AY 2022-2023

RIDING THE WAVE: MAXIMIZING THE OPPORTUNITIES AND MITIGATING THE RISKS OF ARTIFICIAL INTELLIGENCE DISRUPTION

ARTIFICIAL INTELLIGENCE INDUSTRY STUDY GROUP PAPER

DR. JAMES KEAGLE AND MS. LOURDES DUVALL
INDUSTRY STUDY FACULTY

The Dwight D. Eisenhower School
for National Security and Resource Strategy
National Defense University
Fort McNair, Washington, D.C. 20319-5062

Table of Contents

Executive Summary

The rapid evolution of artificial intelligence (AI) is disrupting the world. New capabilities demonstrate AI's immense opportunities, but they also bring great risks: unsustainable power demand, worker displacement, and new ethical dilemmas that challenge global stability. As the People's Republic of China pursues its goal to become the global AI superpower by 2030, the U.S. must act quickly and iteratively in collaboration with allies, partners, and industry to channel the disruption toward positive outcomes in an increasingly AI-driven world.

This paper concludes four months of engagements, research, and analysis by the Artificial Intelligence Industry Study Seminar at the National Defense University Eisenhower School of National Security and Resource Strategy. It presents key actors and salient trends within the strategic environment; the structure, conduct, and performance of major AI industry players; applications of AI that improve society and government; and threats related to computing power, data, people, and ethics—all of which affect society and national security.

Recommendations focus on immediate needs in areas where the United States (U.S.) government is uniquely positioned to help the U.S., allies, and partners safely ride the wave of disruption:

1. **Prepare for Regulation to Compel Industry Transparency; Focus on Efficient Edge Computing for Defense**
    - Monitor computing power needs in preparation for regulation.
    - Pursue low-power, edge options through research funding, prototyping and testing.
2. **Sponsor Grassroots Ecosystems and Loan Programs for Skill-building, Up-skilling, Retraining, and Job Placement**

- With state and local governments and industry, fund grassroots ecosystems and innovation hubs, to mitigate the risks of workforce disruption and spur innovation.
    - Fund educational loans for students seeking degrees in science, technology, education, and mathematics (STEM) fields and expand trade school links with industry partners focused on critical-skills shortfalls.

3. **With Allies, Partners, and Competitors, Establish Global Norms to Promote Safe Civil and Commercial AI Use and Reduce the Greatest Risks for Military Use**
    - With allies, partners, and near-peer adversaries form a global entity to license major generative AI systems and create ethical guidelines and standards for application of AI in society and military use.

Mankind has reached an inflection point that requires the world's leaders to provide guidance and establish best principles to reduce risks and create positive outcomes. To ride this initial wave of change brought by AI, the U.S. government must rally allies, partners, and adversaries alike to create computing-power-requirements transparency and prioritize efficient edge computing, invest in innovation and cultivate the right skills to strengthen workforce resiliency, and develop norms through ethical standards and guidelines.

Disruption Is Here: Will the U.S. Ride the AI Wave?[I]

The rapid evolution of artificial intelligence (AI) is disrupting the world. It promises to usher in utopia or the apocalypse or somewhere in between, depending on whom one asks. New capabilities demonstrate that AI offers immense opportunities to improve life: it is advancing health care, enhancing process efficiency, and strengthening military capability. But AI also brings great risks: it may create an unsustainable power demand, displace large numbers of workers, and introduce new ethical dilemmas that challenge global stability. As the United States (U.S.) grapples with government priorities, the People's Republic of China (PRC) is using its significant resources and technological capabilities to pursue its goal to become the global AI superpower by 2030. The U.S. must act quickly and iteratively in collaboration with allies, partners, and industry to channel the disruption toward positive outcomes and maintain its strategic advantage in an increasingly AI-driven world. To ride the current wave of disruption and brace itself for the AI waves to come, the U.S. must create computing-power-requirements transparency, invest in innovation and cultivate the right skills to strengthen workforce resiliency, and develop norms through ethical standards.

This paper concludes four months of engagements, research, and analysis by the Artificial Intelligence Industry Study Seminar at the National Defense University Eisenhower School of National Security and Resource Strategy. It presents key actors and salient trends within the strategic environment; the structure, conduct, and performance of major AI industry players; applications of AI that improve society and government; and threats related to computing power, data, people, and ethics—all of which affect society and national security.

[I] Much of this research paper is based on individual papers from the AI Industry Study, with individual authors' consent. Those papers will be stored within the NDU Archives and can be retrieved with proper permissions. No further references to individual papers will be included in the remainder of the paper.

Because the industry is changing the world daily, this paper highlights key threats and opportunities at a point in time. Recommendations focus on immediate needs in areas where the U.S. government is uniquely positioned to build the coalitions, institutions, and mechanisms to manage the disruptions across society and lead engagement with industry and global leaders for the benefit and safety of all. Furthermore, Appendix A provides observations and insights on AI industry relevance to the U.S.-China strategic competition, and offers policy prescriptions across the diplomatic, informational, military, and economic instruments of national power to protect American interests, allies, and partners against the backdrop of tensions between the PRC and Taiwan.

Influences on the Strategic Landscape—for Better or Worse?

AI is crashing over the world today like a massive wave, disrupting how people live, work, interact, and learn. At a geostrategic level, these new capabilities are forcing governments to revisit how they wage war, secure their economic prosperity, cultivate a relevant workforce, and govern. The AI landscape is changing nearly every day, pushed by multinational technology giants like Microsoft (through the OpenAI large-language model ChatGPT), Google (via its competitor Bard), Amazon Web Services (through cloud services), and Nvidia (through computing innovation)—all of which are aggressively developing AI capabilities to dominate the marketplace.

AI is crashing over the world today like a massive wave, disrupting how people live, work, interact, and learn.

Numerous factors are converging to shape the strategic landscape for better and worse. For example, emerging technologies are expanding the ability of networks to operate across technical platforms and functional domains. It is also evidenced in how cell phones and

computers work together seamlessly, and in the way military services share data more easily. These advancements are increasing the distance between the haves and have-nots, as wealthier individuals, companies, and countries adopt advanced technologies. The recognition of data as a coveted commodity is changing how industries engage customers and creating privacy concerns. Digitization enables faster storage, processing, and transmission of data and generating immense power demands.

As technology advances accelerate, it is increasingly difficult to predict AI's trajectory and societal impact. Like the Internet, AI has the potential to transform society fundamentally. Like the Internet, AI may alter the way industries function. The implications for individuals and companies that cannot pivot and change with new developments may be catastrophic. Conversely, AI advancements may create opportunities for new entrants and startups to flourish and increase productivity in ways that offset effects of the U.S.'s aging workforce and slowing population growth. But today, no one knows precisely how AI will change our lives for the better or what challenges will emerge.

AI-Driven Fears

The not-knowing leads to speculation and fear. Dr. Geoffrey Hinton, "The Godfather of AI," who began pivotal AI work at the University of Toronto in 2012, punctuated these fears on May 1, 2023, when he resigned from Google so he could speak more freely about the risks of the capability—even the ones that already exist today. "It is hard to see how you can prevent the bad actors from using it for bad things," he said during one of many interviews he gave to news outlets worldwide. "The idea that this stuff could actually get smarter than people—a few people believed that," he added. "But most people thought it was way off. And I thought it was way off. I thought it was 30 to 50 years or even longer away. Obviously, I no longer think that."[1] Hinton's

resignation from Google followed a March 30 letter signed by Tesla and SpaceX chief executive Elon Musk, other business leaders, and academics calling on OpenAI, Microsoft, and Google to stop training more powerful AI systems to allow the industry to assess the potential risks. "Should we automate away all the jobs, including the fulfilling ones? Should we develop nonhuman minds that might eventually outnumber, outsmart, obsolete and replace us?" the letter said. "Powerful AI systems should be developed only once we are confident that their effects will be positive and their risks will be manageable."[2] At this point, can the wave be stopped—or even slowed?

AI-Driven Threats and Opportunities in Business

Despite these efforts to slow AI development and resulting change, the wave is building rapidly. With the launch of ChatGPT in November 2022, large language models (LLMs) put power at the fingertips of every person with an Internet-accessible device. Generative AI for graphics enabled photographer Jonas Bendiksen to create a deepfake that the photography community initially lauded for photographic excellence.[3] What could happen if bad actors were to leverage the enormous power of these AI technologies to fuel widespread deception and societal chaos?

The risks are high, yet AI is transforming society in previously unimaginable ways. For example, Nvidia's powerful graphics processing units (GPUs) and other specialized hardware have enabled the emergence of digital-twin capabilities that are changing the way factory floors are organized and self-driving cars are trained.[4] Near daily announcements indicate impending AI-driven workforce shifts. In May 2023, IBM's anticipated AI-driven productivity and process improvements led the company to publish its intent to freeze hiring of human resources staff.[5] No industry is isolated from the disruption. In March, Bloomberg announced its plans to

build "BloombergGPT," a large language model specific to the financial industry.[6] In April, Forbes reported 19 ways AI may revolutionize health care.[7] Even tech industry giants are taking their plans back to the drawing board after recent advancements.

Threats and Opportunities in AI-enabled Competition Among Nations

AI is not affecting only the business world, it is playing a central role in the strategic competition among nations. Today's nascent AI capabilities are redefining the character of warfare, intelligence, and security—changing the inputs to human reason and shifting war's fulcrum from chance to probabilities. AI is already implemented in some unmanned systems, advanced sensors, and weapon systems. These AI deployments facilitate more effective, efficient, and lethal military operations while protecting human operators from battle wounds. The integration of AI has helped capabilities catch up to operating concepts, allowing a warfighter's first contact to be made via a sensor to support survivability. For intelligence operations, algorithms can process vast amounts of data and identify patterns impossible for humans to detect, enabling better insight and more effective targeting of adversaries.

AI's potential in other areas of national concern is significant. AI will likely bring changes to the global economy by revolutionizing industries, creating markets, and boosting productivity. As AI-advancements become more integral to the global economy, countries that lead in AI research and development will have a major advantage—with obvious implications for U.S. national security and economic strength. Additionally, as AI becomes more ubiquitous, the threat of cyberattacks and information warfare will increase. Adversary employment of AI to conduct sophisticated cyberattacks and manipulate information at scale could have serious national security implications, and the democratization of AI will afford non-state actors and individuals potential to use AI for nefarious purposes.

Threats and Opportunities in AI-enabled Strategic Competition with China

AI is central to the 21st century U.S.-China rivalry. Chinese Communist Party (CCP) leader Xi Jinping is investing trillions of yuan into a strategic technology he believes is critical to all dimensions of national competitiveness, hoping to shift the balance of military power in Beijing's favor.[8] Today, the U.S. leads in nearly all aspects of the AI ecosystem, according to Stanford University's Global AI Index, which ranks nations on their capacity for AI by examining 143 indicators across talent, infrastructure, operating environment, research, development, government strategy, and commercial sectors.[9] However, China may be narrowing the lead, spurred by a command economy, a military-civil fusion strategy that blurs the lines between military and civilian use, and significant funding—some of which comes from U.S. investors.[10] Xi has set the goal of global AI supremacy by 2030.[11] To achieve that, "China is expected to more than double its investment in AI to nearly $27 billion by 2026, with more than half of the spending targeted at the hardware market," according to a recently released report from the International Data Corporation (IDC).[12]

While a lack of transparency in Chinese financial reporting makes it difficult to ascertain the true level of Chinese investment in AI across government and industry, what is clear is that the U.S. is also taking the competition seriously. U.S. AI spending (government and industry) is expected to grow to $120 billion by 2025, representing a compound annual growth rate of 26 percent over the 2021-2025 forecast period. Moreover, all 19 U.S. industries profiled in the latest Worldwide Artificial Intelligence Spending Guide from IDC are forecast to deliver AI spending growth of 20 percent or more. The U.S. also accounts for more than half of all AI spending worldwide.[13]

The DoD is driving some of that growth, integrating AI into its military and business operations to stay ahead of state competitors. In fiscal year (FY) 2022, DoD invested $847 million to support AI emerging technologies including machine learning, quantum science, neuroscience, novel engineered materials, understanding human and social behavior, engineered biology, and manufacturing sciences. A Georgetown University study published in January 2022 found that China's military investment in AI was roughly equivalent to that of the U.S.[14] Again, the CCP's military-civil fusion strategy and general lack of transparency makes it difficult for outsiders to ascertain the true extent of China's investments in AI for military use.

