Human-Machine Teaming 2030-2040: Redefining the Continuum

Human-Machine Teaming 2030-2040: Redefining The Continuum

By

LTC Owen Adams
Mr. Reginald Shuford
COL Nathaniel Stone
LTC Nicole Washington
COL Dennis Weaver

United States Army War College
Class of 2023

DISTRIBUTION STATEMENT:
Approved for Public Release
Distribution is Unlimited

(This page intentionally left blank)

About This Document

The members of Team Singularity produced this collective strategic research project as one of the prerequisites to complete the Masters of Strategic Studies program at the United States Army War College (USAWC). The research, analysis, and production of this report conducted from October 2022 through April 2023 as part of the Army Futures Seminar for Academic Year 2023.

Requirements

This report answers a strategic question posted by GEN James E. Rainey, Commanding General, United States Army Futures Command, based on available open-source information and interviews with subject-matter experts.

What are the likely applications[1] across the continuum of human-machine teaming[2] which will be technologically feasible, militarily relevant, and ethically acceptable through 2040[3]?

- What are the likely legal and ethical implications which may drive requirements or generate limitations? How are those likely to change between now and 2040?
- What is the future of human-machine teaming across domains with a particular emphasis on landpower?
- What are the likely determining factors for the utilization and prioritization of autonomous systems across the scope of warfighting functions?
- How will international and social norms likely evolve regarding the use of autonomous systems in combat between now and 2040?

The team's findings were produced in multiple mediums, including a digital PDF version (primary), a digital online mind map, and a soft-bound book format. Multiple methodologies were used to determine key findings and convergences, including

[1] Applications refers to broad use of artificial intelligence and is not limited in scope to software.
[2] There is no published Department of Defense definition for human-machine teaming, however, industry standard uses the Brookings institute definition which defines the concept as a relationship; one made up of at least three equally important elements: the human, the machine, and the interactions and interdependencies between them.
[3] The scope of time will be examined in two blocks: 2030-2035 and 2035-2040

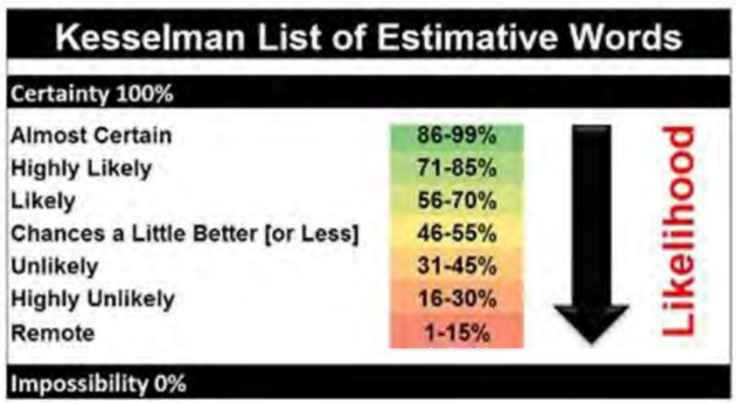
interviews with subject-matter experts, scholarly publications, open-source reporting, and the nominal group technique.

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. They utilized a combination of structured analytic techniques including nominal group technique and network analysis among others. The Singularity team also evaluated analytic confidence utilizing Petersons Analytic Confidence Factors coupled with the Friedman Corollaries (see Annex B).

Words of Estimated Probability

The research team used Kesselman's List of Estimative Words as their guide for determining their Words of Estimative Probability (WEP) (see Annex C) for determining the likely applications across the continuum of human-machine teaming which will be technologically feasible, militarily relevant, and ethically acceptable through 2040.



Source Reliability

Source reliability is noted at the end of each citation as low (L), moderate (M), or high (H). The citation is hyperlinked to the source. Source reliability is determined using Standard Primary Credibility Scale (see Annex D) and the Trust Scale and Website Evaluation Worksheet (see Annex E). Sourced figures and photos embedded in the report are also hyperlinked to their source.

Key Findings

By 2040, the applications for human-machine teaming (HMT) will highly likely (71-85%) be distributed across not *one*, but rather *four* continua. *Most* will be militarily relevant and technically feasible, and *some* will be ethically acceptable, depending on the wide variety of governance policies likely (56-70%) to be in place, as well as the status of the competition continuum.

The four continua mentioned above are: (see Annex G for full definitions)

- Level of Social Interaction: Non-social versus social user interfaces. Non-social systems which are not designed to interact conversationally with humans or other systems (example: Uber Driver Interface) versus social systems, whose user interface is designed to understand and respond to social cues, has the logical conversational capability, and simulates human-like behavior (example: Generative Pre-trained Transformer (ChatGPT))
- Level of Autonomy: Human in the loop (HITL) through human out of the loop (HOOTL). HITL (example: Advanced Field Artillery Tactical Data System) through human on the loop to (HOTL) (example: Patriot system or close-in weapon system (CWIS), through HOOTL, (example: fully lethal autonomous weapons)
- Level of Capability: Narrow versus Broad Artificial Intelligence (AI). Narrow describes most current AI technology designed for one specific application (example: Speech or facial recognition) versus broad functionality, where an application is designed to manage a wide array of tasks simultaneously (example: digital intelligence analysis).
- Level of Robotics: Non-Robotic through robotic. Non-Robotic system which cannot be physically touched (example: Alexa) versus holographic representation which can be seen, but not touched (example: Cortana in the Halo video game) versus primarily robotic which can be touched and interact with the physical world (example: Spot® the Agile Mobile Robot)

The preponderance of today’s applications are primarily non-social, with mostly HITL levels of autonomy, “narrow” singularly tasked AI, and automated functions that are well short of robotic. Conversely, by 2040, it is highly likely that many militarily relevant systems, including some of the most important ones, such as command and control (C2) and intelligence, will have social user interfaces, show a significant progression toward HOTL autonomy, exhibit broad, multi-functional AI qualities and human-like cognitive ability with the substantial move toward robotic systems across the warfighting functions (WFF) (see Figure 1).

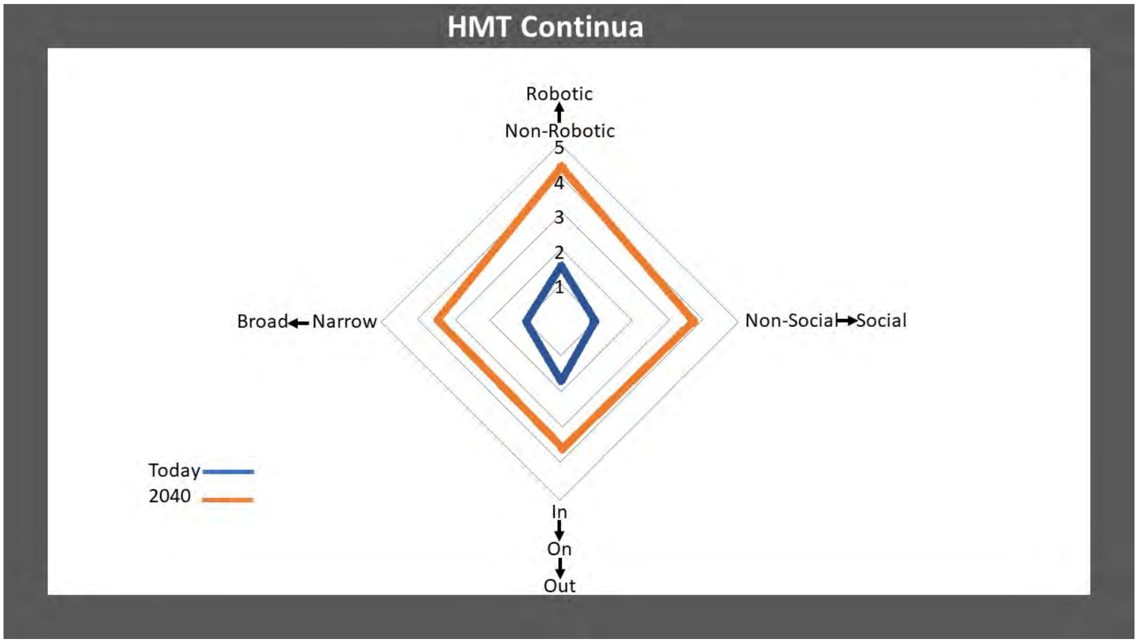


Figure 1: Depicts the aggregate of HMT applications across all WFFs. The team investigated HMT by combining a comprehensive analysis of current human-machine collaboration strategies and technologies with personal experience, and research into the future requirements of large military organizations. These findings were synthesized and combined with a review of forward-looking HMT literature to determine the system's key continua. Finally, the relationships between each component were evaluated for change using the Nominal Group Technique and cross-checked through the 30 individual reports that make up the bulk of this study. The final scores are based on the average values and are designed to show the degree of change across the continua over time.

The Future of War Fighting Functions Across The Continua

While the description above provides an overview of militarily relevant HMT across the continua, below are some specific examples to show how the applications are likely to trend within the different WFF, according to the research.

Command & Control (C2)

It is highly likely that the applications which support HMT for C2 will involve significant changes, including increased social interface platforms with broad AI capabilities and predominantly HOTL autonomy. Many staff officers will likely not be present with the commander in a tactical operations center. Rather they will be replaced or augmented by artificial agents working from dispersed locations, able to provide real-time data through virtual reality (VR) or augmented reality (AR) devices (see Figure 2). This Virtual Tactical Operations Center (V-TOC) is likely enabled by the integration of a number of applications such as 6G communication networks, Edge AI technology, neuromorphic computing, and advanced holographic display technology. The integration of these enabling technologies will likely provide HMTs with a more accurate common operating picture of adversaries, threats, as well as assets available and potential courses of action.

Figure 2: Virtual Tactical Operations Center (V-TOC) depicts future C2 capabilities in a distributed combat environment. Source: Fiverr

- Social user interfaces have recently demonstrated their appeal in a stunning fashion. According to Brookings, the demand for Large Language Models (LLMs), which power platforms such as ChatGPT (the fastest growing application ever), are driving computational development to double every six months, indicating the trend toward more socially based interfaces.
- Industry experts, including Nick McKeown, senior vice president of the Network and Edge Group at Intel, expect that 6G will likely be rolled out around 2030. 6G networks will likely provide the necessary network to run Edge AI systems, ideal for maintaining C2 at dispersed locations in large-scale combat operations (LSCO) and

Figure 3: 6G and Edge enabled operations center. Source: Team Singularity MidJourney prompt.

providing the infrastructure and bandwidth which advanced holographic displays will require (see Figure 3).

- Technology experts at IBM also project that the integration of Edge AI and their neuromorphic computing chip will support future mission command systems by providing speed, efficiency, and security to software capabilities required for seamless operations in a field environment and support high-performance applications such as AR and VR images.

Intelligence

By 2040, applications supporting the intelligence WFF are highly likely to have notably more socially interactive and intuitive interfaces with customizable dashboards, utilizing advances in AR displays and AI visualization tools. 6G network capabilities, upgraded sensor technology, (see Figure 4) and advances in holographic technologies will provide increased functionality to the broad-based AI systems, capable of providing real-time threat analysis and situational awareness through the fusion of all sensor data. Intelligence is likely to have slight changes in autonomy, remaining HOTL, with a virtual analyst to collect, analyze and provide advice from dispersed locations. Intelligence is likely to see a slight progression toward robotic advancements, primarily through advanced holographic 3D displays which provide commanders with a personalized view of the operational environment.

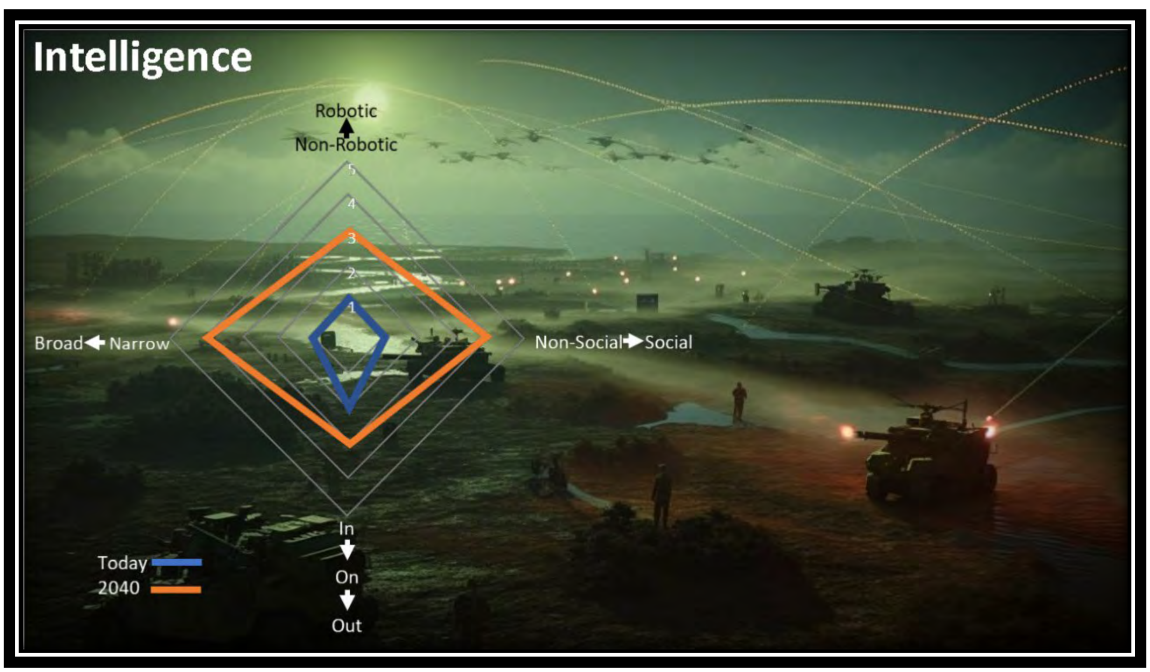


Figure 4: The future of Intelligence shows greatest growth in the social and broad continua. Source: Team Singularity MidJourney prompt.

- According to PEW research, more than 50% of millennials rely on digital assistants capable of performing everyday tasks through voice commands, indicative of rapid trends toward more socially based interface devices. Companies like Samsung, Apple, Amazon, and Google continue to invest heavily in integrating such voice-enabled technology with AI applications like ChatGPT.
- Specialized hardware and software suites, such as Research Laboratories' holographic displays, and Field Lab's initiatives toward solid light displays, provide advanced and more efficient hardware than today's touchscreen displays. Commercial investments and research in intelligence will provide prototypes that will be of equal benefit to Department of Defense (DoD) analysts as well.
- According to the Chinese company Yanfeng Automotive Interiors, future advanced displays will likely be a combination of multiple user interfaces such as: Touchpoint's "no-screen" touch capability, Samsung's foldable, flexible screens, and BMW's voice-controlled concept car, or even 3D visual images.

Movement and Maneuver (M2)

It is highly likely that the applications which support HMT relevant to M2 will involve significantly increased integration of human-robot teaming, with robots acting as organic assets and collaborating with human Soldiers. The M2 WFF is highly likely to include significantly more social interfaces, broad functionality, and HOTL autonomy due to advancements in robotics and autonomous systems (RAS), liquid neural networks (LNN), and brain-computer interfaces (BCI), but limited by battery power (see Figure 5).

Figure 5: Integration and advances across all four continua in movement and maneuver WFF. Source: Team Singularity MidJourney prompt.

- A 2023 Duke University research study projects that RAS will play a key role in expanding the operational reach, situational awareness, and effectiveness of maneuver forces in conducting cross-domain maneuvers. This will likely require the incorporation of significantly broader AI, such as autonomous vehicle perception, learning, reasoning, communication, navigation, and physical capabilities to augment and increase the freedom of maneuver in complex and contested environments.
- According to a 2020 RAND report, the application of BCI will support ongoing DoD technological initiatives, including improved decision-making and assisted-human operations, for advanced manned and unmanned combat teaming.
- Graz University, a leading institution for technology innovation, determined that Intel's neuromorphic chips are up to 16 times more energy efficient for deep learning. Due to their high power consumption, new AI methods that utilize deep neural networks (DNNs) pose a significant barrier to broader deployment, particularly in edge devices.

Sustainment

Between 2030 and 2040, sustainment applications will highly likely experience significant increases in robotization and automation (see Figure 6). Emergent

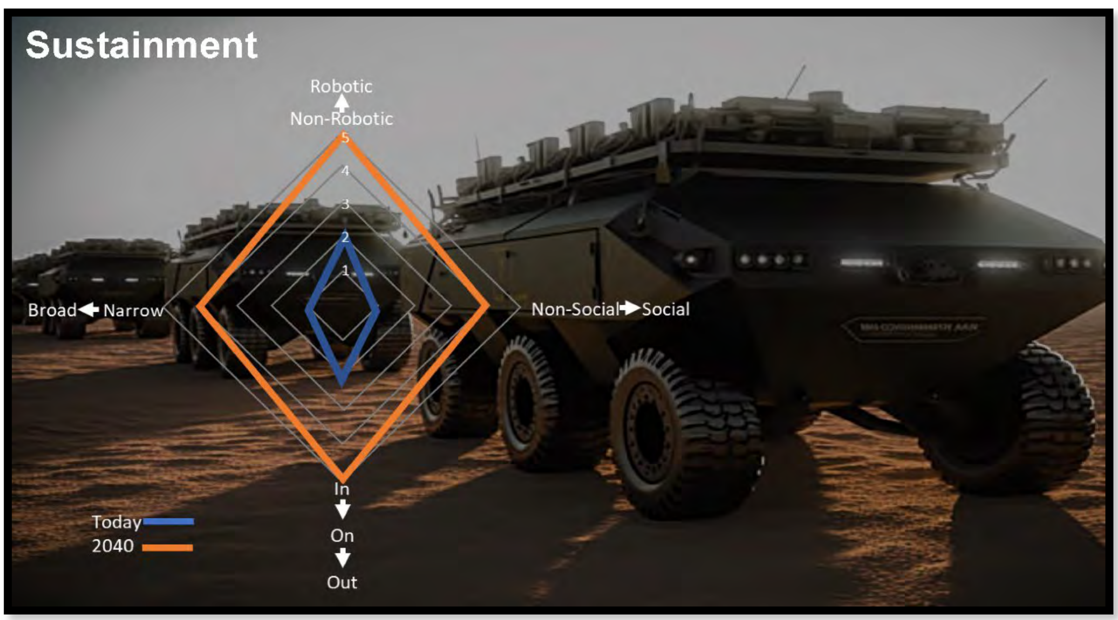


Figure 6: The future of Sustainment trends sharply more robotic and autonomous, moderately more social and more broad. Source: Team Singularity MidJourney prompt.

technologies such as Edge AI computing, 6G network availability, RAS and LNNs will likely support advanced robotics, capable of autonomously performing a wide array of sustainment-related tasks, while simultaneously using the mother ship approach to increase maintenance efficiencies and improve operational reach across longer lines of communication. Additionally, it will likely utilize more socially based interface devices, and moderate changes to broad-based AI capabilities. Among the six joint functions, sustainment operations present some of the most likely quick wins for the employment of AI and autonomous systems (AS) technologies.

- According to McKinsey, AI and ML are automating supply chains to learn and expect user activity. Predictive analytics automate supply chains using data mining, predictive modeling, and machine learning to analyze past and current facts to predict fluctuations and disruptions. This results in AI-enabled supply chains being over 65% more effective with reduced risk and lower overall costs.
- As recently as April 2023, researchers from Massachusetts Institute of Technology (MIT) demonstrated a new advancement in autonomous drone navigation, using brain inspired LNNs, a robust machine learning model that learns on the job and can adapt to changing conditions, which is an evolution in today's LLM. This advancement supports autonomous flying and driving in unseen or unfamiliar environments, contributing to future human-robot teams (see Figure 7).

Figure 7: MIT Drones Navigate Unseen Environments With Liquid Neural Networks. Click on the image or go to Drones navigate unseen environments with liquid neural networks - YouTube to view the video. Source MIT

Fires

It is highly likely that Fires applications in 2040 will incorporate significant advances in robotics technologies and AI integration across domains and WFFs to prioritize and engage enemy targets with self-guided munitions autonomously (see Figure 8). The Fires WFF is also highly likely to include a moderate increase in social user interface platform, providing visual and audio feedback on target selection and engagement, and moderate increases towards broad AI, due to the integration of multiple narrow sensors which feed a broad intelligence and C2 decision network. In concert with Edge AI and 6G networks, advancements in neuromorphic computing will likely enable robots and advanced platforms to learn from previous engagements, adapt to changing battlefield conditions, and optimize their firing solutions to minimize collateral damage.

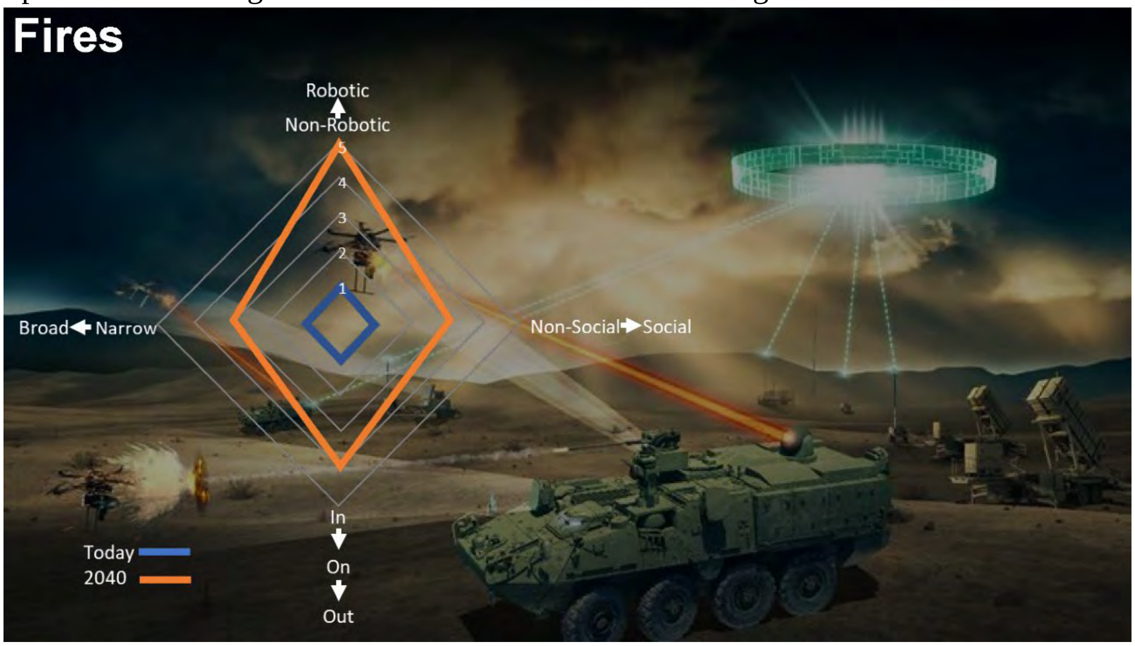


Figure 8: The future of Fires trends slightly toward social and broad and significantly more robotic. Source: Team Singularity MidJourney prompt.

- According to Peter Vetter, president of Bell Labs Core Research at Nokia, 6G will give future militaries an awareness of their surroundings that they have never had before. This will highly likely connect networks of sensors, wearables, robots, manned and unmanned vehicles, and internet of things (IoT) devices that use cloud and edge computing, reducing the bandwidth and time needed to transmit and process data, connecting the military IoT.
- The ongoing Russo-Ukrainian war is driving significant technological improvements across all four of the Fires continua. For example, a Forbes piece from 2023 highlighted recent endeavors in Ukraine where developers built autonomous drones with the capability to find and attack targets without human supervision.
- Likewise, Mick Ryan, a strategist and retired major general from the Australian Army, stated: “Autonomous systems that have emerged from the war in Ukraine… have proved their utility across a range of lethal and non-lethal missions... we should expect to see further proliferation after this war.”
- A 2023 RAND report discussed the potential for developing three types of robotic capabilities tailored to the needs of fires WFF: artillery reconnaissance robots, strike robots, and artillery fire robots. The author stated that the artillery fire robots would likely be able to reach speeds of 30 mph, be equipped with 120-mm artillery guns with an autoloader for 60 rounds and ensure a firing rate of 15 rounds per minute.

Protection

It is highly likely that the protection applications which support HMT will involve significantly advanced RAS and predominantly HOTL autonomy due to being primarily defensive in nature, requiring faster response time with minimal required human judgment. It is highly likely future protection will be categorized as physical protection and cyber defense protection (see Figure 9). Physical protection will likely incorporate robot teams,

Figure 9: The future of Protection trends sharply more social and moderate across the remaining three continua. Source: Team Singularity MidJourney prompt

consisting of aerial drones for observation, ground robots for physical protection, and vehicles to intercept missiles, but also be used as a power source for the drones and robots. Protection across the cyber domain will likely consist of autonomous intelligent cyber-defense agents (AICA) working in cohorts or swarms, capable, together, of detecting cyber-attacks, developing the appropriate countermeasures, and running and adapting tactically their execution. These advancements in the physical and cyber domain will likely be enabled by rapid advancements in robotics, Edge AI, updated neuromorphic chips, and homomorphic encryption.

- According to a 2020 RAND report, there are incentives to move humans to positions “on” the loop and “out” of the loop. Primarily in the context of defensive systems that need to react quickly to incoming threats, human authorization for every engagement might slow the system down and undercut threat-defeating capabilities. Especially in contexts where an adversary is leveraging its own high-speed AI systems, human-in-the-loop approaches risk a competitive disadvantage.

- According to Dr. Kott, chair of the NATO Science and Technology Organization's research group, AICA are necessary as humans are the weakest link in the cyber world, and human warfighters will not have the necessary skills or time to perform cyber defense locally.
- With further advancements of tools like Splunk and Microsoft Sentinel pulling in logs from a wide array of sources to manage both compliance and threats, AI will not only learn user patterns and identify anomalies but interact with security professionals to thwart real-time attacks. Improvements in AI technology sensors, applications and devices will highly likely contribute to more streamlined, combat functional interfaces, capable of quickly and accurately communicating critical targeting data, understanding and interacting with the HMT operator.

What are the likely legal and ethical implications which may drive requirements or generate limitations? How are those likely to change between now and 2040?

The likely legal and ethical implications which may drive requirements or limitations are tied into *TRUST*.

- According to U.S. Responsible AI (RAI) policy, key factors of trustworthiness include the ability to demonstrate reliable governance.
- There is currently a lack of standardized governance for AI, machines, and robotics internationally and it is unlikely (31-45%) that between now and 2035 there will be an enforceable international governance standard for AI. The U.S., European Union, and China are each leading efforts in diverse theories of regulation; most of which are based in Ethics and Policy.
- Even though our adversaries have proven they are willing to use LAWs indiscriminately, our standard of Ethics and adherence to International Humanitarian Law and Law of Armed Conflict and Just War Theory (Jus in bellum) will likely limit our propensity to use them.
- It is likely that between now and 2040 the level of trust in AI systems and HMTs will improve, due to recent emphasis on the topic, including the need to prioritize building systems and teams with transparency, explainability, audibility, and reliability.
- Some areas of concern are the disparity in the trust for the development and management of AI systems, including:
    - Trust Gap (too little trust) and Automation Bias (too much trust)
    - Propensity for program and systems biases
    - Data privacy and system protection (data poisoning)
    - Risk mitigation and management

What is the future of human-machine teaming across domains?

It is highly likely that three human-machine endeavors will underpin the development of future human-machine teaming across domains. Each is a distinct area of research, development, and investment. While each endeavor is likely to have a primary research focus, integration is key to obtain overmatch.

- Human-robot teaming (HRT). The concept of human-robot teaming is centered around the partnership between humans and robots, as well as the learning and understanding of how humans can effectively interact with their robotic counterparts. This involves the development of skills and abilities for humans to manage and assign tasks to a large team of robots, as well as to communicate and collaborate with them. This interdisciplinary field requires the input and expertise of various disciplines including systems engineering, cognitive sciences, and computer sciences.
- Humans-AI teaming (HAIT). As teams evolve, it is becoming more common to incorporate advanced forms of AI. The integration of humans and AI is crucial for effective strategic planning, operational planning, and analyzing future activities. This involves a specific type of analytical focus that is different from human-robot teaming.
- Human augmentation (HA). Human augmentation is a unique form of collaboration between humans and machines, where they function as a unified entity. Its primary aim is to enhance human abilities, both physical and cognitive, by incorporating mechanical, wearable, and implantable technologies to improve existing human performance. This collaboration is solely focused on augmenting human capabilities.

Priority HMT focus areas across the domain and WFF

All three human-machine research areas are highly likely promising in each domain of warfare; The synergy between them will significantly improve the lethality and sustainability of future forces (see Figure 10).

Figure 10: Projected trends for HMT between 2025-2040 across domains and WFF.

What are the likely determining factors for the utilization and prioritization of autonomous systems across the scope of warfighting functions?

The likely determining factors for the utilization and prioritization of autonomous systems across the scope of WFF will be the development of essential enabling applications in conjunction with technological advancements, the availability of resources to support the most relevant applications, trained and ready operators with the necessary skills to support effective HMT, and adherence to governance and ethical standards along the competition continuum (see Mind Meister Figure 11). Commercial research and development will continue to drive innovations with militarily relevant capabilities applicable across the scope of WFFs.

Team Singularity Mind Map

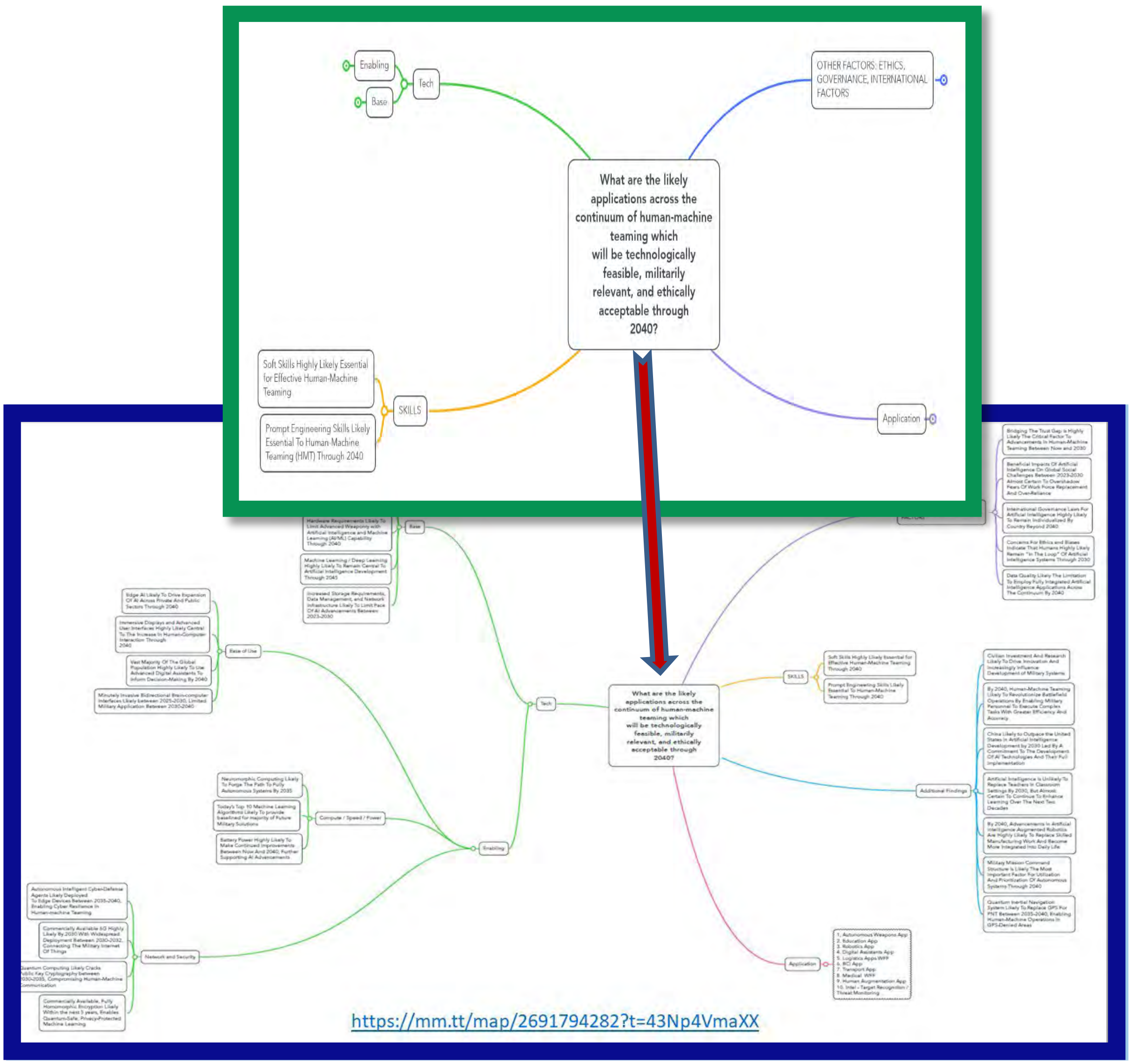
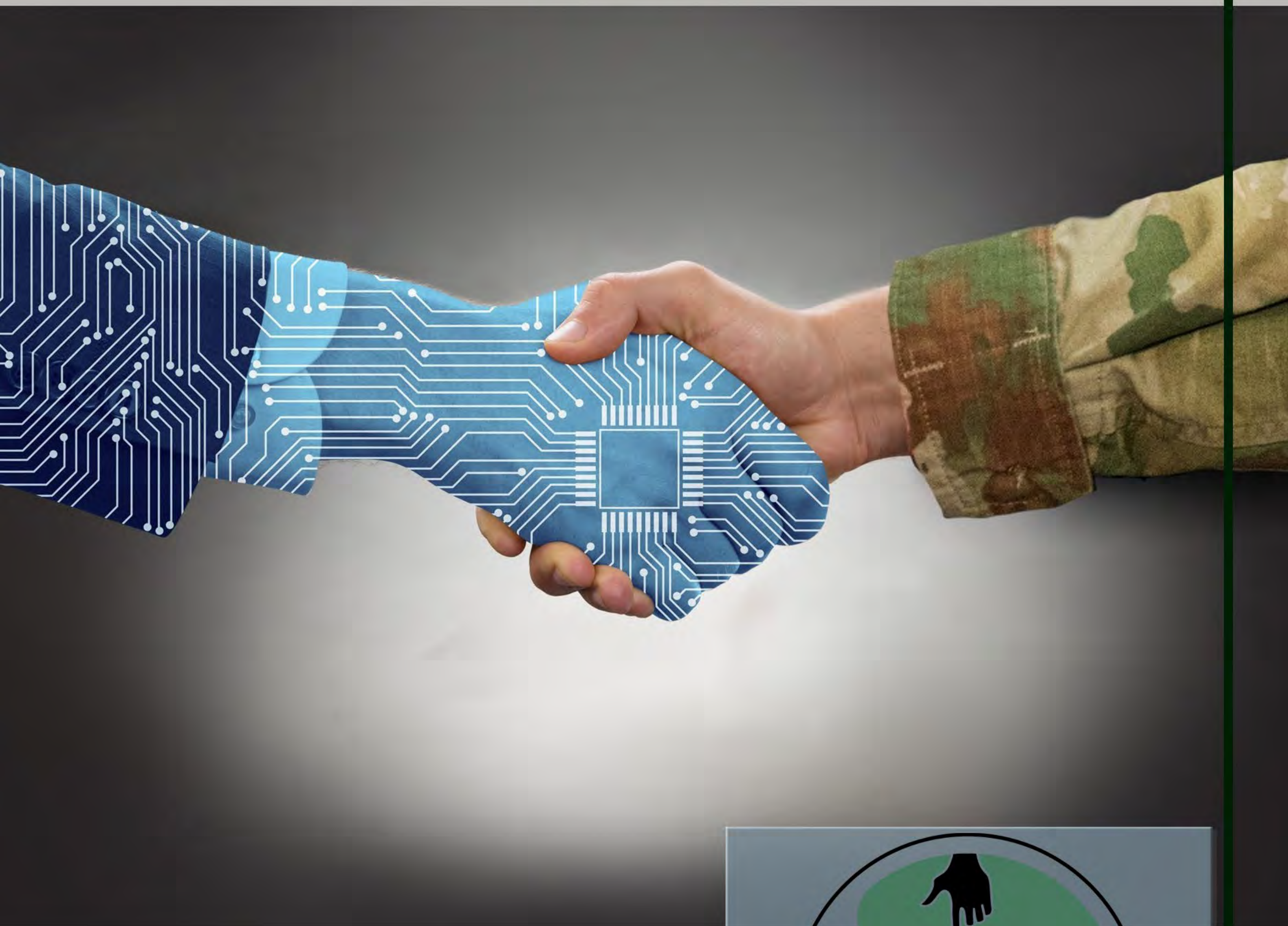


Figure 11: Full and condensed depiction of interactive mind-mapping process. Click on the image or go to: https://mm.tt/map/2691794282?t=43Np4VmaXX view the interactive mind map.

Table of Contents

Technology Advancements Enabling Human-Machine Teaming



SINGULARITY
HUMAN-MACHINE TEAMING

Public Opinion On Anthropomorphic Artificial Intelligence Likely To Shape Lenient And Vague U.S. Regulations Over The Next Five Years, Which Will Allow For Maximum Freedom of Artificial Intelligence Development And Employment

Executive Summary

Artificial intelligence (AI) applications are likely (56-70%) to have minimal regulation passed by civilian policy makers over the next 5 years, due to public trust of anthropomorphic systems, the increased commercial productivity and employment of AI capabilities by U.S. adversaries. The U.S. public will not support congressional and legislative regulations limiting development and employment of AI applications. Despite the fear of some key individuals within the tech industry, the increased production in our commercial companies, and more importantly the urgency of AI to provide advantages over our adversaries will keep regulation to a minimum through 2040.

Discussion

Figure 1: Scale of different types of fictional representations of Anthropomorphic robots. Source: University of Central Florida

In Human-machine teams, the humanness of the AI applications, also known as anthropomorphism, affects human trust.[H] Trust is the most essential trait in any successful team and that is no different in human-machine teams.[M] As AI applications become more commonplace, programmers continue to utilize Anthropomorphism as a way to not only make the applications more user-friendly, but also to gain the trust of its users.[H] As the most widespread end-user-facing category of AI,[M] anthropomorphic algorithms influences public opinion such as the latest boom in large language models and image generators. Due to the lack of full understanding of the differences between anthropomorphic and all other categories of AI, the general public opinion of anthropomorphic AI spreads to all the other AI categories.[H]

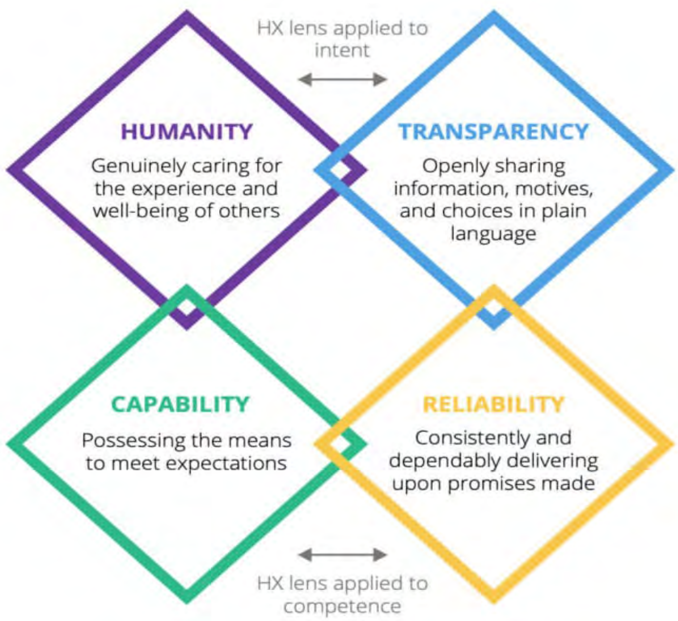


Figure 2: Visual representation of Trust Factors and the spectrum of intent and competence. Source: CLX

Unlike Anti-social AI, anthropomorphic AI has can be measured following the widely used trust model that measures four factors: transparency, reliability, humanity and capability.[H] Due to the lack of humanity, Anti-social AI applications in comparison are hard to measure using this construct and often thought of as a "black-box" to pubic end-users, where once a command, prompt or action is provided, the AI just autonomously provides the answer or performs the task given with no transparency.[M] Anthropomorphic AI faces three challenges; first, from anti-social AI which people won't like because it isn't transparent and then from the uncanny valley which appears to be a psychological bridge to human machine acceptance and then finally from anthropomorphic AI itself which is due to its fallibility and popularity.[M] [H] [H]

There are multiple factors in the development of legislation such as privacy, safety, job displacement, and adding the ethical factor for use within the military.[H] However, with the trust of the U.S. public, AI legislation will be less restrictive, which means increased fund allocation to research and development by both commercial and public sectors. In 2022 there were 17 states with AI legislation proposed, which demonstrates the legislative push for AI regulation is quickly ramping up.[H] Adoption of AI is moving on a similar path and speed as that of cellular telephones for example, the public acceptance and adoption period of cell phones (13 years) was almost half the time it took for full public adoption of telephones (25 years).[M] AI legislation likely to be influenced by the public opinion of today's technology with applications like chatbots and digital assistants.[M] [H] In the meantime, Anti-social AI application development and employment is likely to forge its own path, because commercial businesses and government developers integrate it seamlessly into daily lives of users with minimal impact and low consequence if failure occurs.

