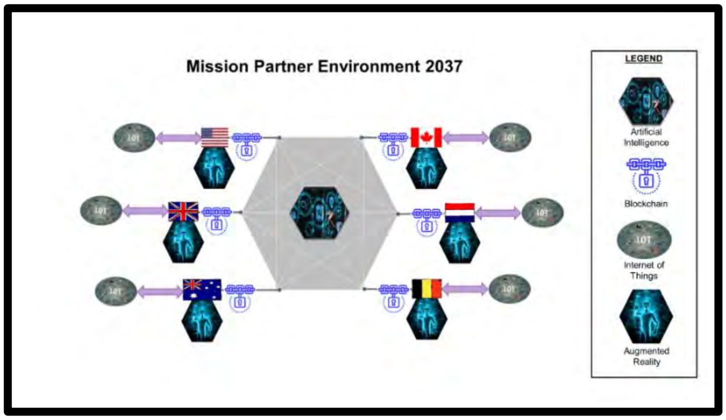


Figure 19. Model of MPE 2037 leveraging Key Emerging Technologies.

During a discussion on November 19, 2022, the G2 outlined an operational vignette that described how the ideal future MPE should enable the sensor-to-decision maker-to-weapon system chain, where the decision maker can be human or non-human and the weapon system can be lethal or non-lethal (see Annex B). Ideally, the system should be able to share data from any mission partner sensor on the batllefield, leverage AI for decision making, and be able to que any mission partner weapon system. Figure 1 provides a model that describes how the U.S. Army can combine the technologies of blockchain, IoT, AI, and AR/MR to build the 2037 MPE. While analog computing is not indicated in the model, it will likely enable faster and more energy efficient AI processing at the edge and in the cloud (see Analog Computing).

Per Figure 1, each mission partner will have an IoT system containing thousands of smart devices spread across the battlefield. Each device will be constantly collecting real-time data and transmitting it back to the mission partner. Once the data hits the mission partner system, edge AI will analyze the data to conduct predictive analysis and identify potential enemy targets that are based on priorities set by the mission partner and/or coalition of partners. As part of the blockchain distributed ledger system, for each piece of data collected, a smart contract will automatically determine how much of the data can be shared with each of the other mission partners and it will automatically send the data to each partner and capture the data transactions in the blockchain, which will enable each partner to track and audit all data transactions to ensure their data is shared at the appropriate level. For targetable data, the smart contract will also send it to a centralized AI decision making system. The centralized AI decision making system will identify priority targets that meet strike criteria and determine the appropriate decision making authority for the target, which can be human or non-human. Once the decision maker decides to strike the target, the AI system will determine the best weapon system to strike the target and a strike order will be sent to the partner that controls the weapon system. The system will send the strike order as a transaction through the blockchain. For non-targetable data, analysts and commanders will use AR/MR technology to develop a common operating picture of the battlefield and collaborate beyond traditional geographic boundaries. The below sections provide additional detail on each of the technologies that need to be combined to create the MPE system described above.

The term IoT is used to describe the billions of devices across the globe that are connected to the internet (see IoT). [M] It is likely that the future battlefield will include thousands of smart devices, such as weapon systems, smart munitions, and sensors, that will be linked together using an IoT type architecture. [MM] These IoT devices will generate large datasets that will require AI DL neural networks to analyze and process (see Narrow AI). Additionally, the adoption of analog computing will make edge AI enabled smart devices and AI cloud processing faster and more energy efficient (see Analog Computing).

Blockchain technology will enable the future MPE to address asymetries of trust between partners (see Blockchain). For the purpose of this assessment, aysmetry of trust is defined as “a situation where different partners have different levels of information that they are willing to share with the U.S. and other partners; some partners may have a zero-trust relationship with other partners” (see Annex A). Individual partners will be able to store the data they collect from their IoT network of smart devices and sensors in highly secured databases that they manage. Partners will then be able to use blockchain tech to create an immutable distributed ledger that validates access to partner data and records all access requests. For routine data sharing events, partners can establish smart contracts that automatically regulate access between various partners, based on previously established trust relationships. The owner of the data controls access through the blockchain. Each partner can audit the distributed ledger at any time to ensure only authorized entities have access to their data. The MIT MedRec project is exploring a similar model for managing Electronic Health Records (EHR) (see Blockchain). [H]

The future MPE will likely leverage AR/MR to go beyond data sharing to enable collaboration. Partners using AR/MR technology will be able collaborate and meet without geograpic limitations (see AR Collaboration). Using AR/MR, military commanders on the battlefield will be able to meet with fellow commanders, as well as regional and technical experts that may be in short supply, from any partner force. This will provide commanders new levels of insight and the ability to conceptualize the battlefield leveraging the data from the thousands of partner IoT smart devices proliferating the battlefield.

The DOD assessment on the Joint Operating Environment 2035 emphasizes that the U.S. military will be forced to operate in an increasingly contested cyberspace domain in the future, which includes telecommunications networks, computer systems, and embedded processors. [M] For the future MPE architecture to be successful, the U.S. military and its partners will have to create a robust communications infrastructure that will ensure reliable data flows in the future contested cyberspace domain. The U.S. Army is addressing this concern by designating modernization of Army network technologies as one of its six modernization priorities. [M] To enable this modernization priority, Army Futures Command established the Army's Network Command, Control, Communication, and Intelligence Cross-Functional Team (N-CFT), which "is responsible for enabling Army formations to reliably communicate anywhere, anytime, in all domains, in all environments, against any adversary." [M]

Analytic Confidence

Overall analytic confidence in this estimate is moderate. The analyst had adequate time, but the task was complex. The analyst has high confidence in the evaluation of the viability of technologies in this assessment. However, the analyst confidence in the timeline is moderate. The ability of the Army to change DoD policy related to classified information sharing will likely have a significant impact on the implementation timeline.

Author: COL Anthony Pollio

Annex A – Terms of Reference

Terms of Reference:
The Future Mission Partner Environment in 2037

For:
LTG Laura A. Potter
Deputy Chief of Staff G2, Headquarters, Department of the Army

By:
Team Trust and Information Eco-System (TIES)
United States Army War College

December 10, 2021

Terms of Reference:
The Future Mission Partner Environment in 2037

Requirement:

What technical and process advancements over the next 15 years are likely to enable dynamic information sharing and decision making[19] within a Mission Partner Environment (MPE)[20] despite asymmetries of trust[21]?

- What data formatting, data routing, and trust relationships are required for the future MPE?
- What technology and or process improvements will facilitate multilateral sharing of information in near real-time?
- How is mission partner information protected from indiscreet sharing amongst partners and allies?
- How does this capability utilize future developments in artificial intelligence to solve above stated problems?
- What policy changes are required to enable the future MPE?

Methodology and Notional Execution Timeline:

The team expects to conduct unclassified research through reviews of academic journals, open-source publications, and periodicals. The team will also interview and correspond with government, academic, and private sector experts in the fields of networking, cyber, intelligence, and modeling. The team expects to focus its research on future models and emerging technical solutions for information sharing.

The following outline of activities is notional. The exact order and types of activities conducted will depend heavily on the kinds of information available:

[19] Decision Making – Human and Automated

[20] MPE – A capability framework that improves partner information-sharing, data exchange and integrated execution through common standards governance and agreed-to procedures. MPE supports commanders' execution of critical joint warfighting functions: C2, information, intelligence, fires, movement and maneuver, protection, and sustainment. To perform these warfighting functions, commanders require services be common to both the enterprise and expeditionary levels of operation for human-to-human collaboration (e.g., chat, secure voice, video teleconferencing, email (with or without attachments), web browsing). (https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/811001p.pdf)

[21] Asymmetry of Trust – represents a situation where different partners have different levels of information that they are willing to share with the U.S. and other partners; some partners may have a zero-trust relationship with other partners.

Step 1: Research (December 2021 – January 2022)

- Describe the desired state in a Mission Partner Environment of 2037.
- Describe existing U.S. technological and policy challenges with information sharing.
- Identify industries that require near real-time data sharing in competitive environments. Identify instances where civil sectors are challenged with similar “zero trust” information environments.
- Potential actors include global stock exchange companies, international banks, technology companies, and cyber security firms.
- Research advancements with the potential to enable near real time sharing of information including the meta-verse, artificial intelligence, automated decision-making, and quantum computing.
- Conduct interviews and outreach with experts, analysts, and strategists who are knowledgeable on emerging solutions.
- Explore potential vulnerabilities of emerging technologies and potential adversarial capabilities to exploit or aggravate a trusted environment.

Step 2: Synthesize and Analyze (February – March 2022)

- Evaluate applicability of technologies and processes.
- Evaluate research for potential material solutions.
- Evaluate research for potential non-material solutions.
- Validate assumptions and, if needed, reframe the desired MPE capability based on research results.
- Provide feedback and conduct additional research as required.
- Identify iterative benchmarks to achieve desired end state.

Step 3: Develop Recommendations and Finalize Results (April 2022)

- Develop vignettes and use cases to describe implementation of future MPE solutions.
- Where applicable, develop new models for information sharing.
- Where necessary, propose new models that conflict with existing information sharing and classification policies.

Step 4: Present Recommendations (May 2022)

- The team will finalize the written report outlining the team’s findings and recommendations.
- Out-brief LTG Potter and her team (9 – 13 May 2022)

Challenges:

- Time. The team is conducting this four-month, unclassified research study to complete a U.S. Army War College requirement and a full graduate course load. The estimated time to complete the research study is between April – May 2022. COVID restrictions imposed may limit the ability to travel and the timely accessibility of resources.

- Accessibility. Commercial, private sector, and international information may be challenging to gather. Research details may be constrained due to language, classification levels, and political policy agreements, which are beyond the scope of this academic approach. Institutions may be reluctant to showcase, discuss or release concepts regarding emergent technologies and proprietary information due to intellectual property constraints.

- Extensiveness. Research team members have limited technical expertise with digital information sharing or existing information-sharing policies. Due to the complexities of established MPEs and innumerable factors impacting the implementation of a future MPE, the team's ability to identify impediments will be limited.

Resources:

- The team will use open-source non-classified media including published information from academic, professional organizations, and Army War College resources.
- The team has a variety of expertise in simulations, military intelligence, human resources, and the signal career fields.
- The team will use the recent Warfighter, Defender Europe, and Joint Warfighter Assessment after-action reviews to understand current MPE challenges.
- The team will use relationships with Army Futures Command and various cross-functional teams to discuss current and future enterprise-level MPE efforts.
- The team will leverage personal and Army War College Staff relationships with domestic and international colleagues spanning military, government, academic, professional organizations, industry, and institutional entities.