The US AI Industry Is Strong and a Critical Government Partner

A deliberate analysis of the AI industry and its associated markets through the "structure-conduct-performance" framework illuminates marketplace dynamics and broader macroeconomic implications. The AI industry has recently experienced meteoric growth as machine learning, natural language processing, and computer vision have transformed various sectors, including government, military, health care, finance, manufacturing, and transportation. Additionally, "the size of the global AI industry was valued at $428.0 billion in 2022 and is projected to grow from $515.3 billion in 2023 to $2.0 trillion by 2030, exhibiting a compound annual growth rate of 21.6 percent."[15]

Structure

A vast body of information suggests that the AI industry comprises a wide range of companies, including hardware manufacturers, software developers, and data firms. Key players include Google, Microsoft, IBM, Intel, Nvidia, and AWS, among others. Based on revenue and market share, these companies dominate the AI market and generate most of the innovation and significant technological development in the AI industry.

Despite the concentration of market power in a small number of firms, the potential for new entrants into the AI market is considered significant. Why? According to a recent report by PricewaterhouseCoopers (PwC), the cost of AI research and development has decreased substantially in recent years, making it easier for start-ups and small firms to enter the marketplace. This trend has accelerated as Meta recently open-sourced its large language model LLaMa, allowing anyone to use the powerful tool for free.[16] PwC also notes that the potential for cross-industry collaboration and partnerships is high, particularly in sectors such as health care and finance, where AI has the potential to make a significant impact.[17] Nevertheless, new entrants wishing to compete at the highest levels of the AI industry may experience higher barriers to entry. More specifically, this level of competition requires access to increased technical expertise, more data, and more expensive computational resources—all of which can be incredibly difficult to obtain without access to significant levels of capital. Innovation is needed to find new ways to reduce computing resource needs or computing power. IBM is researching and experimenting with analog processing as a solution. Nvidia continues its work with more and more sophisticated Graphics Processing Units (GPUs).

Chinese companies are also driving the structure of the global AI industry and, in one instance, triggering alarm among politicians in the U.S. multibillion-dollar technology firms such as Baidu, Tencent, Megvii, Sensetime, and Bytedance are developing and exporting AI-driven tools in a bid to expand their digital footprint with nations participating in the Belt-Road Initiative. For instance, telecommunications giant Huawei is working with Moroccan government officials to adopt Huawei AI capabilities to bring greater operational efficiencies to the country's banks and financial institutions.[18] In the U.S., Montana banned the popular social media application TikTok (a Bytedance subsidiary) on May 17, 2023, in an effort to protect

residents' private information from being accessed by China—a contention Beijing and TikTok officials have long disputed.[19] Montana is the first state to ban the app, possibly signaling similar measures in other states as momentum against Chinese companies' influence in America grows.

Conduct

The conduct of participants in the AI industry is a topic of significant concern to regulators, academics, and consumers. More specifically, many worry that firms might engage in anti-competitive practices, such as price fixing or collusion, to maintain their market share.[20] Furthermore, there are concerns that the lack of transparency in AI decision-making could lead to bias and discrimination against certain groups of people.

To address these concerns, governments and regulatory agencies are starting to implement policies and regulations to help govern the use of AI. For instance, Canada has developed a pan-Canadian AI strategy, and the EU has developed a set of ethical guidelines aimed at promoting transparency, accountability, and fairness in AI decision-making.[21] Similarly, the U.S. Federal Trade Commission issued guidelines on the use of AI in advertising and marketing, which require firms to be transparent about how they employ AI and related technologies to avoid making false or misleading claims.[22]

Performance

Based on growth rates, profitability, and innovation levels, the performance of the AI industry has been remarkable and currently shows no signs of slowing; however, there are potential economic challenges to consider. For instance, AI automation is projected to displace employees across the global workforce significantly. As noted previously, IBM recently announced a hiring pause for jobs that AI can do (impacting about 7,800 employees); and Goldman Sachs recently reported that generative AI could eventually replace an estimated 300

million jobs globally.[23] While proponents of noted 20th century economist Joseph Schumpeter's theory of creative destruction argue that this transfer of human capital is beneficial and will ultimately increase macroeconomic productivity, critics suggest the interim effects could be economically destabilizing in both the short- and long-term. In May 2023, the *Washington Post* published an online tool that leverages researchers' "AI Exposure Score" and indicates the degree professions will be affected by AI. It suggests few are safe from AI disruption.[24]

Significant Factor Conditions

Several essential inputs contribute to the production of goods and services within the AI industry and shape its economic performance. In particular, five inputs have an outsized impact: technological infrastructure, data availability, skilled workforce, research and development, and funding and investment.

Technological infrastructure is the foundation fo the development and advancement of AI. Moore's Law is no longer proving true, and progress in technology and materials science is critical to address the coming crisis driven by computing power requirements. Factors such as Internet connectivity, cloud computing resources, and high-performance computing play a crucial role. Separately, data are considered the "lifeblood" of AI models, and the availability of large and diverse datasets is vital for training and improving their accuracy and performance. This training is overseen and conducted by highly skilled workers such as data scientists, AI researchers, machine learning experts, software engineers, and materials scientists who are essential to driving the research and development necessary for innovation in the industry. Furthermore, adequate funding and investment are critical to afford the cost of research, development and innovation. Additionally, access to venture capital and government funding plays a vital role in achieving the commercialization and profitability of AI technologies.

AI Offers Opportunities to Society and Government

AI has tremendous potential to improve society, commerce, and governance. Already, AI has greatly improved the quality of human life through innovations in predictive healthcare, adaptive education, and optimized crisis response. Many businesses and industries are maximizing their productivity and efficiency through reliance on AI-optimized supply chains and extensive use of autonomous robotics in manufacturing. AI empowers governments, organizations, and communities to build a high-performing ecosystem to not only serve the people within the geographical borders of the countries, but also humanity at large. The following section explores how existing AI applications have changed the landscape within DoD for weapon systems and acquisition processes and within the healthcare community through applications in behavioral health and data processing that mitigate current healthcare worker shortages and how future applications show promise of even more benefits. These examples are representative of military-specific applications and whole-of-society applications, both of which lead to strengthening national security.

AI Is Strengthening Military Advantage and Deterrence

AI provides options to strengthen deterrence and military advantage in today's dynamic strategic environment. Machine learning – the branch of AI that attempts to mimic human learning through complex algorithms and trial-and-error of large data sets – can enhance military technologies by automating systems to react faster to potential threats, identifying and tracking targets while integrating multiple sensors and data sources, improving situational awareness, and enabling systems to make more informed decisions in real-time. For example, the U.S. Army's Integrated Visual Augmentation System[25] and the U.S. Marine Corps' Information Support to Operations are two disparate capabilities that the two services have been experimenting with for

several years and demonstrate how AI software could federate and categorize data into mission-relevant and actionable information or intelligence in two very different applications.[26] Numerous existing, fielded weapon systems already use some form of automation, but they are generally employed in a defensive manner with a human-in-the-loop featuring supervisory controls, such as the AEGIS ballistic missile defense, Phalanx Close-in Weapon System, PATRIOT air and missile defense system, and counter-battery radars.

AI in weapon systems has the potential beyond deterrence and defensive applications and can achieve military goals while keeping soldiers out of harm's way. Lethal autonomous weapon systems (LAWS), offensive weapons, also provide options to strengthen military advantage. LAWS operating at the forward edge of the battle area or fringes of sensor-shooter networks enhance situational awareness and survivability of human operators. The U.S. strategy for implementing LAWS should be based on one principle: The warfighter will not make first contact with the enemy. Autonomous systems and sensors powered by AI, lethal or not, will make first contact. Drone swarms are probably the best know example of this emerging capability. They are relatively inexpensive, low-risk platforms, have already been used for surveillance, reconnaissance, and targeting in the Russia-Ukraine conflict.[27, 28]

Lethal autonomous weapon systems operating at the forward edge of the battle area or fringes of sensor-shooter networks enhance situational awareness and survivability of human operators.

Meanwhile, digital twins are enabling less expensive and faster design engineering, training, and predictive maintenance actions. The aviation community uses a digital twin of the

AH-64 Apache attack helicopter to simulate performance and predict maintenance needs by collecting data from sensors on the helicopter and feeding it into the digital twin.[29] Pilots train with a digital twin in a simulator that accurately reproduces the cockpit and flight controls of the actual aircraft, providing a safe and controlled environment that improves skills and reduces the risk of accidents during actual flight operations. The advancements in AI technologies are having a significant positive impact on national security, enhancing military effectiveness and supporting qualitative advantages over potential adversaries.

AI Is Enabling Defense Acquisition Process Improvements

Nascent efforts to use AI to navigate the ponderous DoD Acquisition System are also bearing fruit. The DoD Acquisition System is purposely onerous, time-intensive and compliance-based to reduce risk before new equipment is provided to the warfighter. The RAND Arroyo Center has developed an underlying analytic infrastructure that uses AI to index and discover relevant contract documents. Arroyo Center researchers are also working to provide additional analytic capabilities on unstructured contract data to maximize the utility of the existing infrastructure. The Institute for Defense Analyses (IDA) conducted a feasibility study to determine if machine learning could be used to analyze contracts to predict program success and found that "text analytics and machine-learning algorithms were well suited for extracting information from contracts and converting this information into a structured dataset."[30] Meanwhile, the Chief Digital and Artificial Intelligence Office (CDAO) is testing a prototype generative AI application, "AcqBot," to accelerate the contract-writing process based on OpenAI's ChatGPT. This combined research sets the stage to use the massive amount of unstructured data to generate many tedious requirements documents and assess program risk during execution, which will enable quicker fielding to the warfighter. Two retired lieutenant

generals, Jack Shanahan of the U.S. Air Force and Michael Groen of the U.S. Marine Corps, envisioned potential applications for generative AI and that "probably the places that make the most sense in the near term… are those back-office business from personnel management to budgeting to logistics," which is encouraging for additional acquisition process improvements.[31] The success of AcqBot and other prototypes offer promise for AI applications to further streamline the Defense Acquisition System.

AI Is Supporting Behavioral Health for the Joint Force

Generative AI in behavioral health shows extraordinary potential as a care extender for the DoD as the department looks to increase the well-being of the joint force. Early studies indicate that generative AI has the potential to aid behavioral therapists in analyzing patients' linguistic patterns to enhance diagnostic accuracy and identify crises.[32] It can detect subtle verbal cues before manic episodes and improve treatment effectiveness by identifying early signs of response and quantifying changes in patient communication, providing real-time clues for mental status exams.[33] Generative AI can offer psychiatrists the latest and pertinent research on treatment options for addressing specific symptoms of individual patients, going beyond their general diagnosis. Such capability would exponentially increase the effectiveness of providers and provide a highly personalized approach to the care of servicemembers and their families. A significant benefit of AI in behavioral health is structural, namely the ability to reach patients in remote areas where therapy services are scarce.[34] Clinical studies suggest this "edge capability" has demonstrated efficacy by reducing depression and anxiety symptoms, aiding patients who have autism and schizophrenia, and increasing the overall quality of life for patients.[35]

AI May Mitigate Health Care Worker Shortages

Advances in AI also promise to revolutionize the health care industry to mitigate the effects of severe worker shortages.[36] The DoD is not immune to these challenges and the director of the Defense Health Agency, responsible for delivering care to the military community, declared the worker shortage a crisis and called Congress to act.[37] According to World Economic Forum (WEF), AI-enabled systems can help reduce waiting times and improve health care systems' efficiency, reducing the burden on the limited health care workforce.[38] AI applications (emerging from companies such as IBM) can analyze enormous amounts of data more quickly than humans and improve the ability for professionals to deliver timely treatment.[39] The time saved through AI-driven efficiencies can allow doctors and nurses to devote time and attention to assess and diagnose patients who are experiencing complex maladies.