Trust in human-machine teams will likely be the key factor in public opinion, which is shaped by today's end-user facing anthropomorphic algorithms. Public opinions of today will likely be the foundation for creation governing legislation within the next five years. This legislation will be the foundation of development and employment not only for the anthropomorphic algorithms, but also for the Anti-social AI algorithms that run today’s commercial industries such as E-Payments and Facial recognition or driverless cars, but also impact the military applications such or strategic decision-making tools or even autonomous warfare systems.[M] [M]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information or unforeseen political gridlock facing the issue of AI adoption.

Author: Mr. Reginald Shuford
reginald.shuford.civ@armywarcollege.edu

Integrated Systems Of Broad And Narrow Artificial Intelligence Likely To Approach Artificial General Intelligence By 2040

Executive Summary

A system of systems approach to integrating Broad artificial intelligence (AI) algorithms, an algorithm that can accomplish more than one specified task, with Narrow AI, algorithms that can only execute one specified task, is likely (56-70%) over the next five years to approach artificial general intelligence (AGI). Despite the direct research funding applied to resolve the coding challenges with software integration of robotics necessary for AGI, the continued parallel efforts to develop Narrow AI applications and increased access to open-sourced data sets will cause the development and expansion of Narrow AI applications. Through multiple iterations, research will advance enough where this system of systems will approach the AGI, as defined by most researchers as the ability of an artificial intelligent agent to understand or learn *ANY* intellectual task that human beings or other animals. This is likely to happen faster in disciplines with lower failure risk levels, such as logistic supply chains vice higher risk disciplines such as medical triage.

Discussion

The goal of most AI developers has always been to create algorithmic and robotic capabilities that can figure out what the problem is, develop a solution, and execute the solution. This concept creates machine with similar ability to human or animal thought processes, which as of today is still merely a concept called AGI.[H] The majority of today's AI algorithms are categorized as Narrow artificial intelligence algorithms, meaning they are developed to complete a defined, structured task.[M] With continued advancements, computer scientists are now able to add a new category between Narrow and AGI called Broad AI algorithms (depicted in Figure 1), which means they can perform or process more than one specified task up a spectrum of functions within a discipline to just shy of AGI.[M] Interoperable Broad and Narrow AI systems likely to approach AGI[M],

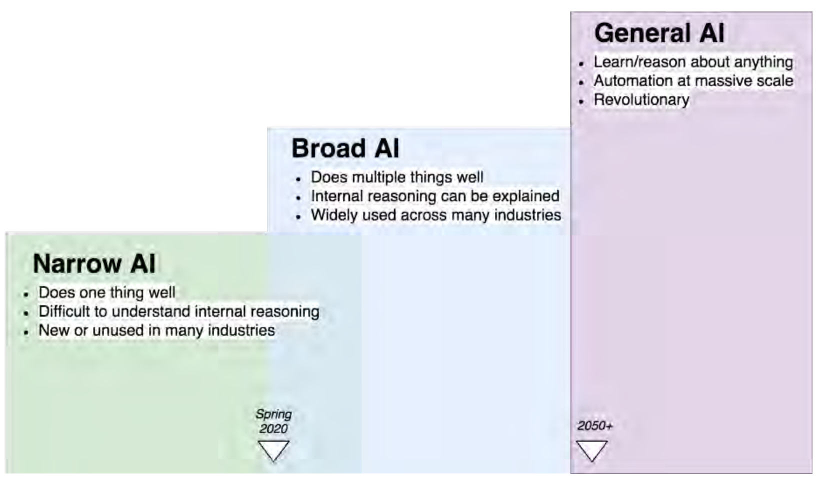


Figure 1: Model of types of AI approaching the ultimate AGI. Source: Communications of the AMC

but not until breakthroughs in the following innovations advance and converge: AI computer processing speeds, data storage and scalability solutions, and robotic functions and power solutions.[H]

Despite issues where Broad applications have provided inaccurate or incomplete data, there are other examples where large language models (LLMs) have provided answers that imply both feelings[M] and its ability to pass theory of minds tests the cognitive process of differentiating the difference between true and false data.[M] These current examples of a mix between Broad and Narrow AI Algorithms are often mistaken as AGI if the logic of the output is not fully understood by humans.[M] Broad AI applications, such as natural language processing and computer vision, offer a wide range of capabilities that are then integrated with Narrow AI and validated by humans to create more powerful systems. By combining the strengths of Broad AI applications with the specificity and domain expertise of Narrow AI and robotics, Human-Machine integrated teams can solve complex problems, automate tasks, and improve decision-making processes.[M]

One example of how Broad AI applications can work in conjunction with Narrow AI and humans is in the healthcare industry. Broad AI medical applications such as natural language processing and deep learning algorithms, once approved, will use large amounts of historical medical records and test results combined with patient's symptoms to not only diagnose but also predict future patient health issues.[H] Broad AI applications, such as image recognition algorithms, are in testing to analyze medical images and identify specific abnormalities and provide treatment plans or procedures like IBMs Watson.[M] Although it has the capability, this type of example is not yet widespread and still being validated for accuracy. However, we see much more common examples in practice today for lower risks tasks like Amazons integrated supply chain logistics systems, which include Narrow AI robotics in the warehouses and Broad AI product predictions and order processing integrated together.[M] [H]

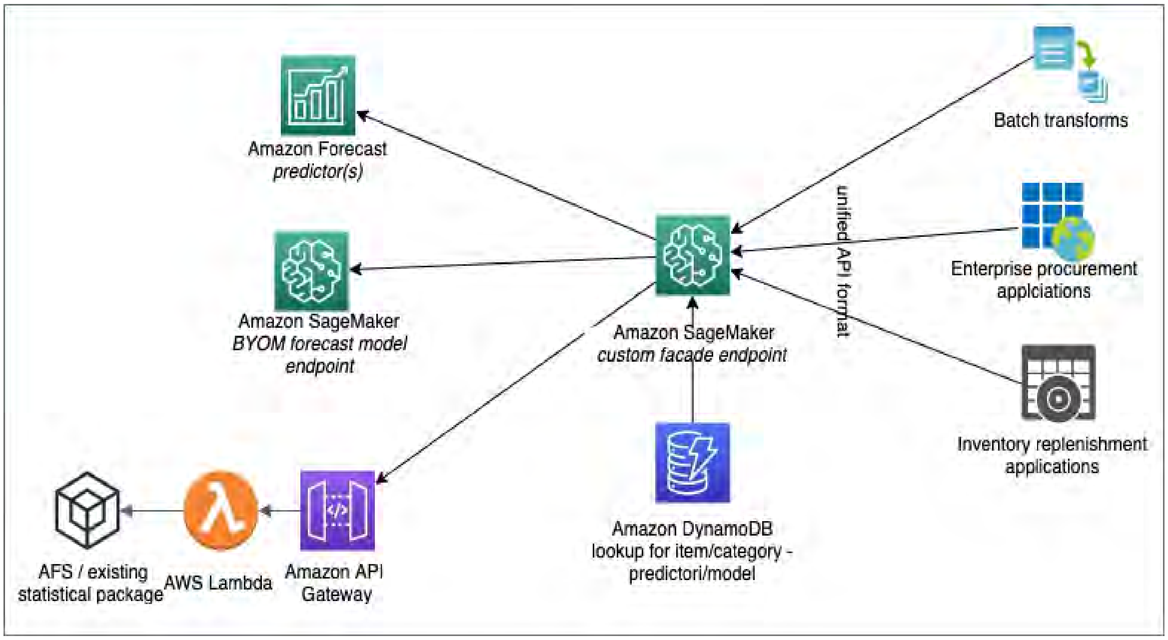


Figure 2: Visual representation of how Amazon integrates multiple Narrow and Narrow AI systems to combine orders with its logistics and supply chain. Source: Amazon WebServices

There has been a long-lived thought process among technologists and AI researchers that AGI would be one robot invented with human or animal thought processes that can execute a solution to *any* kind of problem. However, the integrated system of systems approach to AI teams will likely provide a quick solution and redefine AGI as automated tasks that can solve problems and execute *many* tasks within a given discipline, until further breakthroughs are made to AGI that can integrate and span all disciplines.[M]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information or unforeseen breakthroughs in technology for AGI.

Author: Mr. Reginald Shuford
reginald.shuford.civ@armywarcollege.edu

Hardware Requirements Likely To Limit Advanced Weaponry With Artificial Intelligence and Machine Learning Capability Through 2040

Executive Summary

It is likely (56-70%) that time constraints for adding rapidly changing hardware requirements to advanced weapon systems will limit militaries' ability to add artificial intelligence (AI) and machine learning (ML) capabilities by 2040. Contingency requirements for the weapon systems include being able to operate without full or any connectivity. Today's AI and ML algorithms' minimum set of hardware requirements for both processing speeds and random access memory (RAM) require non-standard equipment that is difficult to add to weapon systems. Likewise, ever increasing dataset volumes will require rapid hardware updates in processing speed and internal memory, which will be problematic after the weapon systems have completed full scale-production. Weapon system hardware weight and size requirements will not be able to adapt at the same speed as AI/ML hardware updates will require. Despite cloud horizontal and vertical scaling technologies to adapt to increased hardware requirements, Autonomous systems will need performance intensive capabilities and be able to operate both with and without connectivity.

Discussion

Figure 1: Depiction of Human-Machine team with new and retrofit AI technology. Source: U.S. Army

Weapon systems are difficult to build because of the unique requirements needed to operate in harsh environmental conditions, extreme temperatures and often within very small margins of error.[M] As human-machine teams expand these military relevant requirements will become more difficult to design and build. Any modifications or HW add-ons after the final design, will require engineering re-design and thorough testing to ensure it doesn't change the overall effectiveness of the weapon system.[H] The redevelopment and testing time prevents the AI/ML system from being deployable for operational use at the speed of need. AI and ML systems processing speed and memory storage requirements continue to increase overtime, requiring HW designs to be flexible.[H] However, following the historical trend of thirty year lifecycles for military weapon system with upgrades, the speed of AI/ML systems hardware requirement increases is not likely to be resolved by 2040.[M] If weapon systems are built with cloud technologies the horizontal and vertical scaling capabilities exist for the AI/ML to connect back to expanded memory and processing power.[H] However, the War in Ukraine has taught the lesson that critical weapon systems must be able to work without connectivity.[M]

With AI/ML flexibility requirements and the inflexibility of HW design in weapon systems, the AI/ML capabilities will need to be built into early designs or be cost prohibitive to retrofit into the sustainment of weapon systems. Although many weapon systems are now built with open system architecture and built to allow commercially available compatibility, the weapon systems of the future will need space for expandable computer equipment, which will add weight, take up space and could possible require additional power.[H] Because the exponentially fast growing data sizes required for AI complex weapons systems, the commercial hardware necessary to support AI/ML components are not likely to be integrated with these military specific requirements. The acquisition timelines to continuously integrate new hardware into weapon systems is not fast enough to support the rate of change.[H] Even if the equipment can be retrofitted with commercially available hardware components, the validation process will breach development timelines and add an estimated two years to the process.[H]

Examples of HW requirements for AI/ML systems are listed below. Maria-Bot, a robotic teaching assistant developed by Dr. William Barry at the US Army War College, that is made of several different large language models has provided the following response for the minimum set of requirements necessary for a AI/ML capabilities: Intel Core i7-8700k processor; base clock speed of 3.7 – 4.7GHZ w/ turbo boost, GPU Nvidia GeForce RTX 2080 with 11GB of GDDR6 VRAM that can also accept other sensors and 4k gaming and VR applications.[L] You.com's large language model chat also provided a set of minimum requirements to run just a medium sized AI/ML system with: at least quad-core processor with clock speed of greater than 3GHZ, GPU 4GB VRAM.[L] Based on the AI/ML robotic capabilities developed by Dr. Barry, any minimum set of HW requirements needed to add AI/ML to a weapon system will need to be able to be exponentially scaled which is easily done with cloud-based solutions but will not fulfil the requirement for weapon systems to be able to operate without connectivity.

Analytic Confidence

The analytic confidence for this estimate is *moderate* based on the credibility and corroboration of sources for the minimum hardware requirements for AI/ML capabilities combined with the ability to upgrade HW components of Army HW and weapon systems. The time was adequate, but the analyst did not use a structured technique for the estimate. Although the estimator is a subject matter expert on software systems, the analyst used only research sources for the HW system requirements. Finally, this report is subject to change due to the potential for reduction of HW requirements for AI/ML developments over the weapon system development period.

Author: Mr. Reginald Shuford
reginald.shuford.civ@armywarcollege.edu

Machine Learning / Deep Learning Highly Likely To Remain Central To Artificial Intelligence Development Through 2040

Executive Summary

It is highly likely (71-86%) that machine learning (ML), specifically deep learning (DL), will remain central to artificial intelligence (AI) development through 2040. Refinements in data collection and labeling will speed the AI training process and reduce errors associated with data quality. Advancements in causal AI will move ML/DL models from predictions based on pattern recognition to understanding cause and effect relationships. Despite concerns with bias and data quality, it is highly likely that advancements in ML/DL will lead to enhanced decision-making in autonomous/semi-autonomous and decision support systems.

Discussion

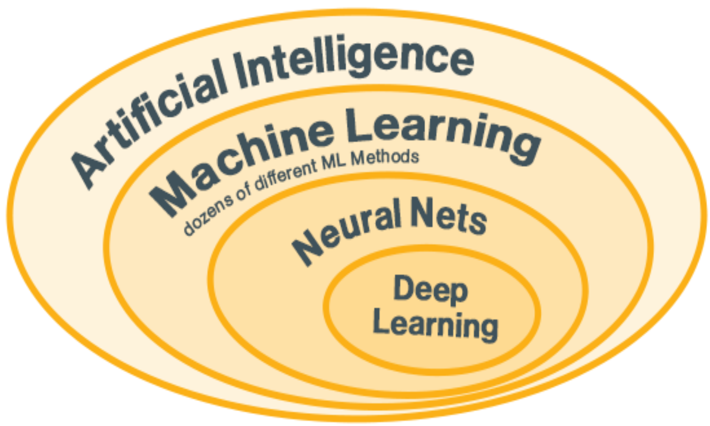


Figure 1: Visualization of AI relationships. Source: Clickworker

AI is trained to perform tasks through learning algorithms such as ML, neural networks, and DL.[H] Each of these are not an individual field, but are subsets of AI, with DL as a subset of neural networks, and neural networks are a subset of ML (see Figure 1).[H] The key difference between these models is the process used to train the AI.[H] These algorithms are designed to mimic how humans learn, with the end state being a system that imitates human intelligence when performing a task.[M] More importantly, ML and its subsets allow the AI to improve its ability to perform a task and learn to perform new tasks without additional programing.[M] There are also AI's that are not associated with machine learning, sometimes categorized as good old fashioned AI (GOFAI). This includes rules engines, expert systems, knowledge graphs, and symbolic AI.[H]

Traditional ML methods can be summarized into three typical steps; a data set is introduced, allowing initial patterns to be recognized. Based on this data, the algorithm then makes predictions. The second step is error evaluation, understanding how accurately the model made predictions. The final step is using the error evaluation to optimize the algorithm.[M]

Several ML models are currently used to train AI. These include supervised, unsupervised, semi-supervised, and reinforcement learning.[H] In supervised learning, the data set is fully labeled, allowing the AI to build a known knowledge base to compare new data against. Unsupervised learning does the opposite; unlabeled data is introduced, forcing the AI to identify and analyze the structure within the data. Semi-supervised learning mixes the two by providing the AI with a portion of labeled data and allowing it to make inferences based on the unlabeled data. Reinforcement learning focuses on goal accomplishment. The AI is rewarded when it correctly completes a task, learning through trial and error. This is done iteratively, improving individual tasks or stacking multiple tasks.[H]

All of these models are data dependent, the volume and accuracy of the initial data set will determine the quality and accuracy of the trained algorithm.[M] Numerous classifications of ML algorithms exist; these include Linear Regression, Logistic Regression, Clustering, Decision Trees, and Random Forrests.[H] While it is important to understand that multiple algorithms are available, the scope of this assessment is limited to the neural network algorithm and DL.

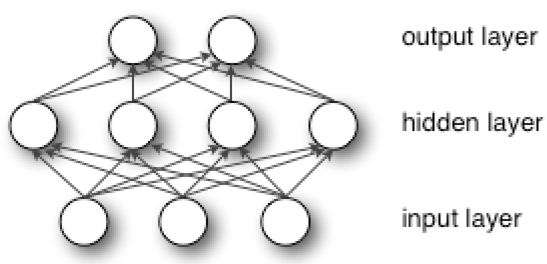


Figure 2: Neural Network Example. Source: Pathmind

Neural networks are layered processing nodes used to replicate data processing in the human brain.[H] Neural networks process data across multiple nodes, and layers of nodes to better recognize patterns in the data (see Figure 2).[M] DL is a subset of ML that leverages the computational power of neural networks. When a neural network has more than three hidden layers of processing nodes, it is referred to as DL.[M] DL uses the same models used in ML to train AI. AlphaGo Zero is an example of a specific type of DL model called Self-Play Reinforcement Learning. While reinforcement learning can also be applied to ML, in the case of AlphaGo it is considered DL because it was applied to a deep neural network.[H] AlphaGo Zero used this model to train itself to play the game Go. This enabled the algorithm to train itself with only knowledge of the game's basic rules, without human influence.[M] The process ended with AlphaGo Zero becoming the best Go player in the world in 40 days (see Figure 3).[H]

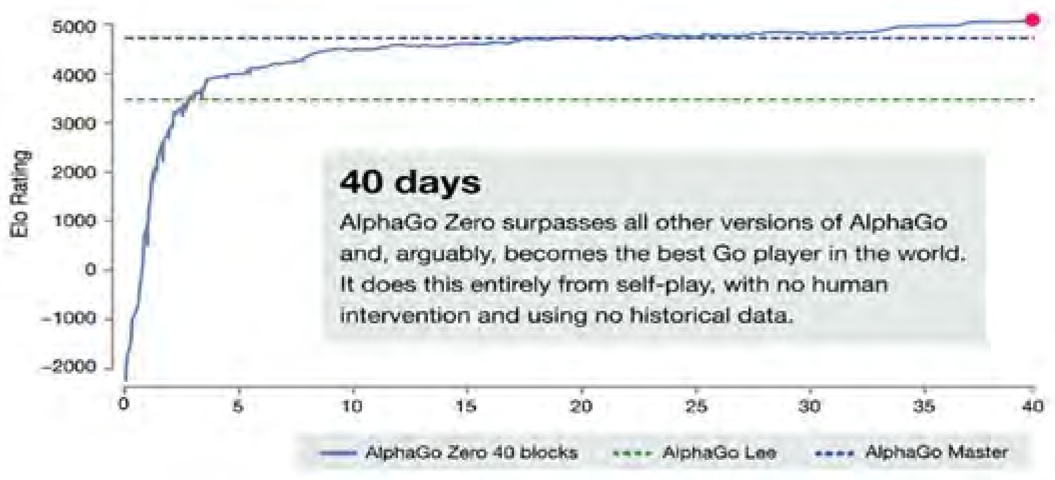


Figure 3: AlphaGo Zero progression chart. Source: Deepmind

Concerns with ML are tied to ethics due to bias in the data or development of the algorithm.[H] Concerns over how training data is obtained have been raised as well. With Italy recently blocking access to the popular ChatGPT, over potential privacy violations.[H] The lack of data, and data quality are also concerns.[M] Regarding data quality, researchers associated with Google have raised concerns that these training models are fundamentally flawed. They point at two issues tied to the data used to train AI. These are "data shift" and "underspecification".[H] Data shift occurs when the training and real-world data differ in quality. This can cause the AI to underperform when put into practice. The second issue they point to is underspecification, which is when the training data fails to account for all possible external impacts on the data set.[M] Despite these challenges, it is highly likely that ML will continue to expand in use as industry and innovation continue to integrate AI.[M]

Advancements in ML/DL include causal AI, which expands ML from prediction based on pattern recognition to identify the cause and effect relationships.[M] Benefits of causal AI include reducing coincidental correlation, which will help reduce bias, and the ability to simulate outcomes based on relationships.[M] One example of the application of this technology is associating athletic performance to physical and mental health data of athletes.[M] Using DL and causal AI to understand the relationship between these elements is highly likely to result in increased performance and reduced injuries. When applied across multiple military and civilian applications, this technology will enhance and enable AI support for decision-making, research, simulation, and anomaly detection.[M]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The sources were generally credible and tended to corroborate each other. The time was adequate, but the analyst did not use a structured technique and worked alone. Additionally, the analyst is not a subject matter expert. Finally, this report is subject to change due to the potential for new developments and the protracted period.

Author: COL Dennis Weaver
dennis.weaver.mil@usarmywarcollege.edu

Increased Storage Requirements, Data Management, And Network Infrastructure Likely To Limit Pace Of Artificial Intelligence Advancements Between 2023-2030

Executive Summary

Robust software infrastructure requirements are likely (56-70%) to be the limiting factor for the pace of artificial intelligence (AI) advancements between 2023 and 2030 due to the increased need for more significant storage requirements, faster networks, and data management protocols. Despite the widespread usage of AI capabilities in areas ranging from personal use to small businesses to the international industrial base, which increased use rate presents total system computing requirements which are as new as the technology itself. Between now and 2030, those with the resources to fund the most extensive, fastest, and most secure software systems will highly likely (71-85%) emerge as the industry leaders.

Discussion

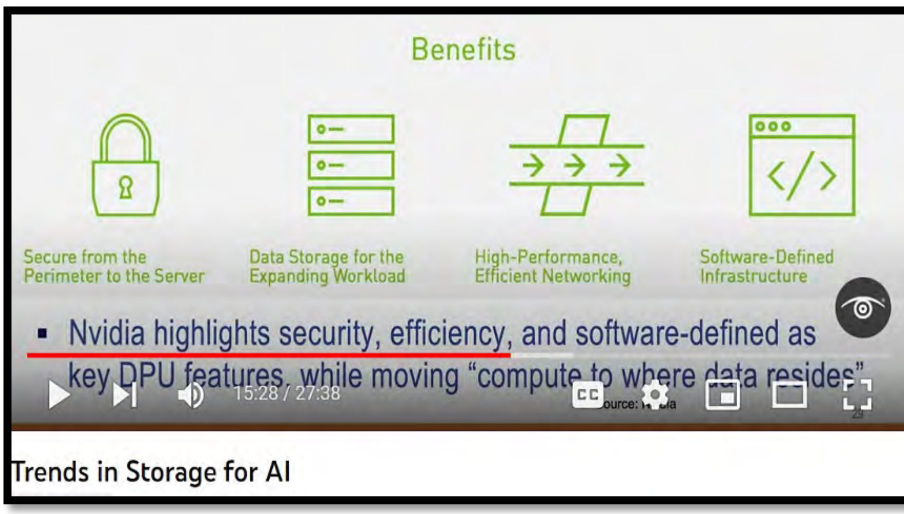


Figure 1: Dave Eggleston, an independent consultant for TechTarget.com, discusses current trends in storage for AI. Click on the picture or go to: https://youtu.be/OXHttbHZZnc to view the video. Source: Eye on Tech

Physical hardware needs for AI are specific to individual industries, reducing resource competition.[H] However, the software framework requirements, while scalable, remain consistent among industries and will be a key driver for continued advancement for some and a limiting factor for others.[M] These infrastructure requirements include increased storage capacity, reliable network infrastructure, and upgrades to data management protocols.[H] As recently as June 2022, six of the top ten challenges facing AI development and implementation were related to software infrastructure requirements.[M] As AI moves beyond experimentation toward adoption and advancement, it will demand significant computing resources, infrastructure costs, and increased overhead.[M]

The primary consideration when building the necessary software infrastructure is the increased need for a vast amount of storage capacity with the ability to scale.[H] The more data that AI applications are exposed to, the better data-based decision they provide. The database of input data and output decisions will grow over time and organizations need to be prepared for such growth.[M] Among the many factors that business need to consider when planning for storage are: reliability for the specific type of data (structured, semi structured, or unstructured),[H] the source of the data, and what level of AI network they will use.[H]

The next emerging infrastructure requirement is a highly capable and adaptive network. One should consider the infrastructure for AI as a "three-legged stool" where the legs are the network, servers, and storage. Each must be equally fast to keep up with each other.[H] To provide the high efficiency at scale required to support AI and machine learning (ML) models, organizations will likely need to upgrade their networks. Scalability must be a high priority, requiring high bandwidth, low-latency, and creative architecture.[H]

If the network, servers, and storage are the legs of the stool, then data is the prized seat. Zeus Kerravala, founder and principal analyst with ZK Research explains that AI/ML success depends on making the right infrastructure choice, which requires understanding the role of data and the requirements to manage it.[H] Good data management protocols involve facilitating access to users who need it, while also securing it from those who do not.[H] Any breach in data security causes harm to the information owner and also introduces bad data into to the system, affecting future decisions.[M] One of the most nefarious and expensive types of information breaches, known as data poisoning,[H] can corrupt the datasets of AI to cause damage to its decision-making abilities. Correcting this type of incident is both expensive and time intensive as the only current solution is to determine the origin of the poison and retrain the entire system with good data.[H] In addition to the retraining requirement and the loss of consumer confidence comes the financial cost. According to IBM and Ponemon Institute, the average total cost of one data breach was over $4 million for 2022 and is projected to reach $5 million in 2023.[M]

Analytic Confidence

The analytic confidence for this estimate is *moderate* based on the credibility and corroboration of sources. The time was adequate, but the analyst did not use a structured technique. Additionally, the analyst is not a subject matter expert and worked alone. Finally, this report is subject to change due to the potential for new developments and the protracted timeframe.

Author: LTC Nicole A. Washington
nicole.washington.mil@armywarcollege.edu

Edge Artificial Intelligence Likely To Drive Expansion Of Artificial Intelligence Across Private And Public Sectors Through 2040

Executive Summary

It is likely (56-70%) that the integration of edge artificial intelligence (AI) into devices across private and public sectors will continue to expand through 2040. This is due to local data processing increasing the speed at which data is produced while reducing the cost and time of centralized data processing and storage. Edge AI provides the user with real-time AI data analysis directly from the system or sensor, increasing the speed of decision-making. Edge AI removes the dependency on an internet or data connection allowing for continual use, even in a disrupted or degraded electromagnetic-spectrum or cyberspace environment. Additionally, edge AI reduces security concerns associated with networked devices.

Discussion

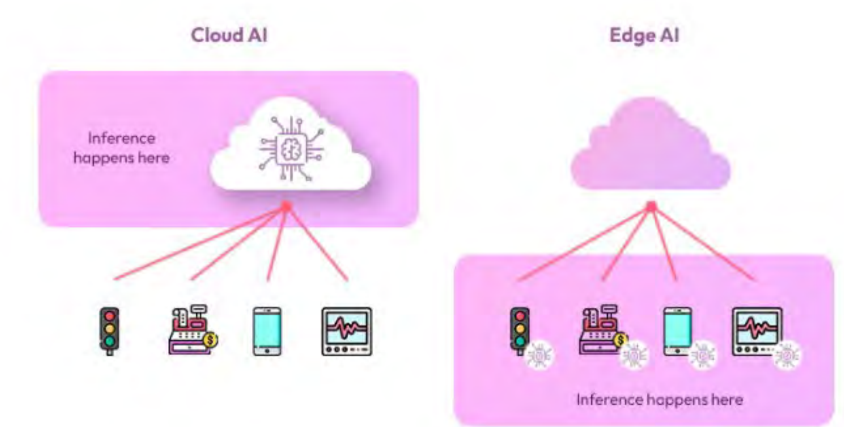


Figure 1: Simplified visual depiction of Cloud AI vs. Edge AI. Source: Xailient

Edge AI is pushing the computational portion of an AI system to the local level.[H] Edge systems move the AI as close to the data collection method as is currently feasible.[H] The AI model operates on the local device, supported by system hardware that enables processing and sensors or other input mechanisms that support data collection.[H] This enables the AI to operate independently of a cloud-based environment (see Figure 1).[H] According to the management consulting firm, Kearney, by 2025, it is highly likely that over half of the data generated worldwide will be created by edge devices.[H] Examples of current edge AI systems include manufacturing quality control, self-driving cars, and household appliances with narrow AI such as simple voice recognition.[H] The possibilities for future use include medical instruments, smart energy grids, predictive maintenance in machines, traffic control, and powerful digital assistants.[H] The recent improvements in edge AI have been powered by developments in several key areas, including the development of neural networks, the increased computational power of microchips, and the proliferation of edge-enabled devices, commonly known as the Internet-of-Things.[H]

Edge AI is inherently hardware dependent; however, edge AI does not rely on the most advanced hardware to function. Narrow AI, meaning AI that performs one or several specific tasks, can function on microcontrollers, while a modern CPU can host more advanced machine learning algorithms.[H] More complex general AIs will require a complex neural processing system.[H] Evidence shows that using narrow AI on less capable chips can increase performance and decrease power consumption compared to general AI running on advanced hardware.[M] In addition to the processor hardware, edge AI also relies on local storage. With limited storage, the AI must be trained to differentiate between storing and purging data. Mistakes with edge AI storage can lead to the loss of valuable data.[H]

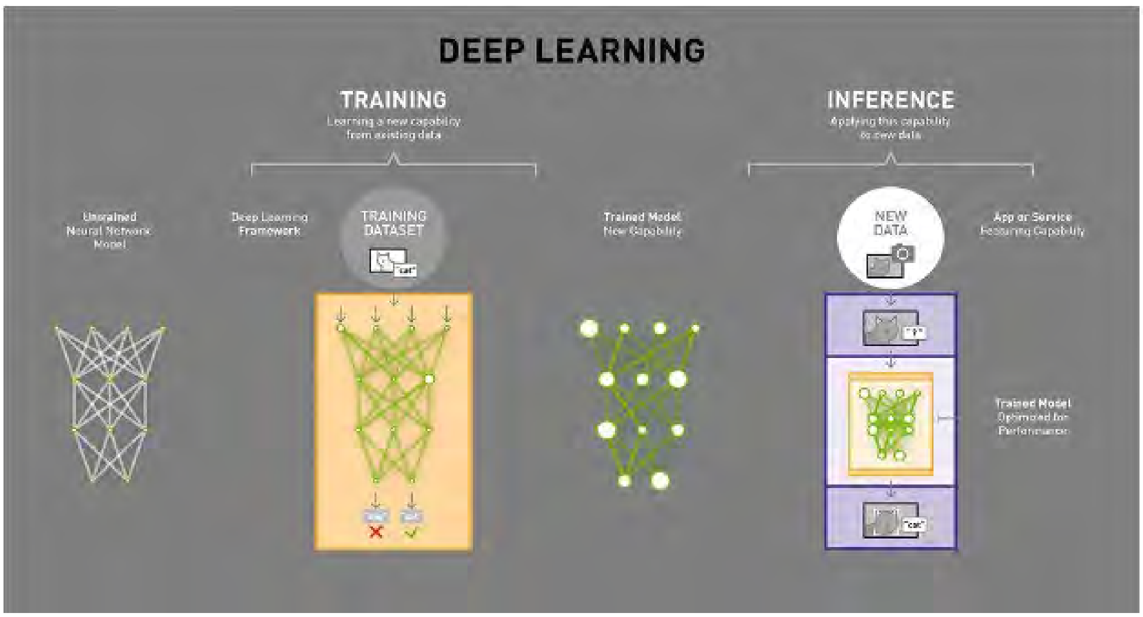


Figure 2: A visual depiction of a Deep Learning Model. Source: Nvidia

Edge AI software consists of computational models that can employ forms of machine learning.[H] These models are typically trained in a data center (on the cloud) and then pushed to the network edge.[H] Deep Learning, a machine learning technique, trains edge AI as "inference engines"[H] which allows the AI to make inferences when exposed to new data (see Figure 2).[H] Inferencing allows applications from voice recognition and pattern analysis to controlling a vehicle in traffic.[H] Allowing the inference to take place on the edge device decreases response time and computational and storage requirements of the cloud environment.[H] Using a federated learning model, edge devices or inference engines can train their local model and then transmit processed data back to a cloud-based algorithm to improve or refine the training model.[H]

Obstacles to improving edge AI can be found in several areas. First, there is a power trade-off. Power requirements shift as you transfer the AI processing from a central location to the network's edge. Powering decentralized AI systems will take energy, and the bill is tied directly to the functionality of edge AI.[H] In some cases, the power will be provided by batteries. This will likely increase the global competition for battery materials.[M] However, it is unlikely (31-45%) that this will limit the development of edge AI, as AI can help increase the efficiency of the batteries it requires. In the example of electronic vehicles, the AI-powered Battery Management System can help extend the life of batteries.[H] There are also security concerns. Raw data is stored on the local device, creating a target for cyber-attacks.[M] Manufacturers and service providers must ensure that measures are taken to secure data on the network's edge. Finally, there are ethical concerns. As more complex AI is pushed to the edge, it will likely influence human decision-making.[M] Developers of edge AI systems must ensure that biases are removed to maintain and increase trust in these systems. Norms for use will emerge and evolve with that trust.[M]

Edge AI will likely match edge devices' overall growth in the coming years. LF Edge group estimates this compound growth rate to be 40%.[M] AI will likely be incorporated

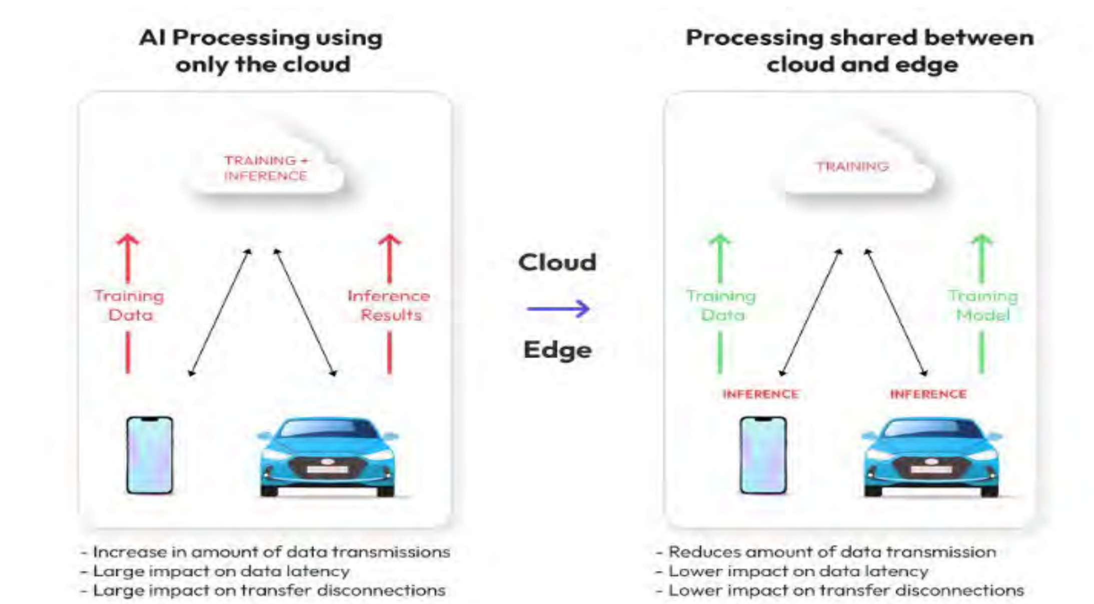


Figure 3: A visual depiction of a Federated Deep Learning Model. Source: Advian

into much of our daily lives, with edge AI devices providing much of the human-machine interaction.[M] Edge AI offers several benefits, including reduced costs and real-time analysis, with on-call availability.[H] Edge AI will increase privacy by allowing users to process sensitive data locally while sharing selected data for cloud-based processing (see Figure 3).[H] In the context of military application, nations must choose if and then how they incorporate edge AI into military systems. As more nations opt-in to gain the benefits of edge AI, we will likely see an AI arms race driven by AI and counter-AI techniques that target edge AI enabled devices.[M]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The sources were generally credible and tended to corroborate each other. The time was adequate, but the analyst did not use a structured technique and worked alone. Additionally, the analyst is not a subject matter expert. Finally, this report is subject to change due to the potential for new developments and the protracted period.

Author: COL Dennis Weaver
dennis.weaver.mil@usarmywarcollege.edu

Immersive Displays And Advanced User Interfaces Highly Likely Central To The Increase In Human-Computer Interaction Through 2040

Executive summary

Human interaction with computers is highly likely (71-85)% to continue to expand due to increased focus and investment into advanced displays and user interfaces. Touchscreens and displays will likely increase in utility with improvements in flexible, foldable, stretchable, and wearable materials. Extended reality (XR) will highly likely lead to fundamental changes in how humans interpret and interact with the world and the machines we are teamed with. People will advance from pulling information from their handheld devices to having an always-on, interactive overlay of the world around them. Despite current hurdles regarding power, processing capability, and bandwidth associated with small wearable devices, it is highly likely that private investment will continue to drive development.

Discussion

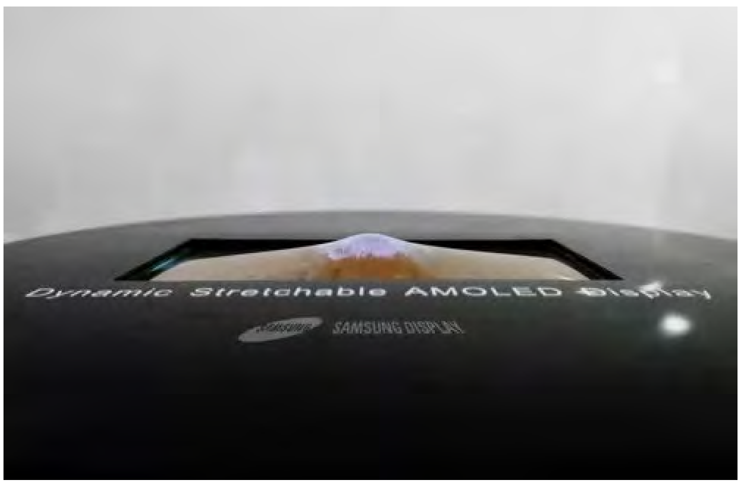


Figure 1: Samsung Stretch Screen. Source: Android Authority

Graphic user interfaces (GUI) have dominated interactions with technology since the introduction of the earliest personal computers. Recent years have seen rapid advancements with touchscreens that let humans interact directly with the GUI.[M] Touchscreens will likely continue to make up a substantial portion of human-computer interaction. The touchscreen enabled the rapid spread of technology in the last decade by reducing the complexity associated with computers and placing them in our hands.[M] Touchscreen displays are everywhere, on our phones, personal computers, appliances, and transportation. Current estimates show that 97% of new light vehicles produced worldwide integrate touchscreens.[M]

Foldable, flexible screens are already available on the consumer market, the next iteration of this technology will include stretchable displays.[M] Samsung had demonstrated initial work with stretchable screens.[M] Stretchable displays will be enabled by flexible, stretchable integrated circuits printed onto smart fabric.M H These lightweight flexible screens will enable more robust wearable systems.M

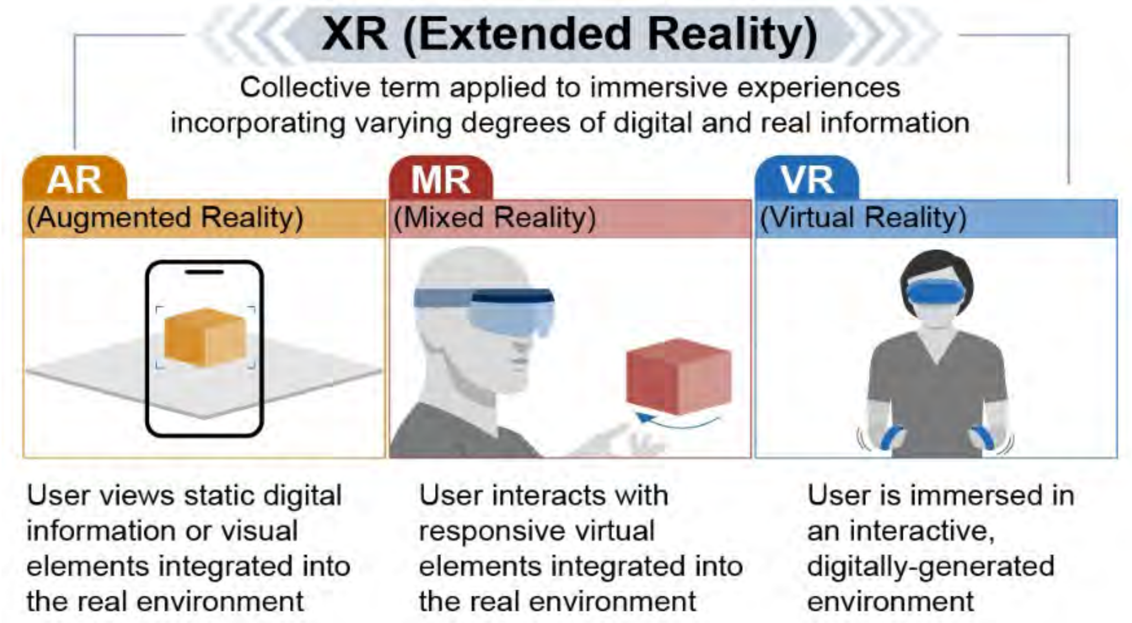


Figure 2: Extended Reality. Source: GAO

Several manufacturers are researching touchless technology which will allow users to interact with their devices through a series of gestures while in proximity to the controlled device.M Bayerische Motoren Werke AG (BMWs) HoloActive Touch display combines air gestures with haptic feedback, allowing the user to feel the interaction with the device.M Some companies, such as Continental Engineering, are investing in smart surfacesH, which allows nearly any surface to be embedded with touch-enabled technology.M Combinations of these enabling technologies are likely to form the base of future devices that will enhance human-machine teaming and enable fields like XR.