Administration:

- The final product will be provided in .PDF format and is for the sole use of LTG Laura A. Potter, DCS G2, USA, and those she so designates.
- The out-brief will be ready for presentation upon peer-review completion, with the final out-brief scheduled for April – May 2022. Therefore, the optimal window for out-brief is 9-13 May 2022.
- The research team is comprised of (all phone numbers are personal cell phones):
  - Primary Point of Contact: LTC Patrick Hofmann
  - Alternate Point of Contact: LTC Nicole Shadley

- Team Members
  - COL Troy Alexander, troy.alexander.mil@armywarcollege.edu, 949-547-1728.
  - COL Gregory Pavlichko gregory.pavlichko.mil@armywarcollege.edu, 334-806-8069
  - COL Anthony Pollio anthony.pollio.mil@armywarcollege.edu, 808-348-0860
  - LTC Patrick Hofmann patrick.hofmann.mil@armywarcollege.edu, 202-725-6084
  - LTC Nicole Shadley nicole.shadley.mil@armywarcollege.edu, 253-370-9110
- Official Mailing Address: 122 Forbes Ave, Carlisle, PA 17013

Annex B - Notes From November 19, 2022 Meeting With The Army G2

G2 Participants:
LTG Laura Potter, HQDA G2
Mr. Alexander Miller, HQDA G2 Senior Science and Technology Advisor
Mr. Anthony (Jamie) McDonald, Director, HQDA G2 Strategic Initiatives Group
Dr. Fisher (I did not get the spelling of his name or his position within the G2)

- Problem: Sharing among any and all US partners has differing levels of trust (i.e. asymmetry of trust), which results in sharing of information at lower levels of usefulness.
- Solving the problem with changes at the technical, process, policy, and analytical levels.
- Possible solutions should not be limited to a specific AOR.
- Mr. Miller suggested that we may want to compare and contrast existing solutions in different AORs. US/FVEY sharing systems are probably the most effective available at this time.
- While solving this problem is important to the G2 for intel sharing, it is a USG problem that effects all aspects of US/Ally information sharing.
- Possible solutions should be scalable, flexible, and able to setup across the spectrum of US partners that may have varying degrees of technical sophistication (i.e. from allies with limited OSINT capabilities thru allies with sophisticated technical capabilities).
- Ideally they want to have a system that enables pushing classified US targeting sensor data directly to an allied decision maker (human or machine) to trigger partner fires and/or effects.
- Mr. Miller stated that we can assume the network and analytic tools already exist and we should focus more on how to get the right data to the right people.
- While they want us to identify potential policy impediments to possible solutions, they do not want us to focus on writing policy.
- Based on the guidance from Mr. Miller, it appears that our primary focus should be on data formatting, data routing, data trust relationships, process, and sensor =>decision maker=>shooter/effect relationships.
- Suggested we should also consider leader to leader and staff to staff sharing.
- Review last year's project to see examples where decision makers may not be human.
- We should look at sharing in both competition and hostilities.
- To get a feel for existing partner sharing challenges see WarFighter 21-4 AAR/lessons learned (in Teams folder). It provides examples for UK, French, and FVEY+1 sharing scenarios.
- FVEY sharing provides the best example that currently exists.
- Policy will be the hardest peace. They do not expect us write policy, but believe it would be helpful if we identify policy impediments.
- If we provide proposed technical, process and system solutions, the G2 will use it to push future policy changes.
- PHALANX system is a good example of an effective kill chain solution.

- Vignette: French sensor queues a US system to “kill” an incoming missile.
- The decision maker can be human/non-human and anywhere in the network.
- Possible data use case can be UNCLASSIFIED commercial imagery as a proxy for partner sharing.
- Will also need to consider how we share crypto keys with partners.
- May also need to consider how to share simulation data.
- We will likely need to work within existing classification boundaries or identify what areas might need to change (i.e. tear-line at the sensor).
- Consider zero trust and/or trust asymmetry solutions.
- The G2 mentioned the Combined Joint All Domain C2 (CJADC2) system. I am not sure what that is.
- The G2 said that she needs a dynamic, scalable sharing environment that is easy to expand and navigate (example - start with UK and AUS, then expand to other ASEAN partners with varying technical capabilities).
- Best case is a single exercise/training and operational system, but the G2 realizes that classification restrictions may prevent it.
- The G2 mentioned Project Convergence. I don’t know what that is.
- The G2 is also interested in federated production in addition to sensor=>DM=>shooter/effect tipping and queuing.
- Data standards will be a key issue.

Annex C – Expert Interview notes

Expert Interview Notes

Telephonic interview with Darci Cavanaugh, Discover Financial Director AML
Interview conducted on 11 March 2022
Discussion on fraud prevention with the use of Artificial Intelligence (AI) and Machine Learning (ML)

Question1: What does her financial institute use to prevent fraud?
Answer 1: Discover uses a combination of human checks and balances with AI and robotic processes executing every day monitoring analysis of activity. Encrypted platforms and AI with ML provide security while reducing risks.

Question 2: What role does the human factor play?
Answer 2: Both humans and bots work in parallel to examine activity with the additional periodic checks and balances. In the initial development stages, we received buy-in early and frequently to help ensure the AI would be programmed to meet the requirements.

Question 3: How did you gain support for AI adoption?
Answer 3: We created incentives for adopting change and those that supported the journey to modernize.

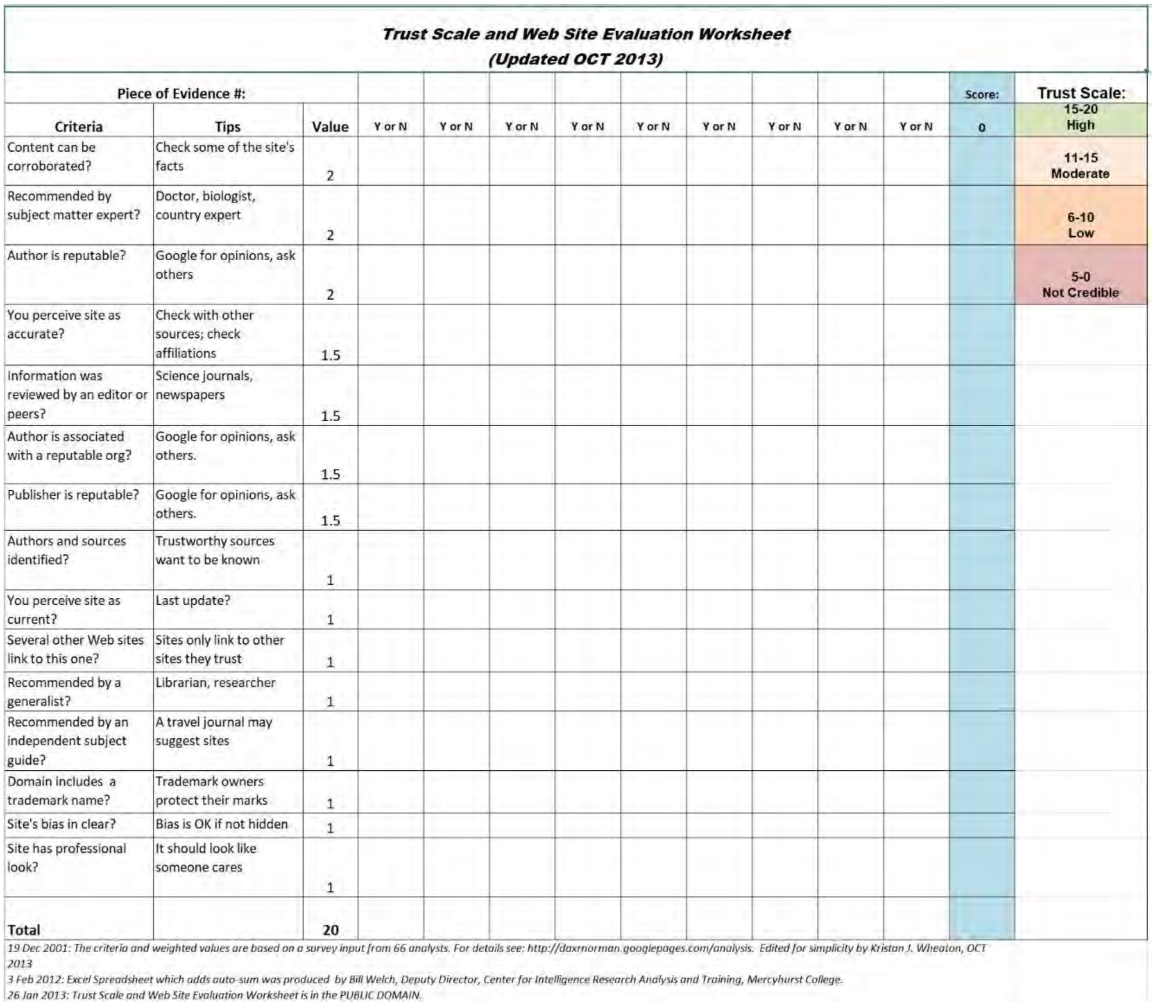
Question 4: What was the process for adoption?
Answer: Enforcement of updated stringent regulations, policies, and standards.

Question 5: How long did it take to get the right AI designed?
Answer 5: We're constantly updating it but coding, technology tests, and feedback are crucial to staying right. We initially established a coalition design group for input and feedback. We identified all parties early and included them in the development.

Question 6: How did you gain/earn confidence in the AI program?
Answer: Metrics reflect the advantages, efficiencies, and reduced risk in time and money that AI provided in preventing fraud.

Annex D - Trust Scale and Web Site Evaluation Worksheet

Each source is annotated based on a trust scale that includes Not Credible (N), Low (L), Moderate (M), and High (H). The trust scale was determined by using the below spreadsheet and examining each factor.



Trust Scale and Web Site Evaluation Worksheet
(Updated OCT 2013)

Piece of Evidence #:												Score:	Trust Scale:
Criteria	**Tips**	**Value**	Y or N	Y or N	Y or N	Y or N	Y or N	Y or N	Y or N	Y or N	Y or N	0	15-20 High
Content can be corroborated?	Check some of the site's facts	2											11-15 Moderate
Recommended by subject matter expert?	Doctor, biologist, country expert	2											6-10 Low
Author is reputable?	Google for opinions, ask others	2											5-0 Not Credible
You perceive site as accurate?	Check with other sources; check affiliations	1.5											
Information was reviewed by an editor or peers?	Science journals, newspapers	1.5											
Author is associated with a reputable org?	Google for opinions, ask others.	1.5											
Publisher is reputable?	Google for opinions, ask others.	1.5											
Authors and sources identified?	Trustworthy sources want to be known	1											
You perceive site as current?	Last update?	1											
Several other Web sites link to this one?	Sites only link to other sites they trust	1											
Recommended by a generalist?	Librarian, researcher	1											
Recommended by an independent subject guide?	A travel journal may suggest sites	1											
Domain includes a trademark name?	Trademark owners protect their marks	1											
Site's bias in clear?	Bias is OK if not hidden	1											
Site has professional look?	It should look like someone cares	1											
Total		**20**											

19 Dec 2001: The criteria and weighted values are based on a survey input from 66 analysts. For details see: http://daxrnorman.googlepages.com/analysis. Edited for simplicity by Kristan J. Wheaton, OCT 2013

3 Feb 2012: Excel Spreadsheet which adds auto-sum was produced by Bill Welch, Deputy Director, Center for Intelligence Research Analysis and Training, Mercyhurst College.

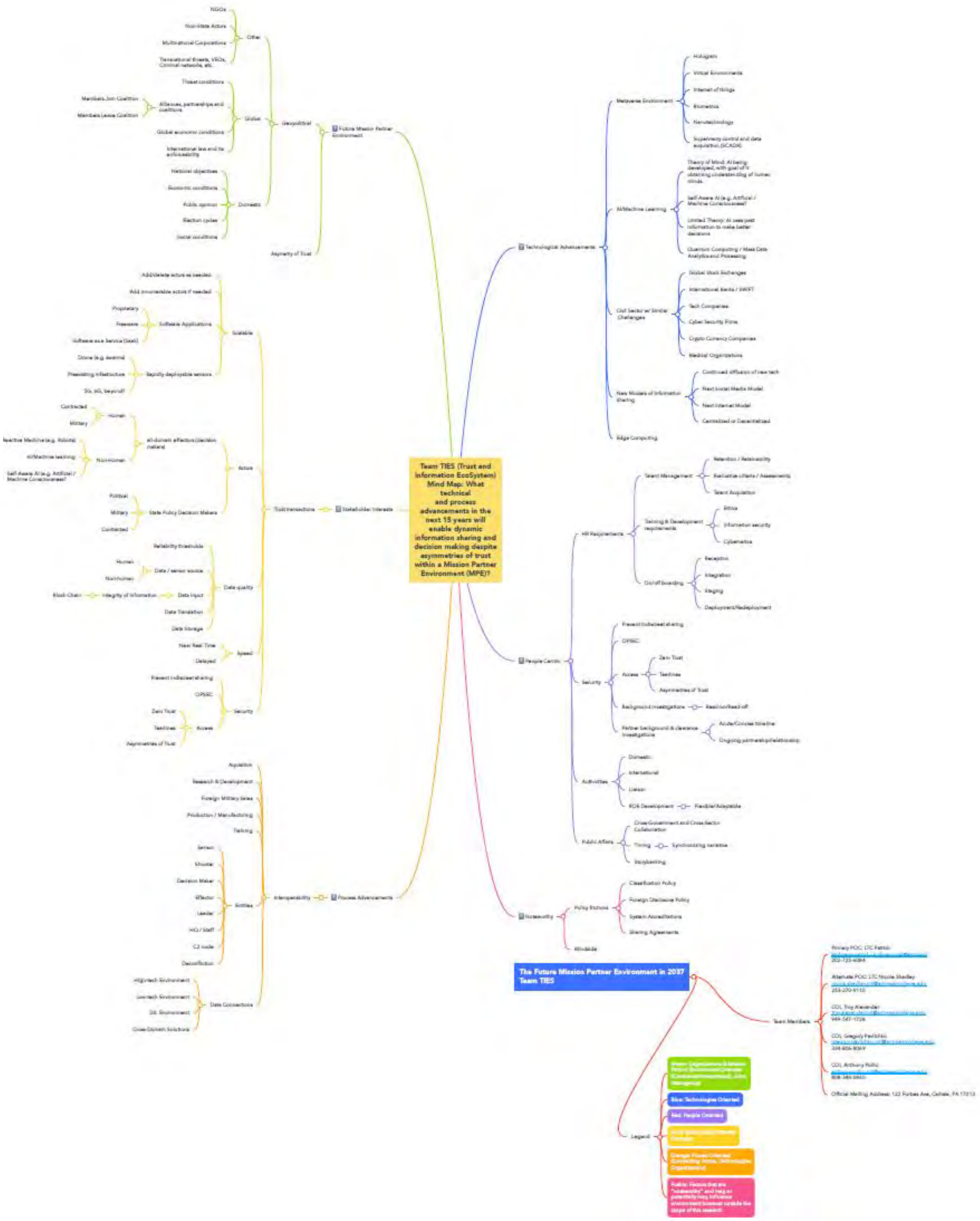
26 Jan 2013: Trust Scale and Web Site Evaluation Worksheet is in the PUBLIC DOMAIN.