Data generated from medical imaging accounts for 90 percent of all healthcare data, and these images are becoming more complicated with in-depth illustrations of the body, down to the cellular level.[40] Accurately analyzing these sophisticated images is difficult and time-consuming for humans, but researchers at the Massachusetts Institute of Technology (MIT) developed a machine learning algorithm that can register medical images 1,000 times faster than humans or in less than two minutes, with graphics processing cutting that time down to less than two seconds with substantially improved the ability for the professionals to deliver timely treatment.[41]

DoD has implemented the largest electronic health records system in the world, consolidating millions of records into a central location that is accessible in seconds.[42] Projections for the next decade show AI producing breakthroughs in predictive care, allowing for early treatment, delivering adaptive experiences for patients and providers, and altering the

dynamic of care where hospitals will only be used for acute illnesses and highly complex procedures.[43] If these projections are realized, AI will be a healthcare force multiplier through cost savings, time savings, and improved accuracy.

AI Presents Risks for Society and Government

The increasing use of AI also presents significant risks to society. Technology companies are setting the agenda, aggressively developing AI platforms to gain an edge against competitors and win market share. They answer to their shareholders and not to the U.S. government, which is trying to leverage AI advances to secure American economic prosperity and enhance military capabilities to compete and deter China. Across the Pacific, Beijing is fostering an AI ecosystem of its own to enhance all instruments of national power and supplant the rules-based global order enforced by Washington. This section discusses some of the biggest AI-related issues facing American leaders, including shortfalls in computing power and data sharing; efforts to strengthen workforce resiliency against AI-driven disruptions; and a lack of ethical norms to govern both societal interactions and the use of AI on the battlefield.

Compute May Become the Next "Natural Resource" Issue

AI advancement critically depends upon exponentially increasing computing power or what some might call "brute compute."[44] A 2022 MIT study showed that statistically, "increases in computing power are at least as important as all other factors put together."[45] Exponential increases in computing power are needed to achieve linear improvements in performance.[46] AI capability against humans can be plotted based on computational power over time (Figure 1). Chess algorithms vaulted from novice capability in the late 1950s to super-human status today by taking advantage of a 10^8 increase in computing power or about 38 percent improvement per year.[47] If advances in computing power stall, AI advances would as well.

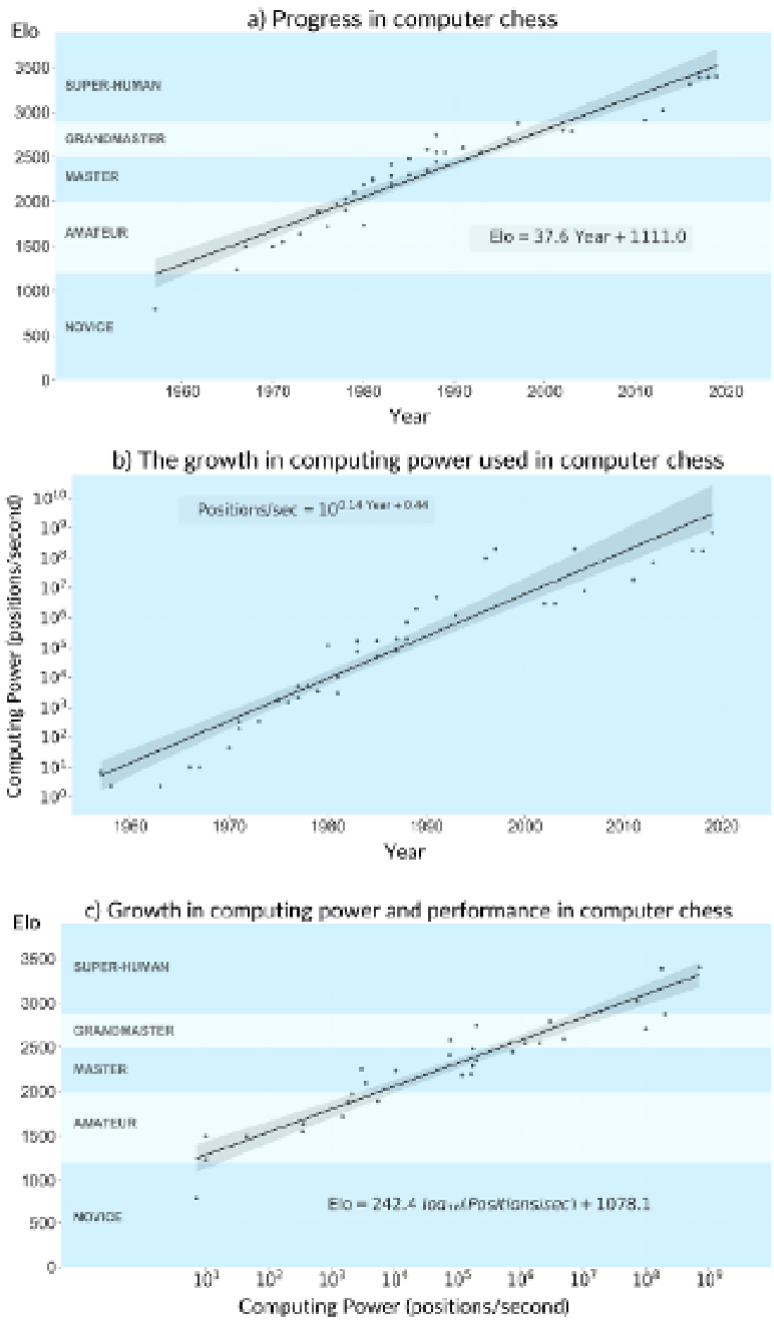

Figure 1. Exponential Computing Power Leads to Dominance in Chess[48]

Moore's Law, which has been the engine behind much of AI's (and humanity's) progress over the last half-century, is now fading. Gordon Moore famously postulated that the number of transistors on a chip would double every two years, leading to a proportional increase in computing power and a decrease in computing cost.[49] However, progress has slowed in recent

years as chip designers hit the known bounds of physics. Overcoming these atomic-scale challenges requires exorbitant capital expenditures for engineering and fabrication. For example, a state-of-the-art three-nanometer chip design may cost $650 million,[50] while a fabrication facility costs $19.5 billion.[51] Chip performance has flattened, but costs continue to rise exponentially. In this new paradigm, AI developers have learned to leverage the parallelization capability of GPUs to continue exponential computing growth through scale.

GPU use as accelerators for AI began to skyrocket after the AlexNet convolutional neural network architecture dominated a high-profile 2012 image-recognition contest. AlexNet became the first successful implementation of deep learning and kicked off the modern AI era.[52] During the 50 years before AlexNet, AI training power generally followed Moore's Law and doubled every two years. Since 2012, AI computing power requirements have doubled every 3.4 months (Figure 2). By 2017, AlphaGo Zero possessed a stunning 300,000-times advantage increase over AlexNet. LLMs continue this trend today.

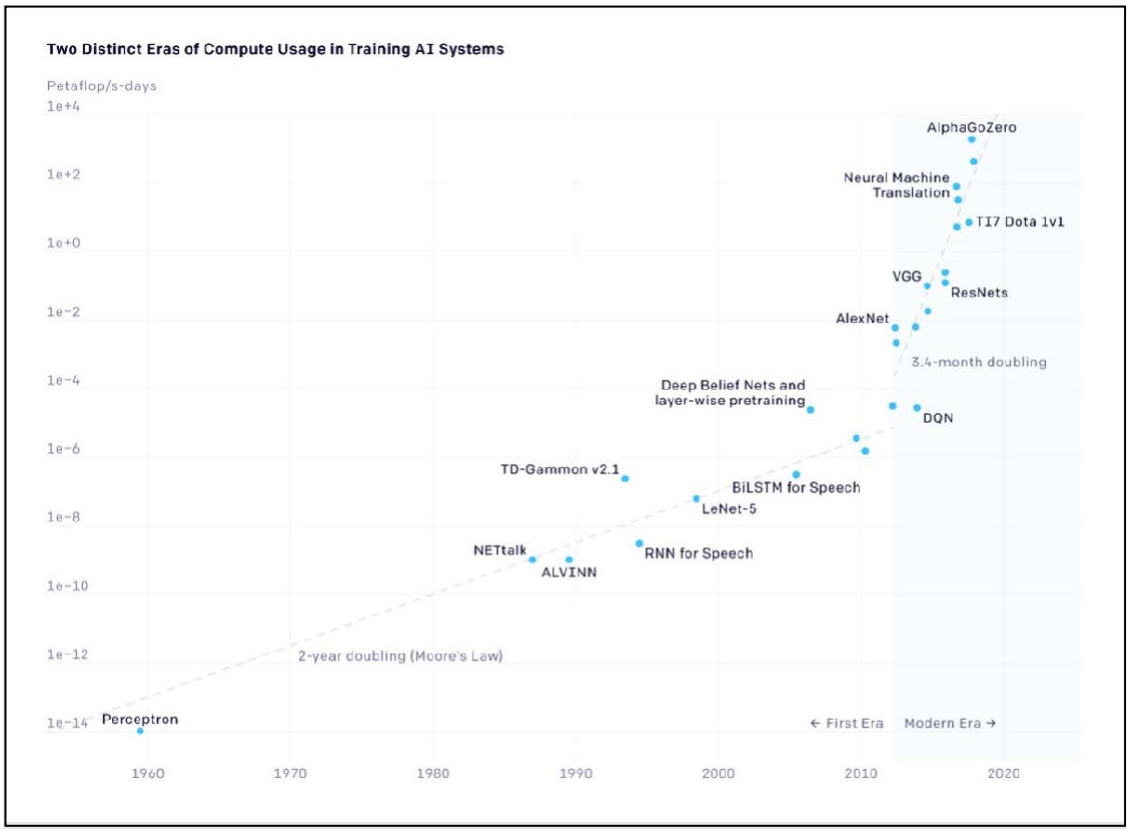

Figure 2. Exponential Increase of AI Compute Usage[53]

Since ChatGPT's release, LLMs and generative deep-learning models have proliferated at an unprecedented pace, but this explosion only occurred after Microsoft assisted OpenAI with achieving scale. Microsoft invested billions in OpenAI and linked tens of thousands of Nvidia GPUs in its Azure cloud to train GPT-3.5, the basis for ChatGPT.[54] Countless competitors, including Google and Meta, have followed suit by launching their own LLMs trained on massive GPU clusters. According to industry insiders, hundreds of startups are pursuing new LLMs, with individual companies seeking to buy as many as 16,000 GPUs.[55]

Some developers now refer to generative AI as simply a "scale-up problem,"[56] but the costs of the brute compute approach are overwhelming. Top-of-the-line Nvidia H100 GPUs now cost $40,000 each.[57] With this extreme price tag, only the wealthiest companies and investors can afford larger, more powerful models. OpenAI CEO Sam Altman recently admitted that his

company spent more than $100 million to train its latest release, GPT-4, and the industry needs to find more practical methods for model growth.[58] If the exponential cost growth trend continues, by 2025 the largest models will have a price tag equivalent to 2.2% of U.S. GDP or the entire Apollo program. Clearly, this path is not sustainable.[59] Unfortunately, the hardware price tag is only half the battle.

The exponential demand for computing power brings a troubling environmental burden. Moore's Law no longer provides the efficiency gains it once promised, as growing AI model sizes demand ever more electrical power and cooling. As a Meta research paper concluded, "resource requirements for strong AI scaling clearly outpaces that of system hardware,"[60] and "the growth of AI in all dimensions outpaces the efficiency improvement at scale."[61]

As model sizes grow, some companies are becoming less transparent about their computational requirements and environmental impacts. OpenAI, for example, ironically stopped sharing detailed information about its latest models.[62] According to a Stanford University study, training GPT-3 consumed enough energy to power the average American home for 121 years, while the carbon footprint was equivalent to one passenger jet flying between New York and San Francisco 507 times.[63] Training GPT-3 in Microsoft's most advanced data center would also require 700,000 liters of fresh water for on-site cooling or enough to fill a nuclear reactor cooling tower[64] With another 2.8 million liters of off-site water required for power generation, the environmental impacts of GPT-3 training are staggering. OpenAI has not released data on GPT-3.5 or GPT-4 training, but trends suggest these impacts may be an order of magnitude higher. With hundreds of companies now training their own AI models, the combined environmental impacts could quickly become overwhelming.