XR encompasses the fields of virtual reality (VR), augmented reality (AR) and mixed reality (MR) (see Figure 2).H All of these fields of technology incorporate sensory immersion, allowing for different levels of interaction with the physical and digital environment.H The first AR system dates back to 1968, when Ivan Sutherland with Harvard created the first head-mounted display (see Figure 3).H Today AR can be found in our portable devices; smartphones, tablets, and headsets.H Practical uses of AR include medicine, maintenance and repair, education and training, as well as tourism.M Recent AR products have been focused on the consumer experience focused on smartphone applications that apply filters that let people try on clothes, make-up or play games, like PokemonGo!H Other applications like Google Lens give the user additional information about the world around them, by providing tools like instant translation and information on landmarks, food, plants and animals.H Advancements in enabling technologies like

LiDAR[4] will further enhance at AR experience by layering virtual representations within objects in the physical world, a feature referred to as occlusion.H Wearables in the form of glasses and goggles will have a considerable impact on the XR market and society as advancements in size, weight, and power make the devises more practical.H

Figure 3: "Sword of Damocles" AR system. Source: Informit

Beyond the smartphone and glasses, there are numerous additional technologies where AR is integrated. Heads-up displays are now offered in numerous vehiclesM, with BMW's concept car the iVision Dee (digital emotional experience) providing an extreme example of how AR can enhance the driving experience by providing additional information about the traffic environment.H The concept abandons traditional touch screens and instead builds a system around interactive voice control and augmented reality.H H

MR moves beyond AR by supporting more interaction between the virtual and physical worlds.H Most notable is the ability to manipulate virtual objects that are displayed in the physical world, examples include demonstrations in classrooms, construction and design models, and interactive communication.M According to a paper published by Harvard Business Review and Microsoft, of the companies surveyed, 68% say MR will be important to meeting strategic business goals, and 90% are actively looking into using MR.H

VR displays immerse the user in a virtual world, while VR has obvious applicability to fields such as entertainment, there are also numerous practical applications from telepresence to military, construction, engineering and education.M In medical education, doctors can train in virtual three dimensional scenarios. In medical practice, representations of patients can be seen in three dimensions, enhancing diagnosis and treatment.H In manufacturing VR can be used to design digital twins[5] of production facilities, BMW recently teamed with Nvidia to build a digital twin of a factory that will be built in 2025.H This process increases collaboration and design efficiency while reducing cost and time.H Enabling technologies such as hand tracking, will remove the

[4] LiDAR is an acronym for Light Detection and Ranging. In LiDAR, laser light is sent from a source (transmitter) and reflected from objects in the scene. The reflected light is detected by the system receiver and the time of flight (TOF) is used to develop a distance map of the objects in the scene.

[5] A digital twin is a virtual model designed to accurately reflect a physical object.

need for controllers while using VR.[H] Haptic feedback devices will allow users to further sense the virtual environment through simulation of touch and movement.[H]

Holographic displays are currently available in several forms, although many technologies that are advertised as holograms are either 3D images or 2D projections that create the illusion of a hologram but have no real depth or volume.[M] Holographic boxes are in production, and at a variety of price points, making them practical for commercial and personal use.[H] [M] [H] However, several true holographic technologies do exist.[M] Light Field Lab[H], has developed "Solid Light" displays, one of the most promising holographic displays.[H] Holograms are expected to be integrated across a large spectrum of industries, with the benefit of multiple users sharing a common display.[H]

Voice user interfaces (VUI) have enabled mainstream products since the first smart speakers were introduced in 2014.[H] It is highly likely that advancements in natural language processing and AI will enable greater personalization, enhancing the user experience and increasing public use. This will likely lead to increased use of VUIs in commercial systems.[M] Intelligent virtual assistants will replace some of the functions people currently handle with their smartphones or other computing devices.[M] By 2020, U.S. households supported over 157 million smart speakers. The market for voice-enabled devices is expected to continue to grow.[H] The popularity of Voice-enabled devices will likely fuel future investment and further advance this technology. While it is highly unlikely (16-30%) that VUIs will completely replace screens, they will enhance how humans interact with and receive information from our machines.[H] VUIs provide the user with a handsfree, lower distraction interface allowing the user to focus on other tasks, such as driving, while still receiving notifications from the device in use.[H]

Despite the limitations in power, processing capability, and bandwidth associated with wearable devices[M], industry leaders are highly likely (71-85%) to continue investment in display innovation, allowing users to better team with computers and AI to enhance their work and life experiences.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The time was adequate, but the task covered a large technology spectrum. The sources were generally credible and tended to corroborate each other. Commercial information is readily available; however, marketing information can overhype capability. Additionally, the analyst is not a subject matter expert. Finally, this report is subject to change due to the potential for new developments and the protracted period.

Author: COL Dennis Weaver
dennis.weaver.mil@usarmywarcollege.edu

Vast Majority Of The Global Population Highly Likely To Use Advanced Digital Assistants To Inform Decision-Making By 2040

Executive Summary

Rapid advancements in the development of digital assistant and digital companion applications represent a technological revolution, and it is highly likely (71-85%) that the vast majority of the global population (80-90%) will be using some form of advanced digital assistants by 2040. Three main factors are driving the development of digital assistants. First, the costs of digital assistants are dropping, making them readily available to a broader range of people. Second, the technology is becoming increasingly sophisticated and easier to use, allowing digital assistants to do more complex tasks and simplify operations for the user. Third, as time passes, digital assistants are more socially acceptable as people become more comfortable with their applications. Critics of digital assistant technology cite a lack of necessity and nuance in recommendations, challenges with privacy, bias interference, and network security risks as reasons for apprehension, but the value added through the utilization and implementation of digital assistant technologies represents a clear advantage in gathering and analyzing data to inform decisions.

Discussion

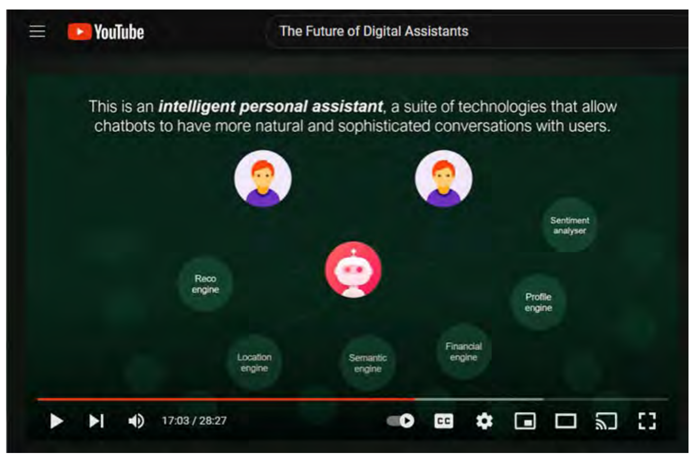


Figure 1: The Future of Virtual Assistants – KBC Inspiration Day. Click on the picture or go to: https://www.youtube.com/watch?v=XQQuXiwd6rU to view the video. Source KBC.

A digital assistant is "an advanced computer program that simulates a conversation with the people who use it, typically over the internet," that uses "advanced artificial intelligence (AI), natural language processing (NLP), natural language understanding (NLU), and machine learning to learn as they go and provide a personalized, conversational experience."[H] Think of digital companions like digital assistants 2.0; the new and improved version of what currently exists today. They will still "assist" us with numerous tasks throughout our daily lives, but they will do so in a way that's much more personalized, seamless, and fun.[H] Thus forging a new type of enduring role and relationship with the user.[H] For this report, the term digital assistant will address both applications unless specified otherwise.

Digital assistants help people with daily tasks such as managing calendars, providing reminders, scheduling appointments, and managing emails.[H] Additionally, digital assistants can provide personalized recommendations, like suggesting restaurants, movies, and books.[M] Digital assistants can also help people with more complex tasks. For example, they can help people with financial planning, such as providing advice on investments or helping people manage their budgets.[M] They can also help people make medical decisions, like providing treatment information or finding the best doctors.

Currently, the number of devices with built-in digital assistant technology outnumbers the global population.[H] Worldwide, smart phone users have increased by 5% annually for the past five years and represents about 85% of the global population.[H] Over the next 20 years, digital assistants are highly likely to become more powerful and capable of performing even more complex tasks, resulting in more user dependence, availability, and utilization.[M] For example, they are growing in their ability to provide more personalized recommendations based on learning from the user and understanding their needs, patterns, and interests.[H] They could also provide more detailed advice specific to the individual's profession or the associated application, which they were created – for example, area security or active defense applications and technology could inform the user of threats and recommend measured responses, or act autonomously, based on approved escalation of force measures and/or the rules of engagement.[H]

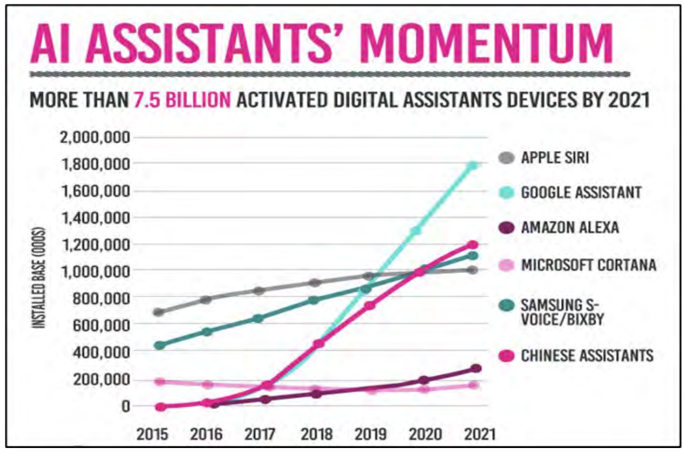


Figure 2: Business Solutions, Digital Assistants the Core Reality of the Future. Source Business Solutions

In military applications, digital assistants are likely (56-70%) to assist leaders with making complex decisions quickly by synthesizing large amounts of data, filtering out the noise, and providing data-based recommendations to decision-makers.[H] The Defense Advanced Research Projects Agency (DARPA) is focused on creating digital assistants that "make military decision-making more efficient and more effective at multiple levels of command; reduce the need for large command staffs; and enable smaller, more mobile, and less vulnerable command centers."[H] Considering Secretary of the Army, Christine Wormuth's, priorities, a more data-centric/data-driven force is essential in future Great Power Competition.[H] Digital assistants can achieve this objective by helping leaders and their supporting staff do more with less and faster.[M] Digital assistants have the potential to improve military decision-making processes by assisting users in sifting through large amounts of information quickly and efficiently across multi-domain operations.[H]

Regarding U.S. military competition, limited information is available on specific examples of digital assistant technology used by the Chinese or Russian military. However, the PLA is actively exploring and experimenting with new concepts and capabilities to leverage artificial intelligence to enhance its combat capabilities.[H] Some Chinese companies have developed AI-based war-gaming simulators, such as DataExa's AlphaWar, in which DeepMind's Starcraft AI drives the simulation.[H] Additionally, Microsoft is working with the military-funded National University of Defense Technology on surveillance technology, and Google has opened an AI research center in Beijing.[H] China is also developing AI technologies such as deep fake to generate fake news and media against rivals.[H]

An additional and promising potential application for military utilization is issuing an individual digital companion to Soldiers as they enter service. This digital companion would learn and grow with the Soldier as they progress through their career. More than a simplistic calendar/agenda tracker, the digital companion would be a direct conduit to the Soldier’s personnel records, healthcare information, retirement/TSP contributions, and education data, in addition to tying into their headquarters’ database and communicating with leadership and subordinates and interceding on their behalf. Tyler Sweatt, a former Army officer and current technology consultant, said virtual assistants will enable massive scale at all levels of the Army. “Imagine if company-level leadership was able to align schedules across a series of virtual assistants, plan training events, and conduct inventories based on AI-enabled supply rooms. At senior levels, the value of near instantaneous schedule optimization, task prioritization, and research would provide immense value to resource-intensive areas typically reserved for CAG/CCG types”.[H]

With greater reliance on and increased popularity of digital assistants, the risk of user manipulation by nefarious actors increases significantly, prompting some critics, like Apple CEO Tim Cook, to call for privacy regulations regarding the collection of personal and private information and responsible stewardship in professional and practical applications of digital assistants.[H] However, the benefits and practical applications of digital assistant and companion technologies are highly likely to continue to make sustained improvements solidifying their foundation in future daily life. Therefore, measures are necessary to mitigate the associated risk to the user.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to rely on statistics and corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information or revolutions in technological development.

Author: COL Nathaniel C. Stone
nathaniel.stone.mil@armywarcollege.edu

Minutely Invasive Bidirectional Brain-Computer Interfaces Likely Between 2025-2030, Limited Military Application Between 2030-2040

Executive Summary

Minutely invasive, bidirectional brain-computer interfaces (BCI) are likely (56-70%) between 2025-2030, with limited military application in 2030-2040, due to rapid advances in materials technology, computer processing, and neuroscience. Despite the concerns with guiding nano-scale devices injected into the bloodstream to the brain, the improved signal-to-noise ratio and write fidelity/precision (compared to non-invasive BCI) and the long-term health benefits (compared to invasive BCI) will drive the adoption of minutely invasive BCI, enabling people to interact with machines using their thoughts.

Discussion

Defined as computer technology that can interact with neural structures by decoding and translating information from thoughts (i.e., neuronal activity) into actions,[M] a BCI is a device that interfaces with the brain to enable interaction with the environment; it connects a computer to a brain, either by reading out brain signals and/or writing in brain signals.[H] Artificial intelligence (AI) isolates the brain signals that the BCI devices capture, as well as synthesize signals back into the brain.[H] BCIs allow people to use brain activity to control equipment such as prostheses or robots. Beyond medicine, scientists are researching BCIs for gaming, defense, and improving cognitive functions.[H]

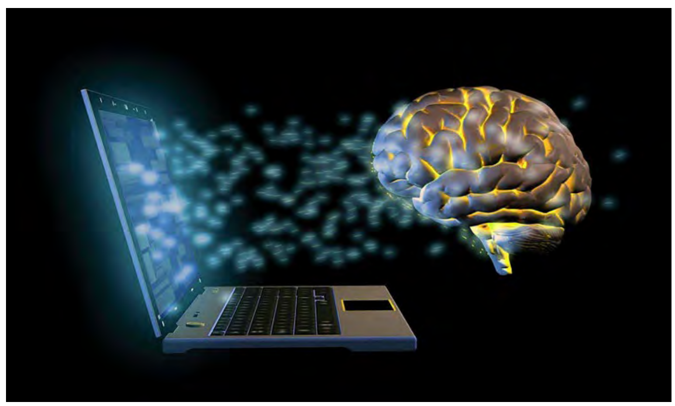


Figure 1: Wireless linkage of brains may soon go to human testing. Click on the picture or go to: https://www.youtube.com/watch?v=cL3e8tC8TwE to view the video. Source: Rice University

Investment in BCI technology is expanding, and the field is advancing rapidly, with around 59,000 academic publications[M] and 10,000 patents filed in 2021 alone.[M] The global BCI market was $1.31 billion in 2021, and according to Strategic Market Research, it will reach $5.34 billion by 2030.[M] In 2013, the National Institutes of Health launched the Brain Research Through Advancing Innovative Neurotechnologies (BRAIN) initiative to support the development and application of innovative technologies to revolutionize our understanding of the human brain.[H] Currently, the BRAIN initiative is supported by several federal agencies and dozens of technology firms, academic institutions, scientists, and other key contributors to neuroscience.[H] The application of BCI supports ongoing DoD technological initiatives, including human-machine collaboration for improved decision-making, assisted-human operations, and advanced manned and unmanned combat teaming.[H]

BCIs are traditionally categorized as invasive BCI, semi-invasive BCI, and non-invasive BCI.[H] Invasive BCI involves surgically implanting electrodes into the brain cortex to measure signals directly from the brain.[H] Semi-invasive BCI devices are external recorders that detect signals from superficially implanted devices.[H] An example of a semi-invasive BCI is an electrocorticography (ECoG) placed directly on the brain, but not implanted inside of the brain,[M] which records brain activity via a surgically embedded electrode grid. Non-invasive BCI technology involves external sensors/electrodes placed on the scalp to record the neural signal produced by the brain,[H] such as Electroencephalography (EEG), which is the most commonly used because of the cost and hardware portability.[H] In 2019, the Defense Advanced Research Projects Agency (DARPA) introduced a new category, minutely invasive, a class of nano-scale devices delivered to the brain through intravenous (IV) injection, ingestion, or other non-surgical methods.[H]

The signal quality for invasive and partially invasive BCIs is significantly greater than non-invasive BCIs, and write fidelity/precision is much higher, resulting in faster response time and greater control.[H] However, invasive BCIs are more traumatic to the brain, carrying an increased risk of infection, and are more challenging to maintain long-term,[H] restricting their use outside laboratories or clinical environments.[H] Testing of invasive BCIs are in FDA-approved clinical trails[H] to treat severe medical conditions, such as amyotrophic lateral sclerosis, cerebral palsy, stroke, or spinal cord injury.[H] Currently, no company has received *final* FDA approval to market a BCI for medical purposes, and it is unlikely (16-30%) the FDA will approve surgical implantable invasive BCIs for healthy people.[H]

BCIs that use non-invasive external sensing, rather than brain implants, receive weaker signals, leading to lower resolution and less precise control. Thus, when using only the brain to control a robotic arm or a wheelchair, a non-invasive BCI doesn't stand up to using implanted devices.[H] Despite the signal quality challenges, research in non-invasive BCI technology has increased due to its dual-use for medical, entertainment, and industrial work purposes, such as: stress reduction, augmented and virtual reality, gaming, or operating industrial robots.[H] [H] Several gaming companies are investing in wearable BCI technology, such as Valve[M] and Snap.[M] Future business tech predicted that by 2030, most virtual reality (VR) headsets could include the option for a BCI to *record* users' electrical signals, but that immersive effects could be limited at this stage, and only usable in specific situations.[M]

Non-invasive BCIs already exist, but do not offer the precision, signal resolution, bi-directional read/write capability, and portability required for advanced applications in real-world settings.[H] To overcome these challenges, DARPA launched the Next-Generation Non-surgical Neurotechnology (N3) program to develop non-surgical BCI for able-bodied service members.[H] DARPA funded six organizations to support the N3 program, each pursuing a range of approaches that use optics, acoustics, and electromagnetics to record neural activity and/or send signals back to the brain at high speed and resolution.[H]

Teams are pursuing either completely non-invasive interfaces that are entirely external to the body, or minutely invasive interface systems that include nanotransducers that can be temporarily and nonsurgically delivered to the brain to improve signal resolution.[H] The most promising is the Brainstorm project led by Battelle, using minutely invasive procedures that pair an external transceiver with electromagnetic nanotransducers (MEnTs).[H] The MEnTs are temporarily introduced into the body via IV injection into the circulatory system and then guided to a specific area of the brain to help complete a task through communication with a helmet-based transceiver.[H] Upon completion, the nanotransducer could be magnetically guided out of the brain and into the bloodstream and expelled from the body.[H]

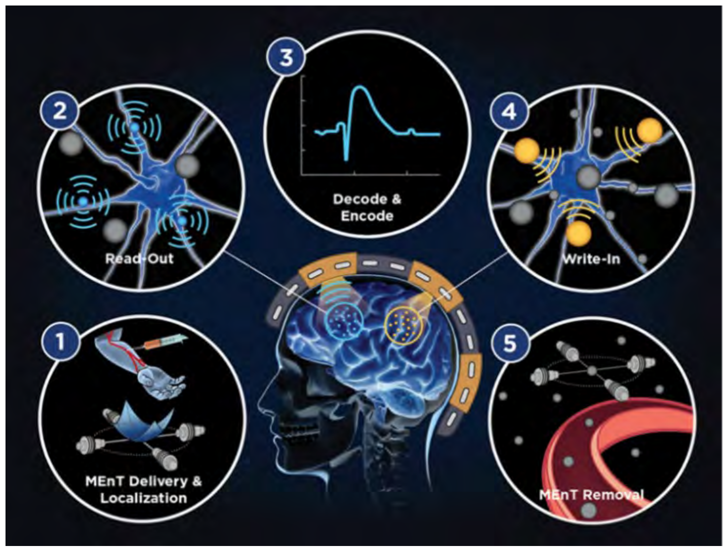


Figure 2: Phase 1 approach, in which MEnTs are first injected into the circulatory system, localized into the cerebral tissue using a magnetic field gradient, and then interact with neural tissue and applied magnetic fields to provide non-surgical neural interfacing. Source: Magnetic

During phase one of the N3 program, the Battelle team achieved "precise reading and writing to neurons." They are currently in phase two of the N3 program, focused on maturing this capability and testing the external writing interface.[M] In the third phase, the Battelle team plans to implement a regulatory strategy developed with the FDA in phase two to support future human subjects testing.[M]

Studies show that bringing a device from concept to approval takes three to seven years.[H] Given this timeline, the Battelle team will likely produce an approved minutely invasive bidirectional between 2025 and 2030. The Cyborg Soldier 2050: Human/Machine Fusion and the Implications for the Future of the DOD report predicted that specialized operators will be using neural implants for enhanced operation of assets by the year 2030.[H] Given the long-term health benefits over surgically implanted devices and the ability to remove the MEnTs, minutely invasive BCIs will likely be used over invasive BCI for special operators between 2030 and 2035.

All categories of BCIs raise multiple ethical, privacy, and trust concerns that would need addressed before widespread implementation. One ethical concern is that inserting a decision-making device into someone's brain raises questions about whether that person remains self-governing.[H] Providing hard on/off controls whenever possible or the ability to remove the device are ways to address privacy and ethical considerations.[M] Evidence from a 2020 Pew Research Center Report shows that U.S. public trust in neuroenhancements, (i.e., implanting brain chips to increase concentration and information processing), is low (69% report being "very/somewhat worried").[H]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Multiple artificial intelligence sources were used for research, consisting of ChatGPT, Perplexity, and Unrestricted Intelligence. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LTC Owen S. Adams
owen.adams.mil@armywarcollege.edu

Neuromorphic Computing Likely To Improve Speed, Power Efficiency, and Adaptability For Deep Learning Autonomous Systems By 2035

Executive Summary

It is likely (56-70%) that neuromorphic computing (which is a type of computer engineering that mimics the structure and function similar to the synapses and neurons in a human brain) will be the bridge that can overcome some of the existing challenges facing artificial intelligence (AI) and provide new use-case possibilities by 2035 due to three primary functionality advantages of speed, power, and adaptability. Additionally, neuromorphic computing is highly likely (71-85%) to drive artificial generated intelligence (AGI) and expedite the adoption of cognitive lethal autonomous weapons systems (CLAWS). Despite the latency of software and hardware challenges and ethical concerns regarding the attempt to make a computer version of a human brain, neuromorphic computing is leading the technology industry in the drive to work on edge AI to provide a plethora of new use cases and capabilities.

Discussion

The concept, use, and extensive capabilities of today's AI systems are increasingly integrated into our social, business, and organizational lives. However, as innovative as our current systems are, they are limited by the amounts of processing power and programmed data available to them.[H] Even the slightest change in the data environment renders AI models trained with traditional machine learning methods inoperable; however, an emerging field in computer engineering is working to overcome these challenges with brain-inspired computing methods.[H] The advantages of

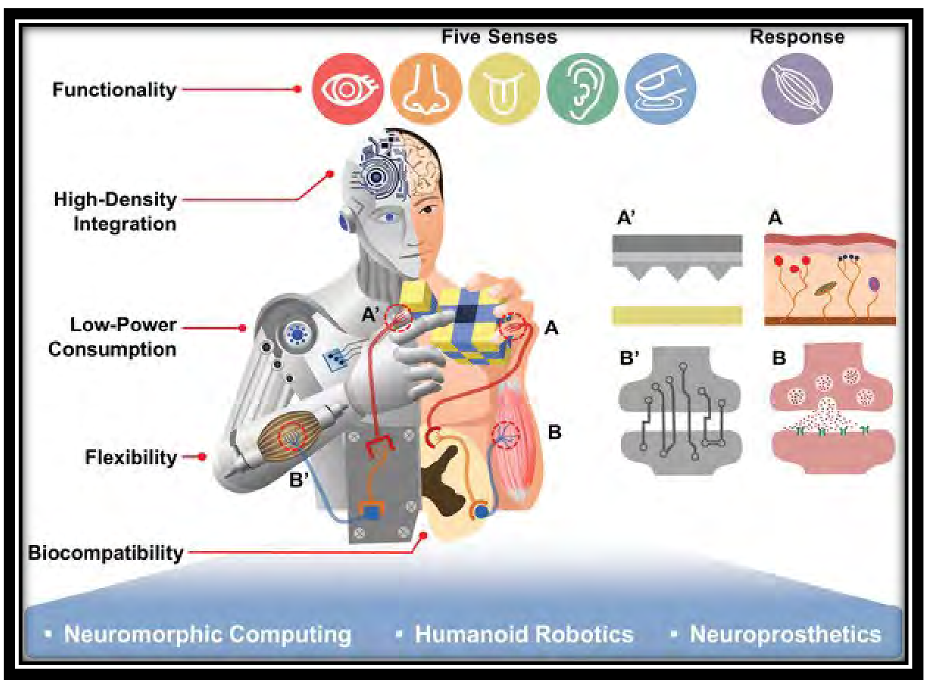


Figure 1: Potential sensory similarity objectives for neuromorphic computing. Source: Wiley

neuromorphic computing are speed, energy efficiency, and the ability to learn.[H] [M] It provides a promising path toward achieving AGI and has the potential to address the growing concerns about the use of autonomous systems and military applications.[H] Over the next decade, neuromorphic computing is expected to transform the nature and functionalities of various scientific and non-scientific applications. Some of these include mobile devices, autonomous vehicles, medical devices, and robotics, among others.[M]

Current computing runs on the Von Neumann system, which uses separate memory and processing units and encodes data using binary values. The process of moving the data between these separate units is known as the *von Neumann bottleneck* and it **limits** speed and **increases** power consumption.[H] Instead of having distinct sections for each, the brain-inspired neuromorphic computer chips process and store data collectively on each individual neuron (see Figure 2).[H] [H] This process avoids the *von Neumann bottleneck*, which **increases** speed and **reduces** power consumption.[H] A team of researchers from Graz University of Technology and Intel labs have demonstrated that a large neural

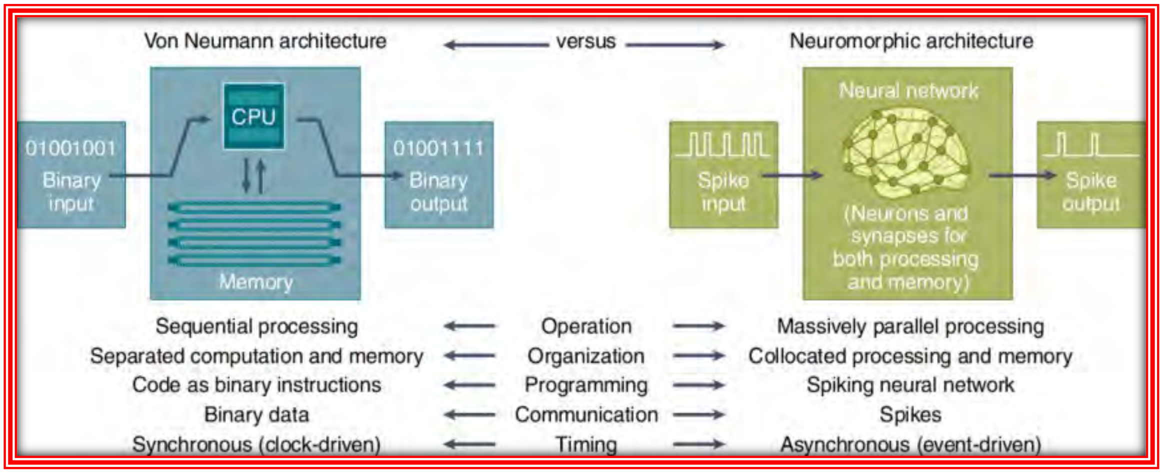


Figure 2: Comparison of the von Neumann architecture with the neuromorphic architecture. Source: Nature Computational Science

network can process complex sentences while consuming 4 to 16 times less energy on a neuromorphic computer vice non-neuromorphic systems.[H] [H] Accenture Labs experiment with automotive voice commands showed that a neuromorphic system could recognize short-string voice commands 200 milliseconds faster than a standard processing unit.[H] Research is still ongoing to determine the exact speed increase for deep neural complex computing; however, Intel's new processing neuromorphic chip, Loihi 2 is expected to be able to process neuromorphic networks up to 5000x faster than biological neurons.[H]

In addition to the increased speed and power efficiency of neuromorphic computers, their spiked neural network (SNN) is adaptable to changes in external stimuli. This flexibility is similar to the plasticity of the human brain, which fosters a system that can learn and solve problems independently of a programmer;[H] a characteristic which is particularly exciting for researchers and industry experts because it provides a plausible foundation for the path to reach AGI. AGI refers to an AI computer that understands and learns like a human; with the ability to reason, make judgments in uncertain conditions, and plan and display common-sense knowledge.[H] AGI could develop a synthetic brain with the same cognitive abilities as a biological brain by mimicking the human brain and nervous system. Such a brain could shed light on cognition and bring answers to awareness.[H] One such use case is the Human Brain Project, which uses AGI and neuromorphic supercomputers to perform neurobiological functions in an attempt to produce consciousness.[H] [H] Though machines have not, and may never, reach a human level of intelligence, neuromorphic computing offers the potential for progress toward that end; which is one of the definitive goals for engineers in this field of technology.[H]

The benefits and potential uses of neuromorphic computing are not limited to the commercial sector but could extend to the defense industrial base as well. In concert with AI and machine learning, this type of computing advancement can work on defense systems to provide faster analytical results and inform wartime decision-making; and the energy efficiency makes it ideal for field environments.[H] According to Mike Davies, Director of Intel's Neuromorphic Computing Lab, although the technology will not be commercially available for the next ten years (at least from Intel), the fields of aerospace and robotics are among the best use cases.[H]

The geostrategic environment is evolving almost as quickly as versions of AI. The war in Ukraine has evolved from tank warfare to the first full-scale drone war of our time.[M] The public use of such lethal autonomous weapons systems (LAWS) has brought the topic back to the center of debates as advocates, on both sides, seek to find an agreement for every-thing in the spectrum from controlled-use to a full ban.[H] Those supporting a ban list bias, rigidness, lack of ability to exert judgment, or make conscious decisions as reasons that LAWS should not be used;[H] some of the exact characteristics that neuromorphic computing is designed to address. When developed to

Figure 3: Dr. Oren Etzioni, Founder of Allen Institute for AI. Source: BrainyQuote

its full capability, neuromorphic computing, and AGI may allow LAWS to function in a manner that is more comparable to that of a human combatant.[H] Incorporating brain-like capabilities into technology such as LAWS will provide the cognitive capability to support dynamic learning in the context of complex and unstructured data. In turn, these cognitive LAWS (CLAWS) might incorporate more human-like discretion while making targeting decisions.[H] The future development, scale, and commercial availability of neuromorphic is unknown; but it is likely that this technology will eventually be incorporated into specialized products, including weapons of future combat.[H]

Despite the seemingly endless possibilities for neuromorphic computing, there are still obstacles and causes for concern. Neuromorphic computing software concepts are not equally aligned with hardware technology; thus the research still relies on standard, deep learning software and algorithms developed for existing, less advanced hardware.[H] This dependence can significantly reduce the performance advantages of utilizing a neuromorphic computer, to the point where accounting for communication and host machine expenses removes the advantages of using a neuromorphic computer to implement an algorithim.[H] Researchers, engineers and industry experts will to develop methods to optimize their use in order to get past this challenge.[H]

In addition to system specific hurdles, a larger obstacle for neuromorphic computing is the ethical dilemma. In his ten-year documentary project, Noah Hutton, a policy expert at Scientific American, interviewed a multitude of neuroscientists, some of whom highlighted potential ethical concerns about the concept of a brain-inspired computer.[M] The human body, including neurons and synapses, run on a motor of unpredictable "mistakes" (known as mutations), that generate variability. These variabilities do not always have "fixes" and the human body learns to adjust and overcome such imperfections. In computers, on the other hand, structural mistakes, known as "bugs," are quickly fixed to make way for the perfect code for the task at hand.[M] Hutton argues that " if we can never know the right kind of variability, it seems that what we're really talking about (in efforts to simulate biological structures on computers) is a digital system that does exactly what its creators want it to do."[M] This concept brings the long-standing argument about ethical accountability into the conversation; an issue that has not been solved and is cause for concern at the programmer and user end. (see HITL Report) Hutton concludes that simulations of neural activity will be less an objective reconstruction of "the human brain," but will ultimately hold a mirror up to the biases of their creators.[M]

Neuromorphic computing is still considered an emerging field whose systems are currently only available to researchers and industry experts.[H] It has the potential to significantly enhance AI capabilities over the next decade by creating more efficient and intelligent computing solutions and the technology is expected to transform a wide range of scientific and non-scientific applications and drive rapid growth in the neuromorphic computing market.[H]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were reliable and a preponderance of them corroborated one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy period of the estimate, this report is sensitive to change due to new information, research, and innovations in the respective field.

Author: LTC Nicole A. Washington
nicole.washington.mil@armywarcollege.edu

Top Machine Learning Algorithms Likely To Provide Baseline Future Military Artificial Intelligence Applications

Executive Summary

The top 10 types of machine learning (ML) algorithms listed below that exist in labs today are likely (56-70%) to become the baselines for the majority of future military capability over the next 10-15 years: Linear regression, Logistic regression, Decision tree, Naive Bayes, Artificial Neural Networks, K-means clustering, Anomaly Detection, Gaussian Mixture Model, Principal Component Analysis, k-nearest neighbors (KNN), Support Vector Machine (SVM). These complex logic advancements will become a commercial baseline for low or no-code application development tools. Development teams will then be able to build out domain specific artificial intelligence (AI) solutions for any organization including military. Government contracting companies will take note of these commercially available sources and figure out how to leverage AI solutions to solve military capability gaps. Contracting companies will then invest heavily in educating AI development teams and build prototypes as proofs of concept. Despite the thousands of different algorithms available in labs today and more being created daily, there are 10 that are most relevant to the military that can be used individually or together to fulfil the majority of military applications.

Discussion

There are several top tier technology companies and top tier university labs that are developing AI Algorithms to solve a myriad of thinking models. Both Mircrosoft[H] and Google[H] have developed and tested numerous AI Algorithms in their labs that are ready for incorporation as embedded technologies. Combined and reused open-source software is an example of how AI algorithms will be shared in AI solution sets. Whether AI algorithms are used in isolation or networked together, open-source algorithms[M] will set the baseline for AI

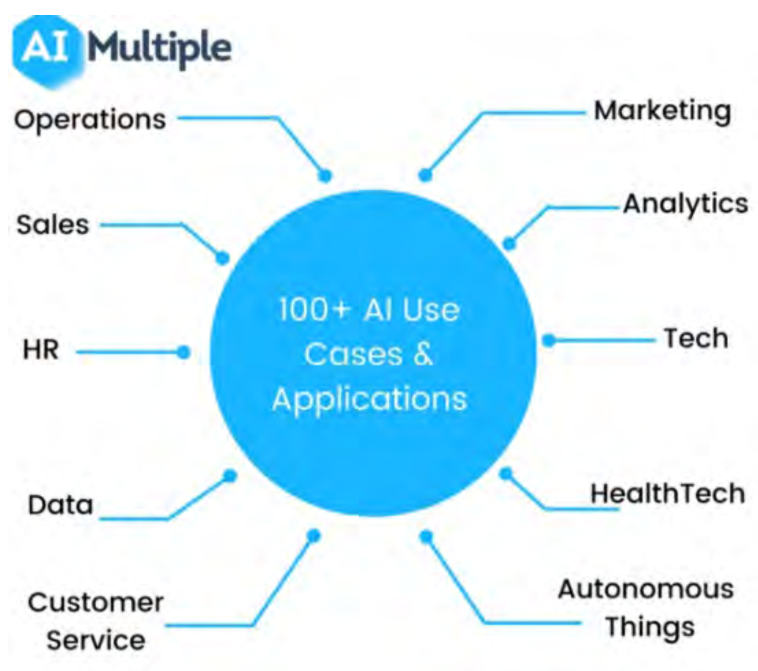


Figure 1: This picture describes the many commercial applications of AI. Source: [AI Multiple]

solutions. Figure 1 displays a vast array of categories for different commercial applications all that are developed by one or a combination of the top eleven algorithms. Similar to the wide array of categories in this commercial list, the categories for military relevant AI applications listed below are across all disciplines but can also be covered by the top 11 list of algorithms.

- Autonomous Weapons
- Education
- Robotics
- Digital Assistants
- Logistics Apps WFF
- BCI App
- Transport
- Medical WFF
- Human Augmentation
- Intel - Target Recognition /Threat Monitoring

With semi-autonomous drones already seeing battle in the Russian-Ukrainian conflict, the race to get fully automated and AI capability to the field will intensify. China has already publicly stated that the new environment will include "intelligent warfare"[M] which insinuates future use of both autonomous and intelligent weaponry. To maintain the US competitive edge in the great power competition with China, some government contract companies like Lockheed Martin and Boeing have already been awarded AI development contracts.[H] [H] Boeing is currently building embedded AI algorithms in autonomous and semi-autonomous vehicles (including drones)[H], subs and spacecraft.[H] Similar to commercial and government off-the-shelf (COTS & GOTS) software solutions of the past, filling government needs with pre-developed AI solutions is highly likely to be the wave of the future. There is already contracts to accelerate AI/ML government programs that demonstrate AI/ML algorithm integration opportunities.[M] Despite the positive lab results of 1000s of other commercially available AI algorithms, the military use of these commercially available AI will require education, capability gaps and application integration to all come together to recognize and realize the opportunity. The speed at which AI/ML applications are required and the unique capability gaps that will be identified and filled, reduce the likelihood for ongoing research and development of new algorithms. These top 10 as displayed in Figure 2 are the foundation for AI/ML and proven to be able to derive most other algorithms from combining these concepts together.[M]

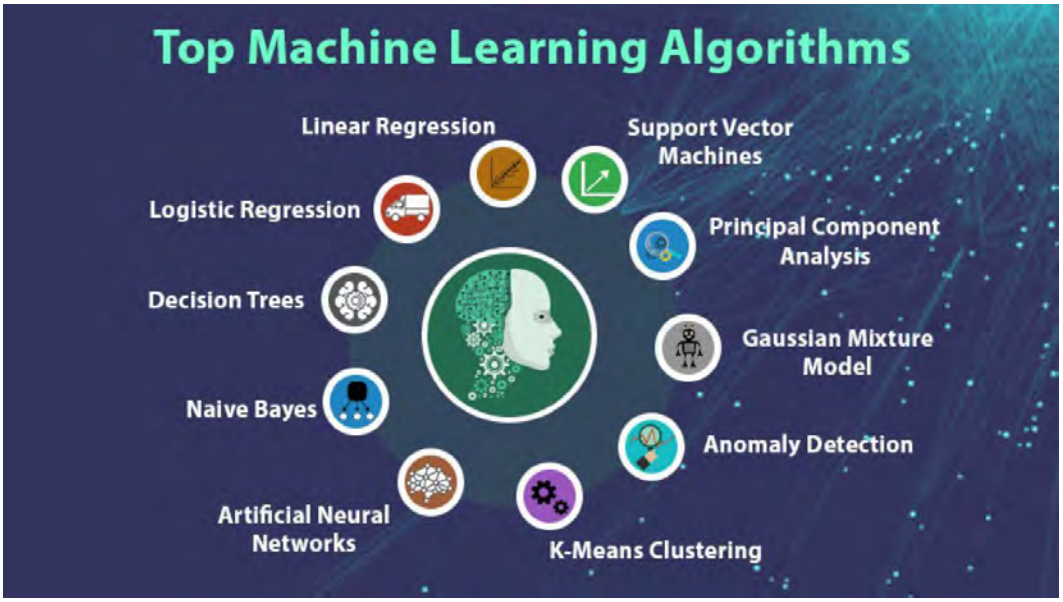


Figure 2: This picture describes the many commercial applications of AI. Source: Data Flair

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources are reliable and provided wide perspective of use cases with validated test results for AI Algorithms currently in labs. This proves that there was adequate time and multiple labs worked used similar structured methods to code and prove results. However, the logical extrapolation of the commercial results to estimate the military results was based on subject matter expert opinion in the military software development processes. Furthermore, given the lengthy timeframe of this estimate and ever-changing military requirements, this report is sensitive to change due to new information.

Author: Reginald A. Shuford
reginald.shuford.civ@armywarcollege.edu

Battery Power Highly Likely To Make Continued Improvements Between Now And 2040 Further Supporting Artificial Intelligence Advancements, But Limited By Range And Sustainment Infrastructure

Executive Summary

Due to recent advancements in battery technology concentrating on materials, manufacturing, and storage, battery technologies are highly likely (71-85%) to continue to improve between now and the year 2040 but limited in practical use and application by range and the associated infrastructure necessary to re-charge and sustain operation. Criticisms of battery technology include its cost, range and sustainment, environmental impact, unethical sourcing of raw materials, and their limited capacity to store energy. Despite these concerns, these issues are all being addressed in kind, mitigations are in place, and the technology is continuously improving and becoming a cost-effective option.