Annex E - Intelligence Community Directive 203 Terms Of Analytic Probability

For expressions of likelihood or probability, this paper used the following set of terms:

almost no chance	very unlikely	unlikely	roughly even chance	likely	very likely	almost certain(ly)
remote	highly improbable	improbably (improbably)	roughly even odds	probable (probably)	highly probable	nearly certain
01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%

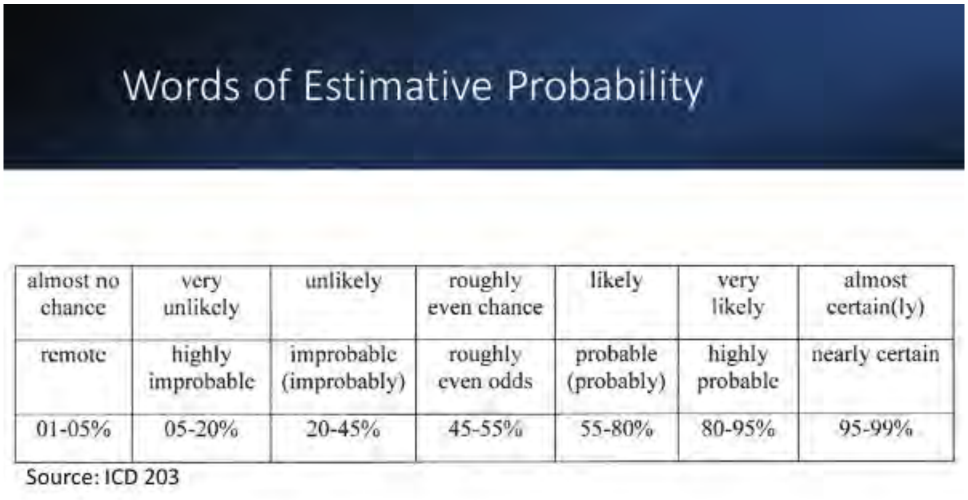
Annex F – Mind Map


Team TIES (Trust and information EcoSystem) Mind Map: What technical and process advancements in the next 15 years will enable dynamic information sharing and decision making despite asymmetries of trust within a Mission Partner Environment (MPE)?
Future Mission Partner Environment
Geopolitical
Other
NGOs
Non-State Actors
Multinational Corporations
Transnational threats, VEOs, Criminal networks, etc.
Global
Threat conditions
Alliances, partnerships and coalitions
Members Join Coalition
Members Leave Coalition
Global economic conditions
International law and its enforceability
Domestic
National objectives
Economic conditions
Public opinion
Election cycles
Social conditions
Asymetry of Trust
Stakeholder Interests
Trust transactions
Scalable
Add/delete actors as needed
Add innumerable actors if needed
Software Applications
Proprietary
Freeware
Software as a Service (SaaS)
Rapidly deployable sensors
Drone (e.g. swarms)
Preexisting infrastructure
5G, 6G, beyond?
Actors
all-domain effectors (decision makers)
Human
Contracted
Military
Non-Human
Reactive Machine (e.g. Robots)
AI/Machine learning
Self-Aware AI (e.g. Artificial / Machine Consciousness)?
State Policy Decision Makers
Political
Military
Contracted
Data quality
Reliability thresholds
Data / sensor source
Human
Non-human
Data input
Integrity of information
Block-Chain
Data Translation
Data Storage
Speed
Near Real Time
Delayed
Security
Prevent indiscreet sharing
OPSEC
Access
Zero Trust
Tearlines
Asymmetries of Trust
Process Advancements
Interoperability
Acquisition
Research & Development
Foreign Military Sales
Production / Manufacturing
Training
Entities
Sensor
Shooter
Decision Maker
Effector
Leader
HQ / Staff
C2 node
Deconfliction
Data Connections
High-tech Environment
Low-tech Environment
DIL Environment
Cross-Domain Solutions
Technological Advancements
Metaverse Environment
Hologram
Virtual Environments
Internet of things
Biometrics
Nanotechnology
Supervisory control and data acquisition (SCADA)
AI/Machine Learning
Theory of Mind: AI being developed, with goal of it obtaining understanding of human minds.
Self-Aware AI (e.g. Artificial / Machine Consciousness)?
Limited Theory: AI uses past information to make better decisions
Quantum Computing / Mass Data Analytics and Processing
Civil Sector w/ Similar Challenges
Global Stock Exchanges
International Banks / SWIFT
Tech Companies
Cyber Security Firms
Crypto Currency Companies
Medical Organizations
New Models of Information Sharing
Continued diffusion of new tech
Next Social Media Model
Next Internet Model
Centralized or Decentralized
Edge Computing
People Centric
HR Requirements
Talent Management
Retention / Retainability
Evaluative criteria / Assessments
Talent Acquisition
Training & Development requirements
Ethics
Information security
Cybernetics
On/off boarding
Reception
Integration
Staging
Deployment/Redeployment
Security
Prevent indiscreet sharing
OPSEC
Access
Zero Trust
Tearlines
Asymmetries of Trust
Background investigations
Read-on/Read-off
Partner background & clearance investigations
Acute/Concise timeline
Ongoing partnership/relationship
Activities
Domestic
International
Liaison
ROE Development
Flexible/Adaptable
Public Affairs
Cross-Government and Cross-Sector Collaboration
Timing
Synchronizing narrative
Storytelling
Noteworthy
Policy Frictions
Classification Policy
Foreign Disclosure Policy
System Accreditations
Sharing Agreements
Wildside
The Future Mission Partner Environment in 2037
Team TIES
Team Members
Primary POC: LTC Patrick
Alternate POC: LTC Nicole Shadley
COL Troy Alexander
COL Gregory Pavlichko
COL Anthony Pollio
Official Mailing Address: 122 Forbes Ave, Carlisle, PA 17013
Legend
Green: Organizations & Mission Partner Environment Oriented
Blue: Technologies Oriented
Red: People Oriented
Gold: Stakeholder Interests Oriented
Orange: Process Oriented (Connecting Actors, Technologies, Organizations)
Pink: Factors that are "noteworthy" and may or potentially may influence environment however outside the scope of this research

Annex G - Power Point Slides

MPE 2037: Decentralized Autonomous Organizations And Trust Enabling Technologies

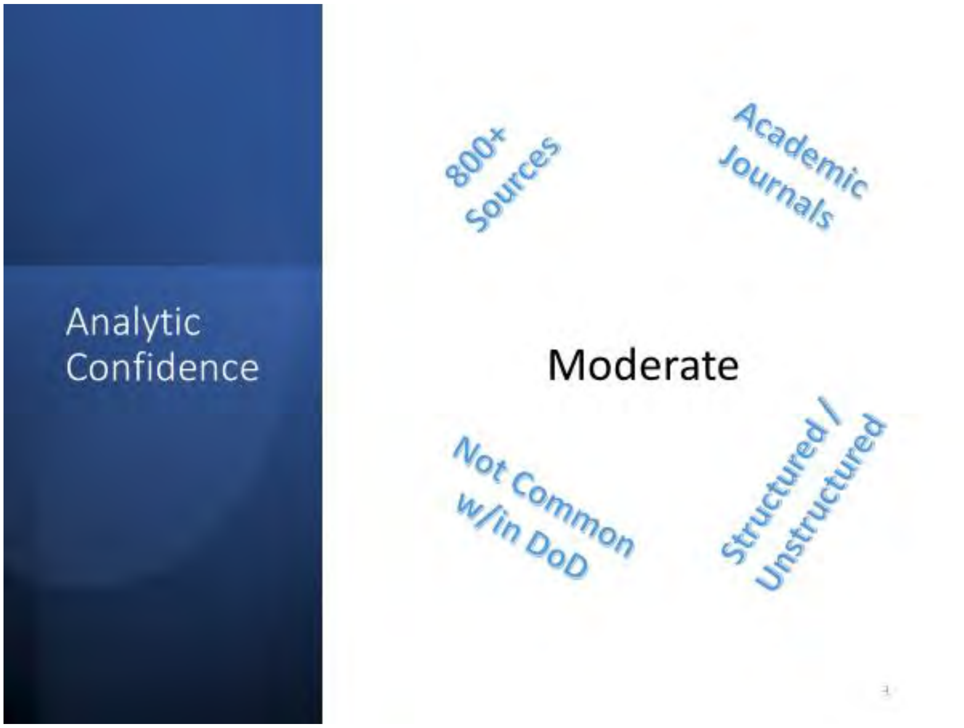
USAWC Futures Seminar
COL Troy Alexander, AG
COL Greg Pavlichko, FA57
COL Anthony Pollio, MI
LTC Patrick Hofmann, MI
LTC Nicky Shadley, SC



Words of Estimative Probability

almost no chance	very unlikely	unlikely	roughly even chance	likely	very likely	almost certain(ly)
remote	highly improbable	improbable (improbably)	roughly even odds	probable (probably)	highly probable	nearly certain
01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Source: ICD 203