To make matters worse, reports often narrowly focus on the computing required for training models and ignore the total lifecycle or "embodied" cost. According to Meta research, training may only account for 20 percent of a model's energy usage. Pre-training experimentation accounts for the initial 10 percent, but inference (running a trained model) accounts for the vast majority at 70 percent.[65] Therefore, the total lifecycle energy usage of GPT-3 might power an American home for 605 years. Other researchers believe the monthly electric bill for heavily used models like ChatGPT could power an entire town of 25,000 homes.[66] ChatGPT's total water impact is unknown, but holding a short conversation with the AI equates to dumping out a 500-milliliter water bottle.[67]

This resource demand trajectory is unsustainable. According to the Semiconductor Research Corporation (SRC), global computing energy, which already accounts for 2 percent of all consumption, is doubling every three years, while global energy production only increases by 2 percent annually.[68] Utility providers cannot keep up with exponential demand. Revolutionary changes, particularly for inference computing, are desperately needed to safely continue the exponential growth of AI.[69]

Future energy needs could be mitigated by looking to the past. Analog computing, once thought dead, may return to save the digital world. These systems were not as accurate or flexible as modern digital machines but provided extremely efficient processing with fast, approximate results. The physical world does not exist in ones and zeros, and conversions between sensing, memory, and digital processing take time and energy. Analog systems avoid the so-called "Von Neumann Bottleneck" and are ideally suited to sense and process the physical world.[70] Prototype analog chips reduce power demand by between 100 to 1,000 times over GPUs.[71]

Neuromorphic chips, which simulate the brain, are a more futuristic option for solving inference computing needs. The human brain's massively parallel structure allows it to perform extraordinarily complex inference calculations using very low precision rates and drawing very little power. Neuromorphic chips and spiking neural networks simulate the brain's processes to provide a "neuromorphic advantage" for far greater AI inference efficiency than GPUs.[72] Neuromorphic and analog chips provide compelling solutions for inferencing but do not have sufficient power to replace GPUs for AI development and training. GPUs will dominate cloud and high-performance computing for the foreseeable future and are the ideal workhorse for AI training. However, neuromorphic and analog computing are ideal candidates for the edge.

Cloud computing has taken over the majority of the world's HPC needs, but the future is on the edge – where humans live, work, and fight. Cloud access is not guaranteed and does not meet every need. Emerging technologies, including robotics and autonomous systems, need extremely low latency, which the cloud cannot provide. Cloud providers are shifting processing and storage to local computing zones or even on-premise, but this does not solve every need. Autonomous systems cannot rely on a 5G connection or stay tethered to ethernet and power cables. Moving processing to the edge enables on-board, real-time decision-making, but comes with a size, weight, and power (SWaP) penalty.

On the edge, SWaP can mean the difference between life and death. A self-driving car must make an accurate decision fast enough to avoid oncoming traffic. Troops must be mobile in a firefight. Small uncrewed aircraft systems can only fly as long as their meager battery packs allow. On the edge,

On the edge, size, weight, and power can mean the difference between life and death.

every second, ounce, and watt matters. Analog and neuromorphic chips offer unprecedented capability to meet these needs.

Developers and engineers must increase hybridization in computing architectures to continue exponential growth in computing power. Future architectures must incorporate highly specialized chips to optimize computational power against energy efficiency for individual tasks. Many applications can avoid using the most advanced semiconductor nodes (i.e., two nanometers) and rely instead on combinations of specialized CPUs, GPUs, and non-Von Neumann architectures like analog and neuromorphic. Until a commercially viable replacement for silicon is found, the future of exponential computing relies on scaling hybrid architectures.

Data-Sharing Challenges May Stall the Flow of America's Most Valuable Fuel

In 2006, Clive Humby coined the statement, "Data is the new oil."[73] Today, the dramatic advancements in AI and the intensifying competition with China dramatically highlight the validity of that bold assertion six years ago. Data is the foundation for AI. The data source for ChatGPT is the Internet, but AI for government applications requires sharing high-quality, situation-specific data streams within and sometimes across organizations. In contrast with China's efforts to build massive data stores--sometimes via collections the U.S. would consider unethical--and conduct big-data analytics, the U.S. government's approach is more targeted. The 2020 *DoD Data Strategy* calls it "data fit for purpose."[74] But even ethical data sourcing requires cultural and technical support to enable data sharing. How effectively is the U.S. government sharing data?

Studies, plans, and guidelines demonstrate progress in data sharing across the federal government, but cultural realities and technical challenges continue to stall the flow of this valuable commodity within the U.S. government, with vendors and researchers, and with allies

and partners. The *Evidence-Based Policymaking Act of 2018* established the Chief Data Officer Council which aims to "identify and solve cross-cutting federal-wide data challenges through collaboration and shared leadership."[75] In December 2022, the Government Accountability Office (GAO) found that the council is making "progress in strengthening evidence-based policy making." In 2021 the council's Data Sharing Working Group assessed U.S. government data-sharing challenges and recommended expedited data agreements, improved data awareness, and improved data trustworthiness. Taken together, the working group's insights indicate fundamental cultural gaps in data-sharing readiness.[76]

The Department of Defense has developed several data-sharing plans that target these and other challenges. The 2009 *Department of Defense Information Sharing Implementation Plan* was an early effort. It highlighted the need to "institutionalize information sharing behaviors while maintaining information assurance and operations security." [77] It provided a framework for action that included 10 focus areas to address challenges in data management, culture, prioritization, classification, technology, standards, and access. The 2020 *DoD Data Strategy* is similarly broad and highlights a lack of enterprise data management, data interoperability, and data awareness as issues the Department must address. Other plans address specific issues, such as cybersecurity, but the challenge of balancing sharing and security persists.

The 2022 *National Security* and *Defense Strategy* documents state that the data solutions lie in institutional reforms,[78] better tools,[79] and a technology ecosystem to promote a free flow of data, with trust among the U.S., allies, and partners.[80] These are not new ideas, but efforts to date have not yet resulted in the kind of progress Congress or department leaders expect. In fact, Section 1513 of the FY 2023 National Defense Authorization Act (NDAA) required the

military services to share data—reinforcing a 2021 Deputy Secretary of Defense memo that imposed the identical requirement on the services.

Craig Martell, the DoD CDAO, has a more nuanced view. "Right now, we treat data as an asset, and that's problematic," he said in a fireside chat in May 2023. "An asset implies that something needs to be protected or safeguarded. Data should be viewed as a product. … Data has customers. Those customers have varying and contradictory needs, and someone has to own that product and help their customer be successful."[81] Functional data governance processes and tools may help. The Acquisition Data and Analytics division of DoD is an early adopter. They led the defense acquisition community in establishing data governance for widely used acquisition data. The process involved curating community-wide data definitions while maintaining military service-specific data sources.[82] The division's models may benefit others and help drive broader culture change.

But DoD's data-sharing challenges are not purely cultural. A 2022 DoD Inspector General report highlighted data architecture and standards as top DoD management challenges related to creating a data-centric culture.[83] A recent study on the state of data science highlighted the widespread nature of this challenge for all industries. "Respondents indicated they spend about 37.75 percent of their time on data preparation and cleansing" before they can use the data for analytics.[84] Alignment to standards helps, but even the most rigid standard will never create perfect alignment.

Emerging AI offers opportunities and Congress agrees. Section 7226 of the FY 2023 NDAA requires the Department to "establish an artificial intelligence capability [in pilot efforts] that solves data access and usability issues with automated technology and eliminates or minimizes the need for manual data cleansing and harmonization efforts."[85] The statute may be

provide good news that the department and broader federal government can scale to improve data sharing both internally and with allies and partners. This provides a great example of AI use... to fuel more AI.

Pink Slips or Paychecks: Bracing for Workforce Disruptions from the AI Wave

People are at the center of the AI ecosystem, creating AI capabilities, bringing disruptive changes to the workforce, and forcing the U.S. government to cultivate the talent necessary to unleash the next wave of innovations to remain competitive on the global stage. People are also at risk of losing their jobs, pushing an estimated hundreds of millions worldwide into skills re-training, unemployment, or despair. The following section examines implications of the current AI wave on the workforce, efforts to retrain and place displaced workers in new jobs, initiatives to nurture the next generation of researchers, and how immigration policies might hinder short-term solutions to address AI research talent shortfalls.

"Could AI Take My Job?"

As ChatGPT, Dall-E, Bard, and other AI commercial offerings become increasingly capable, workers in both blue- and white-collar industries are asking two simple questions. The first is, "Could AI take my job?" The second is, "If AI takes my job, what do I need to do to get a new job?" An assessment of workforce resiliency supports a shared understanding of the extent and depth of potential AI-driven workforce disruption, current thinking about the problem, and possible deficiencies in current government policies.

Economists argue that AI capabilities are introducing efficiencies that are disrupting a workforce dynamic that has existed for the past several decades. More than 75 percent of companies worldwide seek to adopt AI, cloud computing, or big data into their operations, according to the World Economic Forum (WEF). AI is among a family of emerging technologies

that are expected to bring "significant labour-market disruption, with substantial proportions of companies forecasting job displacement in their companies, offset by job growth elsewhere to result in a net positive," the May 2023 WEF report said.[86] Goldman Sachs attracted significant media attention with a report of its own by putting a figure on that disruption, estimating that 300 million positions around the world—including two-thirds of jobs in the U.S. and Europe—could be lost or diminished due to AI-driven automation.[87] Lost amid the alarm following the report's publication, the team of economists who authored the report also concluded that generative AI could eventually boost the global gross domestic product (GDP) by 7 percent.[88] Although these are just forecasts and subject to vigorous debate, they reflect the potential scope of the problem, the depth and breadth of which require government-led efforts to address.

Increasingly capable AI may end up creating jobs that offset the losses, but these new vacancies will not eliminate the tumultuous transition that transforms the design and conduct of work, the supply of labor, and the impact on workers whose positions are eliminated because AI integration renders them obsolete. "Workforce ecosystems are incorporating human-AI collaboration on both physical and cognitive tasks and introducing new dependencies among managers, employees, contingent workers, other service providers, and AI," according to a Brookings Institution report.[89] New technologies like AI will ultimately advance mankind and may improve the quality of life for many people, but the transition period will feature difficult change in the workplace dynamic. In some cases, massive numbers of pink slips will greet workers when they arrive at their desks. In other

"A college degree … is no guarantee of job security when competing against machines that can spot patterns and make decisions on levels the human brain simply can't fathom.

instances, people's work hours will steadily be reduced. Longtime employees may suffer emotional turmoil as their employers enthusiastically hand over more tasks to something that is not even alive. Blue- and white-collar workers are equally vulnerable, as AI futurist Kai-Fu Lee noted in his book, *AI Superpowers: China, Silicon Valley, and the New World Order*. "A college degree—even a highly specialized professional degree—is no guarantee of job security when competing against machines that can spot patterns and make decisions on levels the human brain simply can't fathom," he wrote.[90]

The AI wave will also introduce turmoil on a global scale to places where inexpensive exports developed through cheap labor have either lifted countries out of poverty (China, South Korea, Vietnam, and Singapore) or helped sustain their economies (such as Mexico and other nations in Latin America). As AI tools automate more manufacturing functions in factories of the future, these countries will be forced to grapple with large numbers of unemployed people with limited education and little pathway toward building AI-related skills. Massive unemployment and a widening income gap would undermine the socioeconomic and political order of many nations.

In the U.S. and other countries with significant social welfare systems, people who are laid off or lose work hours might seek to upskill (enhance existing skill sets in the same field), retrain (find a new line of work), unemployment compensation, or a combination of all three. Many jobs that might be affected by AI are generally administrative in nature with repetitive tasks that could be optimized by machines operating as peers or supervisors such as secretaries, postal-service workers, paralegals, cashiers, or data-entry personnel.[91] Among the cross-functional skills most valued by companies worldwide, four of the top five priorities for upskilling in the next five years are more cognitive or empathetic in nature—analytical thinking

(No. 1); creative thinking (No. 2) leadership and social influence (No. 4); and resilience, flexibility, and agility (No. 5). The only technically oriented "hard" skill was AI and big data (No. 3).[92] Figure 3, below, provides a more complete list of companies' desired skills for workers for the next five years.