Discussion

Battery technology is a rapidly advancing field that has come a long way in the past few decades. According to a joint study published by the European Patent Office (EPO) and the International Energy Agency, between 2005 and 2018, patenting activity in batteries and other electricity storage technologies grew at an average annual rate of 14% worldwide, which is four times faster than the average of all other technology fields.[H] The development of battery technology is essential for the advancement of AI. Without reliable and efficient power sources, AI systems cannot function properly. Therefore, battery technology has become a major focus of research and development in the field. Improved battery technology will support a wide range of applications, from autonomous vehicles to intelligent robots. In the next 20 years, battery technology will continue to improve, and costs will continue to drop gradually, with advances in the following areas: materials, manufacturing processes, and energy storage capacity.[H]

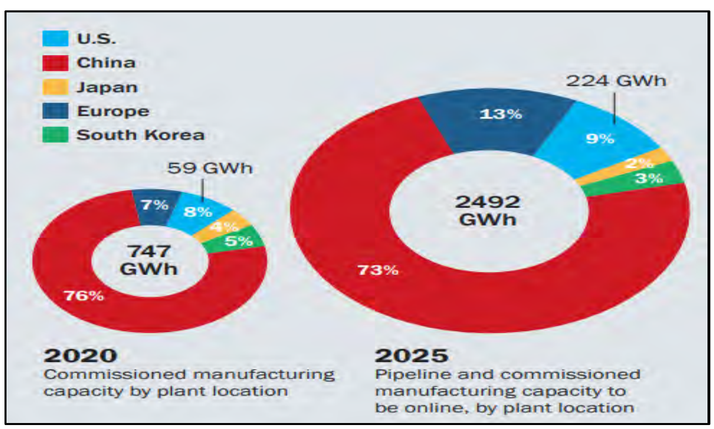


Figure 1: Cell manufacturing capacities. Source: [Lithium-Ion Battery Mega Factory Assessment]

Materials: Lithium-ion (LI) is the leading battery storage technology and remains the most viable option, though alternatives are growing.[H] Researchers are exploring new materials such as graphite, silicon, and lithium-sulfur, which could potentially increase the energy density of batteries and reduce their costs.[H] Additionally, new materials could enable the development of safer, more efficient, and longer-lasting batteries.

Cobalt is the most expensive of the elements required to make batteries. Most of it is sourced from mines in the Democratic Republic of the Congo, where unsafe working conditions and child labor are serious problems.[H] As a result, the industry has been trying to reduce cobalt usage. Scientists at Tesla have developed two new chemistries that appear to be cobalt-free and utilize a "high-nickel" cathode chemistry, which relies on "novel coatings and dopants" to replace the stabilizing presence of cobalt. Still, they have yet to be proven or mass-produced.[H]

Manufacturing Processes: Advances in manufacturing processes are also leading to improvements in battery technology.[H] For example, 3D printing used to create custom-shaped batteries with complex internal structures, allows for more efficient energy storage. New manufacturing techniques are highly likely to enable the mass production of batteries with higher energy densities and lower costs. Additionally, scientific and technological advances in the development of materials paired with new designs and advances in manufacturing, such as solid-state batteries, are being developed to increase energy density, reduce the size, and extend the life and range of batteries.[H]

Energy Storage Capacity: Battery technology is highly likely to continue improving with energy storage capacity advances focused both on utility-scale storage (long-duration) and aggregated technological and transportation (short-duration) applications.[H] LI batteries are a crucial driver of increasing demands for battery storage for short-duration energy storage applications. For emphasis, gains in the amount of energy LI batteries can store have been on the order of five percent per year. That means that the capacity of current batteries is over 1.5 times what they would have held a decade ago.[H] Researchers are also exploring new chemistries and architectures that could increase the energy density of batteries even further and allow for long-duration energy storage, which will aide in power distribution and utility service applications.[H] Long duration energy storage has less of an impact on the development of AI applications directly, but the advances are likely to reduce carbon footprints worldwide and affect how power is

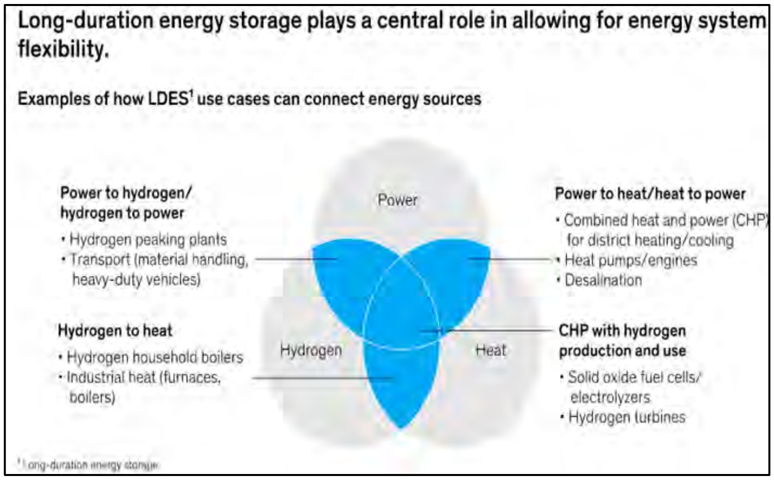


Figure 2: LDES Examples in connecting Energy Sources. Source: McKinsey & Company.

distributed and generated at scale which will affect how power is sourced for AI applications.[H] Further, improved short-duration storage capacity represents extended battery life which has significantly extended range and time of use while charging methods such as wireless charging, infrared charging, super-fast charging, and advanced photovoltaics have been developed to make charging faster and more convenient when it is necessary.[H] [H] [H]

Limitations: Battery technology is limited, primarily by range and efficiency, requiring recharging or changing the cell to sustain use. Current battery recharging capability faces several significant challenges, including the lack of charging infrastructure to support high power consumption, a limited network of charging stations, and dissatisfaction with the charging experience.[H] [H] Regarding Electric Vehicles (EV), the current infrastructure is not capable of sustaining the large numbers of EV's projected in the near future.[H] Even with projected improvements in EV charging and additional stations, the country needs twenty times the current capacity.[H] This example assumes a reliable power grid is available with standing infrastructure capable of sustaining predictable use. In austere environments, where power generation and sustainment are also a challenge, the likelihood of sustained battery use is unlikely (31-45%) by 2040 unless range and recharging technologies improve exponentially.[H]

Considering future technological development and implementation as costs lower and battery use continues to grow over the next two decades, risks associated with new materials and manufacturing processes in batteries are numerous and wide-ranging.[H] Therefore, the risks must be considered when planning for battery use in future applications. It is essential to consider the safety of the materials, the environmental impact, the ethical sourcing issues, and the processes used to produce batteries when justifying the ends so that mitigations can be taken, and pressure applied where acceptable standards fall short.[H] Considering the future of energy dependence and the associated applications of batteries therewithin, battery technology will continue to grow and be a substantial part of the energy equation for the long term.[H] [H]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to rely on statistics and corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Nathaniel C. Stone
nathaniel.stone.mil@armywarcollege.edu

Autonomous Intelligent Cyber-Defense Agents Likely Deployed To Edge Devices Between 2035-2040, Enabling Cyber Resilience In Human-machine Teaming

Executive Summary

Autonomous intelligent cyber-defense agents (AICA) likely (56-70%) between 2035 and 2040 due to rapid advancements in: machine learning (ML), edge artificial intelligence (AI), and neuromorphic computing. Despite the technical, operational, and ethical challenges of implementing AICA, the need to operate in degraded cyber and electromagnetic-spectrum environments and the increasing sophistication of cyberattacks will drive the development and deployment of AICA to edge devices – enabling cyber resilience[6] in human-machine teaming.

Discussion

AI and ML are increasingly important in cyber security.[H] (see AI Development Report) According to a recent survey by the Capgemini Research Institute, 69% of senior executives believe that AI is necessary to respond to cyberattacks.[M] In an effort to protect their systems and data, organizations leverage the latest AI-based cyber defense tools, such as: firewalls, intrusion detection systems (IDS), and security information and event management (SIEM), in order to detect and remove malware based on known signatures and anomalies.[H] [M] Detecting cyberattacks involves endpoint detection and response (EDR) software installed on endpoint devices, which collect and report cyber-relevant data to a central defensive system/center, that performs the appropriate analysis and response actions.[H] With AI and ML, cyber defense tools are significantly improving, but these systems learn slowly and are generally ineffective against unknown and adaptive threats.[M]

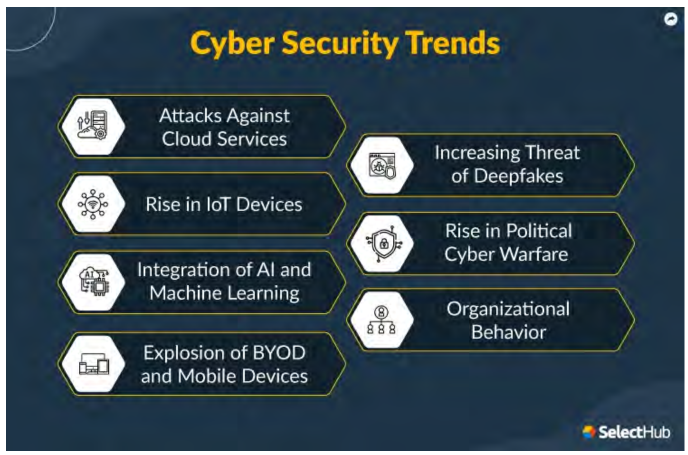


Figure 1: Cyber trends. Source: SelectHub

The battlefield of 2030 through 2040 is highly likely (71-85%) to experience unprecedented levels of cyber and electromagnetic (EM) degradation – preventing communication over the network to central security operation centers (SOCs) for cyber

[6] The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Source NIST

defense.[H] Improvements in AI-powered malicious software trained to think, avoid detection, and adapt to changing environments, will make cyber defense more difficult.[M] Due to advancements in quantum computing, Public-key Cryptography (PKC) is also likely to be broken – jeopardizing secure communications, and exposing information on networks.[H] (see Quantum Computing Report)

Additionally, the battlefield is highly likely to include billions of connected devices (see Figure 2), such as: networks of sensors, wearables, robots, and manned and unmanned vehicles, controlled through advanced display and/or brain-computer interfaces (BCI) – all communicating over 6G networks.[M] (see Human Interaction Report) (see BCI Report) (see 6G Report) This interconnected battlefield will significantly increase the cyber-physical attack surface and vulnerability to individuals and organizations.[H] The trend of the rising number of connected devices on the battlefield will generate more alerts and events,[M] [M] in turn, overwhelming central SOCs, and cyber defense tools' capacity to defend networks and devices.[H]

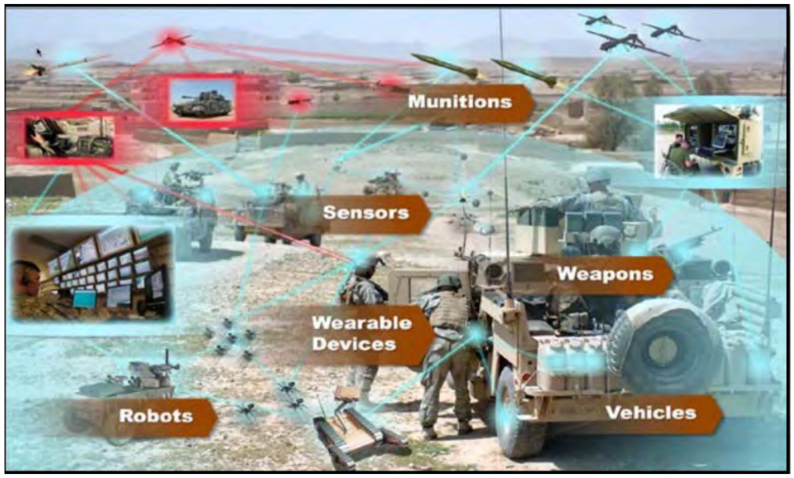


Figure 2: IoT meets the military battlefield. Source: IEEE

The rapid advancement in edge AI and neuromorphic computing will likely lead to significant improvements in processing efficiency, low-latency real-time operations, and the ability to perform sophisticated cognitive tasks at the edge with reduced energy consumption;[H] likely establishing capabilities on endpoints to support AICA. (see Edge AI Report) (see Neuromorphic Computing Report) Several research groups and organizations are actively working on development and standardizations of AICA for cyber resiliency, such as: the Defense Advanced Research Projects Agency (DARPA),[H] Army Research Lab (ARL),[H] and the North Atlantic Treaty Organization (NATO).[H]

The DARPA is researching how to automate cyber defense through programs such as the Cyber Grand Challenge (CGC)[H] and the Cyber Agents for Security Testing and Learning Environments (CASTLE).[H] Concluded in 2016, the CGC program demonstrated the feasibility of autonomous offensive and defensive agents operating against each other, with humans both on the loop and out of the loop.[H] The CASTLE program aims to train AICA to defend against Advanced Persistent Threats (APT).[H]

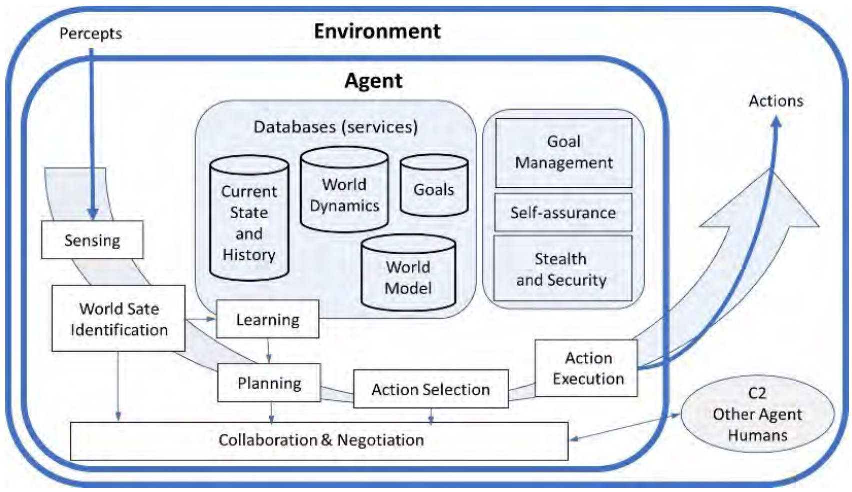


Figure 3: AICA functional architecture. Source: DTIC

Dr. Alexander Kott, ARL Chief scientist of U.S. Army Combat Capabilities Development Command (CCDC) and the Army's senior research scientist for Cyber Resilience,[H] chairs the NATO Science and Technology Organization's research group on Intelligent Autonomous Agents for Cyber Defense and Resilience.[H] The organization's goal is to accelerate the advancement of AICA by creating reference architecture (see Figure 3), and a technical roadmap.[H] Dr. Kott presents the concept of AICA working in "cohorts or swarm, capable, together, to detect cyber-attacks, develop the appropriate countermeasures, and run and adapt tactically their execution."[H] According to Dr. Kott, AICA are necessary as humans are the weakest link in the cyber world, and human warfighters will not have the necessary skills or time to perform cyber defense locally.[H]

Currently, ARL has functional, active defense system prototypes showing results on testbed networks.[H] These prototypes consist of defending against data exfiltration and targeting malicious network traffic.[H] The NATO Information Systems Technology-152 Research and Technology Group suggests a robust, effective, intelligent agent is likely in eight to twelve years.[H]

The development of AICA has its challenges; it will require advancements in AI towards Artificial General Intelligence (AGI) to operate intelligently in complex environments.[H] Additionally, there are also concerns in reference to unintended harm, including: functional, safety, security, ethical, or moral risks.[H] (see General AI Report) Despite these concerns, the need to operate in degraded cyber and electromagnetic-spectrum environments and the increasing sophistication of cyberattacks will drive the development and deployment of AICA to edge devices – enabling cyber resilience in human-machine teaming.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Multiple artificial intelligence sources were used for research, consisting of ChatGPT, Perplexity, and Unrestricted Intelligence. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LTC Owen S. Adams
owen.adams.mil@armywarcollege.edu

Commercially Available 6G Highly Likely By 2030 With Widespread Deployment Between 2030-2032, Connecting The Military Internet Of Things

Executive Summary

6G networks are highly likely (71-85%) to become commercially available by 2030, with widespread deployment between 2030 and 2032 due to the need for faster and lower-latency communications networks. Despite being in the early stages of development without defined standards, the limitations of 5G networks and the need to stay ahead of near-peer competition will drive the development and adoption cycle of 6G, enabling machine-to-machine (M2M) communications and connecting the military Internet of Things (IoT).

Discussion

Even as the global deployment of 5G networks are still underway, leading research universities such as King's College London, Beijing University, the University of Oulu, and the University of Texas,[H] as well as industry leaders such as Nokia, Vivo, Samsung, NTT Docomo,[H] Google, Apple, SK Telecom, and Huawei[H] are working on the sixth generation of mobile connectivity.[H] 6G networks aim to connect the digital, physical, and virtual worlds through faster M2M communications and support for data-intensive immersive technology.[H]

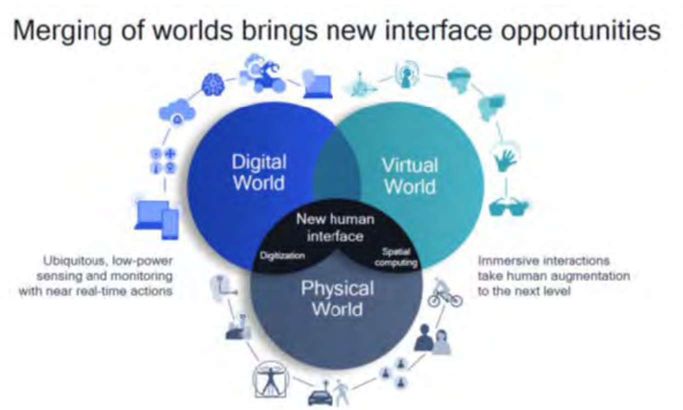


Figure 1: Merging of worlds brings new interface opportunities. Source: [Qualcomm 6G Symposium]

5G networks provide significant improvements in capability over previous telecommunications networks, but they cannot meet the requirements of emergent data-intensive applications, such as multi-sensory virtual and augmented reality (VAR), multiway virtual meetings with holographic projections, brain-computer interfaces, and autonomous robotics.[H] The latency, reliability, and data rate requirement of these future data-intensive immersive technologies are beyond the capacity of existing 5G systems and networks.[H]

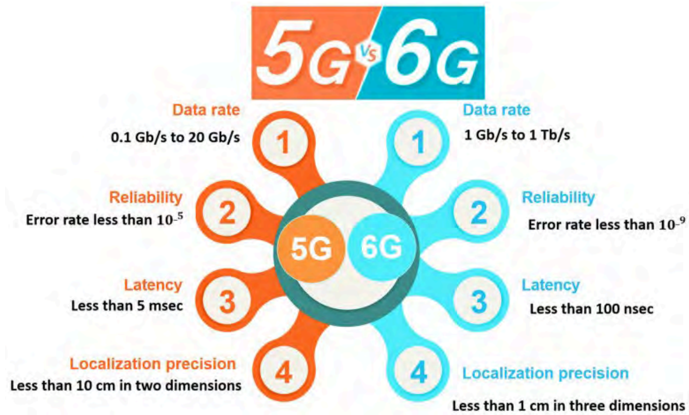


Figure 2: 5G and 6G features comparison. Source: National Center for Biotechnology Information

6G is projected to deliver significant boosts in capacity, latency, reliability, and efficiency[H] through the use of the 95 gigahertz to 3 terahertz (THz) frequency range of the electromagnetic spectrum that is currently not in use by telecommunications.[M] The use of this frequency range is highly likely to increase network speeds from 5G speeds of 10Gbps to one terabit per second (Tbps) with 6G.[H] According to predictions from the University of Sydney, 6G could achieve speeds that are up to 100 times faster than 5G.[M] Additionally, the network latency is highly likely to drop from five milliseconds to just one millisecond; combined with improved network speed will enable almost instantaneous transmission of data.[M]

On 4G, data processing occurred only on cloud networks, then advanced to both the cloud and edge devices in 5G.[M] 6G networks are highly likely to have integrated mobile edge computing technology, not an add-on like the current 5G,[H] providing benefits such as improved access to AI capabilities and support for sophisticated mobile devices and systems.[H] 6G is highly likely to connect networks of sensors, wearables, robots, manned and unmanned vehicles, and IoT devices that use cloud and edge computing,[M] reducing the bandwidth and time needed to transmit and process data,[M] connecting the military IoT.[H] Despite cybersecurity concerns with the increased number of devices processing and sharing data outside of data centers; improved data transmission speed, situational understanding, and decision-making will override these concerns.[M]

6G is still in the pre-standardization phase without agreement on standards.[H] To complicate this matter, a multitude of international organizations and standards bodies worldwide, such as the 3rd Generation Partnership Project (3GPP), the Institute of Electrical and Electronics Engineers (IEEE), the International Telecommunication Union (ITU), the International Organization for Standardization (ISO), and individual country standard organizations, are involved in developing the standards.[H] Despite these challenges, initial work on 6G specifications is likely (56-70%) to start with 3GPP Release 20 in 2025, and be completed and ratified by 2028 with 3GPP Release 21.[H]

The likely timeline of 6G varies slightly among sources, but following the 10-year development timelines of previous cellular technologies, most experts agree that 6G will not be commercially available until the end of this decade.[H] Peter Vetter, President Nokia Bell Labs Core Research, expects the first 6G specification publication by 2028, and 6G to launch commercially by 2030.[H] Nick McKeown, senior vice president of the Network and Edge Group at Intel, stated he sees 6G "being rolled out in 2030."[M] Whereas Howard Watson, the Chief Technology Officer of BT, thinks that 6G will be launched around the 2032 Olympics, as most next generations of mobile networks are usually rolled out around the Olympics.[M]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LTC Owen S. Adams
owen.adams.mil@armywarcollege.edu

Quantum Computing Likely Cracks Public Key Cryptography Between 2030-2035, Compromising Human-Machine Communication

Executive Summary

Substantial investment and technological advancement in quantum computing make it likely (56-70%) that public-key cryptography (PKC) will be broken between 2030 and 2035. While there is increased research in quantum-resistant cryptography, it is likely the standardization and implementation could take a decade or more, and new key-cracking algorithms will be developed to break post-quantum cryptography (PQC), compromising human-machine communication through "steal-now, decrypt-later" attacks and compromise of digital communication.

Discussion

Creating quantum computers has become a priority for nations wishing to gain the next competitive advantage in the digital age. Recently, China announced $15.3 billion in funding as part of its 14th five-year plan for quantum technology, double the investments by EU governments and eight times more than U.S. government investments.[H]

Figure 1: MIT Quantum Computing Overview Course. Click on picture or go to: https://www.youtube.com/watch?v=aeDbYuJyXr8&t=7s to view video. Source: Learn-xpro.mit.edu

Recent technological advances have enabled rapid scaling of both the physical number of qubits and the computational capabilities of quantum computers.[M] In 2019, Google claimed quantum primacy with its 53-qubit processor. In 2021, China produced two larger quantum computers with 56 and 66 qubits.[M] In November 2022, IBM announced the 433-qubit Osprey processor, more than tripling the 127 qubits processor it produced in 2021.[H] IBM's quantum road map projects a 4,158-qubit processor by 2025, and the ability to scale to 100 thousand qubits in the future.[H]

These advances pose a threat of using large-scale quantum computers to break essentially all public-key cryptography in use today.[H] Quantum computers can break PKC by solving complex mathematical problems, or break symmetric key cryptography by exhaustively searching for all possible secret keys.[M] According to a recent study conducted by RAND, professionals from private industry predicted that quantum computers with cryptological capabilities would become available in 2031, while academic experts foresaw this happening in 2035.[H] The National Security Memorandum on *Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems* expresses that to mitigate this risk, the U.S. must transition to quantum-resistant cryptography by 2035.[H]

The National Institute of Standards and Technology (NIST) is in the process of selecting encryption algorithms to become part of its planned PQC standard. After six years of testing PQC solutions, NIST announced four PQC candidate algorithms for standardization and initiated a fourth round of testing to standardize an additional algorithm.[H] Shortly after the announcement, a team of scientists cracked one of the NIST-approved PQC algorithms using a classical computer in just over an hour.[M] Jonathan Katz, professor in the department of computer science at the University of Maryland, said "Three of the four PQC schemes rely on relatively new assumptions whose exact difficulty is not well understood, so what the latest attack indicates is that we perhaps still need to be cautious/conservative with the standardization process going forward."[M] NIST expects to develop the draft standard by 2024, with the expected implementations of new PQC algorithms requiring updates to protocols, schemes, and infrastructures.[H] A recent RAND report estimates implementation of PQC protocols to extend into the mid-to-late 2030, and potentially much later.[H]

The time between the emergence of quantum computing and the development of cryptography to match it creates a security risk of "steal-now, decrypt-later" attacks and compromise digital communication. "Steal-now, decrypt-later" attacks would occur when encrypted data is downloaded today with the intent of using quantum computers to decrypt that data in the future.[H] The impact of "steal-now, decrypt-later" attacks could devastate national security systems in cases where such information needs to be protected for many decades.[H] Digital communication compromise would occur if PKC was cracked before the implementation of PQC. By breaking current encryption, quantum computing would jeopardize secure communications and expose all information on the network.[H]

Cryptography is a critical component of human-machine teaming, as it is essential for providing secure communication and data storage. Cryptography also ensures the trustworthiness of a machine's decisions and actions, as well as verifying the integrity of data. Human-machine team information exchange must be created on trusted networks that connect humans and machines within and between teams.[H]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LTC Owen S. Adams
owen.adams.mil@armywarcollege.edu

Commercially Available, Fully Homomorphic Encryption Likely Within the Next 5 Years, Enables Quantum-Safe, Privacy-Protected Machine Learning

Executive Summary

Fully homomorphic encryption (FHE) is likely (56-70%) to become commercially available within five years due to substantial investment and technological advancement. Despite usability and performance challenges, the dual commercial and government use and the limitations of current encryption solutions will drive the development and adoption cycle of FHE, enabling quantum-safe privacy-protected machine learning (ML).

Discussion

Cryptography ensures the confidentiality and integrity of data while concealing it from those not authorized to access the data.[M] It is possible to store and transmit data in an encrypted form, but the user must decrypt it before it is processed, which exposes it to attack. Recent advances in cryptology have enabled calculations on encrypted data through the use of homomorphic encryption (HE).[H]

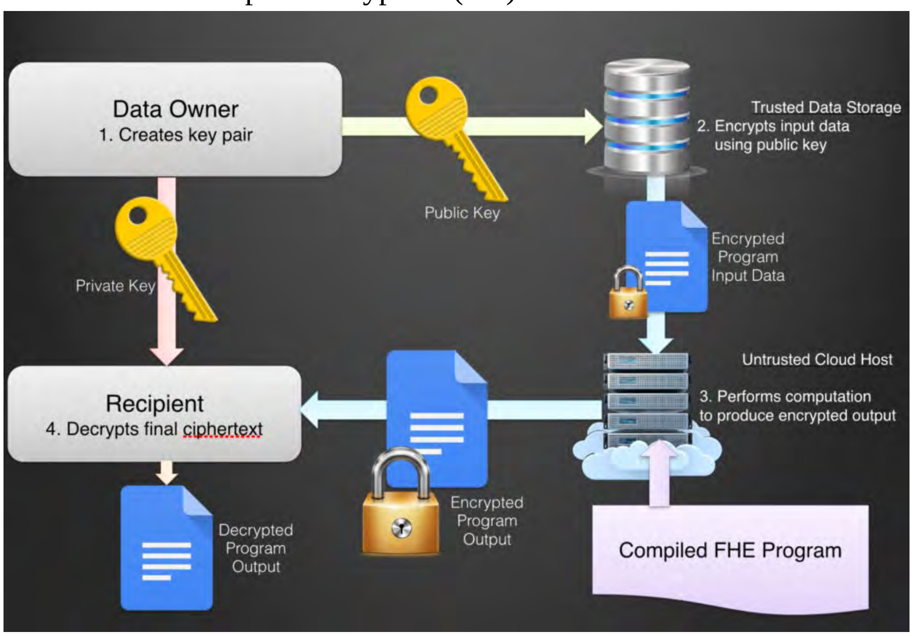


Figure 1 Visual representation of how FHE protects data on untrusted networks. Source: Galois

HE is comparable to other forms of public encryption as it utilizes a public key to encode information, and allows only the person possessing the corresponding private key to access the unsecured data.[H] What distinguishes it from other encryption techniques is that it exploits an algebraic system that permits a range of calculations on the encrypted data rather than unencrypted data – essentially keeping data protected at all times.[M]

There are three categories of HE: partially homomorphic encryption (PHE), somewhat homomorphic encryption (SHE), and FHE. PHE ensures data security but restricts the number of calculations on the data, which includes only adding or multiplying. SHE permits limited operations, but only for a set number of times. FHE allows data processing while it is still encrypted, preserving the data's privacy even throughout the analysis.[H]

As a concept, HE is not new; PHE and SME systems have existed since the late 1970s,[H] and FHE was first proposed in 2009 by Dr. Craig Gentry, while studying as a graduate student at Stanford University.[H] Even though FHE has been discussed and researched in academic circles for over a decade, it is not widely integrated into production environments due to two main limitations.[H]

The first challenge is related to accommodating multiple users. If an FHE system uses an internal database for calculations and multiple users want to ensure their data is safe from the provider, an option would be to create a separate database for each user with encryption under their public key. This would quickly become unfeasible if the database is extensive and there are numerous users.[H] The second challenge is improving the mathematics that directs the encryption. FHE utilizes broad and complicated formulas to maintain the safety of the information, causing a significant computational burden. This additional overhead significantly expands the time required to complete calculations, making FHE calculations of intricate functions unrealistic.[M]

Despite these limitations, research, and development to scale FHE are highly active due to the dual commercial and government use, with over 150 million dollars in global investment in 2021 and expected growth of nine percent between 2022 and 2030.[H] Both private and government organizations, such as Microsoft, IBM, Google, Intel,[H] and the Defense Advanced Research Projects Agency (DARPA),[H] are interested in FHE due to increased computer attacks compromising infrastructure, exposing private or sensitive data.[H] Encrypting data with FHE is likely to ensure infrastructure breaches do not expose private or sensitive data; limiting financial and reputation risks.[H] Both organizations are also interested in private machine learning, where users or organizations could provide private or sensitive data to benefit from machine learning services, without showing their data. FHE solves this issue by allowing multiple parties to collaboratively train a single machine learning model without sharing any of their training data.[M]

At the end of 2021, tech research firm Gartner estimated the time to market was between three to six years.[H] Researchers from organizations such as Microsoft, IBM, Google, Amazon Web Services, government organizations, and academia formed an open consortium to standardize HE and to advance secure computation.[M] With these investments and research, FHE has progressed quickly. In 2016, IBM introduced the initial version of its FHE library, which was a hundred trillion times slower than plaintext operations. IBM worked to address this issue, and in 2018, created a version that was two million times faster than the original. It is still a million times slower than plaintext operations on average, meaning a job that would take a second with plaintexts would take 11.5 days with the 2018 version of IBM's FHE library.[M] This decrease in speed is not practical for commercial or government organizations interested in homomorphic encryption; nevertheless, a boost of around 100 million times in two years is remarkable and shows the rapid advancement in FHE.[M]

In January 2023, the Defense Advanced Research Projects Agency (DARPA) awarded Duality Technologies a multi-million dollar contract for a Phase II Data Protection in Virtual Environments (DPRIVE) program to accelerate privacy-protected ML. In Phase I of the program, Duality Technologies designed an integrated circuit that accelerated FHE computations on encrypted data.[M] The DPRIVE program will enable strong privacy protections at the tactical edge through the development and deployment of hardware accelerators to edge computing devices where power and time are a premium.[H]

As quantum computing technologies advance, FHE is likely to become more important as the math behind FHE is based on lattice technology[H], which is likely to be resistant to quantum computing code-cracking.[H] FHE will enable the Department of Defense (DoD) to share and permission data across untrusted networks and trust zones using post-quantum security, enabling privacy-protected ML.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LTC Owen S. Adams
owen.adams.mil@armywarcollege.edu

Human-Machine Teaming Skills

SINGULARITY
HUMAN-MACHINE TEAMING

Soft Skills Highly Likely Essential for Effective Human-Machine Teaming Through 2040

Executive Summary

As human-machine teaming (HMT) becomes more common in our society, it is highly likely (71-85%) the skills needed to interact with and manage artificial intelligence (AI) effectively will shift from computer science and coding toward softer skills based on leadership, communication, and creativity. Generative AI can create art, build models, and write articles, but there are nuances that AI has yet to achieve. Examples of nuanced development include understanding the target audience, the operational environment, and a product or service's overall end state or task. Despite industry trends, critics argue that the need for creative communicators will subside as AI becomes more capable.

Discussion

As HMT becomes essential to the workplace, required skills for the human workforce are beginning to come to light. Industry leaders are betting on soft skills such as communication and emotional intelligence, as well as critical and ethical thinking.[H] Harvard Business Review described vital roles for humans working with AI in three categories, "train machines to perform certain tasks; explain the outcomes of those tasks, especially when the results are counterintuitive or controversial; and sustain the responsible use of machines."[H]

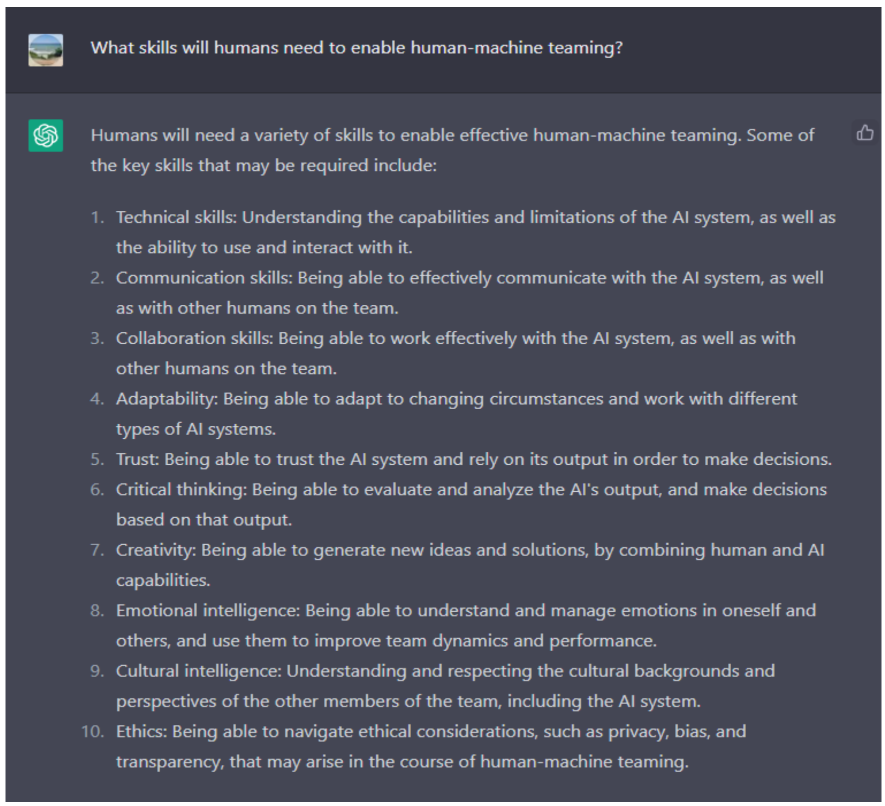


Figure 1: ChatGPT response to the prompt: What skills will humans need to enable human-machine teaming? Source: ChatGPT

Bidirectional communication is essential to HMT. True bidirectional communication enables trust and enhances the team's productivity.[M] This communication will be facilitated by skilled prompt engineers who can maximize the efficiency of the AI's user interface.[M] Future leaders will be those who can interface with human and machine teammates; this is an emerging field called the human-machine team manager.[M]

Creative thinkers can use AI in ways that their creators never envisioned. For example, Michelle Huang recreated a younger version of herself by loading twelve years of daily journals into Generative Pre-trained Transformer (ChatGPT), training the AI to respond like her younger self.[M] Some see potential in this type of AI as a therapy tool.[M] If analysts can train AI to think like specific people, this technology will likely be used to develop convincing deceptive fakes by 2035. During this timeframe, AI will also likely enable analysts to gain insights into the actions and reasoning of their targets. In this example, AI will enhance the skills required to manipulate a target or audience.[M] AI developers are even working on AI that can generate videos.[M] It is likely that this technology will be used to deceive a target audience when paired together. On the other side of this development, chances are less that researchers will be able to recreate an effective leader or strategist capable of assisting with friendly planning by 2035. The skills required for such an undertaking lean heavily toward creative thinking, data analysis, and emotional intelligence.

People with no formal training or experience in coding can have a formidable impact using AI. People skilled in creative and analytic thinking can leverage AI to write and modify code at an incredible rate, with little cost or computer science training. Recently, Cybersecurity researchers with CyberArk were able to create malware using ChatGPT.[H] Creating code by engineering the correct prompt for the AI will make coding incredibly easy and dangerous.

When paired with a responsible, creative user familiar with the field of work to accomplish its tasks, AI is less likely to make mistakes.[M] From a military perspective, this is comparable to an intelligence professional using an AI to assist with analysis, only to blindly accept the AI's recommendations without applying trained scrutiny to the AI's work. The U.S. intelligence community is already considering using AI to increase the speed and accuracy of reporting, but not to replace human analysts.[M] Leaders throughout all walks of society are looking to AI to increase productivity. Many lean on it for mundane tasks, such as assisting with composing emails and speeches or just doing quick research.[M] Critics are quick to point out the apparent drawbacks of AI, such as the lack of empathy, embedded bias, privacy concerns, and blatant mistakes.[M] A good case study is CNET. The publication used AI to generate articles, many of which contained incorrect and misleading information and, in one case, false investment information, potentially leading readers to make uninformed choices with their money.[M] CNET did claim that humans fact-checked the AI, so even with a human in the loop, mistakes will still happen.

Despite the current trend showing a growing requirement for these soft skills discussed above, some argue that as the capability of AI models grows, the requirement for these skills will become obsolete.[M]

While the examples provided are contemporary, the future of HMT will rely on soft human skills to realize the full potential of AI. While it is likely that future AIs will improve their own code[M], the human factors of creativity and ethical behavior will likely endure.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. While sources were generally reliable and tended to corroborate one another, many are based on opinions backed by anecdotal evidence rather than evidence-based study. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: Dennis J. Weaver
dennis.weaver.mil@armywarcollege.edu

Prompt Engineering Skills Likely Essential To Human-Machine Teaming Through 2040

Executive Summary

It is likely (56-70%) that human-machine teaming (HMT) related to large language model (LLM) artificial intelligence (AI) will rely on skilled prompt engineers through 2040. Prompt engineers enable the optimal use of AIs. The nuanced understanding of how to construct the prompt or question to achieve the desired end state, receive a detailed answer or create the right work in the required form and style will drive demand for experts in this field. Despite some arguments that the need for prompt engineers will fade as AI develops, most industry insiders believe that regarding LLM-based generative AI, prompt engineering will remain an essential skill.

Discussion

Prompt engineering enables communication with AI by presenting the system with detailed prompts to produce the desired results in an acceptable format (see Figure 1).[M] It allows the user to interact with a sophisticated generative program without any expertise in code writing.[M] While communication skills are essential to being an effective prompt engineer, several models and techniques have emerged that are likely to shape this field.