Analytic Confidence

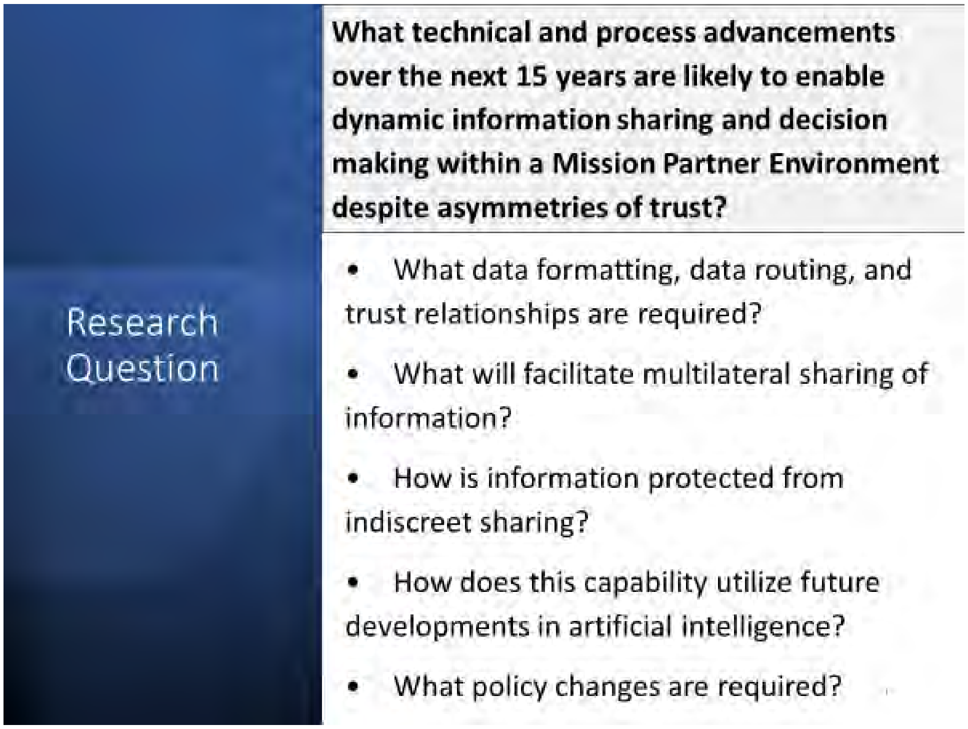
800+ Sources

Academic Journals

Moderate

Not Common w/in DoD

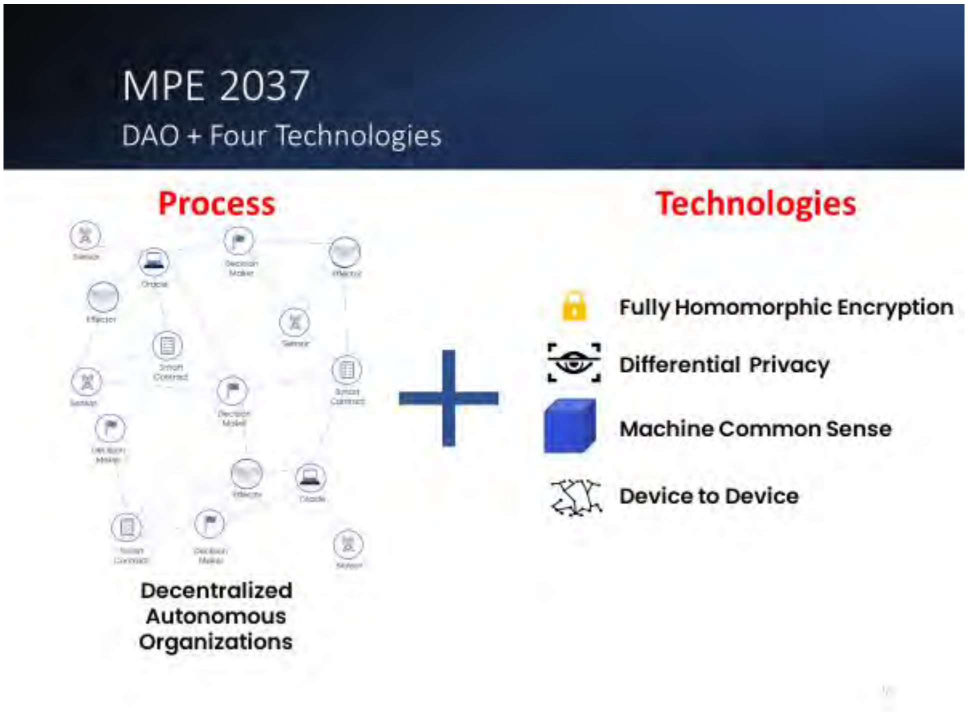
Structured / Unstructured



Research Question

What technical and process advancements over the next 15 years are likely to enable dynamic information sharing and decision making within a Mission Partner Environment despite asymmetries of trust?

- What data formatting, data routing, and trust relationships are required?
- What will facilitate multilateral sharing of information?
- How is information protected from indiscreet sharing?
- How does this capability utilize future developments in artificial intelligence?
- What policy changes are required?



MPE 2037

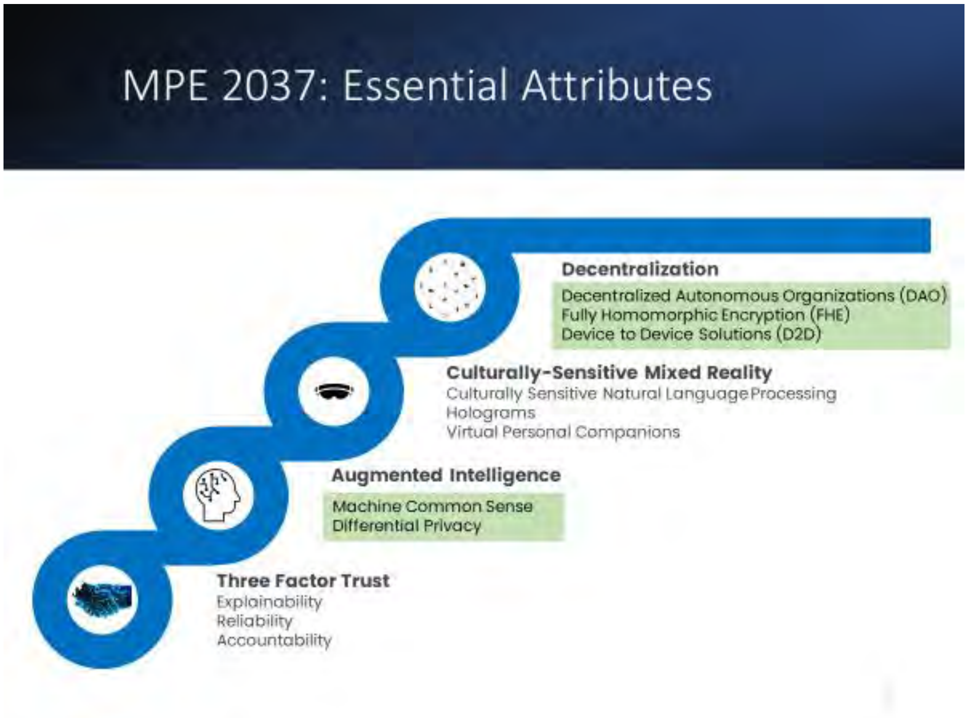
DAO + Four Technologies

Process

Decentralized Autonomous Organizations

Technologies

- **Fully Homomorphic Encryption**
- **Differential Privacy**
- **Machine Common Sense**
- **Device to Device**



MPE 2037: Essential Attributes

Decentralization

Decentralized Autonomous Organizations (DAO)
Fully Homomorphic Encryption (FHE)
Device to Device Solutions (D2D)

Culturally-Sensitive Mixed Reality

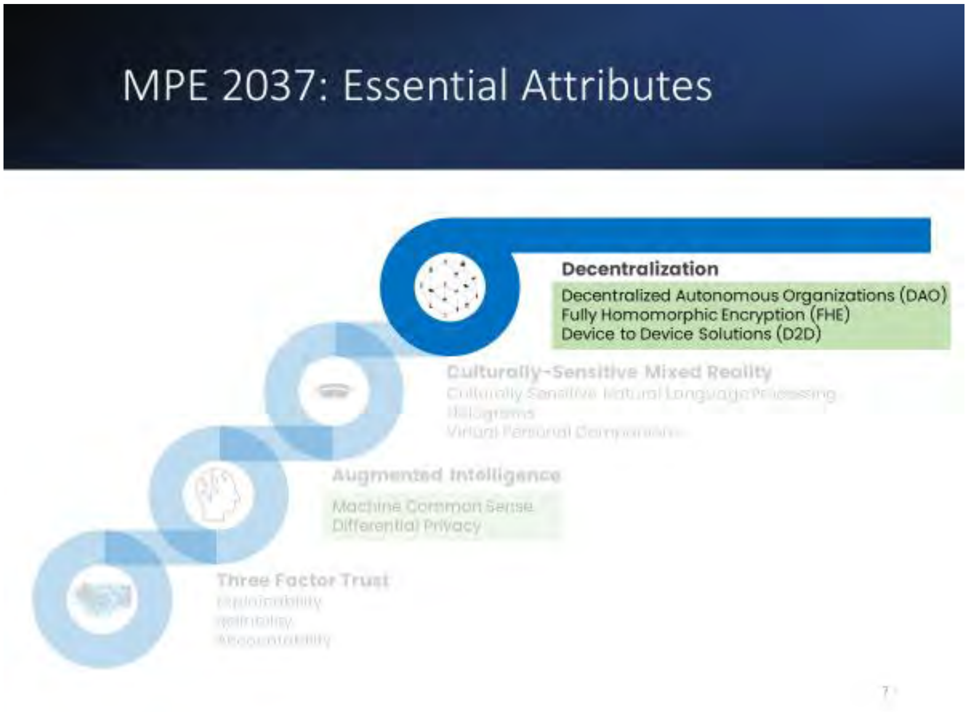
Culturally Sensitive Natural Language Processing
Holograms
Virtual Personal Companions

Augmented Intelligence

Machine Common Sense
Differential Privacy

Three Factor Trust

Explainability
Reliability
Accountability



MPE 2037: Essential Attributes

Decentralization

Decentralized Autonomous Organizations (DAO)
Fully Homomorphic Encryption (FHE)
Device to Device Solutions (D2D)

Culturally-Sensitive Mixed Reality

Culturally Sensitive Natural Language Processing
Holograms
Virtual Personal Companions

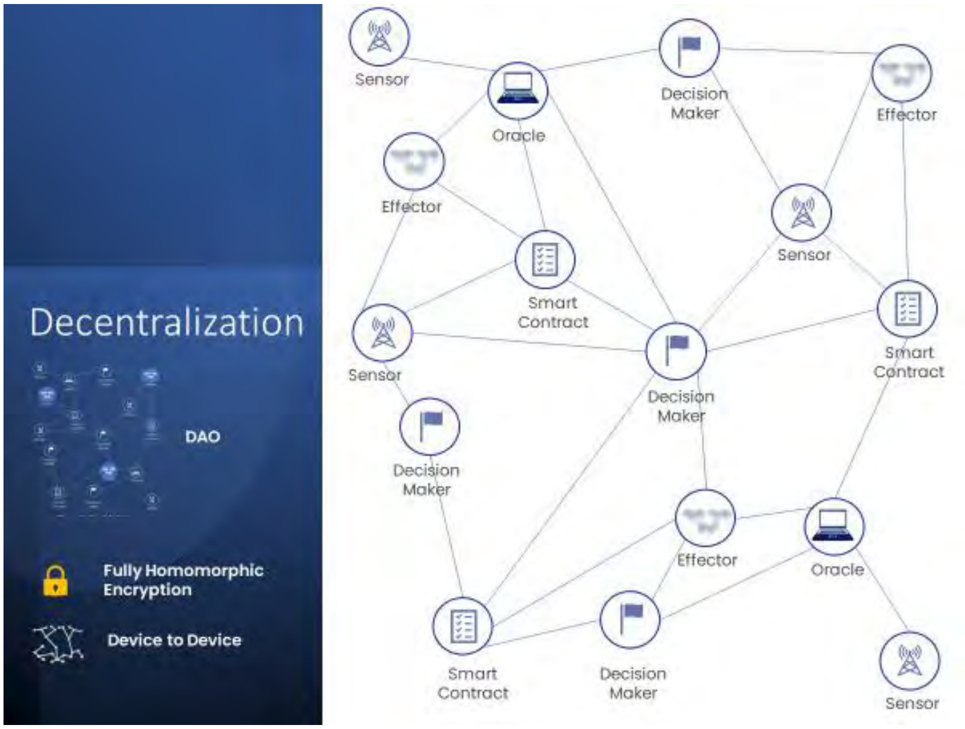
Augmented Intelligence

Machine Common Sense
Differential Privacy

Three Factor Trust

Explainability
Reliability
Accountability

7



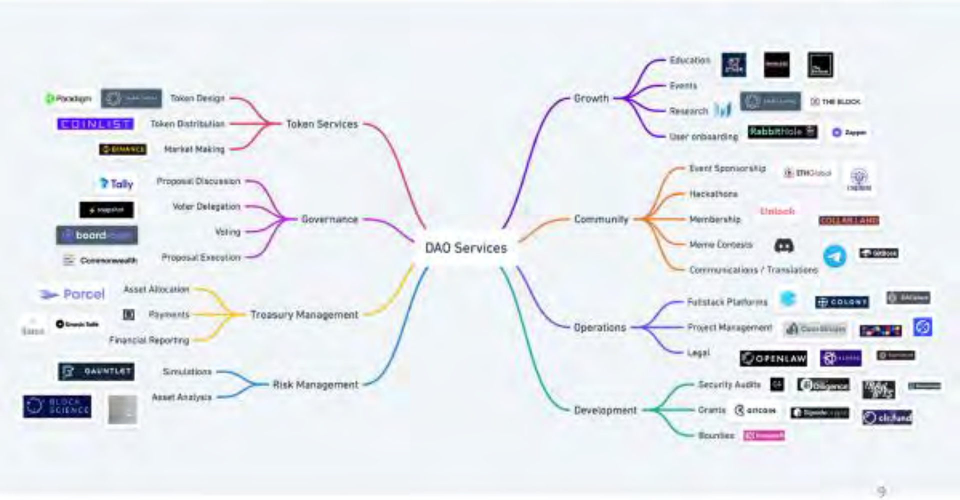
Decentralization

DAO

Fully Homomorphic Encryption

Device to Device

DAOs



DAO Services

Token Services
- Token Design
- Token Distribution
- Market Making

Governance
- Proposal Discussion
- Voter Delegation
- Voting
- Proposal Execution