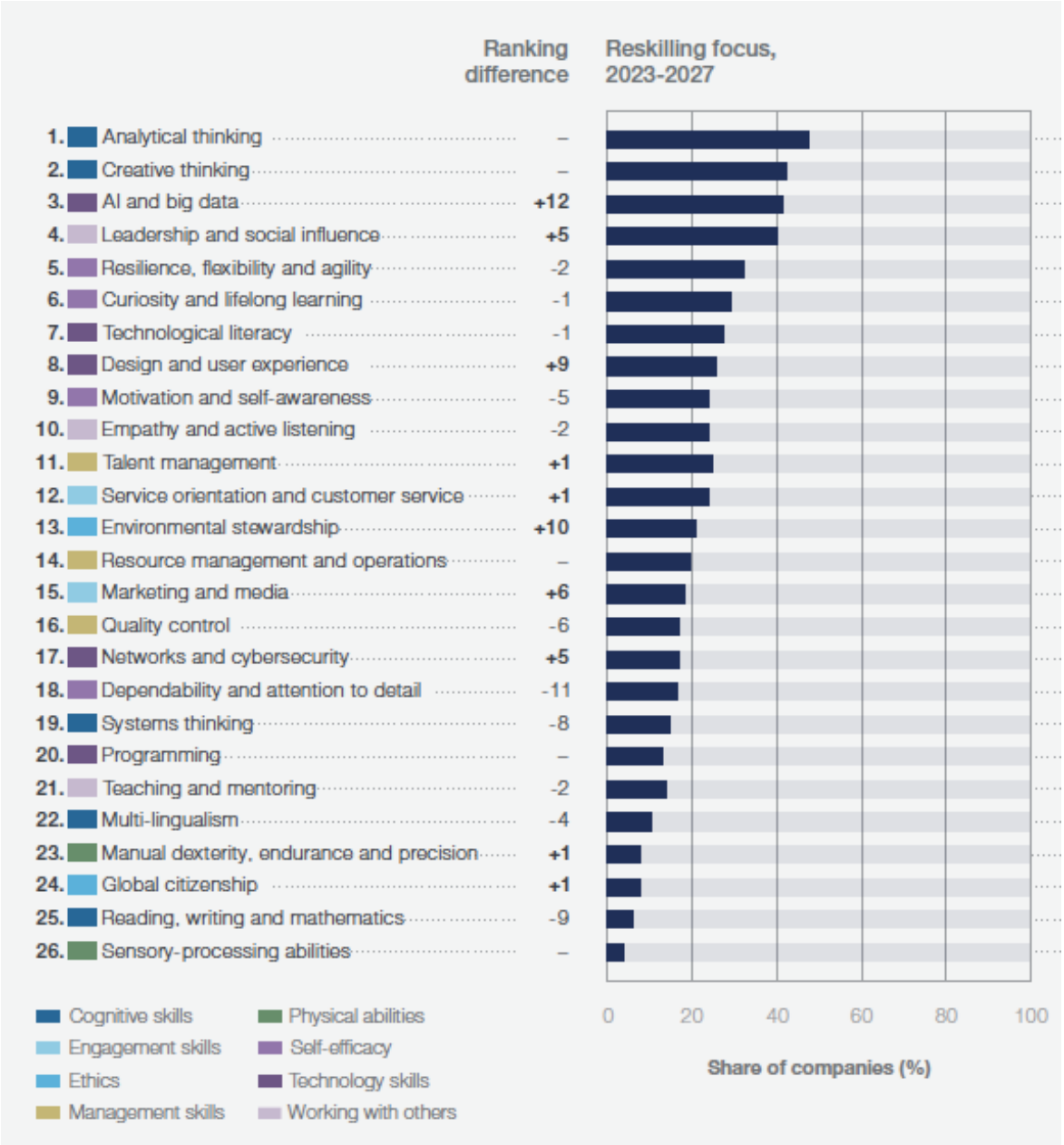

Figure 3. Corporate Reskilling and Upskilling Priorities
Source: World Economic Forum, Future of Jobs Survey, 2023

The popular online learning forum Coursera found a glaring mismatch between the mostly soft skills desired by companies and the hard skills that individual learners try to build from its massive library. In research done in collaboration with the WEF, Coursera concluded that "as emerging technologies such as generative AI are reshaping workforce demands, … employers are placing greater emphasis on 'soft' skills … that allow companies to respond to change and are resistant to automation."[93] Popular classes on programming, resource management and operations, networks and cybersecurity, and design and user experience simply duplicate what AI can eventually do better and faster. On the other hand, socio-emotional skills like analytic thinking or creative thinking might make an individual more difficult to replace. In a similar vein, trade apprenticeships for welders, electricians, plumbers, carpenters, and ironworkers are in steady demand–more jobs that cannot be replaced by AI.[94]

The skills mismatches are just as apparent within the national security realm, where the DoD and Intelligence Community struggle to hire, retain, and develop talent that can create the next generation of AI capabilities. In numerous strategy documents, policy roadmaps, and white papers published by both government organizations and think-tank analysts, "talent" might be Beltway code for individuals with backgrounds, experience, or formal education in science, technology, engineering, or mathematics (STEM). While STEM skills remain essential to develop the next generation of cutting-edge AI capabilities to maintain American technological advantage against peer competitors, observers argue that AI itself will democratize knowledge and allow those without technical backgrounds to make significant contributions to the AI ecosystem.

The National Security Commission on AI's 2020 Report highlighted an "alarming talent deficit" that would inhibit the United States from being "AI-ready by 2025." "National security

agencies need more digital experts now or they will remain unprepared to buy, build, and use AI and its associated technologies," the NSCAI report stated.[95] Across the U.S. government and the DoD, officials have published strategy documents attempting to prioritize desired skills, experience, and professional backgrounds needed to sustain AI initiatives and introduce AI concepts to the existing workforce. However, gaps exist between the guidance and execution. Talent requirements exceed the pool of willing, qualified applicants. The private sector can also offer "more" in several tangible arenas—more pay, more opportunities to work on cutting-edge technologies, and more flexible work cultures.

STEM and "Soft" Skills

Advanced STEM skills are critical to secure the future of U.S. technological superiority, but soft skills are just as important to address private-sector needs. Training and education are becoming increasingly important as the public and private sectors attempt to make the workforce more resilient against AI-related disruptions. Elementary and secondary education in mathematics and science are gateways for postsecondary STEM majors and STEM-related occupations, but performance has lagged over the past decade.[96] The US has experienced a decline in mathematics performance, ranking lower than the average of 37 developed countries, according to the National Science Foundation.[97] Meanwhile, the quality of STEM instruction has been a growing concern at the K-12 level since 2012. As the Congressional Research Service (CRS) recently noted in a report about STEM education, "many U.S. mathematics and science teachers lack degrees in the subjects they teach."[98] Finding teachers with STEM backgrounds is particularly difficult in rural and low-income areas, where schools may struggle to attract and retain teachers with the necessary qualifications and experience, the CRS report said.[99] Addressing this decline in teacher qualifications will be critical in ensuring that the next

generation of students has the skills and knowledge they need to succeed in STEM fields, including those related to national security and the development of AI.

On the other hand, some experts argue for growing skills beyond just STEM in an AI-enhanced economy.[100] Shirley Malcom, head of education and human resources programs of the American Association for the Advancement of Science, believes that creating a workforce ready for the challenges of an AI and digital future requires teaching people to think differently. In its *Future of Work Report*, the WEF emphasized that companies want workers who can perform functions and exhibit skills that AI cannot duplicate easily—analytic thinking, creative thinking, leadership, social influence, and other formerly derided "soft" skills.[101] Aside from a greater emphasis on how people interact with each other and manage their workplace challenges, skills such as prompt engineering will be important for the workforce to effectively use generative AI. "Prompt engineers are experts who write prose rather than code to test AI chatbots."[102] Altman, the CEO of OpenAI, recognizes that prompt engineering is a highly leveraged skill and a precursor to natural language programming. A non-STEM degree like English could help develop and advance LLMs and further develop their capabilities. Andrej Karpathy, Tesla's former chief of AI, said, "the hottest new programming language is English."[103]

Additionally, higher education costs have increased at rates far above inflation, forcing students to attend community colleges to attain an associate degree or certificate. Students interested in pursuing STEM fields may face significant financial barriers, as these fields often require expensive equipment, lab facilities, and specialized training. The cost of education can drive students away from earning STEM degrees and more towards technical degrees so they can enter the workforce early. This can have long-term implications for national security, as it could limit the pool of skilled workers available to develop and implement cutting-edge technologies

related to AI and other areas of national security. Moreover, it could exacerbate existing disparities in access to STEM education, particularly among low-income and underrepresented minority students, who may have fewer resources to pay for college and may be less likely to pursue STEM fields as a result. Addressing the high cost of college education and expanding access to financial aid and other resources will be critical in ensuring that all students, regardless of their background or financial circumstances, can pursue STEM degrees and contribute to U.S. national security.[104]

Immigration to Strengthen American Workforce Resiliency

Meanwhile, existing U.S. immigration policy erects barriers to foreign-born STEM and tech entrepreneurial talent seeking to work in the United States and contribute to the American economy. International students completing their studies in the United States who wish to remain must apply for an H-1B visa. Rather than the candidates' merits – which might include their education or work experience in critical national security issues – they enter an arbitrary lottery with a success rate as low as 11 percent.[105] Observers such as Eric Schmidt, the former chief executive of Google, note that liberalization of immigration policies could provide the United States with a relatively fast way to fill critical-skills shortfalls while the current generation of American STEM students make their way through school, college, and research relevancy. Paradoxically, advocates of a skills-oriented immigration policy can make the same argument for China-born tech innovators, who founded start-ups valued at more than $100 billion since 2000. "Although much has been made in Washington of the security risks posed by a few foreign researchers who have been accused of intellectual property theft, far greater harm will be done to the country over the long term by keeping out entrepreneurial Chinese scientists," he wrote.[106]

Unanswered Ethical Questions May Increase Turbulence in the Wave

AI has presented society with ethical dilemmas related to information transparency and technology explainability. As AI becomes an integral part of more aspects of life, commerce, governance, and national defense, it is likely to introduce new ethical questions leaders must answer. The absence of global guidelines and standards leaves room for independent citizen and nation-state action, which will have unintended consequences and could create chaos in society.

AI creators are calling for Congress to act to navigate the coming wave of ethical concerns. Among them is Altman, the OpenAI founder who told Congress during testimony on May 16 that, "My worst fear is we cause significant harm to the world."[107] An Axios article on the testimony suggests lawmakers know they need to act quickly: "Multiple members said Congress failed to take early action on social media regulation—a mistake they're determined not to repeat with AI."[108] What factors should they consider in developing legislation to enable the United States to benefit from AI innovations while protecting citizens from both intentional harm and unintentional consequences of AI use? Are the considerations the same in civil and military uses of AI? What about when allies and partners are involved?

Trust and Explainability Are the Heart of The Ethical Dilemmas

Before lawmakers can determine what to do, they need to understand the foundational concepts of trust and explainability.

Trust*:* Trust is a crucial factor in successful adoption and use of AI in society. In the United States, AI is already embedded in many day-to-day activities from social media to health care. Americans may enjoy the benefits, such as online purchase suggestions and health-screening reminders, but many also fear the loss of privacy and the potential for deception. Both

unintentional and intentional factors can create negative outcomes that erode trust and either deter use of beneficial AI applications or amplify the effects of harmful ones.