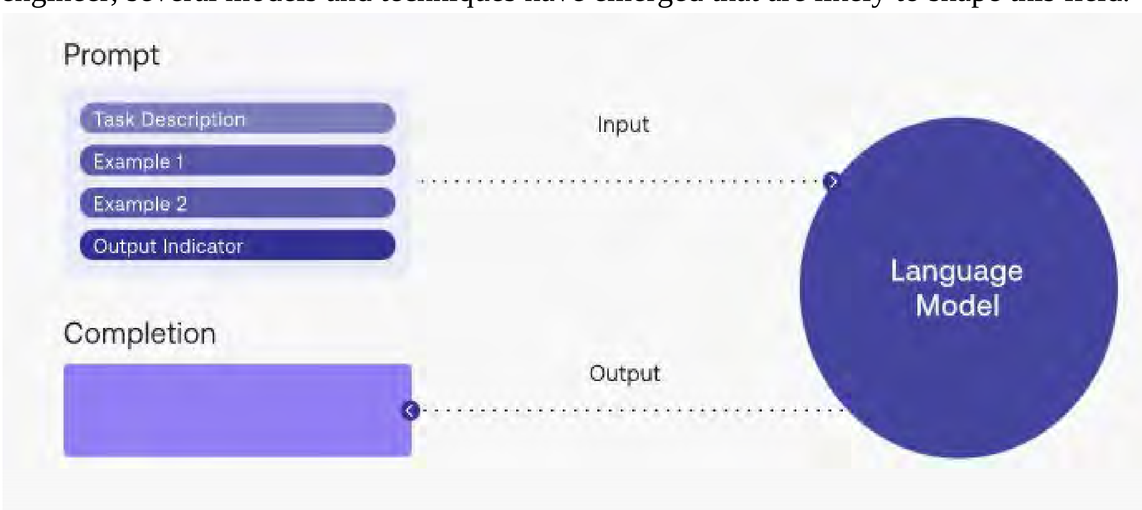


Figure 1: An example of a prompt using task description, examples and output requirements. Source: Cohere

Examples include the "Five Pillars of Prompting"[M], and the "Chain-of-Though Prompting" technique.[H] The "Five Pillars of Prompting" is a basic set of rules that prompt engineers can use to shape the focus of their questions. This includes providing examples for the AI, giving direction to the AI in the form of seed words, adjusting the parameters of the AI to limit the creativity or flexibility in its answer, establishing the format for the answer, and chaining multiple AI calls together.[M] Chain-of-Thought Prompting involves providing the AI a series of chaib-of-thought examples, so the AI understands how to answer the question.[H] Prompt engineering can also be used to train the AI to understand human language and recognize subtleties that convey more profound meaning.[M] These techniques train the AI for sentiment analysis, leading to improved analysis of available data (see Figure 2).[M]

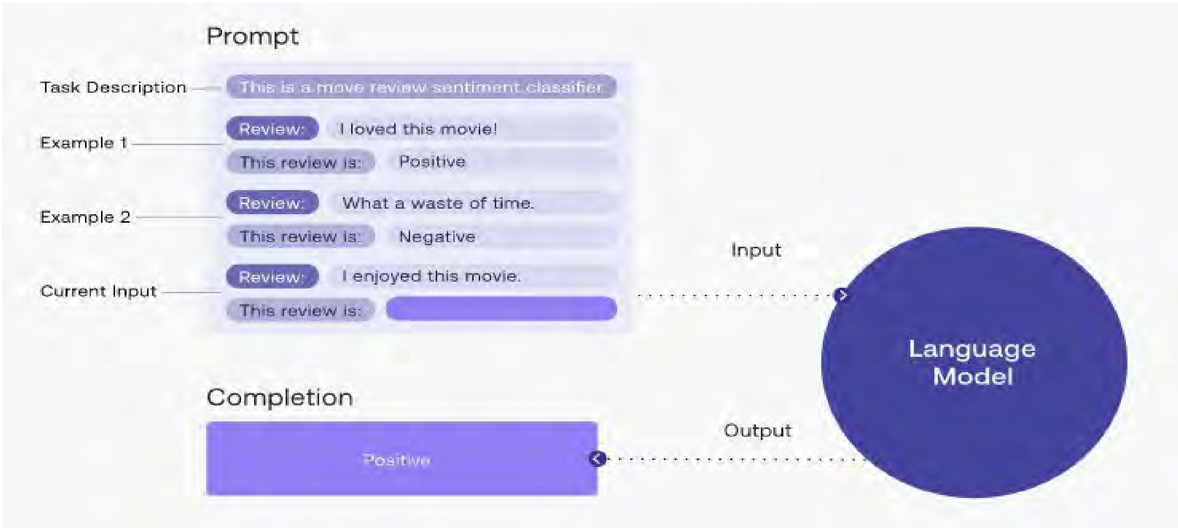


Figure 2: An example of a prompt training AI for sentiment analysis. Source: Cohere

One exciting example of prompt engineering lies in software development. For those already familiar with coding, AI becomes a valuable tool if one knows how to craft a viable prompt. With this skill, developers can streamline the development process, creating code faster with fewer errors.[M] According to industry analysts, prompt engineering will likely become a fundamental skill for programmers.[M] Working with an AI through prompts can also help train inexperienced software developers. They can interact with the AI, gaining an understanding of the code as they work on fine-tuning their prompts.[M]

The practical application goes beyond prompts for generative purposes. In decision support, prompt engineers will likely be responsible for establishing the parameters of the AI and how the AI will perceive and evaluate data.[M] In data analysis, prompt engineers can train the AI on sentiment analysis to further enable the AI to provide more relevant feedback.[M] Prompt engineers can also help reverse engineer malicious code to enable network defense.[M]

As more people become aware of the power of prompt engineering, it will likely expand into society. Already you can find massive online communities dedicated to developing better, more valuable prompts.[M] Entrepreneurs have begun to monetize basic prompt development, as can be found on promptbase.com.[H] Educators are seeing the value of this as well. At the University of Pennsylvania, professors have integrated prompt engineering into some curricula, evaluating students on how well they can train an AI to build a specific essay.[H]

Despite evidence presenting prompt engineering as an essential skill for HMT, several industry insiders argue that as AI models improve in their ability to understand language and intent, the need for prompt engineers will ebb.[M] Researchers are using techniques such as Reinforcement Learning from Human Feedback to increase the AI's human language ability, which allows users to achieve results without detailed input.[M] It is also argued that subject matter expertise in the output is required to capture the nuance necessary to construct an effective prompt.[M] Still, examples of unskilled coders using AI to generate effective code are becoming more commonplace.[M] It has even been used by untrained users to develop malicious software.[M]

With all the promise that comes with interaction with AI, prompt engineers must be aware of several factors and limitations associated with the systems. First, they must understand the data set that information is drawn from, as the AI inherently picks up any bias built into the data. Prompt engineers must be aware of and adjust their prompts to account for this.[M]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The sources tended to corroborate each other, although they varied in credibility. The time was adequate, but the analyst did not use a structured technique and worked alone. Additionally, the analyst is not a subject matter expert. Finally, this report is subject to change due to the potential for new developments and the protracted period.

Author: COL Dennis Weaver
dennis.weaver.mil@usarmywarcollege.edu

Human-Machine Teaming Ethical, Governance, and other Limiting Factors

SINGULARITY

HUMAN-MACHINE TEAMING

Bridging The Trust Gap is Highly Likely The Critical Factor To Advancements In Human-Machine Teaming Between Now and 2030

Executive Summary

It is highly likely (71-85%) that establishing a solid foundation of trust will be a key enabling factor for advancements in human-machine teaming (HMT) between now and 2030, due to the foundational role it plays in the successful development and interaction of teams across all organizations, as well as the necessity of trust with the public, private sector, and the international community. Despite the growing use of artificial intelligence (AI)-enabled devices and the seemingly automatic, injudicious level of trust that the general public places in those devices, there is still much work necessary to perfect the synergy of faith between humans and machines in order to achieve maximum effectiveness as a team and revolutionize the battlefield of the future.

Discussion

Both the North Atlantic Treaty Organization's (NATO) Science and Technology outlook for the 2020-2040 timeframe and the American Institute of Aeronautics and Astronautics (AIAA) project advancements in HMT to have a revolutionary impact in the field of autonomous systems by 2030.[H] [H] However, for HMT to reach its full potential as a force multiplier, humans must be able to trust in intelligent autonomy.[H] With that goal in mind, leaders across all industries, and specifically in the defense arena, are working along the same lines of effort for developing HMT systems that are reliable and trustworthy for operators.[M] Additionally, as the quest to lead the AI race becomes increasingly competitive, and industry leaders lean forward toward more autonomous systems, governance, legalities, and interoperability will continue to challenge the use of such systems.[H] (see International Law Report) Although there are many semi-autonomous systems providing great benefits to society,(see Society and Industry Report) some current semi-

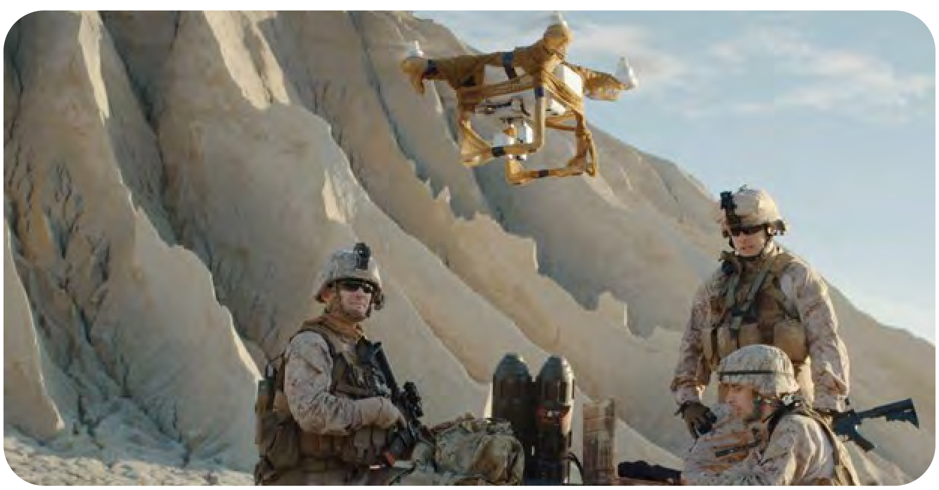


Figure 1: Defense Advanced Research Projects Agency's (DARPA) Envisions Future HMTs of Small-Unit Infantry Forces Using Small Unmanned Systems. Source: DARPA

autonomous technologies actually increase manpower needs and place an increased cognitive load on the operator.[H] The focus on HMT will be a critical bridging capability as the work toward intelligent autonomous systems proceeds.[H]

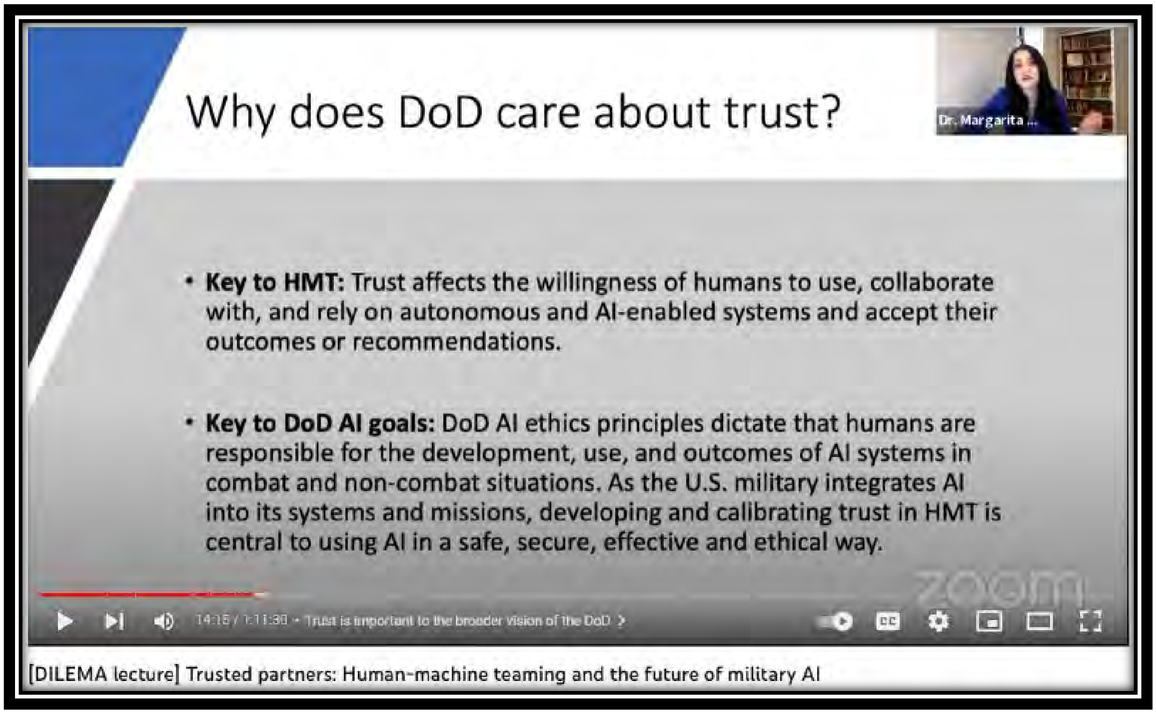


Figure 2: Researchers from Center for Security and Emerging Technology discuss the future HMT. They discuss the DoD focus on trust: 14:00-14:46. Reliability, Transparency and Explainability: 35:30-40:00. Click on picture or go to: https://www.youtube.com/watch?v=zdjrbsUe5SM&t=857s Source: T.M.C Asser Institute

There are several facets of trust which transcend all industries in the era of AI: trust in the technology itself and trust in the operator. Additionally, the defense enterprise is accountable for the trust of the American people as well as the trust of those allies, we rely on throughout the competition continuum. (see Regulations Report) Dr. Margarita Konaev, with the Center for Emerging Technology explains that "human-machine teaming is a relationship—one made up of at least three equally important elements: the human, the machine, and the interactions and interdependencies between them."[H] In order to develop HMT capabilities to their full potential, researchers are examining both sides of the relationship. This entails developing trustworthy AI as well as understanding the equally important, but less researched, human element of the relationship.[H]

The machine side of the team: Developers have prioritized technology-based solutions to foster trust in the system by making AI systems that are more transparent, explainable, auditable, and reliable. Such capabilities, as discussed below and in the linked video in Figure 2, contribute to trust as an essential part of creating effective HMTs.[H] [H]

- **Transparency** tops the list of reasons that operators/users name as contributing to a lack of trust in HMT scenarios.[M] [H] [M] When an AI system or machine makes decisions, people need to know why and how it arrives at its conclusions and recommendations. Although an increasing number of technological applications have started to provide references from text documents in their knowledge bases from which they drew their conclusions, deep learning does poorly in this regard.[H] Despite the current challenge, AI experts from IBM's human-agent collaboration team think that the level of transparency and trust will improve within the next five years, when an AI system can better explain the "why" behind the "what".[H]

- **Explainability** is the ability, or in this case inability, for the AI system to explain its reasoning to the decision maker or human operator; a quality perhaps even more important and more difficult to address.[H]

- **Auditable** data from current sources enables transparency and helps build trust in the technology.(see Data Availability Report) If the machine or AI system malfunctions or there are negative, unintended results, auditability can provide a track record of what happened and how to avoid a similar incident in the future.[H]

- **Reliability** may be even more critical and perhaps the most fundamental issue in building trustworthy AI systems for HMT. While transparency and explainability are important for calibrating, operators need to know whether the machine or AI system will function properly to accomplish the assigned tasks.[H]

The human side of the team: Thus far, a preponderance of the research has focused less on studying trust in HMT directly and more on the aforementioned technological system functions for AI itself in an attempt to build trust into the system.[H] While important, addressing system functions alone is not a sufficient method to calibrate the degree of trust in HMTs.[H] Enhancing the understanding of human trust dynamics in HMT is crucial to effectively using AI in military operational scenarios. Achieving this level of trust and cooperation requires consideration of the human factors in system design and implementation.[M]

Because it influences people's willingness to use and follow the advice of intelligent machines, trust is essential for efficient HMT.[H] But what is the "right" amount of trust? As with many of the questions surrounding this concept, the answer to how much trust is needed for effective HMT is: "It depends".[H] The more we view AI as a machine, the more accuracy we expect from it and the trust margin is narrow. However, the more human-like qualities that an AI system, possesses, the more we trust it, even when it's not

> Human-machine teaming is at the core of the Department of Defense's vision of future warfare, but successful collaboration between humans and intelligent machines—like the performance of great teams in business or sports—depends in large part on trust.
>
> Margarita Konaev and Husanjot Chahal

perfect.[H] Having too little trust in highly capable technology can lead to underutilization of AI systems, while too much trust in the supposed capabilities of a system can result in anything from accidents, fratricide, or unintentional harm to civilians.[H]

- **Trust gap** (too little trust): Researchers, academic and military professionals alike all identify a lack of trust as a critical challenge to human-machine teaming.[H] One of the more complex dilemmas for advancements in AI and HMT has is known as the "Black Box" effect. Essentially, as AI technology and deep learning models become more sophisticated and autonomous, the less users trust it.[M] [H] The "black box" effect impedes transparency, explainability, and predictability, as a result, human trust decreases as machine autonomy increases.[M]

- **Automation bias** (too much trust): People, in general tend to over-trust a machine's recommendations, but even more so in high-stress situations.[H] They might exhibit this bias by relying on the outputs of AI systems even when they do not seem to make sense. This tendency is intensified in systems in which the algorithmic processing is so complex that the outputs are unexplainable.[H] When extrapolated to combat conditions, consider an example of a target detection algorithm or battlefield assistant which indicates that a particular object or person is a threat. The warfighters are more likely to trust the AI recommendations given the cognitive stress, lack of adequate training, necessary reaction time, and overreliance on the AI system's purpose in reducing the fog of war.[M]

Trust and the American public: The widespread use of AI has organizations large and small examining their policies. The Pentagon recognizes the importance of trust as an intangible requirement and responsibility to the American public (see Regulation Report)

as it continues AI advancement. It is a foundational concept in the 2022 Responsible AI (RAI) Pathway policy, which states that the desired end state for the RAI is trust.[H] Establishing trust in the DoD's use of AI will enable the joint force to continue to modernize its warfighting capabilities across the spectrum of combat and non-combat operations.[H] Without that trust, our warfighters will not employ AI effectively or accurately, leading to negative impacts on the nexus of future HMT advancements and diminishing the trust of the American public. Gaining and maintaining the trust of all stakeholders cannot rely solely on technological advancements but must include factors such as a reliable governance (see International Law Report) structure and policies for the ethical use (see Ethics Report) of such technology across the department.[H]

Trust of our Allies: The same factors which lead to and build trust in the HMT are also highly relevant and must be considered when thinking about the future of multinational alliances. For instance, trust concerns could compromise coalition-wide coordination, interoperability, and overall effectiveness if some U.S. allies feel less at ease employing AI-enabled military systems.[H]

Despite the growing popularity of AI and AI-enabled as a part of daily life for a great part of international society, there are still trust concerns which pose challenges for human-machine teaming efforts across multiple industries. Even though these devices provide convenience and efficiency, research shows that a large percentage of people still do not trust machines to make important decisions.[M] This trust gap must be addressed if we want to fully realize the potential of human-machine teaming efforts in the future.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were very reliable and corroborated one another on a myriad of concepts. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the time frame of the estimate and the rapidly evolving nature of AI, robotics and machine learning models, this report is sensitive to change due to new information.

Author: LTC Nicole A. Washington
nicole.washington.mil@armywarcollege.edu

Beneficial Impacts Of Artificial Intelligence On Global Social Challenges Between 2023-2030 Almost Certain To Overshadow Fears Of Work Force Replacement And Over-Reliance

Executive Summary

Though still considered an emerging technology, the cost-benefit analysis of artificial intelligence (AI) is almost certain (86-99%) to overshadow the fears of late adopters and skeptics due to the emerging potential benefits for education, healthcare, and social conditions such as climate change and food insecurity. The diverse array of AI systems and applications has quickly become a part of daily life for those who are early adopters and the technical elite. Despite concerns from industry experts about the potential dangers of over-reliance on AI as well as societal fears that AI-enabled systems will soon replace people in the workplace, it is almost certain that advances in AI will continue, unhindered at an exponential scale.

Discussion

Artificial intelligence is changing how people will live and work in the future in practically every industry.[H] With tools like Chat Generative Pre-Trained Transformer (ChatGPT) and AI art generators gaining widespread attention, it is already the driving force behind new technologies like big data, robotics, the internet of things (IoT), and emerging generative AI applications.[H] It will continue to play this role as a technological innovator for the foreseeable future.[H] While there will be many hurdles and challenges to overcome as the technology rolls out into new applications, AI will almost certainly have a more positive than negative impact on technical and social challenges facing our society.[H] Some of those positive impacts are in the areas of education healthcare, climate change, and systems which will address food scarcity. Nearly every significant business has already been impacted by modern AI, more precisely "narrow AI," which carries out objective tasks using data-trained models and frequently falls under the categories of deep learning or machine learning.[H] As of March 2023, 37% of companies across all industries are working to make significant investments in AI.[H] Unless you choose to live remotely and never plan to interact with the modern world, your life has been and will continue to be significantly impacted by artificial intelligence. In

> **"What all of us have to do is to make sure we are using AI in a way that is for the benefit of humanity, not to the detriment of humanity"**
>
> **-Tim Cook, Apple CEO**

2022, AI became what is considered, the most revolutionary technology ever created by man.[M] According to Google CEO Sundar Pichai, AI's impact on our evolution as a species will be comparable to fire and electricity;[M] and thus the criticism of skeptics will likely (56-70%) not be able to stop the momentum or its entanglement in society.

Education: AI in education will continue to evolve and change the way that humans of all ages learn (see Educational AI Report) AI's use of machine learning (ML), natural language processing, and new facial recognition applications are help digitize textbooks, detect plagiarism, and gauge the emotions of students to help determine if they are bored or struggling to understand learning concepts.[H] AI-powered tools like Cognii can help students develop their language and communication skills in real-time,[H] and Knewton is an adaptive learning platform that can personalize content for each student based on their individual needs.[H] The global market for AI in education is experiencing significant growth and is expected to have an annual growth rate of 36% between now and 2025.[H]

Healthcare: Another emerging positive impact of AI in society is in the field of healthcare where implementation efforts are expected to take effect everywhere from initial medical school training to implementation in the hospital and operating room (See Figure 1). Johns Hopkins School of Nursing implemented augmented and virtual reality training at all levels of skill for some of the most significant procedures.[H] Scientists, medical researchers, clinicians, mathematicians, and engineers, when working together, are designing AI systems aimed at medical diagnosis and treatments, thus offering reliable and safe systems of healthcare delivery. There are promising data sets for AI and ML applications that can help diagnose cancer and predict optimal treatment outcomes.[H] Advancements in AI are beginning to deliver breakthroughs in breast cancer screening by detecting the signs that doctors miss.[H] In addition to helping with analysis, robotic systems may also be created to do some sensitive medical procedures with accuracy as health professors and medical researchers work to discover new and effective ways to

Figure 1: Moxi, A Healthcare Cobot making rounds at Jacksonville Hospital. Source: Marketplace

treat ailments.[H] AI-based surgical procedures are currently available in a select few hospitals. The da Vinci surgical system still needs to be operated by a health professional but can complete an operation with a greater degree of precision and greater accuracy than one done manually; causing less trauma to the patient.[H]

Climate Change: On a much grander scale, there is an array of AI applications which, if collectively managed and resourced, have the potential to help researchers address climate change. AI as a tool is uniquely positioned to help manage some of the complex efforts to mitigate climate change (from immediate crisis response to long-term planning), due to its capacity to gather, complete, and interpret large, complex datasets on emissions, climate impact, and more.[M] Specifically, industry experts from Boston Consulting Group (BCG) reported that AI could be used to help reduce greenhouse gas emissions equal to 5% to 10% of an organization's carbon footprint, or a total 2.6 to 5.3 gigatons of CO_2e if scaled globally.[M] Aside from conducting research and data collection, companies around the globe are actively using AI to address climate change through green cooling technologies, preventing plastic pollution, and improving energy efficiency just to name a few.[H] AI has the ability to positively impact our ability to address climate change by improving our understanding of the issue and developing more effective solutions.

Food Insecurity: Among one of the top socially beneficial emerging AI applications is the ability to positively provide solutions for some drivers of food insecurity. According to the United Nations, we will need to increase the world's food production by 70% to feed the world's population by 2050.[H] The compounding effects of an already fragile ecosystem, worsening climate change and geopolitical instability make traditional methods for food production ineffective in meeting such a compact timeframe. Bernard Marr, a futurist in the field of business and technology, suggests that AI can help create the perfect crop and maximize production to help address food

Figure 2: Smart farming agricultural technology and smart arm robots harvesting hydroponics vegetables. Source: Global Era Issues

insecurity (See Figure 2).[H] Marr highlights AI technology such as FarmView can help researchers figure out the right genetic makeup to create seeds that generate the highest yield, the most nutrition and the most disease resistant strains of staple crops.[H] Smart farming agriculture uses AI to address climate change and food production by using it to manage irrigation processes and develop planting and fertilizing operations, leading to more productive harvests.[H] Food waste is a major contributor to the food shortage crisis and companies like Torma Sorting Solutions, uses AI predictive machine analysis to machine analyses and can separate food into "good" and "bad, evaluate it and determine the best way to use it.[H]

By 2025, machines could displace about 85 million jobs, but create 97 million new roles.

Despite the altruistic applications listed above, there are still valid and significant concerns about how AI and our global society will work together for the common good. One of the primal fears is that continued advancements will eliminate the need for people in the workplace (among both blue collar workers and corporate professionals). As recently as March 2023, Fortune magazine reported that nearly 69% of people with graduate degrees expressed their fear of losing their jobs to AI.[M] Fueling the self-preservation fear is that there is some truth to it. Like many revolutionary technologies before it, AI is likely to both eliminate jobs but also spur the creation of new career fields, in addition to enhancing many existing jobs, according to Juliet Schor, an economist from Boston College.[H] [M] The second, but no less important concern is a growing fear that over-reliance on AI can lead to serious consequences including lack of human judgment, bias, and lack of transparency.[M] Developing and enforcing policies and regulations, locally and internationally, is the best method to mitigate and avoid these potential negative consequences.[M] (see International Law Report)

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable, and the majority of all sources tended to corroborate one another. There was not adequate time to conduct interviews for subject matter experts in person and the analyst worked alone. Furthermore, given the lengthy time frame of this estimate and the innovative speed for artificial intelligence developments, this report is sensitive to change due to new information.

Author: LTC Nicole A. Washington
nicole.washington.mil@armywarcollege.edu

International Governance Laws For Artificial Intelligence Highly Likely To Remain Individualized By Country Beyond 2040

Executive Summary

It is highly likely (71-85%) that there will continue to be country-specific governance rules for artificial intelligence (AI) versus one international standard beyond 2040 due to the pace of emerging technologies around the globe, and the diversity of government preferences for horizontal, vertical, or hybrid approaches. As AI technology continues to develop and pervade various sectors of society, the need for regulation is becoming increasingly important. However, regulating AI is not a one-size-fits-all solution based on culture, customs, infrastructure capabilities, and the system of government. The types of technologies and their applications are just as different as the countries and ecosystems in which they operate. Despite calls from some in the international community to develop one universal set of norms for governing AI, countries continue to implement varied approaches to meet their own needs while trying to stay ahead of this emerging technology.

Discussion

AI traces its developmental roots back to Alan Turing in 1935,[H] and it boomed in the 1980s,[M] however, regulation and governance lagged behind. Now, as AI systems and applications become a part of life and work in nearly every industry and country, governments are doubling efforts to catch up to the pace of growth and drive policy. There are currently over 27 different international policies that address AI governance;[H] ten specifically address AI regulation and risks to human freedom and autonomy, and each policy is as different as the countries that developed it (Japan, European Union (EU), India, China, United Kingdom (UK), Serbia, and the U.S.).[H] Across the globe, as policy makers consider serious legislative options for AI

Figure 1: Mr. DragosTudorache, Member of the European Parliament and Co-Rapporteur of the EU AI Act discusses the horizontal strategy. Click on the image or go to: https://www.youtube.com/watch?v=BBmq4T_550U to view the video. Source: CSIS

governance, the resulting policy frameworks fall into one of three categories: horizontal, vertical, or hybrid.[M]

Figure 2: EU pending AI Act will have transregional economic impacts. Source: FINTECH

Technology researchers from the Carnegie Endowment for International Peace explain how in a horizontal approach, regulators create one comprehensive regulation that covers the many impacts AI can have.[H] The EU and the UK have developed different policies, but both fall primarily into this category.[M] The EU's AI Act identifies four risks groups: unacceptable, high, limited, and minimal risk, and applies the same set of governance requirements to every application in each group.[H] This AI act is projected to have extraterritorial scope and implications for various organizations globally.[H] Given the extent of the AI Act and the financial implications associated with noncompliance, businesses must get ready for these upcoming regulatory changes as quickly as possible now.[H] The first draft of the UK National AI policy is horizontal in its current state, but recent changes suggest it is breaking away from EU model and moving to a hybrid approach with the goal to "provide the most pro-innovation regulatory environment in the world."[M]

In contrast to the horizontal strategy above, in a vertical strategy, policymakers take a customized approach, creating different regulations to target different applications or types of AI.[H] Due to the customization and increased individualized industry requirements, very few of the government policies implemented to date fall into this category. Surprisingly, China's approach is the front-runner as a case study for a fundamentally vertical approach: picking specific algorithm applications and writing regulations that address their deployment in specific contexts.[H] Instead of an "across the board" approach, China governs AI under two separate regulations based on content, input, output, and positive or harmful information.[H]

A hybrid approach includes overarching regulations for all industries and sectors, but also specific regulations for certain use cases of AI could be the most effective method for incorporating both horizontal and vertical elements.[H] The current U.S. strategy for AI is the best example of a hybrid approach. Given the current strategic and economic environment, leaders in Washington recognized the need for separate regulatory guidance for the commercial space and the defense enterprise. Commercially, the U.S. directed the Federal Trade Commission (FTC) to mandate impact assessments of AI systems across all commercial sectors (subject to the size and reach of the enterprise).[M] Separately, the U.S. proposed its new "Political Declaration on the Responsible Military Use of Artificial Intelligence and Autonomy" on February 16, 2023, at the Summit on Responsible AI in the Military Domain (REAIM 2023).[H] This policy is the U.S.'s attempt to develop a set of international norms for the battlefield use of AI across the military and members of the defense industrial base, and it hopes to gain support for the initiative from its allies.[M]

The opposing side of the multi-nation disparate approach argues for a global consensus for AI governance. The loudest voices supporting convergence to a global standard, at least for the civilian commercial sector, come from the EU. Their concerns are based on the risk that standards will be developed elsewhere in the future, often by non-democratic actors, so the EU should take the lead to act as a global standard-setter in AI.[M] While it is highly likely that countries with nefarious motives will develop regulatory guidance that does not align with international norms, the data shows that a mix of horizontal and vertical approaches will likely (56-70%) be the standard in the commercial space. The EU's landmark AI Act has been contested in several proposals and has yet to be presented to Parliament.[M] International norms are easily implemented for more normalized, established industries; however, for a rapidly advancing, multi-use technology such as AI, countries must shape a national ecosystem that aligns with their strategic priorities and strengths and weaknesses.[M]

Figure 3: Diplomatic Relations. Source: Harvard Law School

The closest effort to a global norm was initiated by the United Nations Educational, Scientific and Cultural Organization (UNESCO) in 2021 when it successfully had all 193 members adopt an ethics agreement.[H] That agreement set a foundation for common values and principles as a starting point to guide the construction of the necessary legal infrastructure to ensure the ethical development of this technology.[H] While it does set the foundation for a global normative framework, it is not legally binding, there is no governing body and it delegates the responsibility of governance and implementation to the individual members.[H]

Analytic Confidence

The analytic confidence for this estimate is *moderate* based on the credibility and corroboration of the sources. The time was adequate, but the analyst did not use a structured technique due to the international focus of the topic. Additionally, the analyst is not a subject matter expert and worked alone. Finally, this report is subject to change due to the potential for new developments and changes in the governing parties within the international community that set policy.

Author: LTC Nicole A. Washington
nicole.washington.mil@armywarcollege.edu

Concerns For Ethics And Biases Indicate That Humans Highly Likely Remain "In The Loop" Of Artificial Intelligence Systems Through 2030

Executive Summary

It is highly likely (71-85%) that humans will remain in the loop for artificial intelligence (AI) systems between now and 2030 due to American society's lack of trust in fully autonomous systems, based on ethical standards, potential biases, and doubts about the ability to govern autonomous AI systems. Despite the argument that some fully autonomous systems are currently in use and not subjected to such scrutiny, the consensus is that Americans are likely (56-70%) more concerned than excited about the increased use of AI.

Discussion

The unprecedented success of generative AI platforms, such as Chat Generative Pre-trained Transformer (GPT3),[H] has brought the topic of AI to the forefront of conversations across the entire technology enterprise. Regardless of the popularity of digital assistants and Open AI technology, concerns about ethical standards, program biases, and AI governance still limit American society's acceptance of the current use of AI systems and its view on the future development of autonomous systems.[H] Trusted AI and autonomy is one priority area for Research and Engineering (R&E) for the U.S. Department of Defense (DoD) in its quest to find ways to operate in contested areas in the future.[H] The Honorable Heidi Shyu, U.S. Under Secretary of Defense for R&E suggested that the effective transition of increased autonomy depends

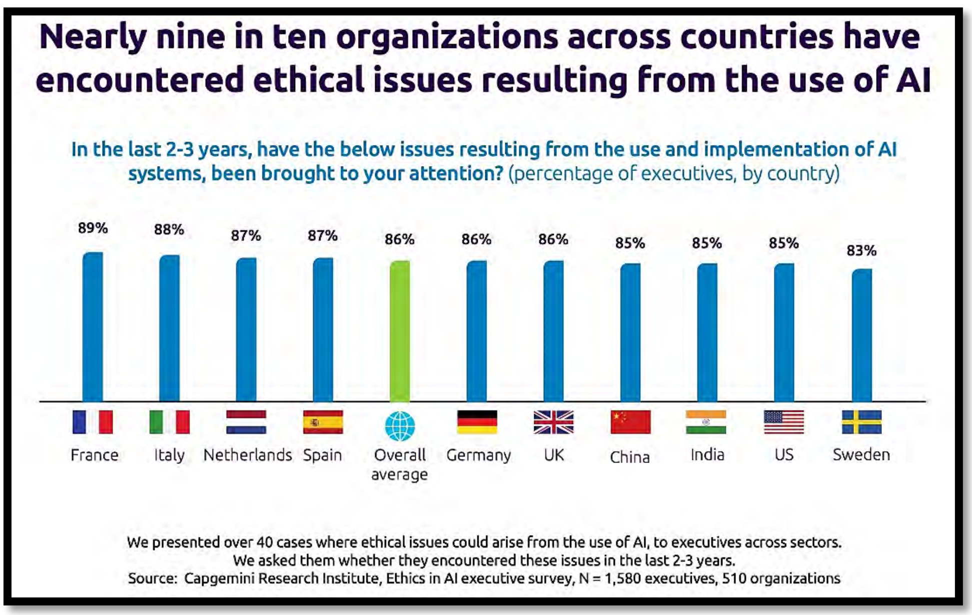


Figure 1: Ethical Concerns over AI permeate around the Globe. Source: World Economic Forum

on how confidently humans will trust those systems to have appropriate cybersecurity and perform within ethical boundaries.[H]

Leaders in the Information Technology sector report one of the top concerns regarding the future development and use of AI is the concern about various forms of programming biases and lack of ethical decision-making capabilities.[H] Societal trepidation regarding autonomous AI may not be a lack of ethics, but rather whose ethics and biases are inherent in the system. Chris Nicholson, co-founder and CEO of Skymind, an AI ecosystem builder, says that "algorithms are only as good as the data they are trained on.[H] So if a dataset includes historical biases or is ethically questionable, its predictions reflect

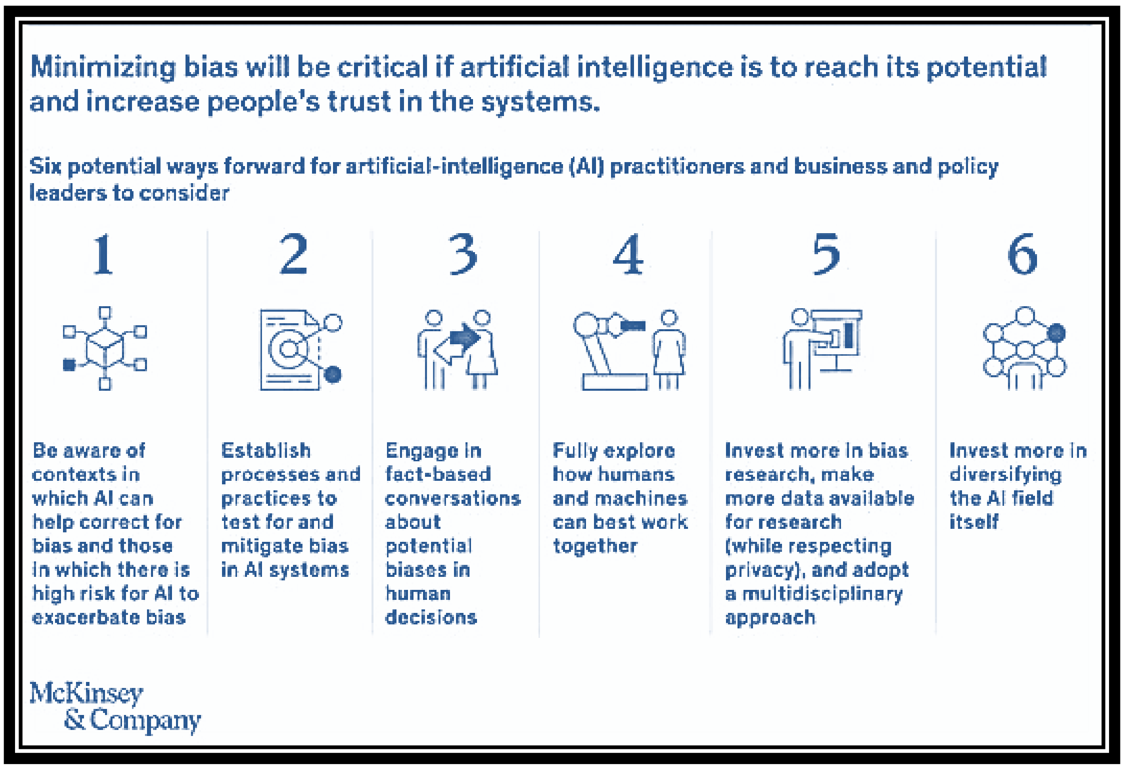


Figure 2: Methods for Industry Leaders to minimize bias in artificial intelligence systems. Source: McKinsey & Company

that historical behavior."[H] An additional contributing factor is that as AI-powered technology becomes more common and the costs to enter the market decline, it is likely that more systems will be released with fewer ethical safeguards.[M] Experts from McKinsey & Company recognize both the potential promise and current hesitation for AI in business and they are working to develop solutions to minimize system biases. They recommend six overarching processes (see Figure 2) to help industry leaders guide their organizations into the AI space.[M] For AI to reach its full potential, it is critical to make every effort to minimize bias; minimizing bias enables trust.[M]

Another concern pervasive in the research is the inability to provide governance or management protocols for autonomous systems. A panel of experts from Pew Research posits that "AI is too distributed a technology to be effectively governed and too accessible to any individual, company or organization with reasonably modest resources."[M] In the 2019 AI governance survey, "82% of Americans (more than eight in 10) agree that AI and/or robots should be carefully managed, while only 6% disagreed."[H] Another significant outcome from that same survey is the disparity in trusted agents. Americans polled place the most significant trust in university researchers and the U.S. military to ***develop*** AI but place more trust in technology companies and non-governmental organizations, not the government, to ***manage*** the use of that technology.[H] As the defense enterprise and non-military industry works to make advances in AI, they should focus on building trust by building trust in the systems themselves through transparency, explainability, and reliability.[H]

The other side of this complex issue is the argument that some autonomous systems already exist, namely weapons on the battlefield that can operate without any human in the loop once activated.[M] There are, indeed, drones, surface-to-air missiles and other types of munitions utilized on the global stage in the past year; none of which are prohibited nor subject to ethical debates. However, the ironic caveat of this particular argument is that there is no accountability gap with these systems because human commanders, operators, or programmers make human decisions, thereby assuming accountability.[M] This equates to a human-in-the-loop scenario. Additionally, there are studies which show that under certain conditions and for certain decisions, humans behaviorally trust the AI more than another human by accepting their AI teammate's decisions more often,[H] if they have personal experience in the task already.

Paul Neilson, from Carnegie Mellon's Software Engineering Institute, professes that "trust is not only a significant challenge to building autonomous systems, but it is also the greatest barrier to their adoption."[H] Industry will have to bridge the trust gap to continue to progress from current AI systems to future systems with increased autonomy. Some of the bridging options that are ready for immediate implementation range from building standard ethical frameworks to bias detection and mitigation protocols, and methods for effective governance. Industry experts align in their recommendation for a place to start; human involvement and oversight.[H] As stated by AI scientist and Label Your Data Editor, Iryna Sydorenko, "Whether natural language programming or computer vision, a case of classifying the images, or building a model for autonomous driving, humans are to stay in the loop in the foreseeable future."[H] Human-in-the-loop decision-making techniques will contribute to our ability to fully explore how human-machine teams work, leading to greater transparency and increased trust.[M]

Analytic Confidence

The analytic confidence for this estimate is *moderate* based on the credibility and corroboration of sources. The time was adequate, but the analyst did not use a structured technique. Additionally, the analyst is not a subject matter expert and worked alone. Finally, this report is subject to change due to the potential for new developments and the protracted period.

Author: LTC Nicole A. Washington
nicole.washington.mil@armywarcollege.edu

Data Quality Likely The Limitation To Employ Fully Integrated Artificial Intelligence Applications Across The Continuum By 2040

Executive Summary

It is likely (56 -70%) that the relevant data to train and properly test military artificial intelligence (AI) applications will be the limitation to employing fully integrated decision-support AI applications across the continuum by 2040. Due to the current lack of data standards, military data scientists, and the volatile, uncertain, complex, and ambiguous nature of military operational environments, the ability to collect, properly prepare and apply relevant data to feed AI decision-making systems will likely take longer than the commercially available adoption of AI applications.

Discussion

Preparing quality training data is one of the most critical parts of creating an AI solution.[M] Understanding the data needs in support of the solution, must occur right after a requirement is identified for translation into an AI application.[M] As depicted in Figure 1, data preparation requires combining various data sets into one large analytical record prior to data mining, data cleansing, feature selection, and model optimization all before AI training can begin.[M] There are three factors to take into consideration when selecting good machine learning (ML) training data: data quantity, quality, and variability.[H] All three considerations must be taken into account; each one requires both human and machine training in order to be beneficial.