Treasury Management
- Asset Allocation
- Payments
- Financial Reporting

Risk Management
- Simulations
- Asset Analysis

Growth
- Education
- Events
- Research
- User onboarding

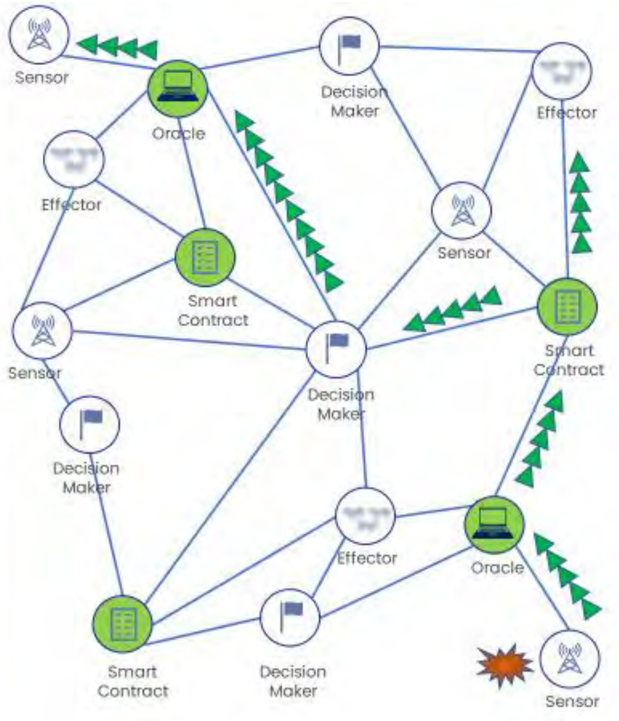
Community
- Event Sponsorship
- Hackathons
- Membership
- Meme Contests
- Communications / Translations

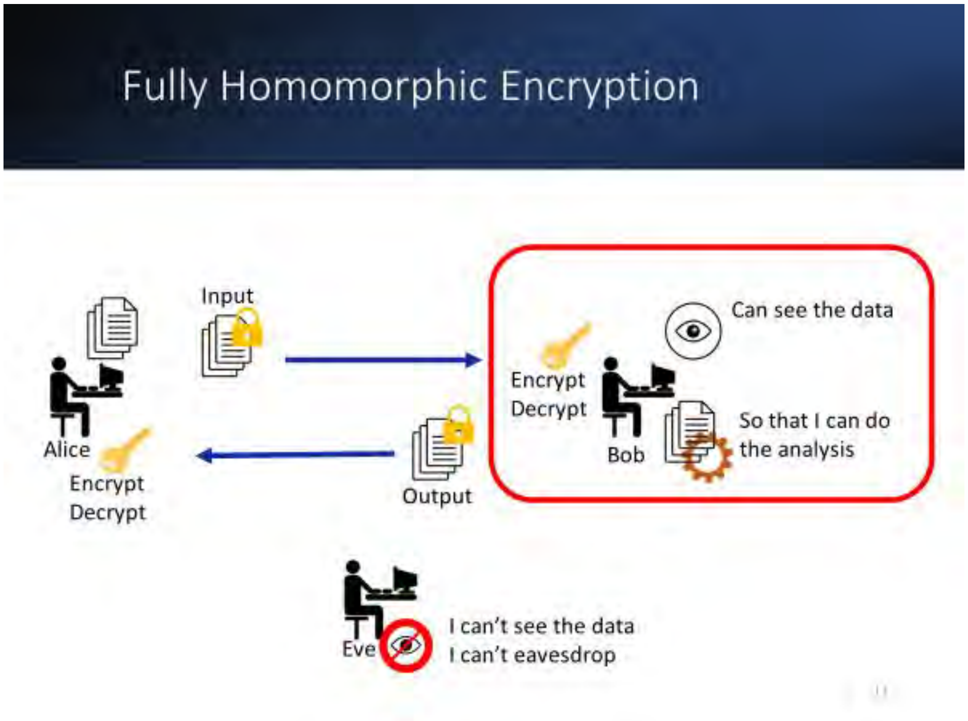
Operations
- Fullstack Platforms
- Project Management
- Legal

Development
- Security Audits
- Grants
- Bounties

DAO Components:

- Blockchain
- Smart Contracts
- Oracles





Fully Homomorphic Encryption

Input

Alice

Encrypt
Decrypt

Output

Encrypt
Decrypt

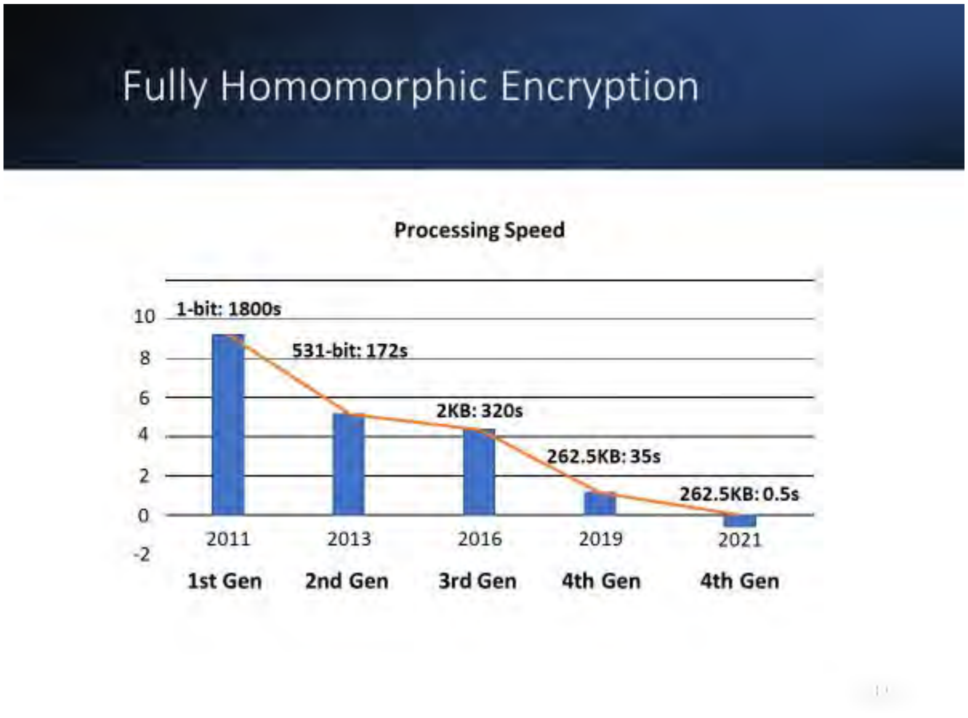
Bob

Can see the data

So that I can do the analysis

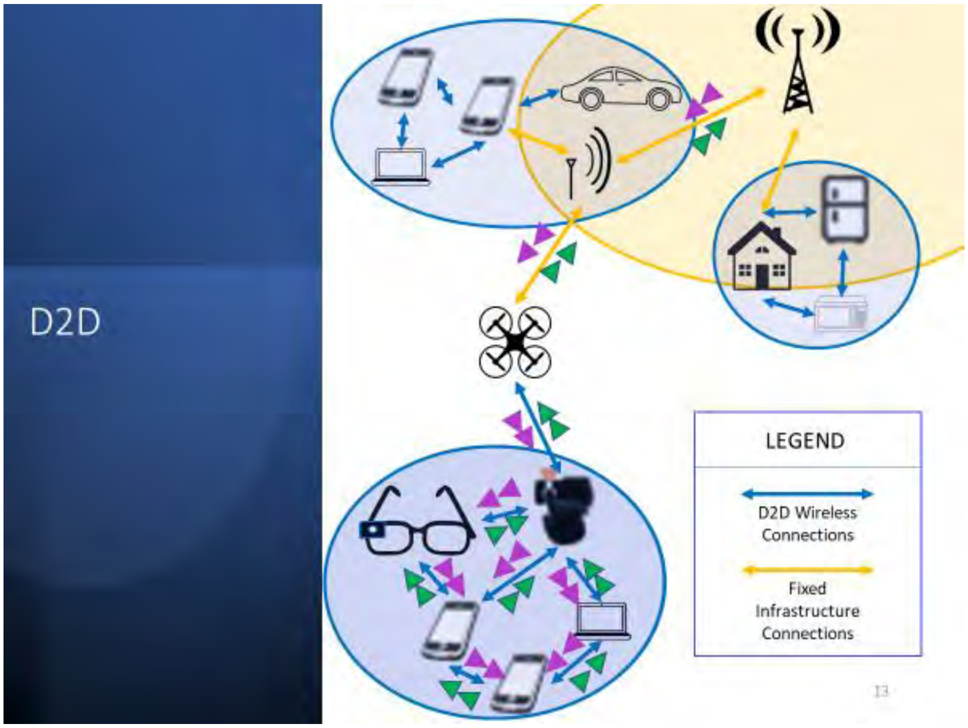
Eve

I can't see the data
I can't eavesdrop



Fully Homomorphic Encryption

Processing Speed



D2D

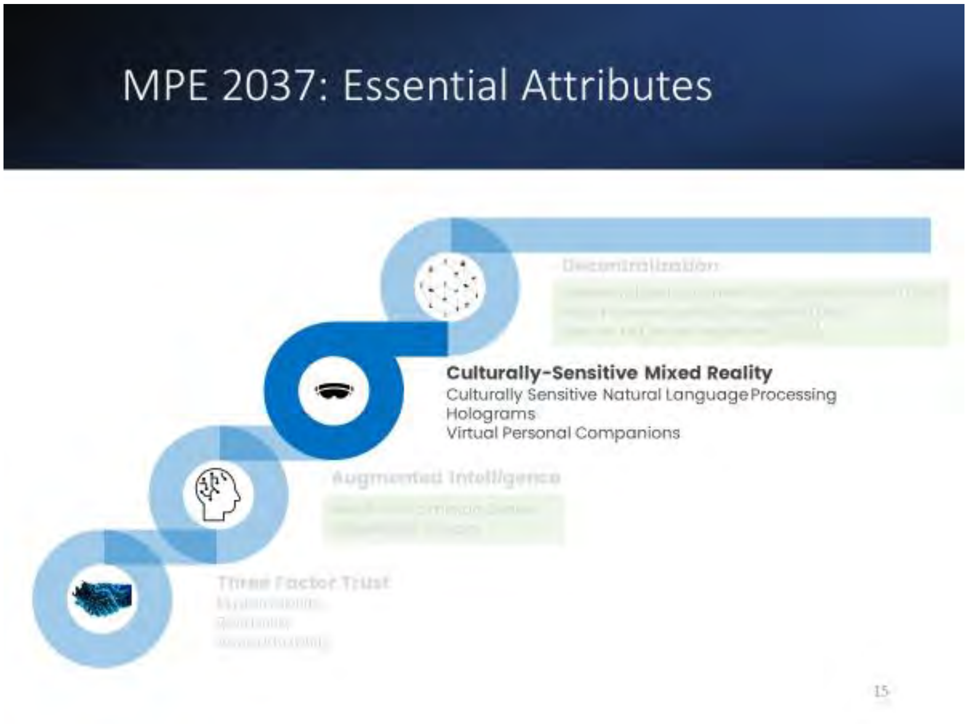
LEGEND

D2D Wireless Connections

Fixed Infrastructure Connections

13

D2D



MPE 2037: Essential Attributes

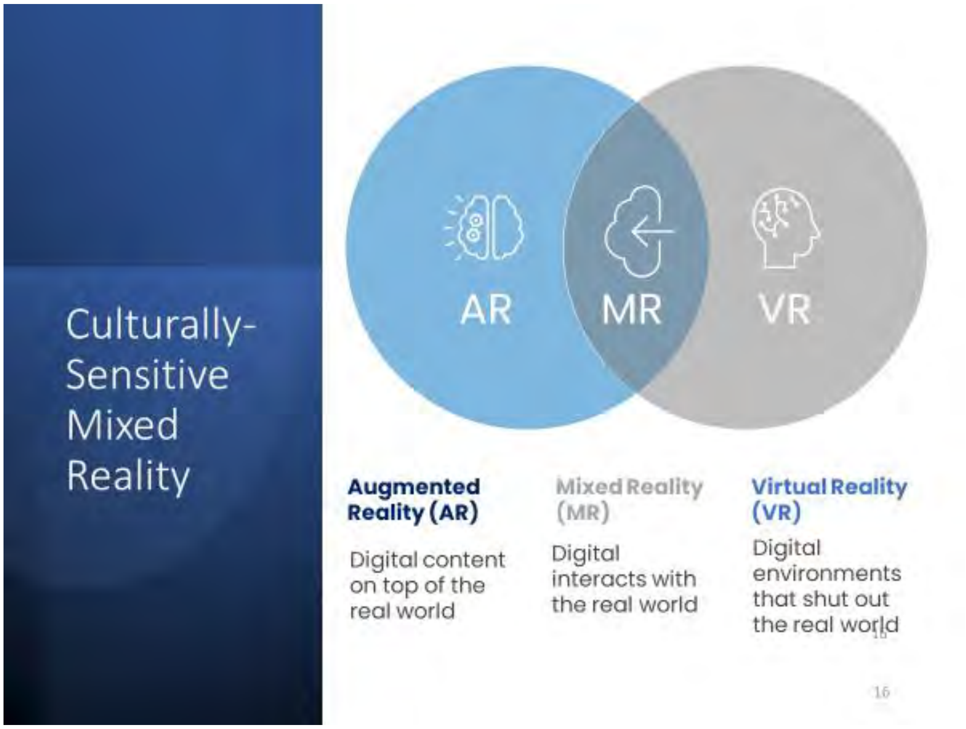
Decentralization
[illegible]

Culturally-Sensitive Mixed Reality
Culturally Sensitive Natural Language Processing
Holograms
Virtual Personal Companions

Augmented Intelligence
[illegible]

Three Factor Trust
[illegible]

15



Culturally-Sensitive Mixed Reality

Augmented Reality (AR)
Digital content on top of the real world

Mixed Reality (MR)
Digital interacts with the real world

Virtual Reality (VR)
Digital environments that shut out the real world

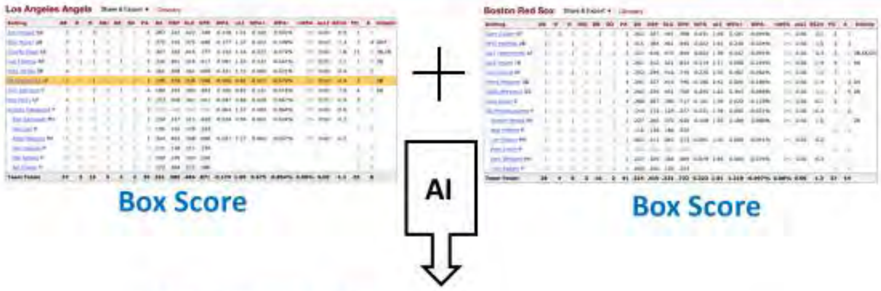
16

Culturally-Sensitive Natural Language Processing

Translation Storytelling

17

Sharing Data Through Story Telling



AI Generated Story

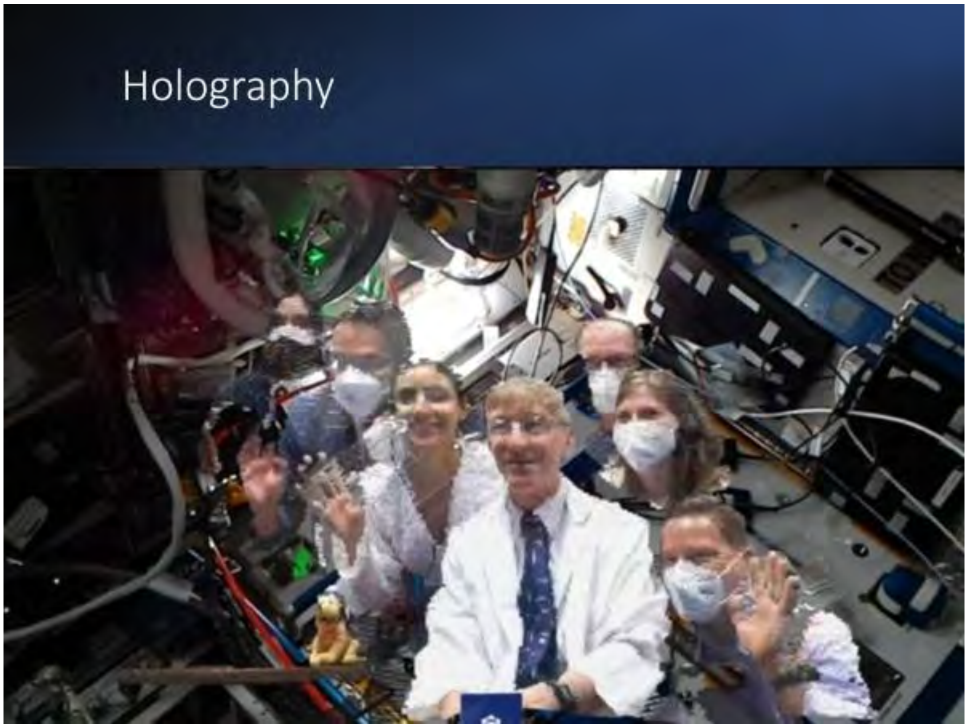
BOSTON (AP) — Shohei Ohtani struck out 11 over seven shutout innings, had two hits and drove in a run in the Los Angeles Angels' 8-0 win over the Boston Red Sox on Thursday.

Making his pitching debut in Babe Ruth's original ballpark, the sport's biggest two-way star since Ruth induced 29 swings and misses from Boston batters — a career high for Ohtani (3-2) and the most for any pitcher this year.

18

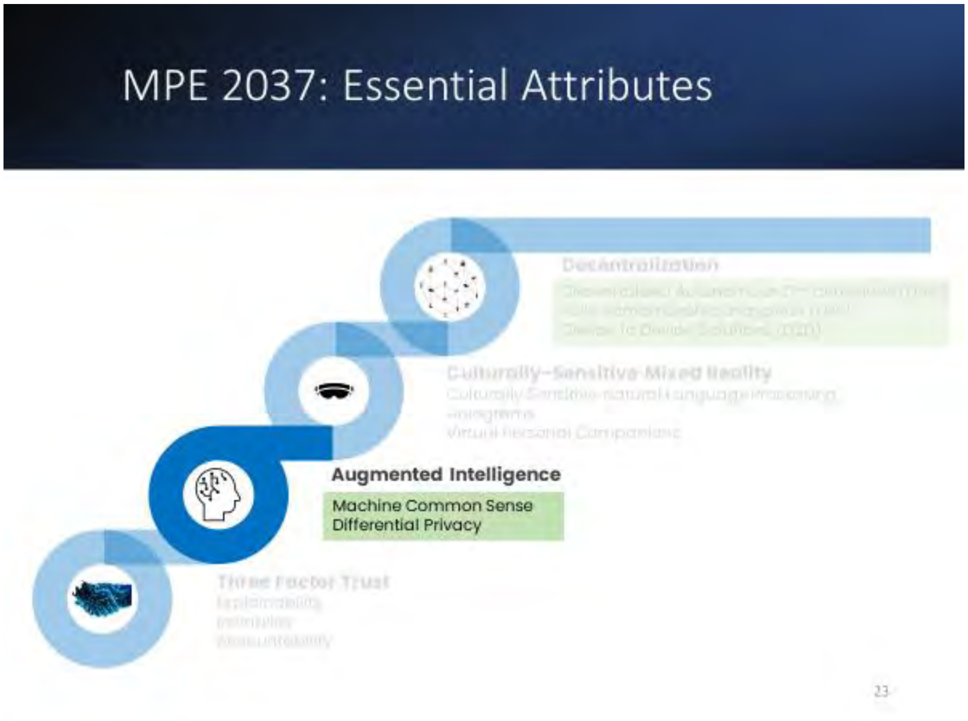
Holography

Holography



Holography

Virtual Personal Companions



MPE 2037: Essential Attributes

Decentralization

Decentralized Autonomous Organizations (DAO)
[illegible]
Device to Device Solutions (D2D)

Culturally-Sensitive Mixed Reality

Culturally Sensitive Natural Language Processing
Holograms
Virtual Personal Companions