The primary unintentional factor is bias. There are two chief causes of unintentional bias in machine learning: under-sampling and proxy issues. Today's widely available trained LLMs, such as ChatGPT, provide a current example of issues from under-sampling, which is use of a segment of a larger set of data. ChatGPT's data source is the Internet, which includes content from many sources with many different perspectives. While ChatGPT's technology can process vast amounts of information very quickly, any "conversation" with ChatGPT will produce a response that leverages some portion of that vast data store. The response may be inaccurate or discriminatory, depending on what data was used and how the algorithm processed it. But even using a larger data set cannot guarantee unbiased results. Proxy bias is another issue. MIT warns AI developers about proxy bias stating, "An algorithm can have an adverse effect on vulnerable populations even without explicitly including protected characteristics."[109] A 2019 study published in *Science* magazine determined that a medical-care algorithm used to identify patients needing specific medical screening under-identified black patients by as much as 46 percent, due to black patients' unequal access to medical care. The bias created life-and-death consequences for some patients who did not receive the needed screening and subsequent care.[110]

While some AI developers work hard to avoid unintentional bias, others intentionally misuse and abuse the capabilities. Some misrepresent AI-produced work as human or create misinformation known as "deepfakes." Deepfakes can result in social harm to individuals (e.g., sexual harassment via AI-generated pornography or cyberbullying), or a society (attempts to change a political election outcome). Some deepfakes are criminal. An early documented case of a criminal use of a deepfake occurred in 2019, when a United Kingdom-based energy company

CEO was convinced that he was talking to the CEO of his parent company, who directed him to transfer €220,000 to a bank account in Hungary. In fact, he was talking to a scammer using advanced AI voice technology that could be widely sourced.[111] In March 2023, the *Washington Post* reported on scammers who used AI voice technology to impersonate close family members to scam thousands of dollars from victims.[112] More ambitious misuse and abuse could have far more significant effects, such as using AI to impersonate a government leader to incite a political incident.

Explainability: Explainability reflects how well one can explain how AI arrives at a specific decision, outcome, or recommendation. Similar to trust, poor AI explainability can create ethical dilemmas rooted in bias or discrimination. The issue is growing as AI becomes more advanced.

Not all uses of AI require explainability. For example, the use of AI to identify storm damage using satellite images presents fewer bias or discrimination risks and technical challenges than the use of AI for loan underwriting. If a satellite image misidentifies roof damage, no one is hurt, and no laws are broken. If a mortgage applicant is denied a loan, federal law requires the lender to explain the reason if the applicant requests it. Implementing explainability can also help with troubleshooting algorithms. However, current models have difficulty proving data traceability, which enables explainability. Even with the labeling of input-data origin, identifying what data has been used to determine a machine learning model's outcome is challenging to achieve.[113]

In War, AI Trust and Explainability May Have Life-or-Death Consequences

Trust and explainability are critical concepts for the use of AI in war. Global military adoption of AI has increased the speed and precision of weapons and AI-enabled autonomous

action. These improvements and capabilities raise many ethical questions. Four occasionally overlapping issues emerge due to their potential impact on global stability: the ethics of AI-enabled precision strikes, the use of autonomous weapons, accountability, and any of these activities performed in coordination with allies and partners.

Are We Targeting "Leaders" or a Specific Leader Who Looks Like Bruce Lee Eating Lunch at His Kitchen Table on Tuesday?

Through the industrial age, weapon systems became progressively more accurate, shifting from a more indiscriminate form of warfare (force-on-force, close-quarters infantry combat or ships in the line-of-battle formation), to the longer-range and more-distributed combat characteristics of the modern age. Generally, the trend toward more precise and discriminant weapons has been accepted and gained widespread use. Modern long-range precision weapons afford direct engagement of enemy combatants, limit collateral damage, and minimize impact on non-combatants.

With increased use of AI in precision weapons, the world could see more targeted attacks on individuals. One expert who spoke to Eisenhower School students in 2023 described a small, autonomous drone equipped with facial recognition capability and an explosive device capable of killing a specific individual.[114] The capability could be useful to a commander in challenging environments like densely populated and urbanized area. It could also enable highly-discriminant targeting of individuals in assassination-style attacks. In February 2023, the Israeli Defense Force announced that it had employed AI to develop exploitation profiles on Hamas military units and leaders and used employed AI-enabled weapons to prosecute Hamas targets.[115]

Advocates of an AI-enabled kill chain assert that greater targeting precision reduces collateral casualties to noncombatants and combatants alike. However, critics argue that AI-enhanced capabilities can facilitate what amounts to targeted assassinations in a boundless

battlespace. And what if the AI incorrectly identifies an individual and kills the wrong person? The traditional values of warfare have discouraged assassination-style tactics and avoided targeting leadership for lethal attacks. Existing U.S. policy—Executive Order 12333—prohibits assassination.[116]

Did The AI Get the Bad Guy... or Was That Someone Else?

How does the situation change if the actor is a machine rather than a human? The debate on the ethics of autonomous weapons has been an enduring issue for some time. A 2018 *Arms Control Association* article crystalizes the fundamental ethical question related to autonomous weapons: "Whether the principles of humanity and the dictates of the public conscience can allow human decision-making on the use of force to be effectively substituted with computer-controlled processes, and life-and-death decisions to be ceded to machines. It considers the risk of unintended loss of human life should the system fire at targets human decision-makers would not want them to hit."[117]

These ethical concerns are not shared by other nations around the world, particularly among adversaries that have a lower threshold for the acceptable employment of lethal autonomous weapon systems. If these ethical concerns persist, Western forces will be at significant disadvantage on the battlefield because of the adversaries' enhanced ability to use AI/ML-enabled weapons to sense, assess, make decisions, and execute against U.S., allied, and partner-nation militaries. Even among U.S. allies and partners hold differing views on the definition of "autonomous weapon systems," how they should be developed and employed, and what ethics should be applied to their use.

Autonomous systems could be valuable in tactical combat engagements. Organizations use various terminology to describe a series of actions that result in combat action and post-

combat feedback. Terms include detect-to-engage, the observe-orient-decide-act (Boyd's) loop, sensor-to-shooter, find-fix-finish-exploit-analyze (F3EA). Each term represents multiple steps that can be AI-enabled to assist the warfighter. Some of the activities are similar, if not identical to civil uses of AI and pose no novel ethical considerations. For example, after a sensor detects a new object, AI-enabled classification algorithms used in the public sector can identify and classify that object, just as they do when they note the difference between dog and giraffe pictures on the internet. That initial sensing and classification step may not have significant ethical considerations. However, if AI is applied to subsequent steps in the process such as weapons selection, ordinance pairing, or effects-based engagement, public and civil algorithms can't help, and ethics may be an issue. The most critical, ethically charged step in the process is the firing, launch, or trigger pull of the weapon system. The National Institute of Standards and Technology (NIST), has considered these and other government-wide AI risks. In its *NIST AI Risk Management Framework 1.0*, the organization offers "a resource to the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems," which may help leaders navigate AI ethics challenges as the industry continues to evolve.[118]

The Office of the Secretary of Defense has directed that all autonomous weapon systems be designed and used with a human in the decision cycle.[119] However, some argue that U.S. DoD must consider scenarios in which joint force commanders should approve the use of lethal autonomous weapons to keep pace with enemies whose ethical standards allow them to take humans out of the decision loop to gain an asymmetric advantage. As lethal autonomous weapons and their AI-enabled targeting systems become more effective, efficient, and responsive for both the U.S. and near-peer adversaries, senior DoD leaders will have decisions to make.

When and how should joint force commanders pull the human off the loop and allow the "killer bot," AI-enabled capabilities, to take over?

It's Your Fault!

If you take a human out of the loop, whom do you blame if something goes wrong? Accountability is an important factor in AI governance, particularly AI for military use. Some say the buck stops at the commander who releases the AI-enabled weapon, and he or she should be held responsible in the event of unintended casualties. This scenario would require the commander to have high confidence in the AI or would leave the capability unused. Some say the force requestor should be accountable. This is usually the geographic combatant commander, who is responsible for identifying the forces and capabilities needed to execute theater plans. Traditionally, accountability for tactical weapons employment is not held at such a high level, but the scale of capability could warrant such a precedent. Some say the industry partner should be accountable for the performance of the weapon it produced. Properly acquired, fully tested weapons developed to include government-specified limitations and constraints, should work as designed. Therefore, abnormalities in performance could be attributed to the designer. Determining who should be accountable is rarely straightforward. These and other scenarios highlight the complexity policy makers face.

Friends Playing by Different Rules

Determining accountability becomes even more challenging when allies and partners are involved. One country may decide that data delivered by a sensor system to an autonomous weapon system bears some responsibility for the fire command of a weapon. But do its allies and partners agree? What if the data is coming from an ally's data system into an autonomous weapon system owned and operated by the U.S.? Does the rules-of-engagement authority of the

nation providing that data take any responsibility for the engagement, or does the authority of the autonomous weapon system take full responsibility for the weapon launch?

Understanding the differences and friction points in the rules-of-engagement (ROE) authorities among nations is essential for successful joint battle.[120] The potential differences in individual nations' designation of hostile forces can further complicate ROE. U.S. policy details a hostile force as "Any civilian, paramilitary, or military force or terrorist(s) that has been declared hostile by appropriate US authority."[121] Individual nations' interpretations of the broad policy will determine which individuals their forces can legitimately target in conflict. In a coalition force, differing interpretations of the policy may mean that soldiers sharing the same battlefield are not allowed to hit the same targets on that battlefield. Policy compliance would be difficult or impossible if the shooter is an autonomous system with no human oversight, either in-the-loop or on-the-loop, to validate the target and make the authorized the life-and-death decision. The risk is that one nation's autonomous system may be programmed to engage a legitimate hostile force in their authority that is not so justified in the sensor nation's ROE directive.

Government Actions to Help the U.S. Ride the Current AI Wave and Prepare for the Next

After examining the opportunities and challenges across the dynamic AI landscape, the Eisenhower School AI Industry Study Seminar offers the following recommendations for potential U.S. government intervention to mitigate risks and optimize opportunities in three areas. First, the U.S. government should prepare for development of regulations that create greater transparency regarding AI natural resource requirements of their tools. Second, the federal government should work with partners at the state and local levels and private sector to

bolster workforce resiliency—sponsoring grassroots ecosystems that support upskilling, retraining, and job placement in an increasingly AI-driven world. Third, the U.S. government must work with allies, partners, and even state adversaries to establish global norms through ethical standards to ensure safe civil and commercial use and reduce the greatest risks for military use.

1. **Prepare for Regulation to Compel Industry Resource Transparency; Focus on Efficient Edge Computing for Defense**

   Action 1: The U.S. government should require transparency from technology companies regarding their resource consumption for AI model development and use. The federal government mandates that all vehicles, appliances, and electronic device producers disclose their product's energy requirements so consumers may understand their environmental impact. Congress can ensure industry-wide consistency and accountability by establishing reporting standards, creating a central repository for data sharing, and empowering regulatory agencies for oversight and enforcement. Public awareness will encourage AI developers to adopt sustainable practices and prioritize openness in their operations. Consumers should have the knowledge to choose from not just the best-performing models but also the most efficient ones.

   - **Alignment to National Security Strategy:** Climate and energy security is a global priority; the strategy includes the vision to cooperate to address shared challenges in an era of competition and specifically identifies climate change as a potentially existential problem for the United States and the world.[122]
   - **Lead Organization:** U.S. Congress

- **Supporting Organizations:** U.S. Department of Energy, U.S. Department of Commerce, Environmental Protection Agency, National Climate Change Task Force, and industry partners.
- **Proposed Timeline:** Immediately. Due to the rapid increase of global power and water requirements, every day without this information puts the US at greater risk of increased environmental damage and fuel and water source depletion, which would affect both individual and national security.

Action 2: The DoD should prioritize emerging edge computing technologies. In a distributed, high-end fight, tactical users will struggle to secure enough energy, computing, and bandwidth to meet mission needs. Traditional computing methods will not solve future problems on the tactical edge. The semiconductor industry is investing trillions of dollars to incrementally improve CPUs and GPUs while minimally resourcing emerging research areas despite exponential growth potential. DoD should bet big on options like analog, neuromorphic, and silicon alternatives through research funding, prototype development, and real-world testing opportunities.

- **Alignment to National Security Strategy:** Modernizing and strengthening our military.
- **Lead Organization:** U.S. Department of Defense
- **Supporting Organizations:** Industry partners
- **Proposed Timeline:** Immediately

2. Sponsor Grassroots Ecosystems and Loan Programs for Skill-building, Upskilling, Retraining, and Job Placement

Action 1: The U.S. government should reshape partnerships with state and local governments and the private sector to develop and fund grassroots ecosystems, innovation hubs, that mitigate the risks of major workforce disruption caused by the initial wave of AI and fuel innovation across the country. These ecosystems would build on existing public-private partnerships to serve as hubs for upskilling, retraining, job placement, and guidance for displaced or at-risk workers. The federal government would provide the funding, in coordination with state and local governments and select industry partners that stand to benefit from greater workforce stability. Regional officials would identify evolving skills requirements in the industries most impacted by AI implementation in their areas and align upskilling/reskilling curricula to those needs.