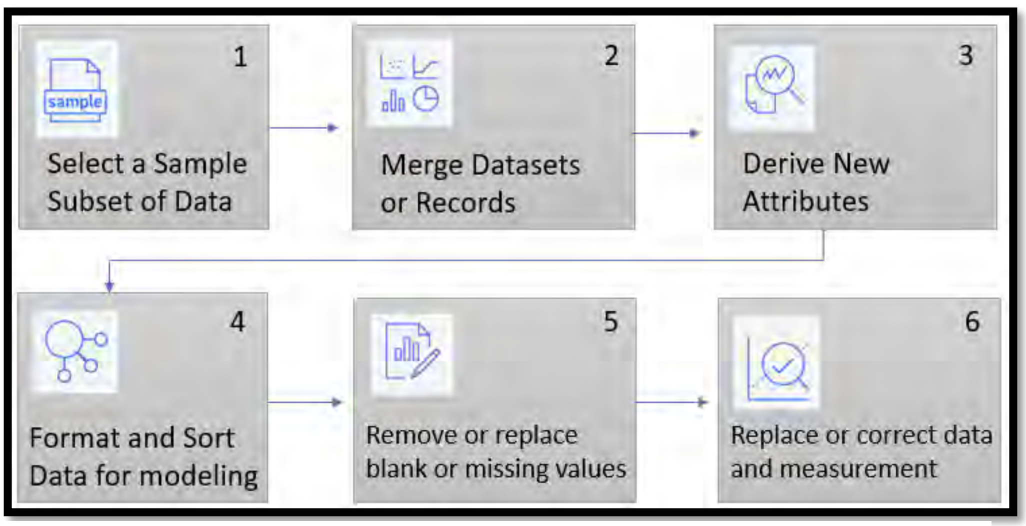


Figure 1: Diagram on how to prepare training data for Machine Learning Algorithms Source: IBM

Data Quantity:

ML is the engine behind the AI application's ability to learn without specific programming, mostly using an iterative experiential method to modeling data called training to improve or execute a set of tasks.[H] AI Training starts with a dataset that is applied to rulesets, once exercised, the results are then added to the dataset. This constant training causes the data size to grow exponentially which is why machine learning training is computationally intensive.[M] The data models are also tweaked and filtered by a humans to assist in accuracy, but the more iterations, the more accurate the application.[H] When filtered and trained to be as accurate as possible, military data collected across all war fighting functions across the continuum will produce massive application sizes. [H]

By 2025, International Data Corporation (IDC) predicts that worldwide data will grow 61% to 175 zettabytes and that 75% of the world's population will interact with data daily.[M] The size of data has an impact on AI performance and possibly the accuracy.[H] The more vast the dataset with clean data the better accuracy, but large data sets often introduce cleanliness issues and timing issues dealing with each and every node.[H] The best example of this is Generative Pre-trained Transformer (chat-GPT3) with over 45 terabytes of data and 175B parameters, but had to be trained across 100s of GPUs and for many months.[M] ChatGPT and other large language models (LLM), today are trained daily by their public users and teams setting the parameters.[M] For obvious security reasons, some LLMs have been trained to prevent military responses.[H] In order for a military to use this type of technology, it would need to have data available for training and have a proportionally set number of users and parameters to make the LLM as effective. There is no military in the world that can train it's own LLM with the amount inputs and parameters that has been applied to ChatGPT.[M] The most common way to define whether a data set is sufficient is to apply a ten times rule.[M] This rule means that the amount of input data (i.e., the number of examples) should be ten times more than the number of degrees of freedom a model has.[M] Degrees of freedom for machine learning means the number of values in the final calculation of a statistic that are free to vary within your data set.[M] Extrapolating out this example means ChatGPT3 would need 1.75 Trillion parameter data set for additional training.

Similarly to the exponential growth in the commercial space, military "digital universe" was above 40 billion terabytes in 2020, from below 500 million terabytes in 2005.[H] This means that without further advancements in formatting and sorting training data sets, the Army could cause overfitting the ML algorithms. Overfitting is when the algorithm memorizes the dataset only and not how to process data, causing it to negatively perform on new data sets.[M] There are a number of techniques, such as holding out data or cross-validating the array, to prevent overfitting, but they require time to test and validate data.[M] The other issue with data sizing and overfitting for Army capability, is it introduces vulnerabilities for the adversary to either overload systems with massive amounts of data.[H] These challenges could be overcome, but require additional time.

Data Quality: With the boom in AI algorithms fueled by the release of LLMs, now more than ever creative computer learning algorithm development is increasing exponentially.[H] Although there are hybrid models as depicted in Figure 2, all of these models are

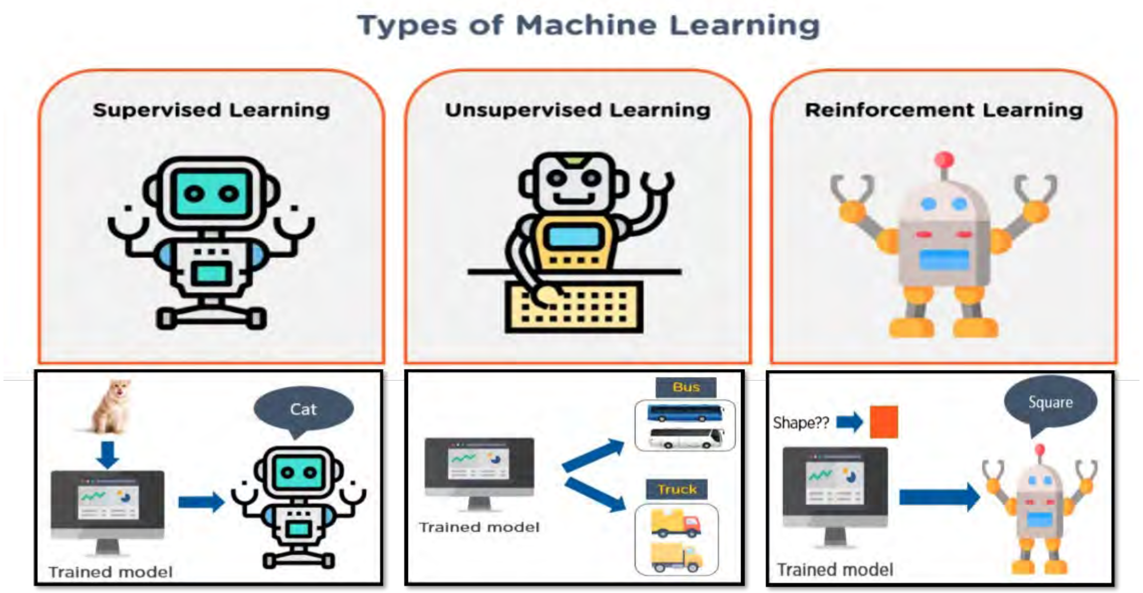


Figure 2: Depiction of Types of Machine Learning. Source: Simple Learn

categorized in one of three main categories: Supervised, unsupervised, or reinforcement learning.[H] Supervised ML has the data labeled with the known outcome; unsupervised ML uses unlabeled data to train the machine and reinforcement ML uses an agent to produce actions and get rewards after processing data.[H] Within each category there are a number of different algorithms that are used across commercial ML applications. Finding the right ML algorithm requires a cross functional team that may span across many disciplines. The following are the four rules to determine the right ML for an application[H]:

1. Know the data – this requires expertise in not only the functional area for the characteristics and behavior of the data, but also the data engineering to understand the size and data types for labeling
2. Data Accuracy – is the data correct, and how hard is it to predict new data that comes in
3. Speed – is the data needed fast to complete the mission or is more time allowed to get a more precise answer
4. Features and Parameters – how often and how the data needs to be manipulated or answered, what kind of response is expected from the ML

Understanding these rules and who understands the data required is key to picking the right team members to develop the most critical part of an AI application, the ML algorithm category and develop the training data.[M]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The analyst used multiple artificial intelligence sources for research which included ChatGPT, You.com's chatbot, and Unrestricted Intelligence. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: Mr. Reginald Shuford
reginald.shuford.civ@armywarcollege.edu

Additional Key Findings

Civilian Investment And Research Likely To Drive Innovation And Increasingly Influence Development of Military Systems

Executive summary

Due to limited budget flexibility, government technology investments will likely (56-70%) shift to adapting consumer-driven technological development for military purposes to maintain a technological edge over adversaries. Private sector investment in technology research and development has outpaced that of the federal government and academic institutions combined since the early 2000s. The gap between the two grows wider each year. This trend in private sector investment will likely continue to increase, widening the gap with government funding through 2040. The U.S. defense budget will likely remain flat relative to inflation, limiting potential research and development (R&D) investment increases. Requirements for smaller, lighter, and more capable commercial systems will fuel continued growth in private investment. Despite greater overall investment in R&D, the U.S. government investment is needed to ensure systems are developed ethically and identify potential dual-use technology.

Discussion

Investment trends show that government funding of R&D dropped 10% between 2010 and 2019, to represent 21% of the U.S. total for R&D (see Figure 1).[H] While the FY22 DoD budget reached a high point for research, development, testing, and evaluation (RDTE) with $123 Billion, with only $34 Billion dedicated to innovation.[H]

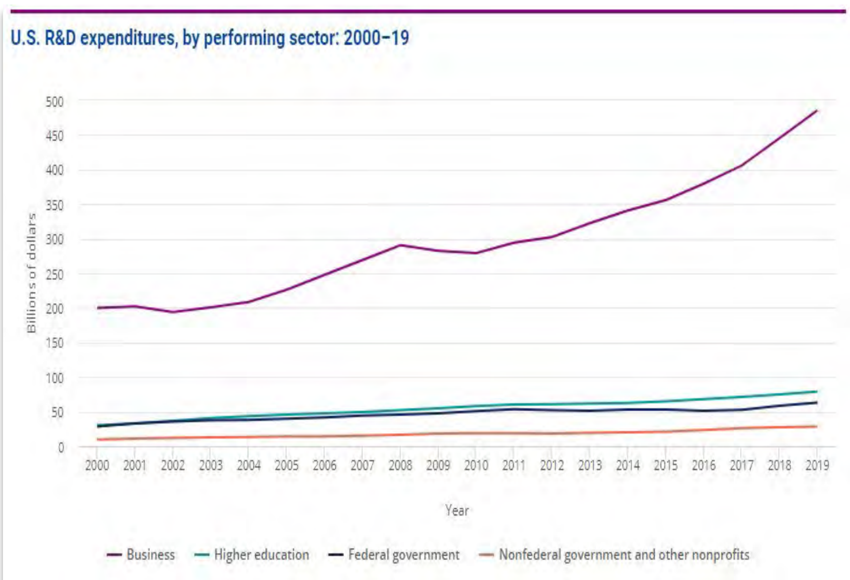


Figure 1: R&D expenditures by sector. Source: National Science Foundation

Overall, the U.S. government still leads in the world in investments in basic research and academic funding.[H] This level of investment will likely force the U.S. government to choose which technology development to support. The result of this will likely be the private sector, consumer, and business, driving the direction of R&D.[H] Several R&D

areas will likely influence the private and government sectors to include edge AI and extended reality (XR).[M] [H]

Rapid edge computing and AI advancement have fueled internet-of-things (IoT) developments. (see Edge AI Report) Neuromorphic computing architectures will increase device processing and storage while decreasing power consumption and physical size.[M] (see Neuromorphic Computing Report) Enabling technologies will also contribute to consumer availability and demand. More portable and wearable devices will continue to drive R&D in batteries. (see Battery Power Report) 6G networks will further enhance edge networks and devices. (see 6G Report) Edge networks allow IoT devices to communicate on a local network, communicating to the cloud only when required. This will allow future internet of military things (IoMT) to operate with little degradation to capabilities while operating in remote areas or in a degraded or contested electromagnetic spectrum environment.[M]

With the integration of advancements in supporting technologies, wearables will become lighter, contain more processing power, have longer battery life, and house AI inference engines.[M] Commercially practical glasses and goggles will enable the use of XR technology for commercial and business applications.[M] AI integration with enhanced digital assistants will drive consumer demand for systems, which will likely increase investment. The consumer market for XR products is projected to grow annually by over 40%(see Figure 2).[M]

Figure 2: AR/VR Market. Source: Grandview Research

The Army's Integrated Visual Augmentation System (IVAS) is an example of a commercial product that is being adapted for military use. The IVAS incorporates Microsoft's HoloLens technology to provide soldiers with an augmented reality heads-up display.[H] When integrated into training, XR will not only lead to long term reduced cost, but also allow for more and new types of data to be collected on the training audience.[M]

Continued generative AI developments will likely change how humans' team with AI. Conversational digital assistants will require nuanced prompt engineering to evoke the desired output. (see Engineering Skills Report) The widespread use of conversational digital assistants will likely increase trust in AI. (see Digital Assistants Report) Research has shown that public trust in those systems grows as the commercial sector adopts new technology, even if people answer otherwise when surveyed. Research shows that when new technology isn't fully understood, people tend to trust it too much, creating liabilities.[M]

Adversary investment in dual-use technology such as AI is threatening U.S. military advantages. (see China AI Development Report). Chinese investment, both government and commercial, have increased steadily over the past 20 years, and are now comparable to U.S. investments.[M] On top of increased investment, the Chinese Communist Party (CCP) also engages in intellectual property theft, including requiring overseas students to report on their research activities.[H] The CCP uses the Military-Civil Fusion (MCF) strategy to streamline the development between commercial and military, to enhance benefits to both sectors.[H]

Despite the increased level of private investment in R&D, those investments tend to focus on technology that projects to create the largest return on that investment rather than focusing on technology that will benefit society or improve military capability.[H] Public/government funding is required to ensure that consumer and business markets don't completely drive investment in R&D.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The sources were generally credible and tended to corroborate each other. The time was adequate, but the analyst did not use a structured technique and worked alone. Additionally, the analyst is not a subject matter expert. Finally, this report is subject to change due to the potential for new developments and the protracted period.

Author: COL Dennis Weaver
dennis.weaver.mil@usarmywarcollege.edu

By 2040, Human-Machine Teaming Likely To Revolutionize Battlefield Operations By Enabling Military Personnel To Execute Complex Tasks With Greater Efficiency And Accuracy

Executive Summary

Due to advances in artificial intelligence (AI), machine learning (ML), unmanned systems, robots, and additional capabilities to supplement human capability, human-machine teaming (HMT) is likely (56-70%) to revolutionize battlefield operations by 2040, enabling military personnel to execute complex tasks with greater efficiency and accuracy – particularly in the areas of Command and Control, the employment of Fires, and anti-access/area denial (A2AD). Despite unfamiliarity with current technologies on a broad scale and a lack of training and trust in the systems and platforms, HMT is a critical aspect of the Department of Defense's (DoD) vision of future warfare. As a result, the focus is shifting toward a more technology-reliant Military.

Discussion

HMT is considered the future of military operations across the land domain.[H] The concept is increasingly gaining attention from military experts, as it combines human cognitive abilities with the precision and speed of machine automation.[H] The successful collaboration between humans and intelligent machines depends largely on trust.[H] Trust is a complex and multilayered concept. Still, in the context of HMT, it speaks to an individual's confidence in the reliability of the technology.[H] Trust will always be a challenge because of new and emerging technologies, and, over the next two decades, emerging technologies will make way for the creation of new human-machine partnerships that adapt to the expanding capabilities of human-machine teams.[H] However, the more users train with and utilize new and emerging technology, the greater their understanding, acceptance, and knowledge, thus establishing a greater level of trust and confidence (see Figure 1).[H]

Figure 1: The U.S. military is integrating AI by using the technology aboard the U-2 spy plane, and in December flew the plane with AI as a working crew member. Source: Brookings

Focusing mainly on the land domain, advances in AI and MLwill enable machines to learn from human behavior and adapt to changing circumstances more effectively, thereby enhancing mission execution.[H] Expectations for HMT project significant growth in unmanned systems (air, sea, & ground), robots, and digital assistants (see Digital Assistants Report) (see Robotics Report). None of these technologies, in and of themselves, represent a revolution in military operations, but when applied precisely as a system of sensors and applications, they represent the capability to synthesize data and provide information orders of magnitude faster than humanly possible.[H] The Great Power who is the most effective in developing and implementing these applications stands to gain an overwhelming advantage (see China AI Development Report). HMT is poised to become a game-changer in military operations across the land domain. As military organizations seek new ways to improve their operational effectiveness, HMT will emerge as a powerful tool that can enhance mission capabilities while keeping personnel safe.[H]

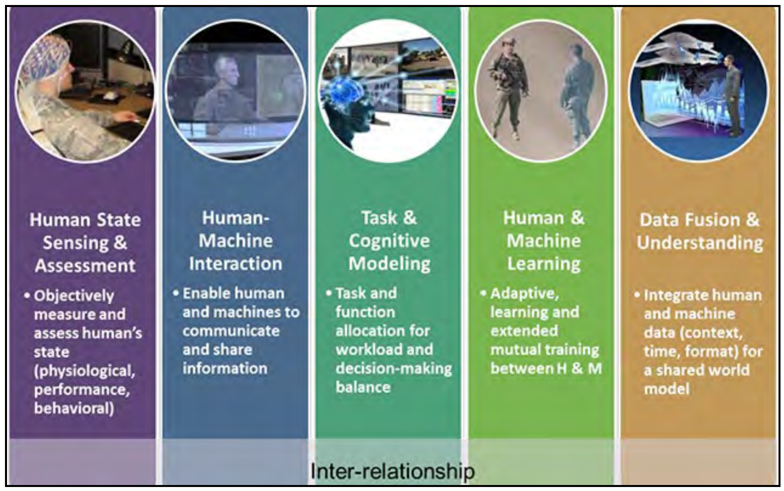


Figure 2: The Inter-relationship of HMT in Military Applications. Source: Defense Innovation Marketplace

While the future of HMT in military applications is promising, there are significant challenges and risks; particularly when dealing with austere environments.[H] HMT systems and platforms require considerable power resources, which represent a new and dynamic burden in sustainment operations.[H] [H] Additionally, the necessity of maintaining communications, network, and cyber security to support all the aforementioned systems requires significant effort, maintenance, and training[H] [H] (see 6G Report) (see AICA Report). These challenges represent new and abstract problem sets for leaders to solve while planning for and executing operations across domains. The necessity to preserve these capabilities across the joint force is paramount in maintaining a competitive edge in the future operating environment, which requires change and action now to address these projected shortfalls.[H]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to rely on statistics and corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Nathaniel C. Stone
nathaniel.stone.mil@armywarcollege.edu

China Likely To Outpace The United States In Artificial Intelligence Development by 2030; Led By A Commitment To The Development Of Artificial Intelligence Technologies And Their Full Implementation

Executive Summary

Due to the U.S.'s lack of commitment, focus, and support of crucial artificial intelligence (AI) projects and China's ambitious AI strategy, it is likely (56-70%) that China will overtake the U.S. in AI development and implementation by 2030. Despite the current U.S. standing as the global leader in AI, the People's Republic of China (PRC) has taken deliberate and precise measures to overtake the U.S., and the world, as the leader in AI technology while simultaneously constructing the appropriate AI ecosystem to support their ends.

Discussion

The U.S. currently holds the lead over China in AI, drawing from strength in higher education and research institutes, the most prominent venture capitalist ecosystem, and the most significant number of innovative start-ups.[H] Militarily, the U.S. leads in the aspect of AI utilization, but this is likely to change due to China's commitment to AI development and its, near unlimited, access to data and cloud computing.[M] Until recently, the U.S. held solid leads in research, talent, development, and hardware, but China is dedicating significant resources and citizenry to accelerate the pace of AI development and utilization across all aspects of Chinese society.[H]

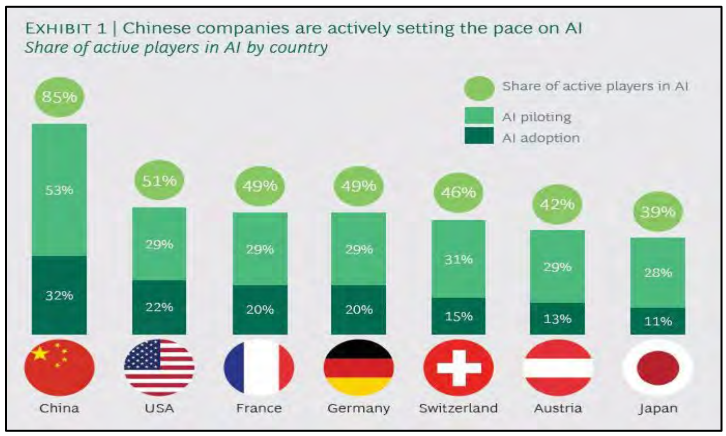


Figure1: How China is Dominating Artificial Intelligence. Source: Forbes

China is leading in several specific AI technologies. From a research perspective, China has become a world leader in AI publications and patents and is poised to become a leader in AI-empowered businesses, such as speech and image recognition applications.[H] [H] China is also making significant strides in narrowing the gap in AI chipsets, with many firms motivated to develop AI chips due to the vast market in China.[H] China's "14th Five-Year Plan" targets 7% annual growth by 2025 for R&D expenditure, with at least 8% devoted to basic research, and one area of focus is AI.[H] According to Grace Haaf, Assistant Professor and Faculty Fellow of Business Analytics at NYU Shanghai, "China has more resources available, multiples more well-educated incredibly talented people available to do AI-focused work, and many programs popping up, both at Chinese and joint international universities."[H]

In addition, China is leading in AI technologies aimed at connecting and upgrading the entire Chinese industry by 2025, such as producing goods and controlling companies while balancing supply and demand.[H] China's AI strategy is ambitious and provides the most resources worldwide for its implementation, combining a gigantic amount of data with talent, companies, research, and capital to build the world's leading AI ecosystem.[H] There is a tremendous opportunity for AI growth in new sectors in China, including automotive, transportation, logistics, manufacturing, enterprise software, and healthcare.[H]

Figure 2: China's Race for AI Supremacy. Click the image on the image or go to: https://www.youtube.com/watch?v=zbzcZr_Nadc to view this video. Source Bloomberg.

In recent years, specific measures taken by China in AI development were an empowerment of national tech companies to lead innovation over government agencies developing advances in AI hardware and software (mainly financial, facial recognition, speech, surveillance, and data collection technologies).[H] Militarily China focused on a holistic prioritization of AI and cyber capabilities over traditional military spending.[H] In addition, China has focused its educational emphasis on science, technology, engineering and mathematics (STEM) fields, further supporting the Party's AI objectives by generating a willing and available workforce.[H]

Despite signs and actions taken by China that demonstrate their commitment to gaining a competitive edge in AI, in all aspects of Great Power Competition, some experts feel that the U.S. will continue to foster conditions that promote AI development and utilization to a degree that will allow America to maintain the lead.[H] Some feel that the race isn't even close, and rhetoric indicating otherwise is generated to drum up funding for defense and government spending on AI.[M] Either way, China has taken measures to counter the current world order, and an appropriate response is necessary to counter their ambition, or they will succeed in achieving their objective.[H]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to rely on statistics and corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Nathaniel C. Stone
nathaniel.stone.mil@armywarcollege.edu

Artificial Intelligence Is Unlikely To Replace Teachers In Classroom Settings By 2030, But Almost Certain To Continue To Enhance Learning Over The Next Two Decades

Executive Summary

It is unlikely (31-45%) that artificial intelligence (AI) will replace teachers in classroom settings in the near future (2030-2040), but almost certain (86-99%) that AI's presence in classrooms will continue to grow and enhance learning. Due to continued advancements in AI applications focused on education, the use of AI in classrooms continues to become more prevalent. Both teachers and students lean on AI to aid in instruction, improve communication, personalize individual learning, and quickly assess progress and give/receive feedback. Critics cite the ethical concerns associated with a reliance on technology impeding the development of critical thinking, a potential for the dehumanization of education/instruction, and concerns about biases in AI systems that could perpetuate educational inequalities. Despite these concerns, with mitigation and conscious advancement, AI improves the quality of instruction and assists teachers and students in achieving the utmost of the associated learning objectives.

Discussion

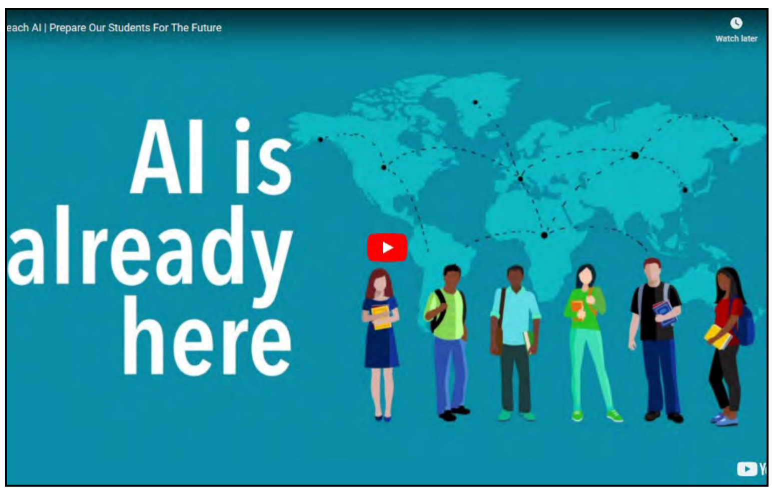


Figure 1: Teach AI, Prepare Our Students for the Future. Click the image on the image or go to: https://www.youtube.com/watch?v=ympzqGzfl0U to view this video. Source: ISTE.

AI is almost certain to revolutionize the way students learn and teachers teach.[H] AI algorithms can analyze student data/information and adapt to their specific style of learning, providing feedback and recommendations that are tailored to their individual needs and abilities.[H] Utilizing AI in classrooms can help keep students engaged and motivated, which results in improvements in their academic success.[H] While AI may become an increasingly valuable tool for educators, it is unlikely to completely replace human teachers anytime soon. The human touch and interaction between teachers and students are essential components of education that cannot be replicated by machines.[H]

AI is already in use in education as a tool for educators. For example, diagnostic tests for placing a student in a class and tailoring the curriculum to meet their needs utilize AI.[H] China is also using AI as a teacher's assistant to conduct administrative tasks and analyze teachers' methods and monitor their performance.[H] Decreasing teacher workload is highly likely (71-85%) to reduce their stress and allow them to be more effective and attentive as instructors.[H]

According to a Global Market Insights Study, more than 50% of schools and universities rely on AI for administrative assistance.[H] Analyzing the future by studying financial trends, the global market for AI in education project reaching 3.68B USD by 2023.[H] These numbers clearly predict the continued use of AI in the classroom and a greater reliance on AI in future applications.

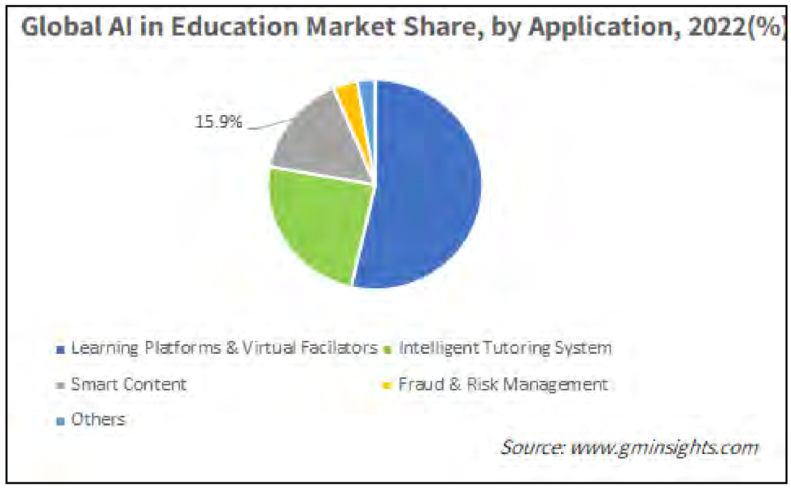


Figure 2: Global AI Share by Applications. Source: Global Market Insights

When considering the benefits of and potential applications for AI in education, the following trend at the top of the list: Personalization, Task Augmentation, Improved Communication, Enhanced Lesson Plans, Better Assessment, Increased Accessibility, and Cost Effectiveness.[H] [H] [H] Examples for each of the listed trends follow:

1. Personalization. Personalized instruction applications allow systems to adapt to users' specific learning styles and target instructions based on their personalities.[H]

2. Task Augmentation. Task Augmentation applications such as checking homework, grading tests, organizing research papers, maintaining reports, and making presentations will assist teachers in focusing on instruction and direct connection with students, while AI helps in the administrative minutia of managing a classroom setting – saving time.[H]

3. Improved Communication. Communication applications, in the form of digital assistants, represent AI-powered chatbots available to students at any time and assist with tutoring, finding answers, and solving problems.[H]

4. Enhanced Lesson Plans. AI applications can identify knowledge gaps among students within the course material and adjust lessons accordingly to address the gaps.[H]

5. Better Assessment. AI algorithms can analyze student data from various sources such as attendance records, assignments, tests, quizzes, etc., assisting teachers in grading assignments, shortening the feedback time, and providing insight into how well their students are doing in class, helping them to know where to emphasize focus and review.[H]

Figure 3: Students Interact with AI in the Classroom. Source: The Tech Edvocate.

6. Increased Accessibility. AI-powered tools like speech recognition software and text-to-speech programs help English as a second language students and students with certain disabilities overcome barriers to keeping up with traditional classroom instruction.[H] [H]

7. Cost Effectiveness. Incorporating AI into classrooms may seem expensive at first, but it is cost-effective in the long run because it saves time for teachers and improves academic performance for students.[H] [H]

Additionally, AI creates virtual classrooms tailored to individual students' needs and interests. Militarily, this generates significant advantages for a soldier or leader who is trying to develop an understanding of an objective or region that is contested.[H] Virtual classroom applications represent the potential for Soldiers to simulate a training or combat environment without actually being there – saving time, money, and, potentially, lives.[H] Apart from the known values that virtual classrooms provide to remote learning environments, they also link geographically separated users, creating opportunities for collaboration and training that would not exist otherwise.

AI has the potential to transform education and instruction by providing personalized learning, analyzing student performance, and freeing teachers from time-consuming ancillary tasks, but it is not without criticism.[H] [H] The cost, a lack of personal connection, information breaches, and potential bias all threaten the sanctity of education and a positive learning environment.[H] Therefore, developers and users need to consider the ethical implications and potential downfalls of AI technology in teaching and mitigate accordingly.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to rely on statistics and corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Nathaniel C. Stone
nathaniel.stone.mil@armywarcollege.edu

By 2040, Advancements In Artificial Intelligence Augmented Robotics Are Highly Likely To Replace Skilled Manufacturing Work And Become More Integrated Into Daily Life

Executive Summary

Due to steady improvements in artificial intelligence (AI) capabilities, advancements in robotics are highly likely (71-85%) to integrate into people's daily lives by 2040. Robotic technology is advancing rapidly and will revolutionize many industries over the next two decades. Robotics will be used to automate mundane tasks, improve safety and efficiency in hazardous environments, and raise the quality of life of its users. Despite realistic fears of job losses due to automation and ethical concerns with its implementation, robotics will increase economic growth and productivity while creating new career opportunities.

Discussion

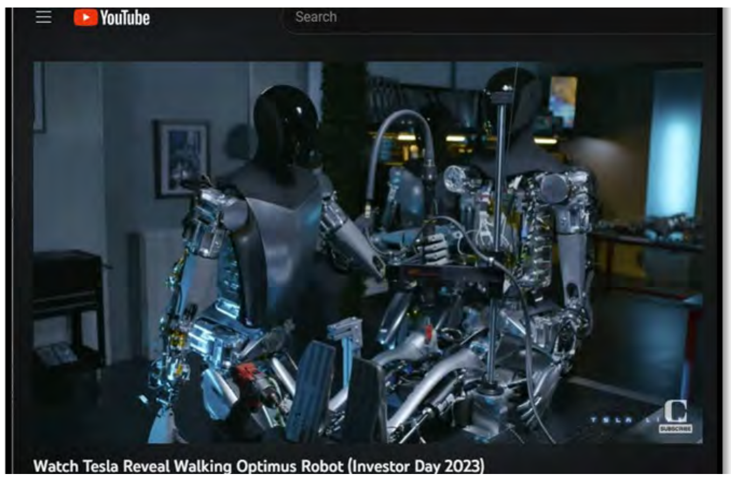


Figure 1: Tesla Reveals Walking Optimus Robot to Investors. Click the image on the image or go to: https://www.youtube.com/watch?v=2dS0aDMQoD4 to view this video. Source: CNET.

The next two decades will be a period of rapid growth in the field of robotics, and AI will be the primary driver of this growth.[H] AI will enable robots to become autonomous, intelligent, and capable of performing complex tasks.[H] AI will also enable robots to interact with humans in more natural ways, allowing them to understand better and respond to human needs, which will foster interactions and build a reliance on the technologies.[H]

Several different AI technologies are and will continue to enable robots to become more autonomous, intelligent, and capable of performing complex tasks.[H] The most common AI technologies used for this purpose are machine learning (ML), deep learning (DL), and natural language processing: ML is a type of AI technology that enables robots to learn from data and make decisions based on that data.[H] [H] DL is a type of AI technology that enables robots to learn from large amounts of data and make decisions based on that data.[H] Natural language processing is a type of AI technology that enables robots to understand and process natural language.[H]

Other technologies used to enable robots to become more capable of performing complex tasks include computer vision, advancements in mobility, and reinforcement learning: Computer vision is a type of AI technology that enables robots to recognize and interpret images.[H] Advancements in mobility are enabling robots to interact with their environment and better perform physical tasks.[H] [H] Reinforcement learning is a type of AI technology that enables robots to learn from their environment and make decisions based on that learning.[H] In addition to all these AI technologies, robots are enabled by sensors, actuators, and other hardware components specific to the robot's task. Sensors enable robots to detect and measure the environment around them, while actuators enable robots to interact with the environment.[H] [H] Other hardware components, such as motors and batteries, enable robots to move, repair/recharge, and power themselves.[H] It is highly likely that, in the case of robotics, the hardware will be the limiting factor in development versus the software and processors in most AI applications dealing with robotics.

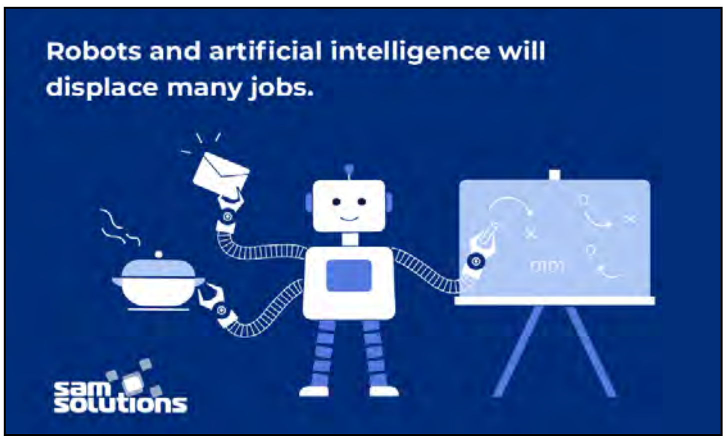


Figure 2: For More on How AI and Robotics Will Influence Daily Life. Source: Sam-Solutions

Regarding manufacturing and industry, the International Federation of Robotics predicts the market exceeding $33 billion by 2025.[H] Current trends for robotics in manufacturing include hardware integration with smart technologies such as internet of things (IoT) solutions, artificial intelligence and machine learning algorithms, Big Data, and cloud computing.[H] [H] Additionally, agriculture is among the leaders in the implementation of robots and AI as well.[H]

Holistically, this implies a massive change in the way we work, and it will be necessary to put measures in place to counteract job losses.[H] Retraining the workforce, rethinking how entry-level jobs work, and taking advantage of countless new jobs created by merging AI optimization with human skills are some of the measures that can be taken.[H] The challenge for leaders will be to develop ways to integrate advanced robotics technologies in a manner that augments human performance where applicable and, in scenarios where humans have been replaced, find suitable alternatives.

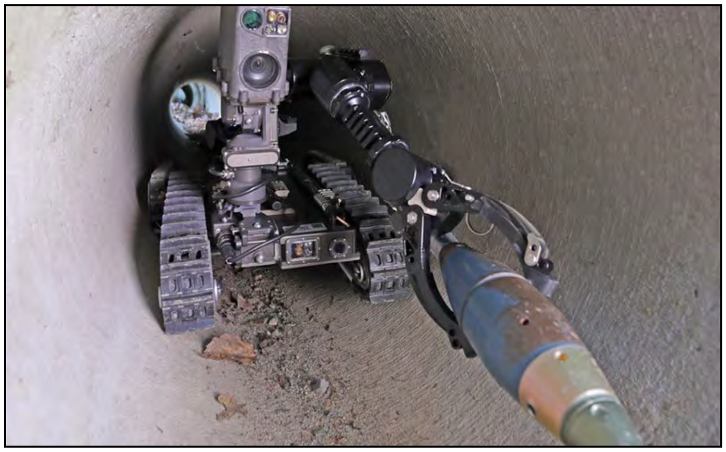


Figure 3: An Un-Exploded Ordinance Disposal Robot Safely Handles an Unstable Mortar Round. Source: ADS, Inc.

When considering military applications for robotics, there are a variety of purposes, including reconnaissance, surveillance, and combat. Robots can enter unsafe spaces and record video or audio to broadcast back to a secure location away from the threat. They also deliver ammunition, carry loads, network with air and ground drones, surveil high-risk areas, and fire weapons when controlled by humans.[H]

The military's use of robots raises ethical concerns about the role of humans in warfare. However, proponents argue that robots can significantly reduce the risk for Soldiers on the battlefield.[H] As robotics progress from hands-on tools to partners in combat, they will become essential components of future military operations.[H] [H] [H] [H]

In addition to independent robots, exoskeletons are becoming increasingly popular in heavy industries, physical rehabilitation, and other sectors.[H] [H] The global exoskeleton market projects reaching $5.4 billion by 2028.[H] Soft exoskeletons, consisting of fabric and flexible, artificial muscles, are becoming more common as they are lighter and offer more range of motion than their metal counterparts.[H] Incorporating sensors and artificial intelligence in exoskeletons is a natural next step.[H] The future of exoskeletons is promising, with lighter loads, limbs, and more.[H] Researchers at MIT have developed an exoskeleton designed to be lighter and requires less power than similar devices already under development.[H] Berkeley Bionics and the University of California, Berkeley, have developed two exoskeleton systems, the ExoHiker for walking and the ExoClimber for climbing.[H] A third system that combines the capabilities of the walking and climbing systems will be introduced soon.[H] [H]

While considering the realistic fears associated with potential job losses due to automation and ethical concerns with the implementation of robotics on a grand scale, there are also constraints associated with safety, power use, and noise pollution. Robots are incredibly loud and require significant power stores to operate, which significantly limit their applicable use in a domestic setting - without direct current relays and sound reduction measures. Developers must overcome each of these shortfalls before robots are used in a practical setting, but considering the technological advances currently, and the projected goals, gradual improvements will make way for robots in daily life by 2040.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Sources were generally reliable and tended to rely on statistics and corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: COL Nathaniel C. Stone
nathaniel.stone.mil@armywarcollege.edu

Mission Command Likely The Most Important Factor For Utilization And Prioritization Of Autonomous Systems Through 2040

Executive Summary

Unlike the financial driver for commercial research and innovation, mission command is likely (56 -70%) the key military factor for utilization and prioritization of autonomous weapon projects across the warfighting functions (WFFs). Due to the quick decisions needed in the ever-changing operational environments of the battlefield, geographical combatant and field level commanders get final decision on utilization and significant input on prioritization of new capabilities. Although commercial companies are also investing heavily in research and development (R&D) for autonomous weapons, the mission command structure is not the leading factor. Despite leveraging commercial R&D, projects to support WFF, the DoD will continue to rely on mission command concepts as the basis for utilization plans and its prioritization of artificial intelligence (AI) research initiatives and autonomous systems.