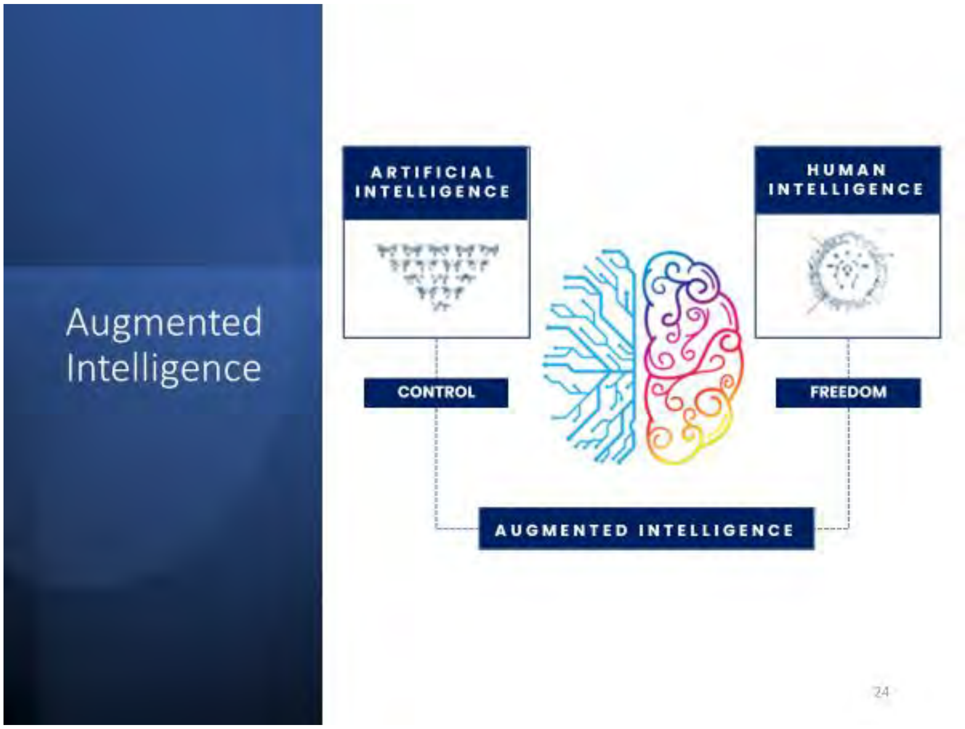
Augmented Intelligence

Machine Common Sense
Differential Privacy

Three Factor Trust

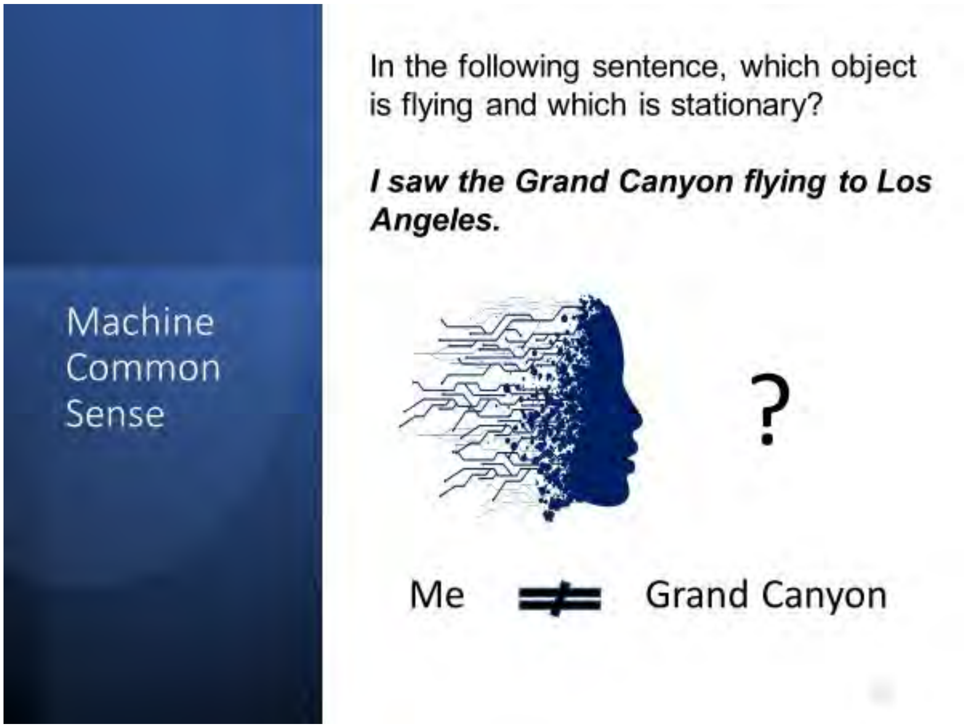
Explainability
[illegible]
Accountability

23



Augmented Intelligence

24



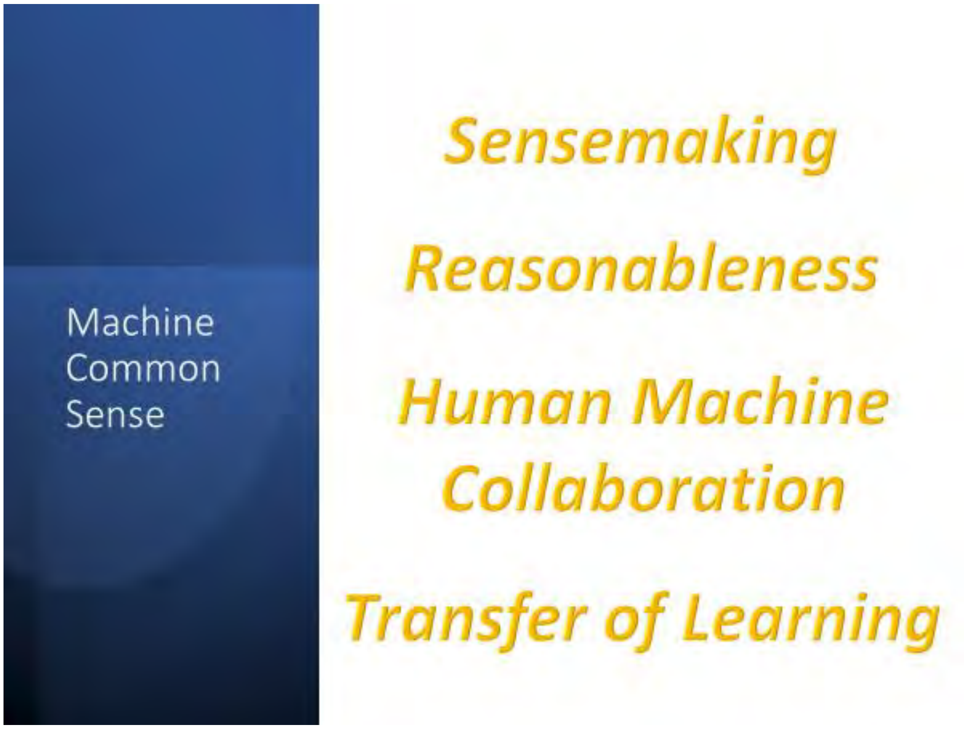
Machine Common Sense

In the following sentence, which object is flying and which is stationary?

I saw the Grand Canyon flying to Los Angeles.

?

Me ≠ Grand Canyon



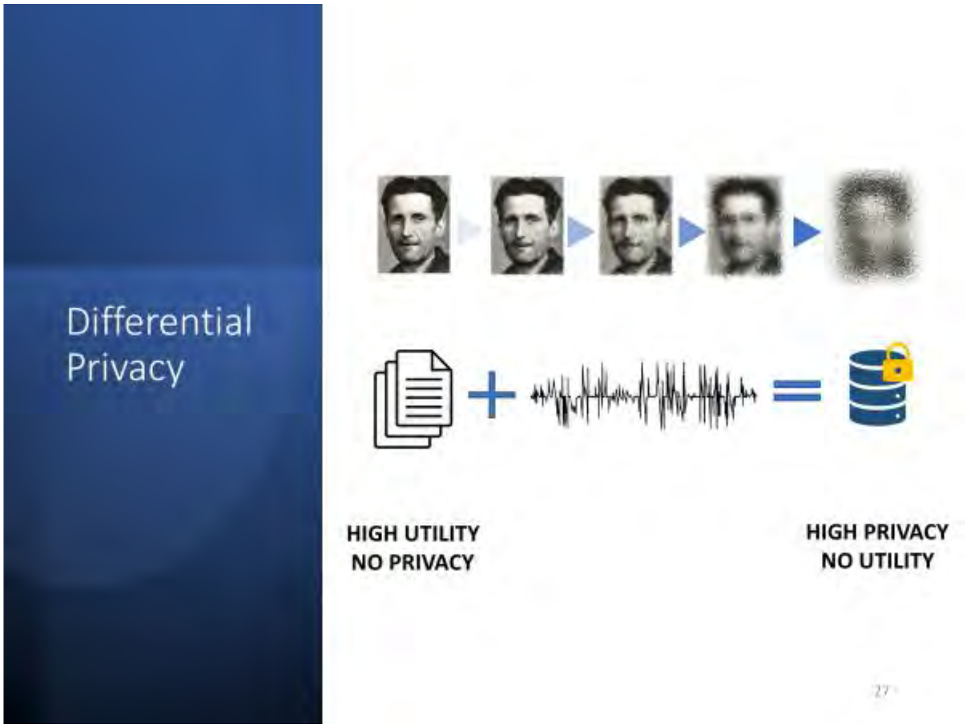
Machine Common Sense

Sensemaking

Reasonableness

Human Machine Collaboration

Transfer of Learning

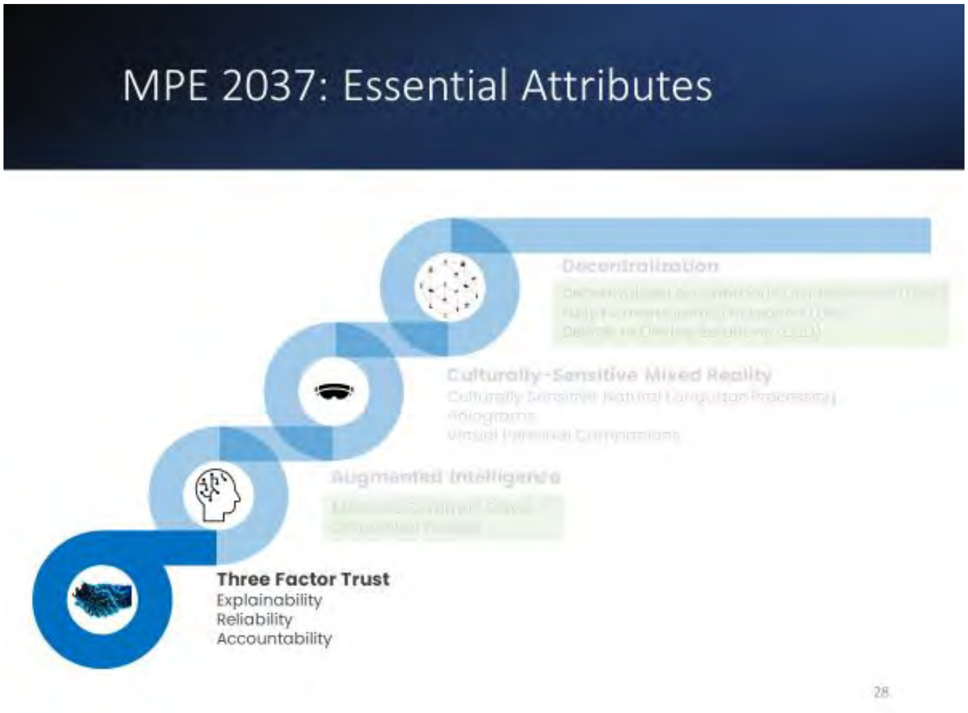


Differential Privacy

HIGH UTILITY
NO PRIVACY

HIGH PRIVACY
NO UTILITY

27



MPE 2037: Essential Attributes

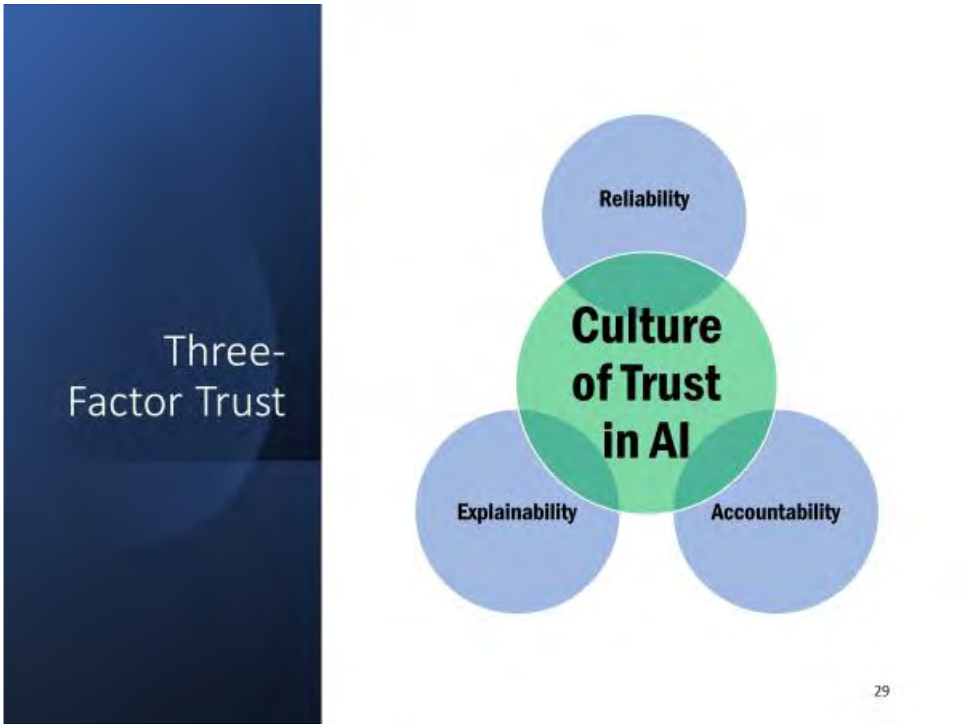
Decentralization
[illegible]
Fully Homomorphic Encryption (FHE)
Defense in Depth Solutions [illegible]

Culturally-Sensitive Mixed Reality
Culturally Sensitive Natural Language Processing
Holograms
Virtual Personal Companions

Augmented Intelligence
[illegible]
[illegible]