- **Alignment to National Security Strategy:** Investing in our people is an investment in our national power to maintain a competitive edge.[123]
- **Lead Organization:** U.S. Department of Commerce
- **Supporting Organizations:** U.S. Departments of Education and Labor, state and local governments, industry partners, and trade unions
- **Proposed Timeline:** Develop a proof of concept in five of the most affected metropolitan areas by the 1st Quarter of FY 2027.

Action 2: The U.S. government should fund educational loans for students seeking degrees in STEM fields and expand trade school links with industry partners focused on critical skills shortfalls (i.e., welders, electricians, and plumbers to support U.S. efforts to maintain an edge in emerging technologies critical for national security such as AI). These low-interest loans would help address the rising costs of college and university educations and incentivize students to pursue STEM fields. The loans would offer up to 100 percent

tuition coverage for STEM degrees in exchange for graduates to serve in the U.S. government, work on federal government research projects, or teach STEM subjects to grades K-12 for a specific time. This program should target aspiring STEM students in low-income areas or underrepresented minorities who may face significant financial barriers to pursuing these fields. Meanwhile, trade school expansion provides mutual benefits for young people or displaced workers seeking entry into valuable trades and companies seeking to fill vacant positions.

- **Alignment to National Security Strategy:** Investing in our people is an investment in our national power to maintain a competitive edge.[124]
- **Lead Organization:** U.S. Department of Education
- **Supporting Organizations:** U.S. Department of Labor, state and local governments, industry partners, and trade unions.
- **Proposed Timeline:** 1st Quarter FY 2025

3. With Allies, Partners, and Competitors, Establish Global Norms to Promote Safe Civil and Commercial AI Use and Reduce the Greatest Risks for Military Use

Action 1: Form a global entity—with allies, partners, and peer competitors—to license major generative AI systems and create ethical guidelines and standards for application of AI in society and military use. The group should leverage *NIST AI Risk Management Framework 1.0*, which offers "a resource to the organizations designing, developing, deploying, or using AI systems to help manage the many risks of AI and promote trustworthy and responsible development and use of AI systems."[125] The group should also consider the issues associated with the use of AI in joint warfare with allies and partners.

- **Alignment to National Security Strategy:** The goal of the strategy is "a free, open prosperous, and secure international order."[126] It recognizes that "alliances and partnerships around the world are our most important strategic asset and an indispensable element contributing to international peace and stability"[127] and includes the vision to cooperate to address shared challenges in an era of competition. The rapid pace of AI adoption and innovation, absent ethical guidelines—or in an environment of significantly different ethical standards among nations—presents risks to global stability that the global community must address together. Risks may include the potential for debilitating humanitarian crises due to AI-driven environmental issues and unintended military action due to AI-enabled autonomous weapons.
- **Lead Organization:** U.S. Department of State
- **Supporting Organizations**: U.S. Department of Commerce, the United Nations, and industry partners.
- **Proposed timeline:** Immediate action is necessary to prevent potential negative effects of ungoverned AI use.

Action 2: U.S. leaders should advocate for an additional protocol to the Geneva Convention that explicitly addresses the use of AI for military purposes. First, the AI protocol would prohibit the use of AI to conduct command-and-control of nuclear weapons, ensuring that a human was permanently in the control loop for release authority. Second, the AI protocol would establish guidelines for the use of AI to support lethal autonomous weapons. Signatories would revisit the protocol annually to address evolving capabilities. Much as the U.S. and Soviet Union collaborated during the Cold War to counter the

proliferation of nuclear weapons and nuclear tests, the United States and China should identify mutual areas of interest and risk as a starting point to develop a multilateral regime on the military use of AI.

- **Alignment to National Security Strategy**: Arms control and non-proliferation. AI alone is not considered a nuclear, chemical, or biological weapon, but the destructive potential that these technologies offer is a risk that strategists, ethicists, and military professionals seek to control. Verifying compliance to AI control regimes would be difficult because of the limited number of external observables. Restrictions on computing infrastructure such as the graphics processing units and advanced semiconductors needed to support computing power and algorithm development are the most realistic measures of a prospective AI arms control regime.[128]
- **Lead Organization**: U.S. Department of State
- **Supporting Organizations**: U.S. Department of Defense
- **Proposed Timeline**: 1st Quarter FY 2025

Conclusion

AI is crashing over the world, and no one is ready for the changes that are starting to occur across all segments of society. The disruptions are starting as little ripples, introducing fresh perspectives to how we live, work, learn, and create. However, mankind has reached an inflection point that requires the world's leaders to provide guidance and establish best principles to reduce risks and create positive outcomes. To ride the current wave of change brought by AI, the U.S. government must rally allies, partners, and adversaries alike to compel industry partners to be more transparent about computing power requirements, cultivate the right skills to strengthen workforce resiliency, and develop norms through ethical standards.

Appendix A: Impact of AI on China-Taiwan Tensions

Artificial intelligence (AI) is rapidly advancing and has significant implications for national security interests of the United States (U.S.) and its allies and partners, particularly in the context of the competition with the People's Republic of China (PRC) and the mutual dependence on Taiwan. The use of AI to improve productivity in the military and more broadly in society can provide the U.S. with significant battlefield and economic advantages over its adversaries, including the PRC. However, AI also presents new challenges and potential threats that affect everyone on the globe. Those issues may present areas for collaboration.

The increased military and commercial use of AI presents opportunities for the U.S. and its allies to maintain a strategic advantage over the PRC. For the military, AI can enhance situational awareness, automate processes, and improve military effectiveness while energizing the defense industrial base and boosting the economy. Commercial advancements in AI can drive innovation for additional economic benefit and possible future dual-use applications.

But the U.S. is not alone in seeing the opportunities AI offers. The PRC is also investing heavily in AI research and development, leveraging its military-civil fusion strategy to drive military capability advancement and its economy. Xi's goal is for China to be the preeminent AI superpower by 2030[129]. The result: a new AI arms race between the two superpowers, which threatens global stability and complicates the U.S. relationship with Taiwan.

The U.S.—and the rest of the world—rely on Taiwan for semiconductor manufacturing.[130] Semiconductors provide computing power for artificial intelligence. The U.S. passed the Chips and Science Act of 2022 to begin onshoring semiconductor manufacturing, but efforts will take time, and the PRC is not the only threat. The National Security Commission on Artificial Intelligence (NSCAI) states, "The dependency of the United States on semiconductor

imports, particularly from Taiwan, creates a strategic vulnerability for both its economy and military to adverse foreign government action, natural disaster, and other events that can disrupt the supply chains for electronics."[131] As the U.S. experienced during COVID-19, any disruption to the supply chain severely limits the US ability to continue production of equipment and capabilities that rely on semiconductors—everything from automobiles to large language models. However, a China-Taiwan crisis within the next decade wouldn't be just "severely limiting." It could mean disaster for U.S. economic stability, technology innovation, and military capability—and possibly the current world order.

The PRC's investments in AI research and development have the potential to shift the balance of power in its favor. The PRC could leverage AI-based surveillance technologies, which it uses in mainland China to monitor its citizens and suppress dissent, to undermine Taiwan's democracy. Additionally, AI-powered autonomous weapon systems and innovation in AI-enabled logistics and readiness support systems could provide the PRC with a significant military advantage, challenging U.S. military dominance in the Indo-Pacific region.

An issue for all: all AI requires energy. In fact, the exponential demand for computing power brings a troubling increase in energy consumption. According to Semiconductor Research Corporation (SRC), global computing energy needs are doubling every three years, while global energy production only increases 2 percent annually.[132] This challenge can limit AI advancements and may create additional environmental issues that feed global tensions.

To address these challenges and protect its national security interests, the U.S. needs to leverage all instruments of national power:

1. Diplomacy – AI has the potential to benefit and to harm all of global society. Diplomatic efforts, such as working with international organizations to establish norms and

regulations for AI development and deployment, may guard against misuse of the capability and forge positive relationships—with the PRC as well as allies and partners—through collaboration.

2. Information – AI is the primary resource for the creation and proliferation of dis- and misinformation, and it becomes more available and easier to use every day. The U.S., its allies, and its partners must educate citizens about the methods and risks of the distribution of such information and establish regulations to help identify and limit the release and exposure of dis- and misinformation. In addition, the U.S. must publicize its AI advancements in ways that do not compromise security and call out the PRC's attempts to steal US intellectual property.

3. Military – The U.S. must continue and increase AI research and development in collaboration with allies and partners (particularly those in the Indo-Pacific region, including Japan, South Korea, and Australia) to maintain its competitive edge on the battlefield. Near-term, critical areas include cybersecurity, surveillance, logistics, and materiel readiness. These capabilities may do as much for deterrence as the most sophisticated AI-enabled military equipment. They may also bring participation from military-averse industry partners and allow time for the maturation of ethical issues related to using AI at the pointy end of the spear.

4. Economic – The US government should embrace the private sector as its primary source for technological innovation and leverage its outputs for military application. Strategies may include developing clear problem statements that do not prescribe a solution to entice private sector participation in AI development for military use.

AI is moving fast. As a result, the US Great Power Competition with the PRC may become a relay race to the finish line with AI as the baton. To win, the US must use all instruments of national power, in collaboration with allies and partners, to maintain access to Taiwan-produced semiconductors and secure the US competitive advantage.

Appendix B: AI Industry Study Seminar Engagements

Methodology

This group paper is the result of seventeen weeks of study, over sixty-five field study engagements, and sixteen individual papers. Field study engagements were all non-attribution and included discussions with representatives from government, academia, and industry. Understanding of this complex topic was further informed by the parallel Industry Analysis course. Below is a summary of engagements and speakers and a list of the individual papers used to formulate this group analysis.

Field Studies Hosts and In-class Guest Speakers (in chronological order)

Mr. Paul Scharre, Vice President and Director of Studies, Center for a New American Security (CNAS)

Mr. Maynard Holliday, Deputy Chief Technology Officer for Critical Technologies, Office of the Under Secretary for Defense for Research and Engineering

Dr. Kimberly Sablon, Principal Director for Trusted AI and Autonomy at the Undersecretary of Defense for Research and Engineering

Dr. Tai Cheung, Director, Professor at the School of Global Policy and Strategy at UC San Diego

Mr. Shane Shaneman, Strategic Director, National Security and Defense, Adjunct Professor, Carnegie Mellon University

Mr. Tom Longstaff, Chief Technology Officer (CTO), Software Engineering Institute (SEI)

Mr. Matt Blackburn, Senior Manager, Government Relations Aurora Innovation, Inc.