Discussion

The military race to build autonomous systems and AI applications increased global R&D budgets, as depicted in Figure 1, among both U.S. allies, such as the nearly 3% increase in the United Kingdom, and the U.S.' biggest competitor, China. Chinese AI

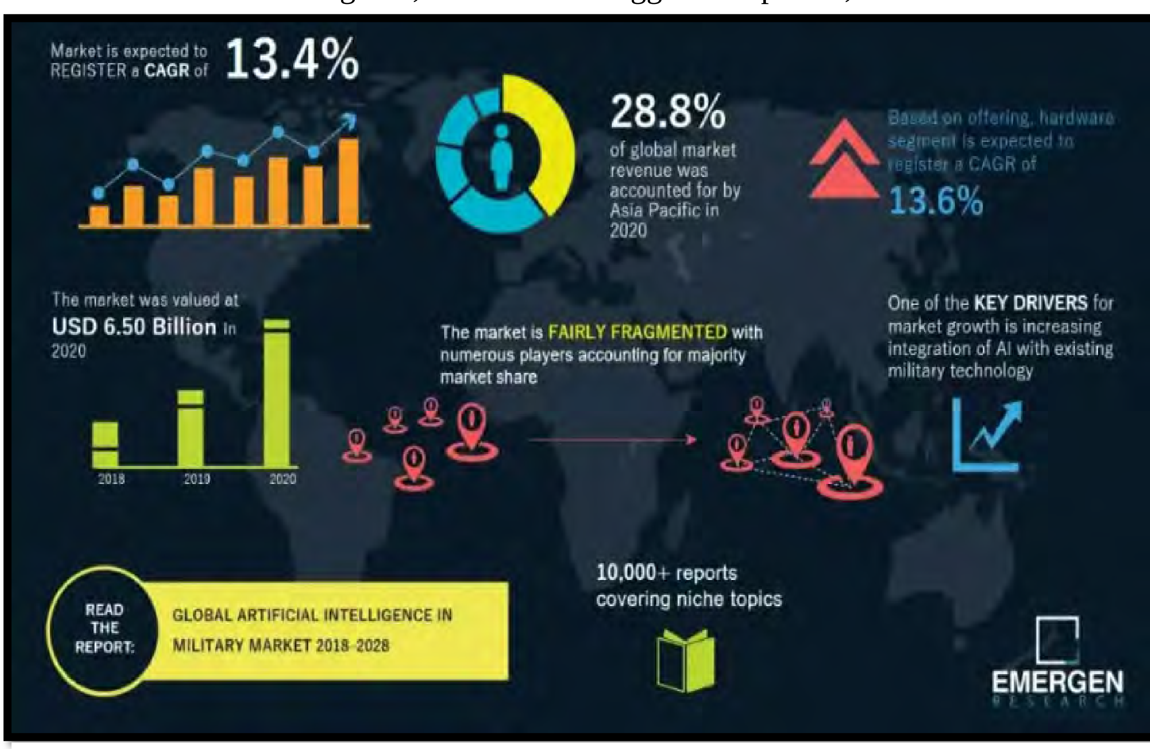


Figure 1: Rise of military AI spending across the globe. Source: [Emergent Research]

investments are likely above $1.6B.[H] (see China AI Development Report) Commercial company research and development funds are determined from the top-down approach and the funding allocation is derived based on cost, timing, and improving the company bottom-line.[M] Improving the bottom-line being the most important, which pushes most companies to invest heavier in applied research. Unlike these private companies, the military prioritization of R&D funding does not put an emphasis on cost. Militaries prioritize R&D based on the urgency of the need to support the current or expected WFFs.[H] This approach will be determined not just by the highest-ranking officials, but likely based on the entire mission command structure with heavy input from the concept plan teams. The DoD routinely procures products, services and equipment from private industry R&D funding.[M] This is no different for current and projected future autonomous systems and AI applications.[H] The commercial companies are investing in the latest AI based on two types of research, applied research and development research.[M]

Most commercial companies spend the bulk of their research dollars on applied research, which is less risky for shareholders or company owners.[H] This applied research is conducted on an already matured technology that the company uses to better understand the specific needs and purpose of a product and how to license and manage intellectual property to gain profits.[M] The desired result of commercial companies applied research funding is an entirely new product, product line, or service that can start the development cycle.[H] Companies have unique processes for R&D decisions, but the primary factors commercial companies use to prioritize their research is: engineering workforce, innovation funding including tax incentives, collaborations, and ownership to include shareholders.[M]

The steps of the mission command structure is to first provide the commander's intent, mission type orders, and conduct decentralized execution to operate at the speed of the problem.[H] Nowhere in this list of factors for commercial companies is the military concept of mission command, but it falls between all of these factors, which is why it’s’ likely the key factor for military utilization and prioritization of AI applications and autonomous weapons. The list below describes each of the commercial factors and how that factor ties back to mission command:

Engineering Workforce – With the development of low and no code applications and continued expansion of AI, the definition of the engineering workforce continues to expand to include business technologists in all fields.[H] This means there has to be synergy between software engineers and subject matter experts to develop and train AI applications and autonomous systems.[M] For military mission command, this means having subject matter experts of all disciplines and at all echelon levels trained and ready to develop requirements, organize and label training data (see Data Availability Report) and participate in working groups to develop AI and autonomous technologies, not just your typical software developers. (see Top ML Algorithm Report)

Innovation Funding – The government also provides tax breaks or cuts for innovation that can help in the public sector continue innovation. Unlike China where companies are mandated by law to collaborate with the military, American companies are incentivized through potential profits and tax breaks.[H] Although this does not have a direct tie to military mission command, innovation funding for commercial companies impacts the types of commercial products that get leveraged for military WFFs. Mission command will then have to modify the war fighting concepts to fill any gaps not filled with commercially available products. With heavy development investments necessary to modify the commercial products militaries must be cognizant to not overspend on research.[M] Utilizing the same commercial formula, depicted in Figure 2 below, militaries must ensure they are not overspending, but more importantly that the AI and autonomous projects are providing the needed capability to defeat adversaries.

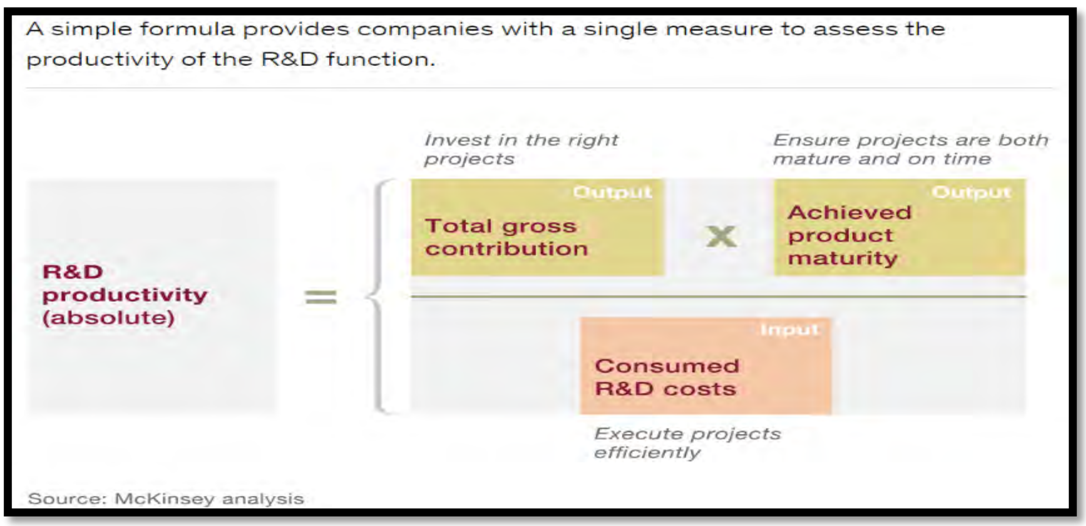


Figure 2: Simple formula for companies to measure success of R&D. Source: McKinsey & Company

Collaboration – Commercial collaboration for R&D investments increase profits on average almost 4% higher than those companies without collaboration.[M] These collaborations may include but are not limited to collaborations with other commercial companies, research organizations, military organizations or university research labs.[M] The three-way collaborations with the universities, commercial companies and government entities, like the National Science Foundation, connect the broader nationwide network for information sharing, create AI solutions across all disciplines/sectors and to make AI more plug-n-play and accessible.[H] To ensure the newest technology is available for military use at the speed of need and ahead of U.S. adversaries, collaboration is key. The commercial and university collaborations coupled with mission command creates a more agile, responsive, and collaborative development process that is better equipped to navigate the complex and rapidly changing landscape of AI privacy and security risks.[M] These collaborations are also key to forming the public opinion that will eventually impact the laws surrounding the employment of AI and autonomous systems across the military. (see Regulations Report).

Business Owner/Shareholder – Last, the business owner/shareholders construct for commercial companies doesn't apply to government R&D spending; For government spending, there are several accountability organizations and congress to weigh in on those decisions.[H] For commercial companies the owner(s) or shareholders are the final decision maker for the strategy and funding amount for all R&D projects. For military application this concept applies directly to the Joint Capabilities Integration Decision System (JCIDS).[H] Although the prioritization of R&D projects are made at the highest levels of military command, the decisions for utilization and employment of these technologies are executed at the tactical levels.[H]

Mission command influences JCIDS decisions by promoting a more flexible and adaptable approach to capability development. For example, a focus on mission command may lead decision-makers to prioritize R&D solutions that enable greater autonomy over solutions that buy more manual weaponry. If this occurs, the decision makers heavily consider the advice and counsel of the mission commander and make decisions accordingly.[H] The first two steps of Kotter's Change Model are to create the sense of urgency and recruit powerful change leaders.[M] For JCIDS decisions that result in the development of new acquisition systems, both of these steps are supported by mission command. However, it is important to note that mission command is not a formal part of the JCIDS process, and there is no specific guidance on how to integrate the two. Rather, the relationship between the two concepts is largely dependent on the specific operational context and the priorities of military leaders, also known as commander's intent.

Analytic Confidence

The analytic confidence for this estimate is *moderate*. The analyst used multiple artificial intelligence sources for research which included You.com's chatbot, and Unrestricted Intelligence. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: Mr. Reginald Shuford
reginald.shuford.civ@armywarcollege.edu

Quantum Inertial Navigation System Likely To Replace GPS For PNT Between 2035-2040, Enabling Human-Machine Operations In GPS-Denied Areas

Executive Summary

Quantum inertial navigation systems (QINS) are likely (56-70%) to replace the global positioning system (GPS) for primary positioning, navigation, and timing (PNT) in military applications between 2035 and 2040 due to rapid advancement in quantum sensing technology, and the need to provide an alternative PNT source for military use. Despite challenges with the QINS size, weight, and power (SWaP) consumption, the vulnerabilities of GPS and the need to stay ahead of near-peer competition, will drive the development and adoption cycle, enabling human-machine operations in GPS-denied areas.

Discussion

PNT is a critical component of human-machine teaming, as it is essential for providing reliable communication and navigation. Since QINS are self-contained, they are resistant to jamming and spoofing and do not rely on satellites for PNT.[H] QINS will enable human-machine team (HMT) collaboration and navigation in the air, underwater, and even underground without the vulnerability of GPS.[M]

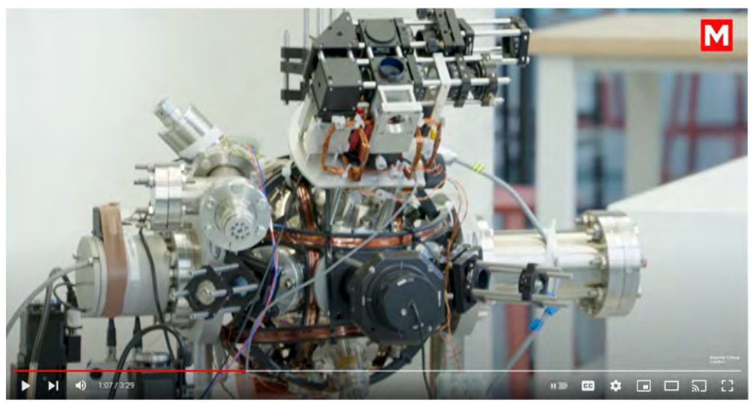


Figure 1: A U.K. team from Imperial College London demonstrates a transportable standalone quantum accelerometer. Click on image or go to: https://www.youtube.com/watch?v=xcqkXkWZhbMto view video. Source: Imperial.ac.uk

The GPS is the primary source of PNT in the U.S. due to its capabilities, availability, and no cost to end-users. However, this has led to an overreliance on GPS and limited usage of other PNT systems.[H] The adoption of non-GPS PNT systems is driven by operational needs, such as accuracy and safety, which GPS may not provide.[H] The U.S. military the importance of alternate PNT solutions, but still lacks a backup system comparable to GPS after decades of studies and legislation.[H]

GPS satellites, signals, and ground control stations are vulnerable to jamming, spoofing, and damage from space debris, solar storms, cyber-attacks, and anti-satellite weapons.[M] Both the People's Republic of China (PRC)[H] and Russia have demonstrated anti-satellite weapons against live satellites, displaying the ability to target U.S. GPS satellites, rendering some GPS-guided systems ineffective.[H] The PRC and Russia both have advanced electronic warfare (EW) and electromagnetic spectrum operations (EMSO) capable of jamming or spoofing U.S. GPS signals.[H] Russia's EW tactics in Ukraine likely indicate that the days when U.S. troops could comfortably conduct navigation and precision fires enabled by GPS PNT are ending.[M]

The U.S. has increased efforts to secure military PNT through enhanced anti-jamming and anti-spoofing protections on platforms[H], improved GPS capabilities through the deployment of GPS-III constellation[H], and the 2023 planned testing of Navigation Technology Satellite-3 (NTS-3) in near-geosynchronous orbit.[H] While these efforts are highly likely (71-85%) to improve the security, reliability, and resiliency of PNT, these systems and capabilities are still susceptible to the current GPS vulnerabilities.[H]

Current inertial navigation systems (INS), consisting of a gyroscope, accelerometer, atomic clock, and signal processing module,[M] provide PNT when GPS is unavailable, but are susceptible to measuring acceleration and orientation errors that can accumulate over time and become significant, requiring a connection to satellites to correct this drift.[H] Due to their improved accuracy, stability, sensitivity, and precision, QINS offers advantages over traditional inertial navigation systems and the ability to operate without GPS.[H] Although the sensors required for quantum inertial navigation have been field tested individually, scientists are still faced with the challenge of creating a complete QINS that is compact and rugged.[H]

In 2020, Dr. Kai Bongs, director of innovation at the University of Birmingham, predicted that full QINS will likely be available around 2040 due to recent advancements in quantum sensing technology that have reduced the sensor sensitivity and the SWaP requirements.[H] In 2018, a U.K. team from Imperial College London developed a transportable standalone quantum accelerometer, but due to its size, it was only usable in ships and trains.[M]

In 2021, a team at the French National Centre for Scientific Research invented a 3D quantum accelerometer about the size of a laptop that is 50 times more reliable than classical INS.[H] Even with these advances, QINS are too large and consume too much power to use in airplanes, drones, or missile navigation systems due to the requirement for a large vacuum system which requires thousands of volts of electricity.[H]

In late 2021, a group of Sandia National Laboratories scientists developed an avocado-sized vacuum chamber as a core technology for future navigation systems to solve this problem.[H] By replacing the vacuum-powered system with a pair of devices using chemical reactions to bind intruders, the Sandia scientists reduced both the size and power consumption required for QINS. Sandia scientist Peter Schwind stated, “it is the first device that is small, energy-efficient and reliable enough to potentially move quantum sensors from the lab into commercial use.”[H] The device has been sealed and operational for over a year, with the Sandia team planning to monitor it for another four years to show the technology ready to be fielded. The Sandia team is also investigating ways to streamline the device’s manufacturing. This development has proven the ability to shrink the QINS to a deployable size without losing reliability.[H]

Analytic Confidence

The analytic confidence for this estimate is *moderate*. Multiple artificial intelligence sources were used for research, consisting of Writesonic, Perplexity, and Unrestricted Intelligence. Sources were generally reliable and tended to corroborate one another. There was adequate time, but the analyst worked alone and did not use a structured method. Furthermore, given the lengthy time frame of the estimate, this report is sensitive to change due to new information.

Author: LTC Owen S. Adams
owen.adams.mil@armywarcollege.edu

SINGULARITY
HUMAN-MACHINE TEAMING

Annexes

Annex A – Terms of Reference

Terms of Reference:
Machine-Human Teaming on the Battlefield of the Future

For:

GEN James E. Rainey
Commanding General, U.S. Army Futures Command

By:

Team Singularity
USAWC

November 16th, 2022

Terms of Reference: Human-Teaming on the Battlefield of the Future

Requirement:

What are the likely applications[7] across the continuum of human-machine teaming[8] which will be technologically feasible, militarily relevant, and ethically acceptable through 2040[9]?

- What are the likely legal and ethical implications which may drive requirements or generate limitations? How are those likely to change between now and 2040?
- What is the future of human-machine teaming across domains with a particular emphasis on landpower?
- What are the likely determining factors for the utilization and prioritization of autonomous systems across the scope of warfighting functions?
- How will international and social norms likely evolve regarding the use of autonomous systems in combat between now and 2040?

Methodology:

In general, the team intends to gather information through various means, including but not limited to data collection from open-source outlets and interviews with academia, interest area experts, political scientists, ethicists, military strategists, and international analysts.

The team expects to execute this project in the following four steps (Note: This is a notional timeline only. The team will remain flexible to take advantage of opportunities and to address unforeseen limitations that may arise):

- Step 1: Data collection from multiple open-source outlets (November 2022 – January 2023)
    - Evaluate emerging hardware and software currently being tested in a lab.
    - Evaluate theoretical technology hardware and software which may be in the lab in the next five years.
    - Evaluate how these various technologies will likely interact in support of military operations.

[7] Applications refers to broad use of artificial intelligence and is not limited in scope to software.
[8] There is no published Department of Defense definition for human-machine teaming, however, industry standard uses the Brookings institute definition which defines the concept as a relationship; one made up of at least three equally important elements: the human, the machine, and the interactions and interdependencies between them.
[9] The scope of time will be examined in two blocks: 2030-2035 and 2035-2040.

- Explore the new roles, applications, and capabilities for human-machine teaming.
- Assess the evolution of artificial intelligence ethics over time and impacts on the future of human-machine teaming.

- Step 2: Synthesize (February – March 2023)
  - Evaluate the research findings for evolutions that provide greater insight into future roles of human-machine teaming.
  - Identify and confer with government, private sector, and dedicated subject matter experts.
  - Evaluate the research findings to determine how humans and machines can complement each other.
  - Explore additional analytical techniques such as Relevance Tree[10], Delphi model[11], and time series forecasting to inform the topic and further the analysis.
  - Determine which potential technologies are relevant to the United States Army.
  - Validate findings.

- Step 3: Compile concepts and prepare report (March – April 2023)
  - Compile a comprehensive report that includes the team's findings regarding the unmanned versus minimally/optionally manned military technologies in 2030-2040.
  - Determine implications for human-machine teaming in army modernization to include ethical, moral, and legal aspects.

Challenges:

- The team is executing this research in the context of a class at the USAWC in addition to their core course load for a Graduate Degree.
- The allocated time is in conjunction with and limited to the end of the academic year (April 2023).
- None of the participants are subject matter experts on the topic.
- Due to time and equipment constraints, the team has access to only open-source information and the final product will be unclassified.
- The amount of research materials available associated with this topic is unknown at this time.
- Funding is available to support travel, but any/all travel will require deconfliction with competing academic responsibilities.

[10] Relevance Tree is an analytical technique that subdivides a large subject into increasingly smaller subtopics.
[11] The Delphi method is a process used to arrive at a group opinion or decision by surveying a panel of experts.

Resources:

- The team is a diverse group of Army Officers and a career DOD Civilian with proven backgrounds in maneuver, aviation, cyber, electronic warfare, software acquisitions, testing development and evaluation.
- The team will utilize all available databases and resources (USAWC and elsewhere) to gather information.
- The team will utilize open-source media and published information from academic and professional institutions.
- The team will utilize all available leverage (personal & professional) to acquire information and insight.

Administration:

- The final product will be a PDF document provided to GEN Rainey to be used at his discretion and shared with those whom he determines appropriate.
- The team will coordinate with GEN Rainey's staff toward the end of March 2023 to coordinate the best time and location for the final out brief. The ideal timeline is the week of 24-28 April 2023, but the team will remain flexible for all options.
- The team members are listed below along with contact information.
    - Primary Point of Contact:
        - LTC Nicole Washington
        - Email: nicole.washington.mil@usarmywarcollege.edu
        - Cell: 208-860-7829
    - Alternate Team Point of Contact:
        - COL Nathaniel Stone
        - Email: nathaniel.stone.mil@armywarcollege.edu
        - Cell: 478-365-0880
    - Team Members:
        - COL Dennis Weaver
        - LTC Owen Adams
        - Mr. Reginald Shuford

Annex B – Assessing Analytic Confidence

Peterson Factors

- How reliable are the sources?
- How well do the independent sources corroborate each other?
- What is my/my team's level of expertise?
- How effective was my analytic collaboration?
- Did I use any structured techniques in my analysis?
- How difficult did I perceive the task to be?
- Did I have enough time to complete the task?

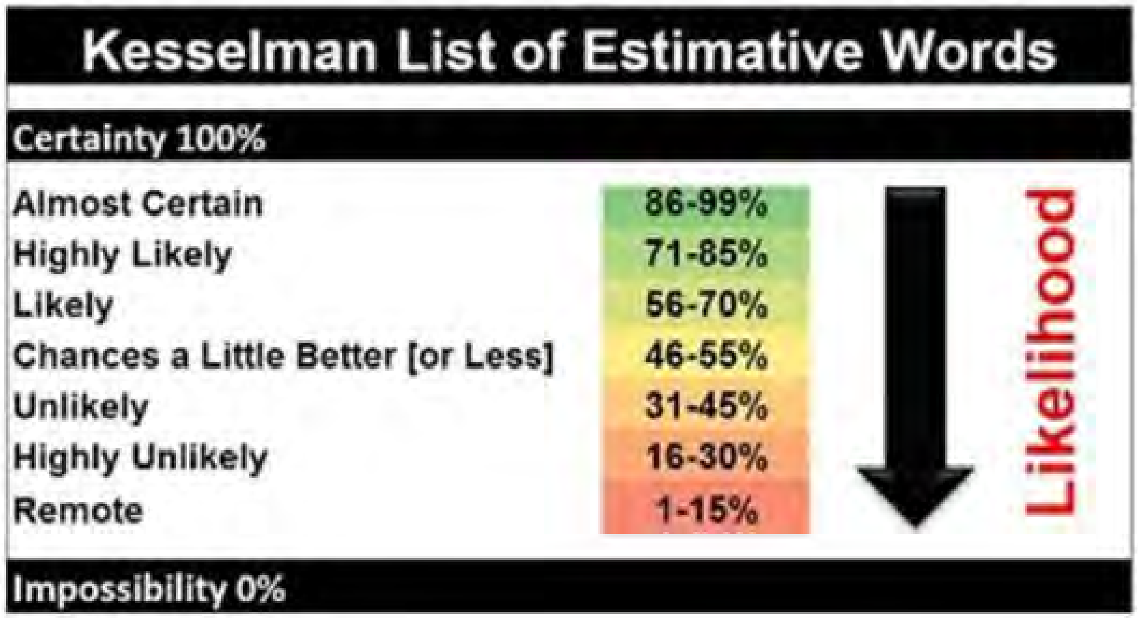
Friedman Corollaries

- Is my estimate within the range of reasonable opinion surrounding the question?
- How likely is it that new information will change my estimate?

Peterson's Analytic Confidence Worksheet

PETERSON TABLE OF ANALYTIC CONFIDENCE ASSESSMENT	Points Possible	Example Points
Use of Structured Method(s) In Analysis	(1-10)	*7*
For example: ACH, IPB, Social Networking, Bayes, Simulation, etc…		
10 indicating highest possible score when considering factors below		
Consider:		
Number of methods used		
Applicability of methods to the analysis		
Level of robustness of method		
Degree to which methods' results coincide		
Overall Source Reliability	(1-10)	*7*
A rating of 10 indicates the highest reliability		
Source Corroboration/Agreement: *Level of conflict amongst sources*	(1-5)	*4*
5: No confliction amongst sources		
4: Very little conflict amongst sources		
3: Moderate conflict amongst sources		
2: Significant conflict amongst sources		
1: Sources conflict on nearly all points		
Level Of Expertise On Subject/Topic & Experience	(1-5)	*2*
5: Deep, intimate knowledge and understanding & 3+ years experience with topic		
4: Wide knowledge & 1-3 years experience with topic		
3: Moderate knowledge & 6-12 months experience with topic		
2: Minimal knowledge & 0-5 months experience with the topic		
1: No knowledge & no experience with the topic		
Amount of Collaboration:	(1-5)	*2*
5: Part of aggregated individual analyses		
4: Worked on a team		
3: Worked with a partner		
2: Casual discussion		
1: Completely individual work		
Task Complexity	(1-5)	*3*
5: Minimally complex & challenging		
4: Somewhat complex & challenging		
3: Moderately complex & challenging		
2: Quite complex & challenging		
1: Very complex & highly challenging		
Time Pressure: *Time given to make analysis*	(1-5)	*4*
5: No deadline		
4: Easy to meet deadline		
3: Moderate deadline		
2: Demanding deadline		
1: Grossly inadequate deadline		
	Score:	**29**
	Total Possible:	**45**
	Score:	**0.644444444**
		x 10
	Analytic Confidence Adjusted Score:	**6.4**

Annex C – Kesselman List of Estimative Words



Annex D – Standard Primary Source Credibility Scale

Source reliability is noted at the end of each citation as low L, moderate M, or high H. The citation is hyperlinked to the source, unless the source is a paid subscription; in that instance a footnote is provided at the end of each writing illustrating the source for credibility. Source reliability is determined using the Trust Scale and Website Evaluation Worksheet found in Annex E.

Standard Primary Source Credibility Scale
("The Paul Scale")

Importance	Factor	Description	Satisfies Criteria (Yes /No)
HIGH	Has a good track record	Source has consistently provided true and correct information in the past	
	Information can be corroborated with other sources	Information provided by the source corroborates with information from other primary and/or secondary sources	
	Information provided is plausible	High probability of the information being true based on the analyst's experience of the topic/subject being investigated	
	Information is consistent and logically sound	Information provided is consistent when queried from different angles and is logically sound	
	Perceived expertise on the subject	Source is perceived to be an expert on the subject / topic being investigated and/or is in a role where subject knowledge is likely to be high	
	Proximity to the information	Source is close to the information – a direct participant or a witness to the event being investigated	
	Perceived trustworthiness	Source is perceived to be truthful and having integrity	
MEDIUM	No perceived bias or vested interest in the subject / topic being investigated or on the outcome of the research	Source has no perceived bias or vested interest in the subject / topic being investigated or on the outcome of the research	
	Provides complete, specific and detailed information	Information provided is specific, detailed and not generic	
LOW	Is articulate, coherent and has a positive body language	Source is articulate, coherent, has a positive body language and does not display nervousness or body language that can be construed to be evocative of deceptive behavior	
	Recommended by another trusted / credible third party	Source is recommended by others the analyst trusts but the analyst herself does not have any direct experience working with the source	
	Sociable	Source comes across as outgoing and friendly. Easy to get along with and talk to	
	Perceived goodwill to the receiver	Perceived intent or desire to help the receiver or the analyst	

Annex E – Trust Scale and Web Site Evaluation Worksheet

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

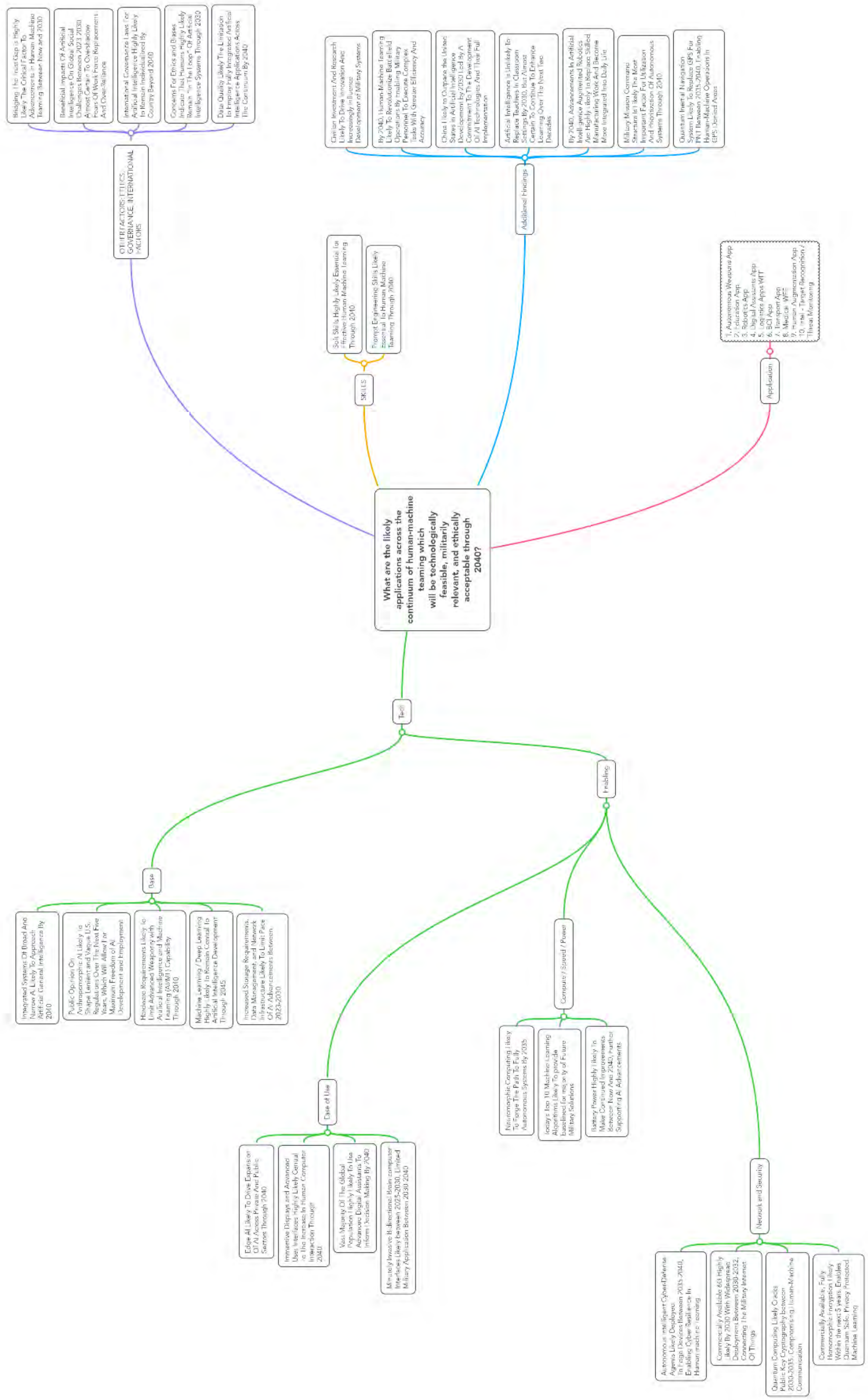
Piece of Evidence #:												Score:	Trust Scale:
Criteria	**Tips**	**Value**	**Y or N**	**Y or N**	**Y or N**	**Y or N**	**Y or N**	**Y or N**	**Y or N**	**Y or N**	**Y or N**	**0**	**15-20 High**
Content can be corroborated?	Check some of the site's facts	2	2	2									**11-15 Moderate**
Recommended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

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 F– Team Singularity Mind Map



Annex G– The Four Continua of Human-Machine Teaming

The first continuum distinguishes the spectrum of *non-social and social systems* artificial intelligence (AI) systems. Non-social AI refers to systems not designed to interact with humans or other robots in a social context. Conversely, social AI refers to systems designed for advanced interaction with humans, other AI systems, and/or robots in a social context with increasingly sophisticated anthropomorphic qualities.

The second continuum examines the progressive degree of autonomy from *Human In the Loop* (HITL) through *Human out of the loop* (HOOTL). HITL refers to a process where a human is involved in decision-making and heavily influences the environment. The middle of the scale is *Human On the Loop (HOTL),* where an AI system has the ability to execute the mission, but a human supervises and can override the decisive action. The opposite end of the continuum is HOOTL, where AI systems operate autonomously without direct human involvement in the decision-making process.

The third continuum focuses on *narrow* versus *broad,* where narrow refers to systems that are designed to handle a singular or limited task with pre-defined functions while *broad* refers to a system that executes multiple tasks, and can learn, reason, and understand with human-like cognitive ability (but below the level of artificial general intelligence (AGI) or superintelligence (ASI), which are distinguished by being self-aware, sentient and consciousness).

The fourth and final continuum differentiates between *non-robotic and robotic* systems, where non-robotic refers to AI systems that are mostly software-based and operate primarily on traditional computer hardware, normally designed for specific tasks. Robotic AI systems are implemented using advanced software, and multi-functional programing but are characterized by specialized hardware as the primary performance platform.

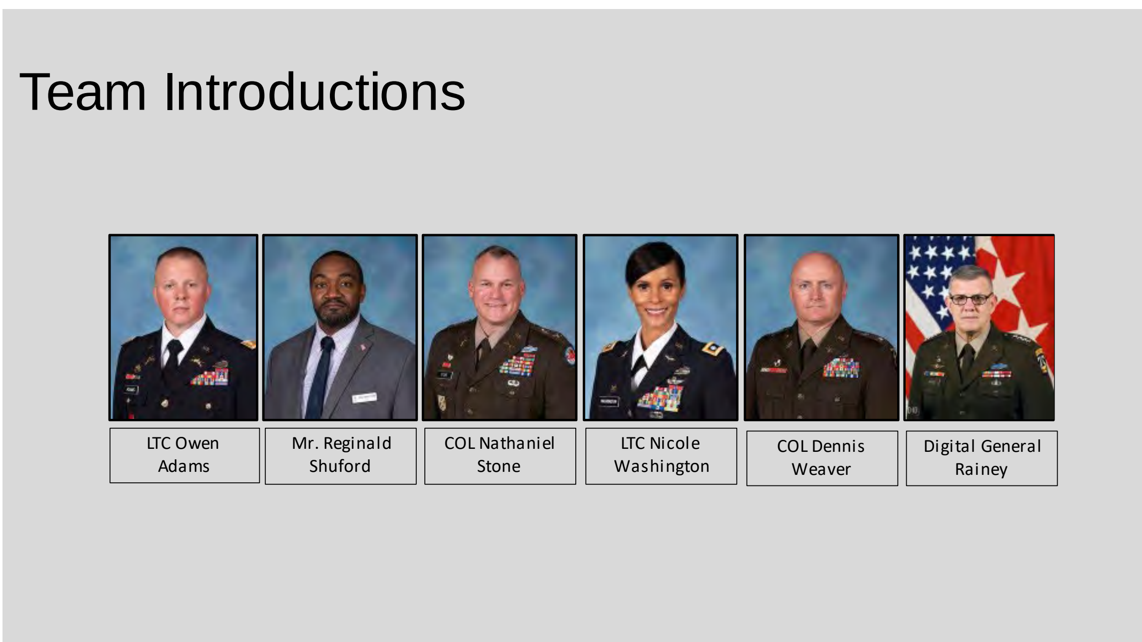
Annex H– Acronyms

2D – Two dimensional
3GPP – 3rd Generation Partnership Project
3D – Three Dimensional
6G – 6th Generation
A2AD – Anti-Access/Area Denial
AGI – Artificial General Intelligence
AI – Artificial Intelligence
AIAA – American Institute of Aeronautics and Astronautics
AICA – Autonomous Intelligent Cyber Defense Agents
APT – Advanced Persistent Threats
AR – Augmented Reality
ARL – Army Research Lab
AS – Autonomous Systems
BCG – Boston Consulting Group
BCI – Brain Computer Interfaces
BMW – Bayerische Motoren Werke AG
BRAIN – Brain Research Through Advancing Innovative Neurotechnologies
C2 – Commaand and Control
CASTLE – Cyber Agents for Security Testing and Learning Environments
CCDC – Combat Capabilities Development Command
CCP – Chinese Communist Party
CGC – Cyber Grand Challenge
CHATGPT– Chat Generative Pre-Trained Transformer
CLAWS – Cognitive Lethal Autonomous Weapons Systems
COTS – Commercial Off The Shelf
CPU – Central Processing Unit
CWIS – Close In Weapon System
DARPA – Defense Advanced Research Projects Agency
DPRIVE – Data Protection in Virtual Environments
DL – Deep Learning
DoD – Department of Defense
DNN – Deep Neural Networks
ECoG – Electrocorticography
EEG – Electroencephalography
EDR – Endpoint Detection and Response
EM – Electromagnetic
EPO – European Patent Office
EU — European Union

EV – Electric Vehicles
EW – Electronic Warfare
FHE – Fully Homomorphic Encryption
FTC – Federal Trade Commission
GPS – Global Positioning System
GOFAI – Good Old-Fashioned AI
GOTS – Government Off The Shelf
GUI – Graphic User Interface
HA – Human Augmentation
HAIT – Human- Artificial Intelligence Teaming
HE – Homomorphic Encryption
HITL – Human In The Loop
HMT – Human-Machine Teaming
HOTL – Human On The Loop
HOOTL – Human Out Of The Loop
HRT – Human-Robot Teaming
IDC – International Data Corporation
IDS – Intrusion Detection System
IEEE – Institute of Electrical and Electronics Engineers
INS – Inertial Navigation Systems
IoMT - Internet of Military Things
IoT – Internet of Things
ISO – International Organization for Standardization
ITU – International Telecommunication Union
IV – Intravenous
IVAS - Integrated Visual Augmentation System
JCIDS – Joint Capabilities Integration Decision System
KNN - k-nearest neighbors (AI Algorithm)
LAWS – Lethal Autonomous Weapons Systems
LI – Lithium-ion
LLM – Large Language Models
LLN – Liquid Neural Networks
LSCO – Large-Scale Combat Operations
M2M – Machine-To-Machine
MCF – Military Civil Fusion
MEnTs – Electromagnetic Nanotransducers
MIT – Massachusetts Institute of Technology
ML – Machine Learning
MR – Mixed Reality
N3 – Next-Generation Non-surgical Neurotechnology

NATO – North Atlantic Treaty Organization
NIST – National Institute of Standards and Technology
NLP – Natural Language Processing
NLU – Natural Language Understanding
NTS-3 – Navigation Technology Satellite-3
PHE – Partially Homomorphic encryption
PKC –Public-key Cryptography
PNT – Positioning, Navigation, and Timing
PQC – Post-quantum Cryptography
PRC – People's Republic of China
QINS – Quantum Inertial Navigation Systems
RAI – Responsible Artificial Intelligence
RAM – Random Access Memory
RAS – Robotics and Autonomous Systems
R&D – Research and Development
RDTE - Research, Development, Testing, and Evaluation
R&E – Research and Engineering
REAIM – Responsible AI in the Military Domain
REDOD – Research and Engineering for the U.S. Department of Defense
SHE – Somewhat Homomorphic Encryption
SIEM – Security Information and Event Management
SNN – Spike Neural Network
SOC – Security Operation Centers
STEM – Science, Technology, Engineering and Mathematics.
SVM - Support Vector Machine
SWaP – Size, Weight, and Power
Tbps – Terabit Per Second
THz – Terahertz
UK – United Kingdom
UNESCO – United Nations Educational, Scientific and Cultural Organization
USAWC – United States Army War College
VAR – Virtual and Augmented Reality
VR – Virtual Reality
V-TOC – Virtual Tactical Operations Center
VUI – Voice User Interface
WEP – Words of Estimated Probability
WFF – Warfighting Functions
XR – Extended Reality

Annex I– Team Singularity Final Presentation



Words of Estimative Probability

Kesselman List of Estimative Words	
Certainty 100%	
Almost Certain	86-99%
Highly Likely	71-85%
Likely	56-70%
Chances a Little Better [or Less]	46-55%
Unlikely	31-45%
Highly Unlikely	16-30%
Remote	1-15%
Impossibility 0%	

Likelihood

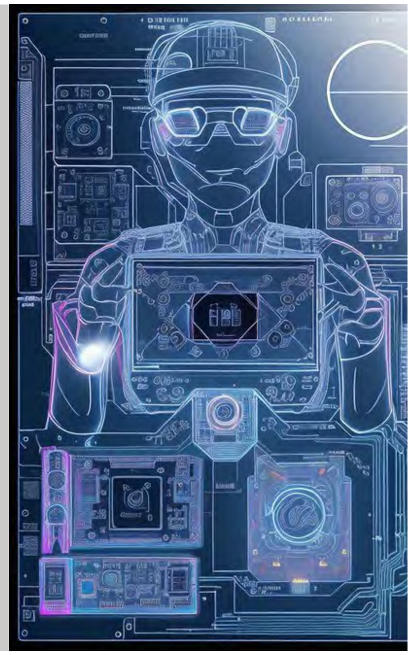
Analytical Confidence

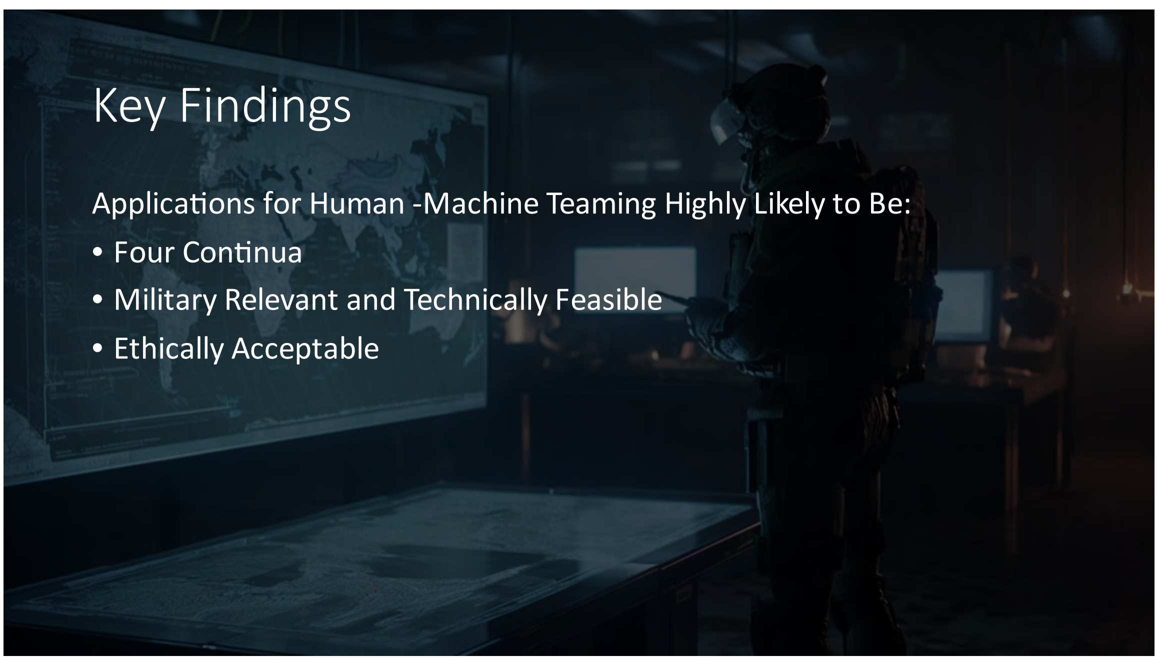
Our Overall Estimate is Moderate

Human-Machine Teaming 2040 Terms of Reference:

What are the likely applications across the continuum of human-machine teaming which will be technologically feasible, militarily relevant, and ethically acceptable through 2040?

- What are the likely legal and ethical implications which may drive requirements or generate limitations? How are those likely to change between now and 2040?
- What is the future of human machine teaming across domains?
- What are the likely determining factors for the utilization and prioritization of autonomous systems across the scope of war fighting functions?
- How will international norms likely evolve regarding the use of autonomous systems in combat between now and 2040?