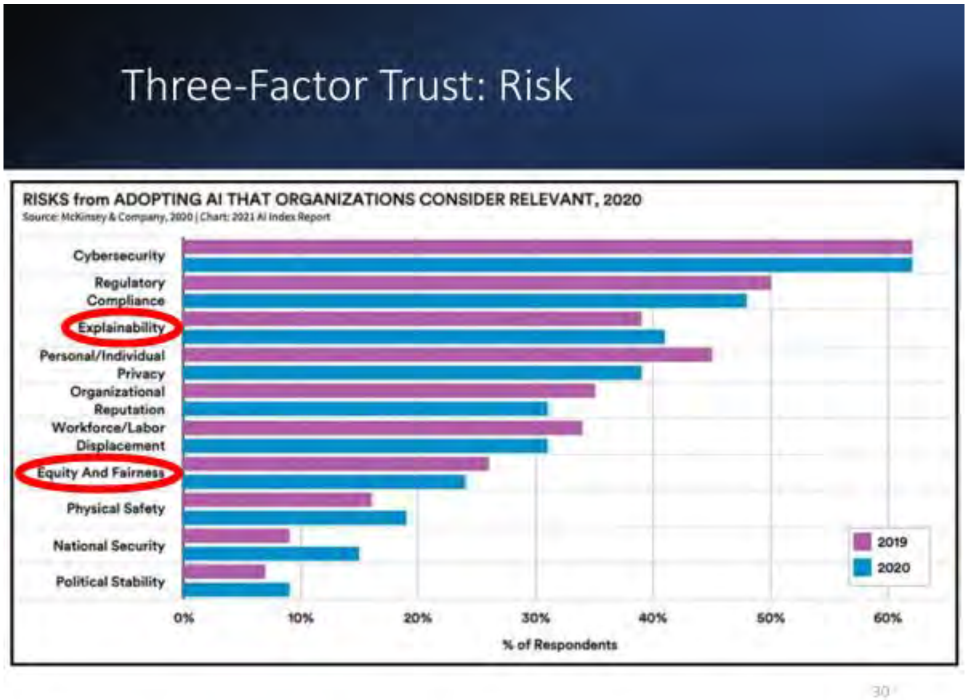
Three Factor Trust
Explainability
Reliability
Accountability

28



Three-Factor Trust

29

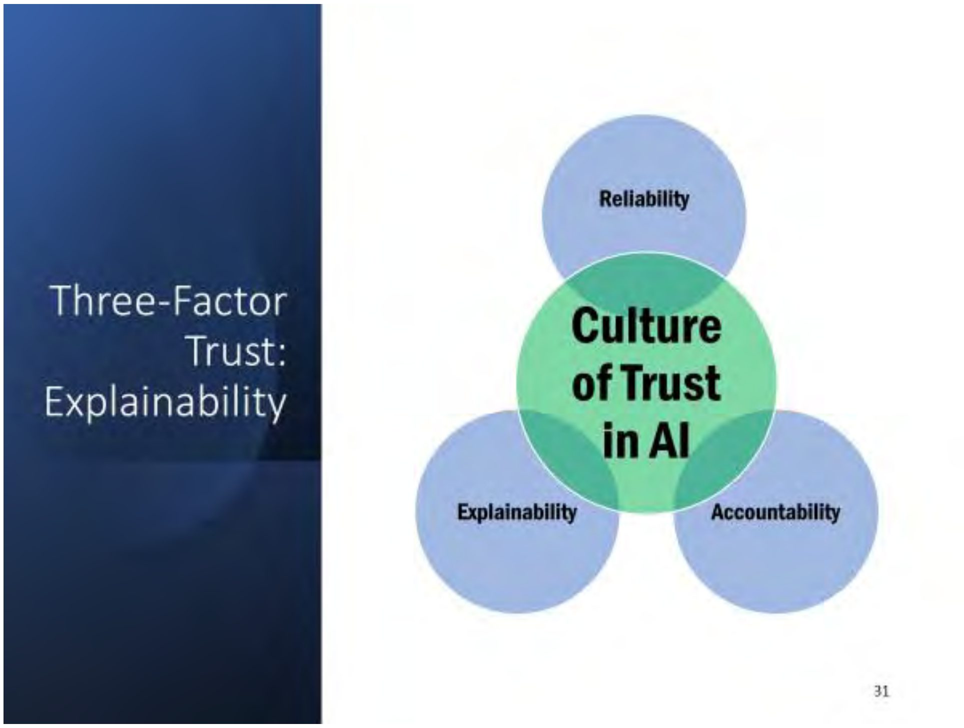


Three-Factor Trust: Risk

RISKS from ADOPTING AI THAT ORGANIZATIONS CONSIDER RELEVANT, 2020

Source: McKinsey & Company, 2020 | Chart: 2021 AI Index Report

30



Three-Factor Trust: Explainability

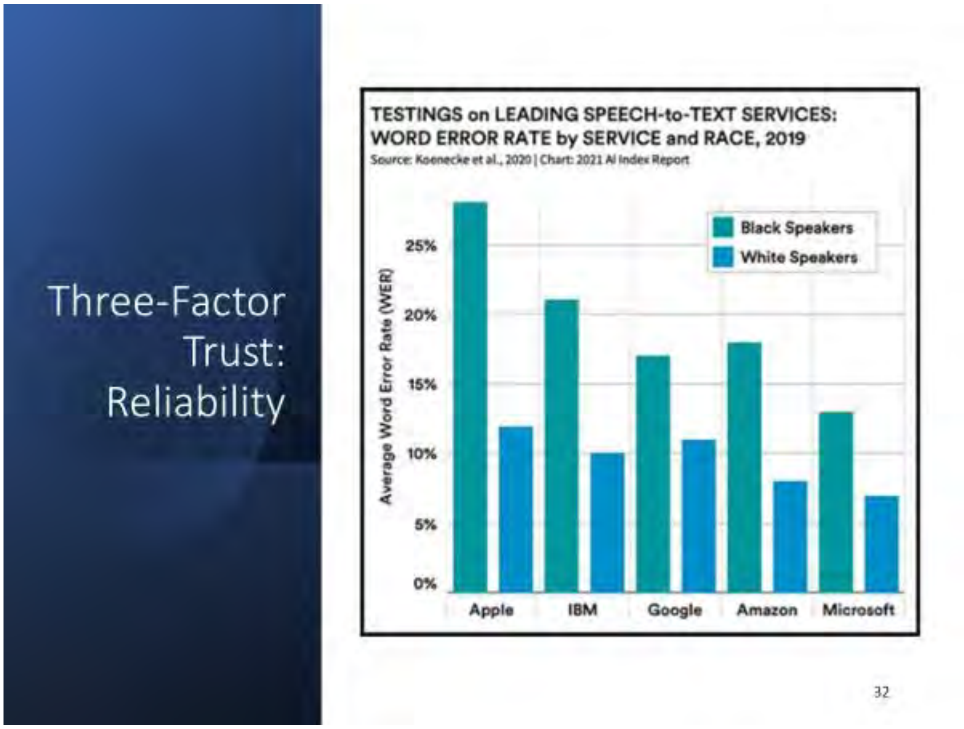
Culture of Trust in AI

Reliability

Explainability

Accountability

31



Three-Factor Trust: Reliability

TESTINGS on LEADING SPEECH-to-TEXT SERVICES: WORD ERROR RATE by SERVICE and RACE, 2019

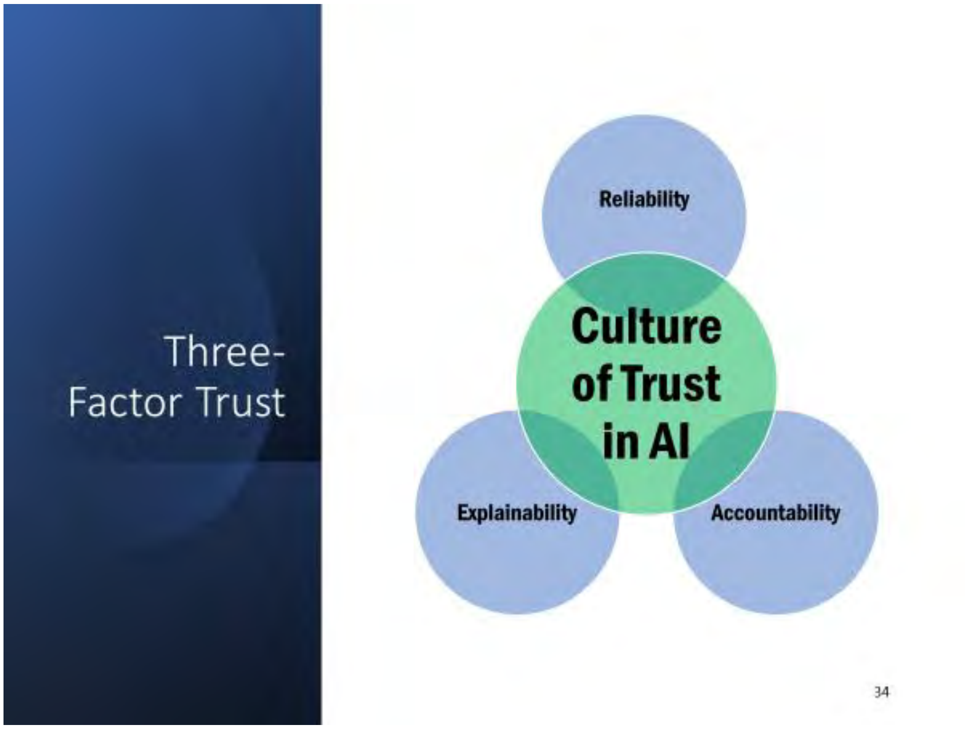
Source: Koenecke et al., 2020 | Chart: 2021 AI Index Report

32

Three-Factor Trust: Accountability

33

Three-Factor Trust



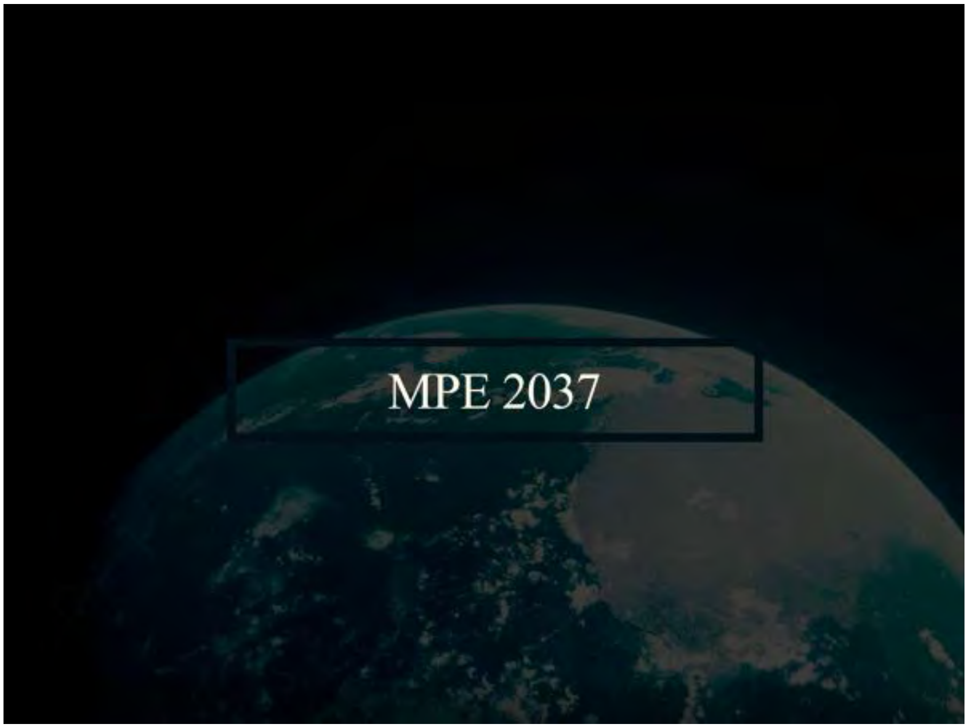
Reliability

Culture of Trust in AI

Explainability

Accountability

34



MPE 2037

"The robots have become self-aware and self-loathing. Now all they do is write novels."

TIES

TRUST AND INFORMATION ECO-SYSTEM