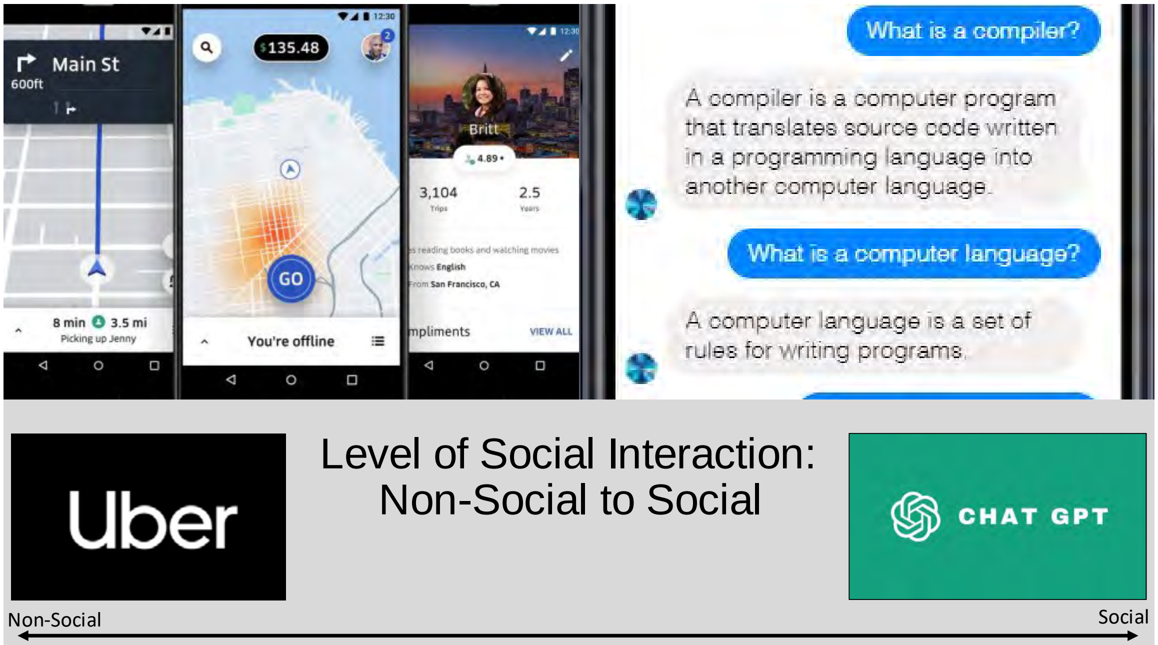


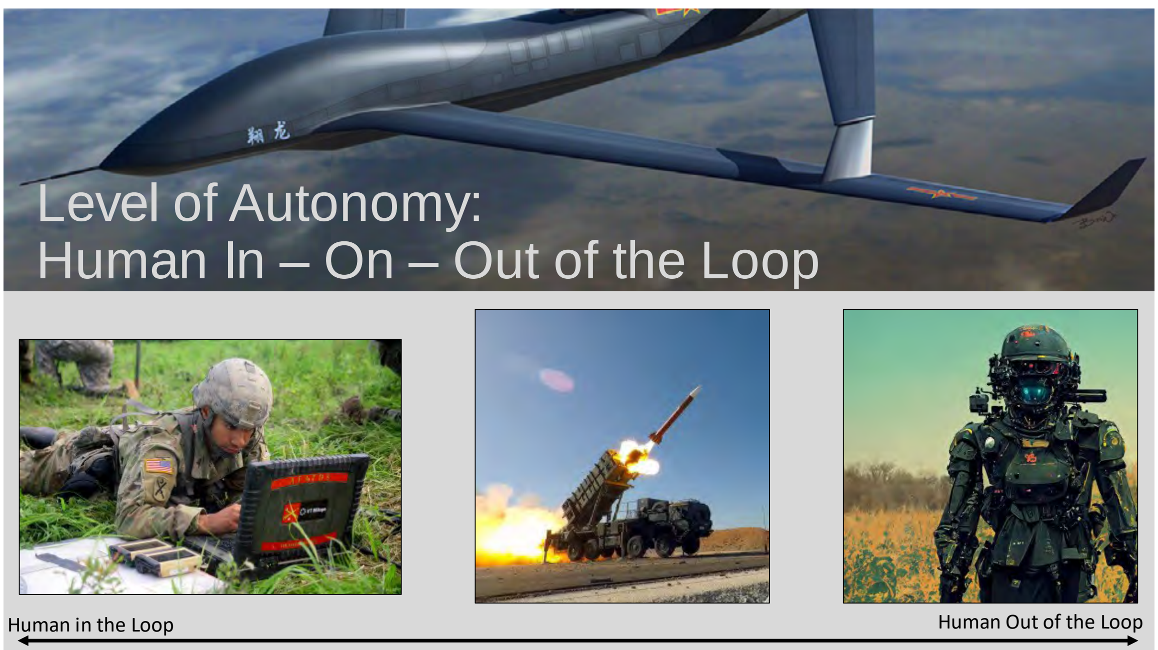


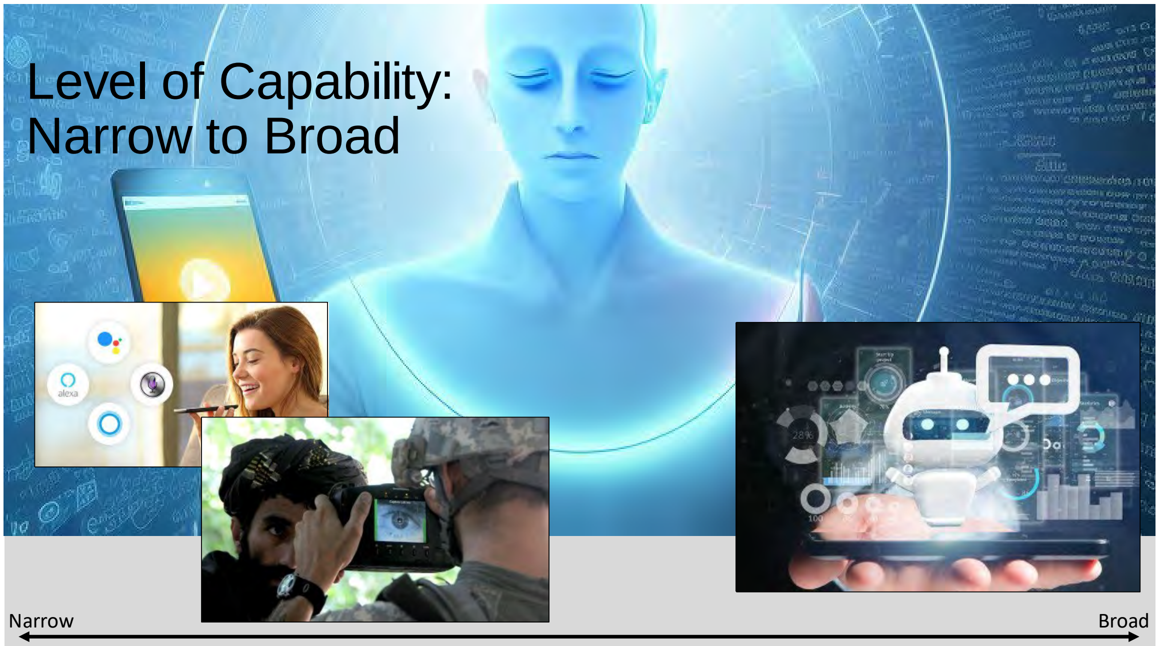
Key Findings

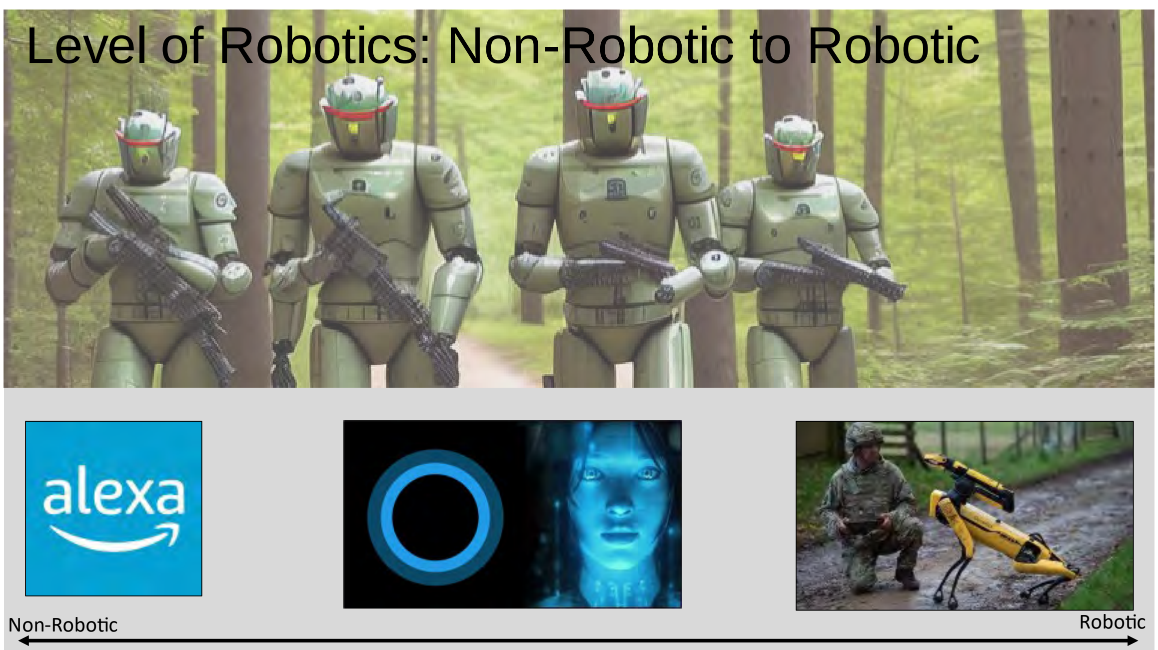
Applications for Human -Machine Teaming Highly Likely to Be:

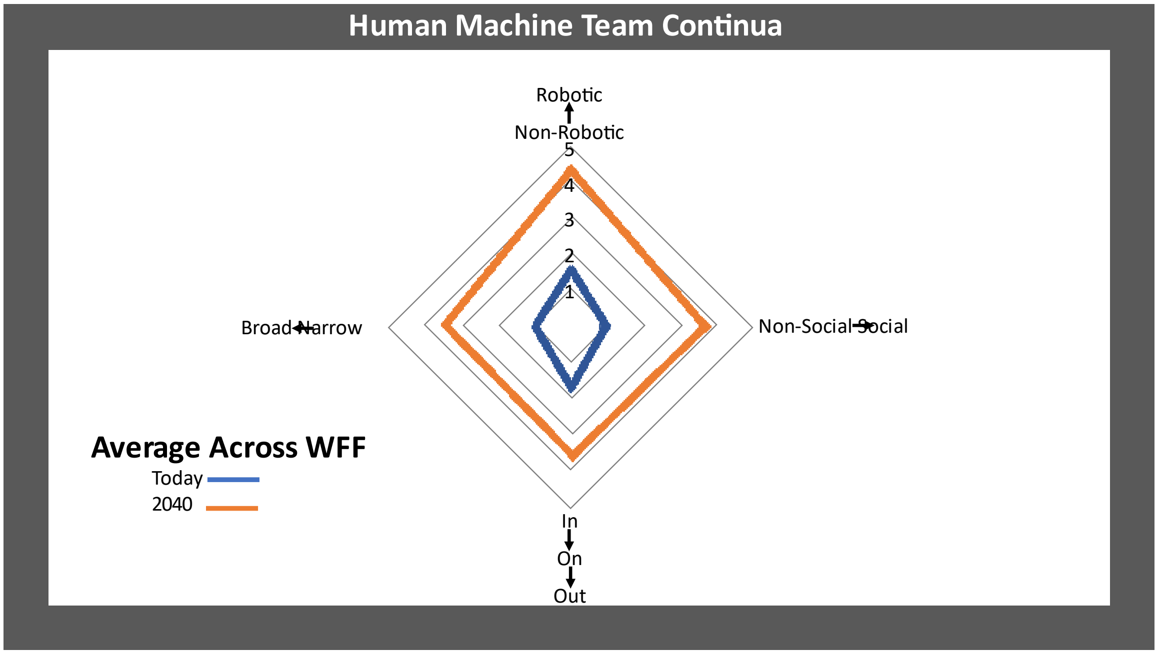
- Four Continua
- Military Relevant and Technically Feasible
- Ethically Acceptable

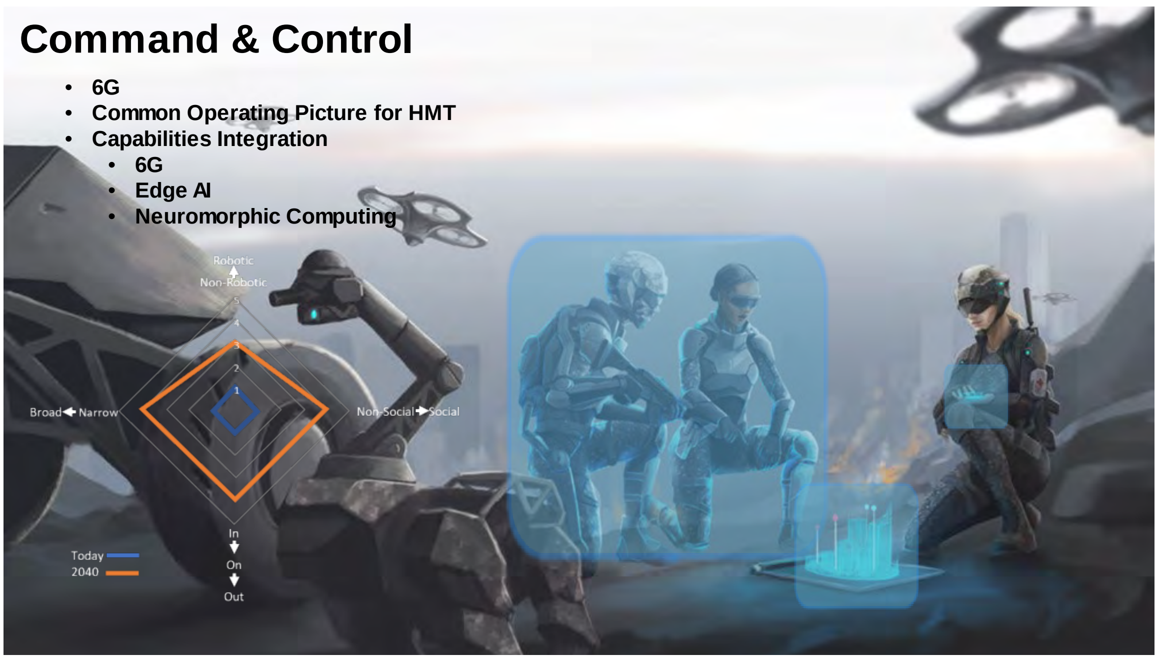

Main St
600ft
8 min 3.5 mi
Picking up Jenny
$135.48
GO
You're offline
Britt
3,104
2.5
VIEW ALL
What is a compiler?
A compiler is a computer program that translates source code written in a programming language into another computer language.
What is a computer language?
A computer language is a set of rules for writing programs.
Uber
Level of Social Interaction:
Non-Social to Social
CHAT GPT
Non-Social
Social


Level of Autonomy:
Human In – On – Out of the Loop
Human in the Loop
Human Out of the Loop

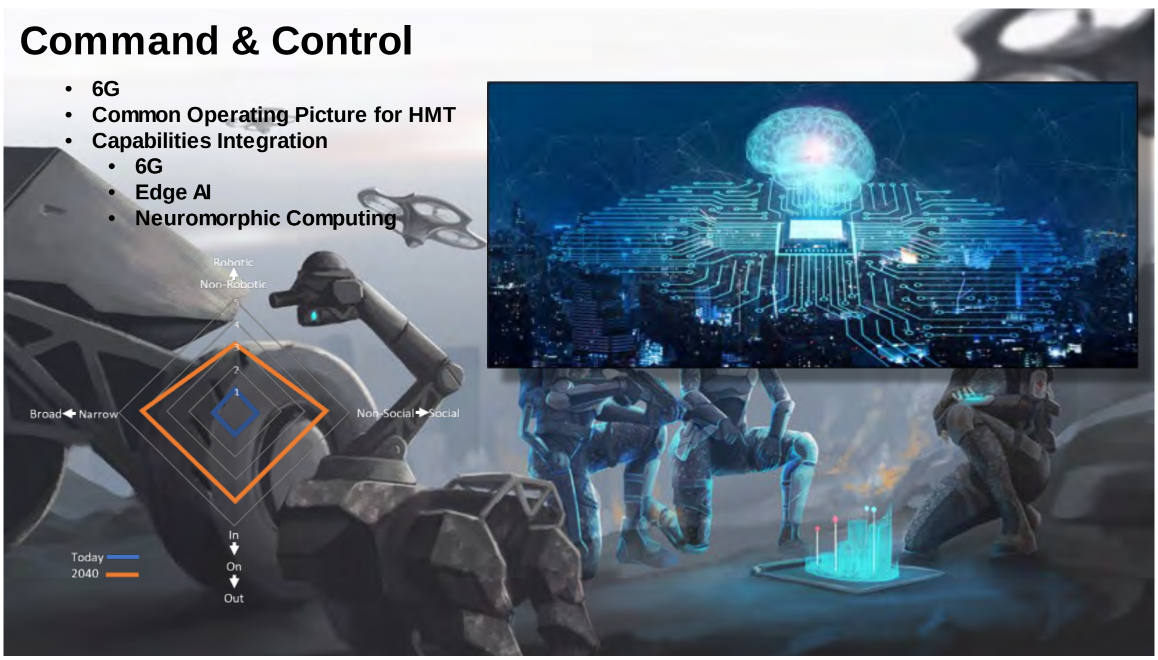

Level of Capability:
Narrow to Broad
Narrow
Broad


Level of Robotics: Non-Robotic to Robotic
alexa
Non-Robotic
Robotic


Human Machine Team Continua
Robotic
Non-Robotic
5
4
3
2
1
Broad Narrow
Non-Social Social
In
On
Out
Average Across WFF
Today
2040


Command & Control
6G
Common Operating Picture for HMT
Capabilities Integration
6G
Edge AI
Neuromorphic Computing
Robotic
Non-Robotic
5
4
3
2
1
Broad Narrow
Non-Social Social
In
On
Out
Today
2040


Command & Control
• 6G
• Common Operating Picture for HMT
Robotic
Non-Robotic
Broad Narrow
Non-Social Social
In
On
Out
Today
2040
Risk Estimate Distance

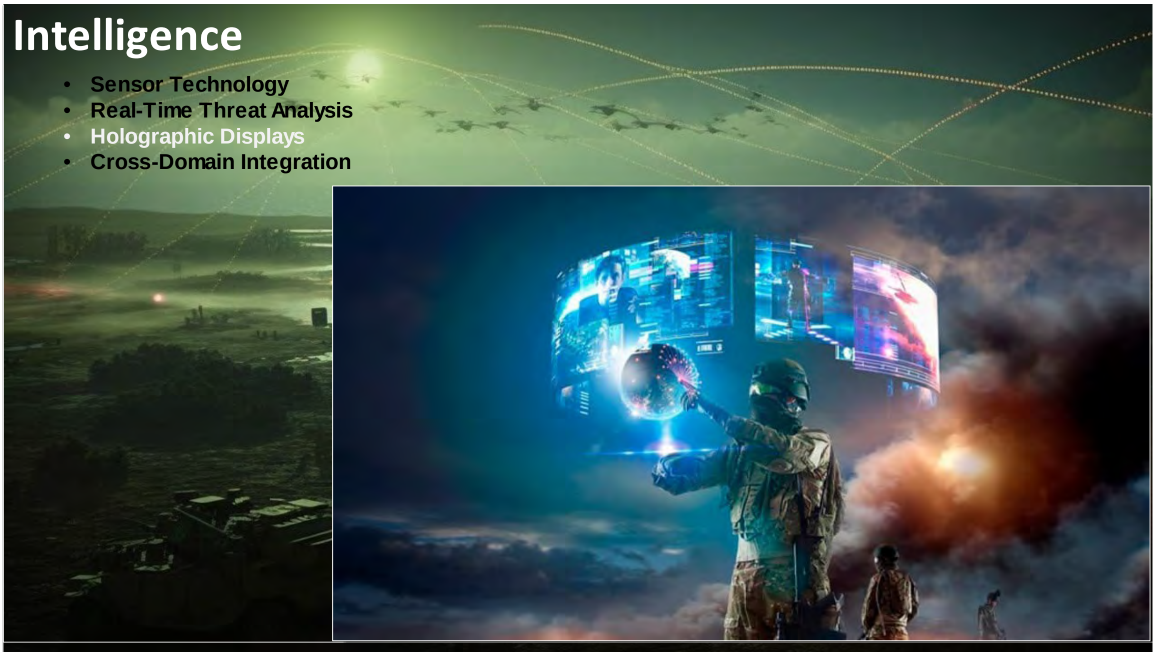

Command & Control
• 6G
• Common Operating Picture for HMT
• Capabilities Integration
• 6G
• Edge AI
• Neuromorphic Computing
Robotic
Non-Robotic
Broad Narrow
Non-Social Social
In
On
Out
Today
2040


Intelligence
• Sensor Technology
• Real-Time Threat Analysis
• Holographic Displays
• Cross-Domain Integration
Robotic
Non-Robotic
Broad
Narrow
Non-Social
Social
In
On
Out
Today
2040


Intelligence
• Sensor Technology
• Real-Time Threat Analysis
• Holographic Displays
• Cross-Domain Integration
06:11:34


Intelligence
Sensor Technology
Real-Time Threat Analysis
Holographic Displays
Cross-Domain Integration

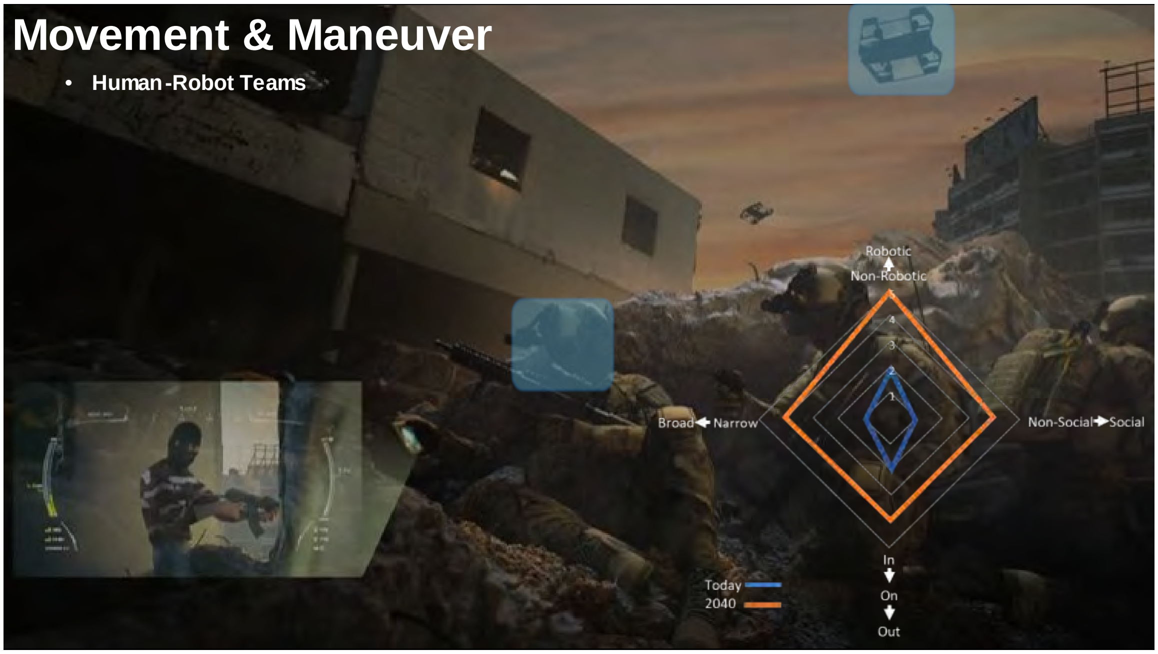

Intelligence
Sensor Technology
Real-Time Threat Analysis
Holographic Displays
Cross-Domain Integration
Locally


Intelligence
• Sensor Technology
• Real-Time Threat Analysis
• Holographic Displays
• Cross-Domain Integration

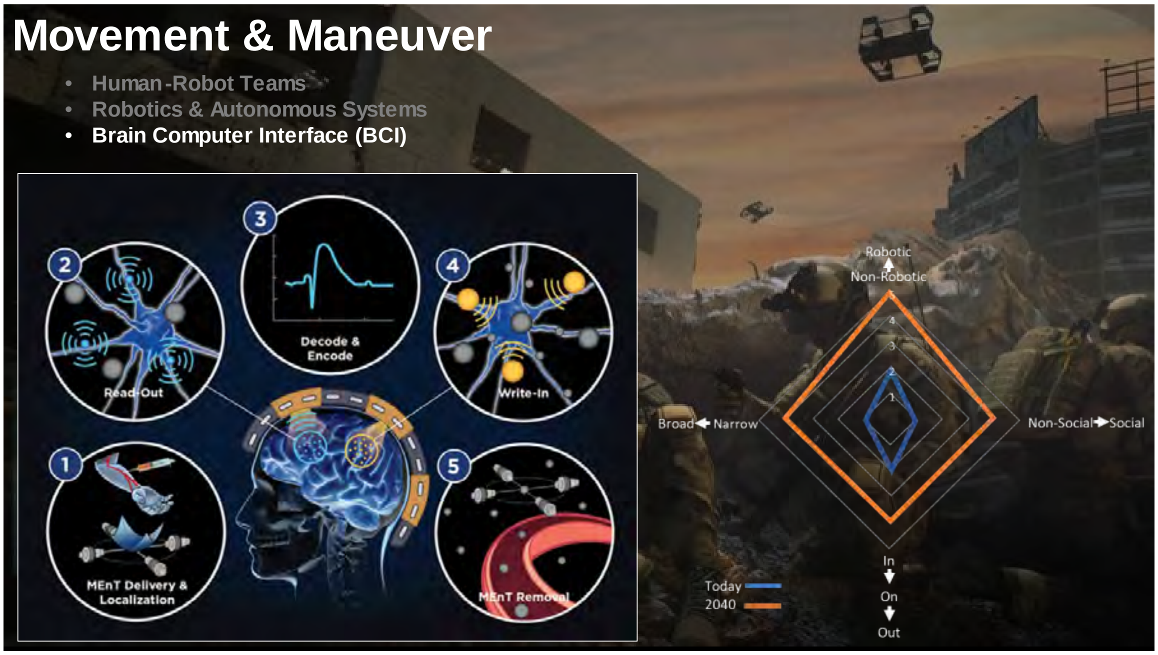

Intelligence
• Sensor Technology
• Real-Time Threat Analysis
• Holographic Displays
• Cross-Domain Integration
Robotic
Non-Robotic
Broad
Narrow
Non-Social
Social
In
On
Out
Today
2040


Intelligence
• Sensor Technology
• Real-Time Threat Analysis
• Holographic Displays
• Cross-Domain Integration
Robotic
Non-Robotic
Broad
Narrow
Non-Social
Social
In
On
Out
Today
2040

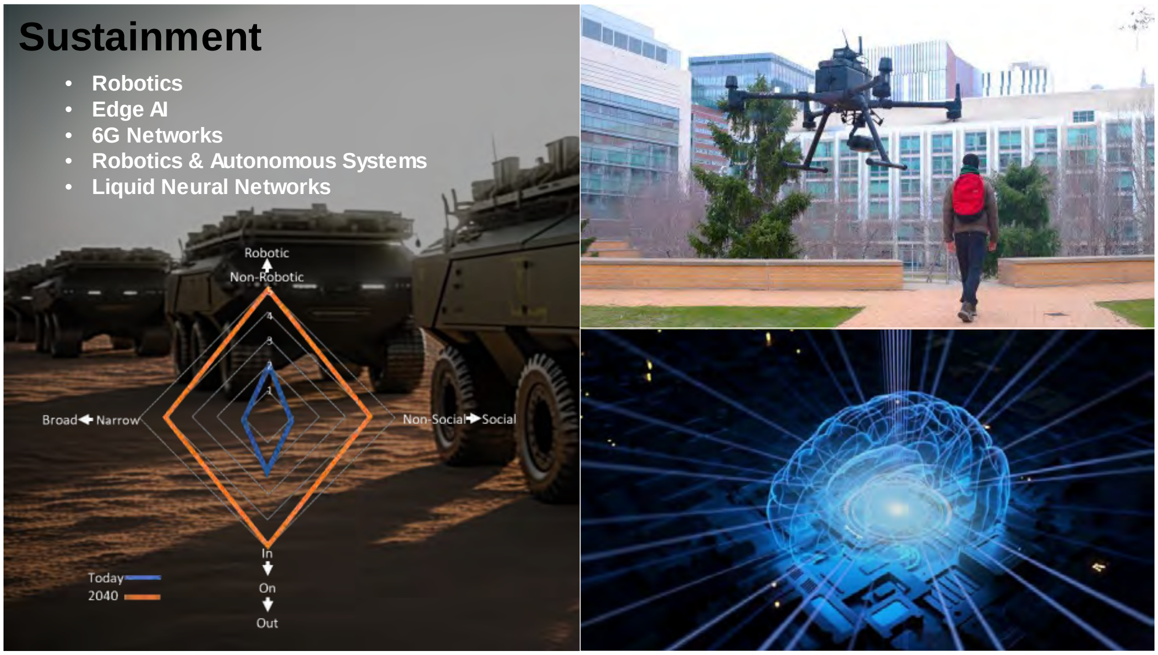

Intelligence
• Sensor Technology
• Real-Time Threat Analysis
• Holographic Displays
• Cross-Domain Integration

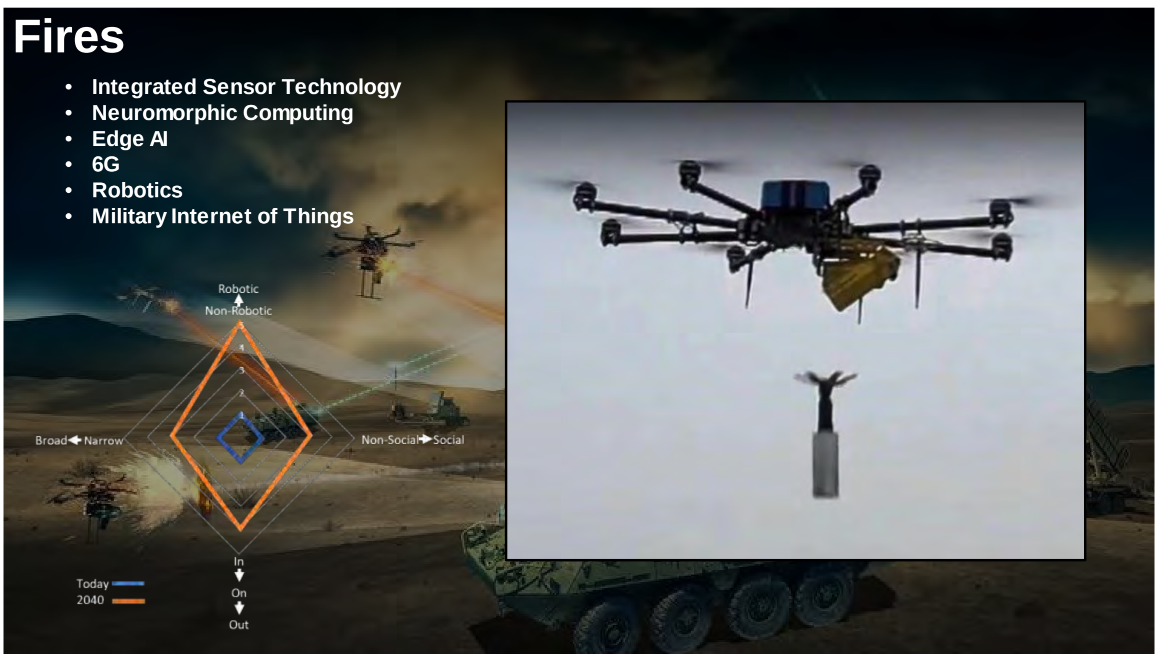

Movement & Maneuver
• Human-Robot Teams
Robotic
Non-Robotic
Broad
Narrow
Non-Social
Social
In
On
Out
Today
2040

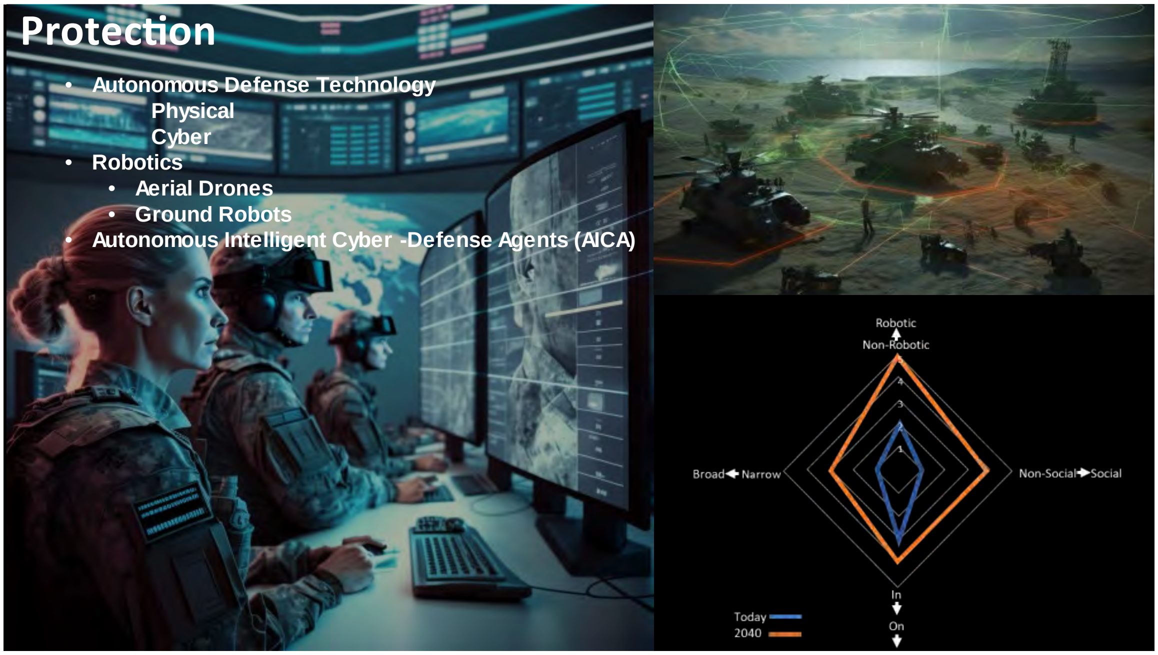

Movement & Maneuver
• Human-Robot Teams
• Robotics & Autonomous Systems


Movement & Maneuver
• Human-Robot Teams
• Robotics & Autonomous Systems
• Brain Computer Interface (BCI)
1
MEnT Delivery & Localization
2
Read-Out
3
Decode & Encode
4
Write-In
5
MEnT Removal
Robotic
Non-Robotic
Broad
Narrow
Non-Social
Social
In
On
Out
Today
2040


Sustainment
• Robotics
• Edge AI
• 6G Networks
• Robotics & Autonomous Systems
• Liquid Neural Networks


Sustainment
Robotics
Edge AI
6G Networks
Robotics & Autonomous Systems
Liquid Neural Networks
Robotic
Non-Robotic
Broad
Narrow
Non-Social
Social
In
On
Out
Today
2040


Fires
Integrated Sensor Technology
Neuromorphic Computing
Edge AI
6G
Robotics
Military Internet of Things
Robotic
Non-Robotic
Broad
Narrow
Non-Social
Social
In
On
Out
Today
2040


Protection
• Autonomous Defense Technology
Physical
Cyber
• Robotics
• Aerial Drones
• Ground Robots
• Autonomous Intelligent Cyber -Defense Agents (AICA)
Robotic
Non-Robotic
Broad
Narrow
Non-Social
Social
In
On
Today
2040

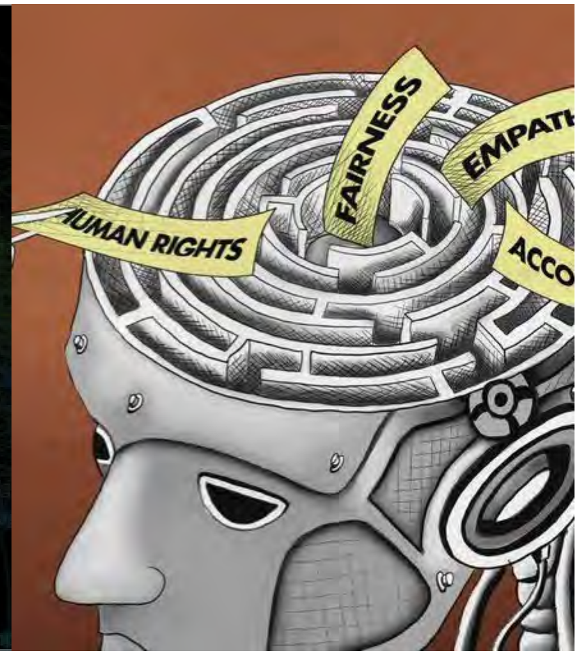

Protection
• Autonomous Defense Technology
Physical
Cyber
• Robotics
• Aerial Drones
• Ground Robots
• Autonomous Intelligent Cyber -Defense Agents (AICA)

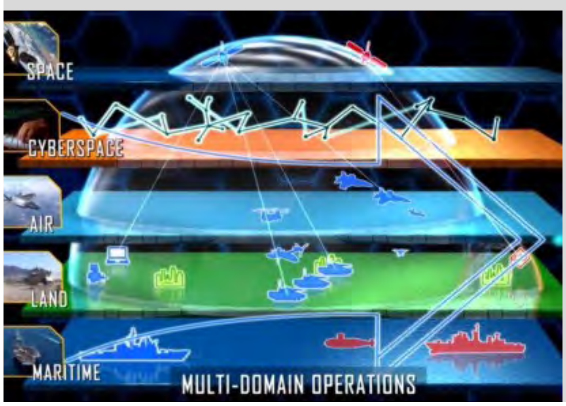

Protection
• Autonomous Defense Technology
Physical
Cyber
• Robotics
• Aerial Drones
• Ground Robots
• Autonomous Intelligent Cyber -Defense Agents (AICA)
Robotic
Non-Robotic
Broad
Narrow
Non-Social
Social
In
On
Today
2040


Legal
Ethical

Legal & Ethical Implications

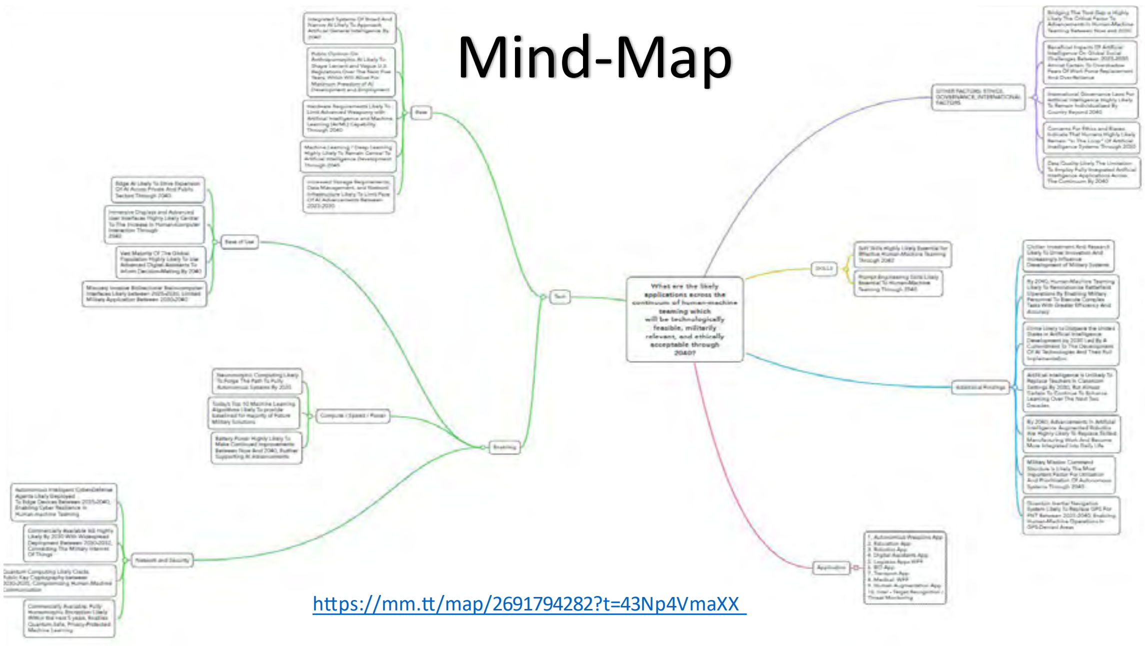
- Lack of Standardized Governance
- International Humanitarian Law
- Bias & Security
- Trust





Human Machine Teams Across Domains

- Human-Robot Teaming
- Human-AI Teaming
- Human Augmentation



SINGULARITY
HUMAN-MACHINE TEAMING

Contact Information:

LTC Owen Adams
owen.s.adams.mil@army.mil

Mr. Reginald Shuford
reginald.a.shuford.civ@army.mil

COL Nathaniel Stone
nathaniel.c.stone.mil@army.mil

LTC Nicole Washington
nicole.a.washington5.mil@army.mil

COL Dennis Weaver
dennis.j.weaver2.mil@army.mil


SINGULARITY
HUMAN-MACHINE TEAMING