Mr. Rory Cooper, Director, The University of Pittsburg, Human Engineering Research Laboratories

Dr. Rita Singh, PhD, Associate Research Professor Language Technologies Institute, Carnegie Mellon University

Mr. Jordan Marinkovich, Platform Community Manager and Colleagues Alpha Lab Gear

Mr. Martin Stanley, Chief of the Strategic Technology Branch, Cybersecurity and Infrastructure Security Agency

Mr. Timothy Janssen, Operations Lead for Artificial Intelligence Technical Governance, National Security Agency (NSA)

Dr. Thomas Walcott, Technical Director w/in Engagement and Policy, National Security Agency (NSA)

Honorable Heidi Shyu, Under Secretary of Defense for Research and Engineering

Dr. Tanya Harrison, Chief Impact Officer, Planet Labs

Dr. William Streilein, Chief Technology Officer, Chief Digital and Artificial Intelligence Office (CDAO)

Mr. Gilman Louis -Presidents Intelligence Advisory Board / National Security Commission on Artificial Intelligence (NSCAI)

Mr. Benjamin "Bach" Bishop, US Air Force Operational Liaison, Defense Advanced Research Agency (DARPA)

Mr. Reece Smyth - Department of State and Emerging Technology

Mr. Michael Chang, Managing Director of Microsoft Taiwan Development Center

Ms. Liying Wang, General Counsel and Head of Public Policy, AppWorks

Mr. Ken Lau, Intel Taiwan

Mr. Yeewei Huang, Vice President, RealTek/ Taiwan Semiconductor Industry Association

Mr. David Ku, Corporate Executive Vice President and Chief Financial Officer, Media Tek

Dr. James Newman, Chair, Space Systems Academic Group, Naval Postgraduate School

Dr. Brij Agrawal, Director, Spacecraft Research and Design Center, Naval Postgraduate School

Dr. Jennifer Hudson, Research Associate Professor. Mechanical and Aerospace Engineering

Dr. Jessica Herman, Professor of Practice, Mechanical and Aerospace Engineering

Mr. Joe Felter, Center Director, Stanford University Gordian Knot Center for National Security Innovation and Hacking for Defense

Mr. Steve Blank, Co-Founder, Stanford University Gordian Knot Center for National Security Innovation and Hacking for Defense

Mr. Bradly Boyd, Professor, AI, Autonomy, and the Future of Warfare, Hoover Institution
Dr. Illan Kramer, Director of International Research Partnerships, University of Toronto

Dr. David Wolfe, Co-Director, Innovation Policy Lab

Dr. Shiri Breznitz, Director of Research. Professor, Munk School of Global Affairs & Public Policy, University of Toronto

Dr. Joseph Wong, Roz and Ralph Halbert Professor of Innovation

Mr. Cameron Schuler, Chief Commercialization Officer and Vice President, Industry Innovation

Congressman Ted Lieu, 36th District, California

Dr. Jean-Marc Rickli, Geneva Center for Security Policy (GCSP)

Organizations Visited (in alphabetical order)

Acceleration Consortium, University of Toronto

Amazon Web Services

Army Intelligence Integration Center (AI2C)

Canadian Institute for Advanced Research (CIFAR)

Creative Destruction Lab (CDL), Rotman School of Management

Downsview Aerospace Innovation & Research (DAIR) Hub

Dream Port / Maryland Innovation and Security Institute (MISI)

Google AI Lab

Hewett Packard

IBM Research

IBM Watson Center

Innovator's Showcase, Canadian Companies

JABIL

Johns Hopkins University Applied Physics Laboratory

Lawrence Livermore National Laboratory (LLNL)

Ministry of Digital Affairs - National Institute of Cybersecurity (NICS)

Mitsubishi Heavy Industries Canada Aerospace (MHICA)

Munk School for Global Affairs, University of Toronto

NVIDIA

Oracle Corporation

Quantum Bridge, University of Toronto

Research Security, University of Toronto

Scale AI

The Center for Security Studies (CSS) at ETH Zurich

U.S. Army AI/AR Applications, Program Executive Office (PEO) Soldier

VentureLab

Appendix C: Individual Paper Authors and Topics

Brandon L. Bowman, LTC, USA	U.S. Government Oversight of Artificial Intelligence: A Critical Requirement Now
Jason Coleman, Lt Col, USAF	Optimal Strategies for Implementing AI in the Department of Defense Using A 'Fail Fast' Policy
Laura Cooper, CIV, OSD	Opening the Valve: Progressing Toward Free-Flowing Data in Defense Business Operations
Andreas V. Flowers, Lt Col, USAF	Can Artificial Intelligence Solve the Department of Defense's Behavioral Health Care Provider Gap?
Ryan M. Hiserote, Lt Col, USSF	The Exponential Power Behind A.I.
Michelle Hodges, CIV, Army	Intelligent Army Contracting
Richard C. Kipp, Lt Col, USAF, MC, CFS	Integration of Artificial Intelligence into High Reliability Organizations
Joshua Lail, CDR, USN	If China Invades Taiwan, Are High U.S. Casualties Inevitable? A Historical Approach to Developing Fully Autonomous Submarines to Give the United States a Competitive Edge
Wardrias Little, Col, USAF	Artificial Intelligence in DoD Healthcare, a Game Changer
Nicole D. Matos, CIV, NGA	Strategies for Attracting and Retaining Artificial Intelligence Professionals in the Department of Defense: A Focus on Human Capital and Technical Infrastructure Modernization
Matthew S. Metcalf, CIV, Army	Implications for the Convergence of Artificial Intelligence and Air Defense Technologies
Nicole L. Neal, CIV, USAF	Artificial Intelligence and National Security: Addressing Fears and Preparing for Implications of Emerging Technologies
Owen Rodger, Captain, RNZN	Artificial Intelligence – A Coalition Force Multiplier or Potential Derailer?
Muhammad Shamraiz, BG, Pakistan Army	Human-Centered Artificial Intelligence (HAI): Optimizing Human Experience with Artificial Intelligence
James Strickland, CAPT, USN	Emergence in Artificial Intelligence
Jefferey Wong, LtCol, USMC	ALEXA, Write My OPORD: Promise and Pitfalls of Machine Learning for Commanders in Combat

Endnotes

[1] Cade Metz, "'The Godfather of AI' Leaves Google and Warns of Danger Ahead," New York Times, May 1, 2023, https://www-nytimes-com.nduezproxy.idm.oclc.org/2023/05/01/technology/ai-google-chatbot-engineer-quits-hinton.html?searchResultPosition=1.

[2] Gerrit De Vynck, "Elon Musk and a Handful of AI Leaders Ask for Pause on the Tech," Washington Post, March 29, 2023, https://www.washingtonpost.com/technology/2023/03/29/ai-letter-pause/.

[3] Jonas Bendiksen, "The Book of Veles," Magnum Photos, accessed on May 18, 2023, https://www.magnumphotos.com/arts-culture/society-arts-culture/book-veles-jonas-bendiksen-hoodwinked-photography-industry/.

[4] Eisenhower School AI Industry Study Seminar visit to Nvidia, April 10, 2023.

[5] Brody Ford, "IBM to Pause Hiring for Jobs That AI Could Do," Bloomberg News, May 1, 2023, https://www.bloomberg.com/news/articles/2023-05-01/ibm-to-pause-hiring-for-back-office-jobs-that-ai-could-kill#xj4y7vzkg.

[6] Bloomberg Professional Services, "Introducing BloombergGPT, Bloomberg's 50-billion parameter large language model, purpose-built from scratch for finance," March 30, 20203, https://www.bloomberg.com/company/press/bloomberggpt-50-billion-parameter-llm-tuned-finance/.

[7] Forbes, "19 Ways AI May Soon Revolutionize The Healthcare Industry," April 18, 2023, https://www.forbes.com/sites/forbestechcouncil/2023/04/18/19-ways-ai-may-soon-revolutionize-the-healthcare-industry/?sh=4bd162611bb8.

[8] Elsa B. Kania, "Chinese Military Innovation in Artificial Intelligence," Testimony before the U.S.-China Economic and Security Review Commission Hearing on Trade, Technology, and Military-Civil Fusion, June 7, 2019, https://s3.us-east-1.amazonaws.com/files.cnas.org/backgrounds/documents/June-7-Hearing_Panel-1_Elsa-Kania_Chinese-Military-Innovation-in-Artificial-Intelligence.pdf?mtime=20190617115242&focal=none.

[9] Nestor Maslej, Loredana Fattorini, Erik Brynjolfsson, John Etchemendy, Katrina Ligett, Terah Lyons, James Manyika, Helen Ngo, Juan Carlos Niebles, Vanessa Parli, Yoav Shoham, Russell Wald, Jack Clark, and Raymond Perrault, "The AI Index 2023 Annual Report," AI Index Steering Committee, Institute for Human-Centered AI, Stanford University, Stanford, CA, April 2023, https://aiindex.stanford.edu/report/.

[10] Aaron Kliegman, "US firms pumping billions into China's AI sector," *New York Post*, February 6, 2023, https://nypost.com/2023/02/06/us-firms-pumping-billions-into-chinas-ai-sector/.

[11] Amy J. Nelson and Gerald L. Epstein, "The PLA's Strategic Support Force and AI Innovation," Brookings, December 23, 2022, https://www.brookings.edu/techstream/the-plas-strategic-support-force-and-ai-innovation-china-military-tech/.

[12] Ben Wodecki, "IDC: China set to more than double AI spending by 2026," AIBusiness.com, October 12, 2022, https://aibusiness.com/verticals/idc-china-set-to-more-than-double-ai-spending-by-2026.

[13] Mike Glennon, "Spending on Artificial Intelligence Solutions Will Double in the United States by 2025," International Data Corporation, March 17, 2022, https://www.idc.com/getdoc.jsp?containerId=prUS48958822.

[14] Jon Harper, "China Matching Pentagon Spending on AI," *National Defense*, January 6, 2022, https://www.nationaldefensemagazine.org/articles/2022/1/6/china-matching-pentagon-spending-on-ai.

[15] "Artificial Intelligence [AI] Market Size, Share & Forecast, 2030," Artificial Intelligence [AI] Market Size, Share & Forecast, 2030, Accessed May 7, 2023, https://www.fortunebusinessinsights.com/industry-reports/artificial-intelligence-market-100114.

[16] Cade Metz and Mike Isaac, "In Battle Over A.I., Meta Decides to Give Away Its Crown Jewels," NY Times, May 18, 2023, https://www.nytimes.com/2023/05/18/technology/ai-meta-open-source.html.

[17] Rao, Anand, "PWC's Global Artificial Intelligence Study: Sizing the Prize," PricewaterhouseCoopers (PwC), accessed May 7, 2023, https://www.pwc.com/gx/en/issues/data-and-analytics/publications/artificial-intelligence-study.html.

[18] Sara Zouiten, "Huawei Encourages Adoption of Artificial Intelligence in Moroccan Financial Institutions," *Morocco World News*, May 16, 2023, https://www.moroccoworldnews.com/2023/05/355489/huawei-encourages-adoption-of-artificial-intelligence-in-moroccan-financial-institutions.

[19] Ayana Archie, "Montana Becomes the First State to Ban TikTok," NPR, May 18, 2023, https://www.npr.org/2023/05/18/1176805559/montana-tiktok-ban.

[20] Benjamin R. Dryden and Kate E. Gehl, "Collusion & Competition: What Antitrust Means for AI in Health Care," Foley & Lardner LLP, April 25, 2023, https://www.foley.com/en/insights/publications/2023/04/collusion-competition-antitrust-ai-health-care.

[21] "The EU's Artificial Intelligence Act, Explained," World Economic Forum, European Union, March 28, 2023, https://www.weforum.org/agenda/2023/03/the-european-union-s-ai-act-explained/.

[22] Andrew Smith, "Using Artificial Intelligence and Algorithms," Federal Trade Commission, FTC, April 8, 2020, https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms.

[23] Verma, Pranshu, "IBM Could Replace 7,800 Jobs with Artificial Intelligence, CEO Says," The Washington Post, WP Company, May 2, 2023, https://www.washingtonpost.com/technology/2023/05/02/ai-jobs-takeover-ibm/.

[24] Yan Wu and Sergio Peçanha, "Opinion: Type in your job to see how much AI will affect it" Washington Post, May 9, 2023, https://www.washingtonpost.com/opinions/interactive/2023/ai-artificial-intelligence-jobs-impact-research/.

[25] Frederick Shear, "'IVAS' Campaign of Learning Ensures Development, Production and Fielding Remain on Track," Army.mil, March 14, 2023, https://www.army.mil/article/264773/ivas_campaign_of_learning_ensures_development_production_and_fielding_remain_on_track.

[26] "U.S. Marine Corps Warfighting Laboratory Information Support to Operations (IS2OPS) Project Overview Presentation," January 20, 2023.

[27] Jason Sherman, "Russia-Ukraine Conflict Prompted U.S. to Develop Autonomous Drone Swarms, 1,000-Mile Cannon," Scientific American, February 14, 2022, https://www.scientificamerican.com/article/russia-ukraine-conflict-prompted-u-s-to-develop-autonomous-drone-swarms-1-000-mile-cannon/.

[28] Benjamin Jensen, "Send in the Swarm," blog post, *Center for Strategic and International Studies*, March 24, 2022, https://www.csis.org/analysis/send-swarm.

[29] Lisa Ferguson, "Collaboration with Academia Moving Army Aviation into the Future," U.S. Army Public Affairs, August 1, 2022, https://www.army.mil/article/258948/collaboration_with_academia_moving_army_aviation_into_the_future.

[30] Davis, Gregory A, Travis L DePriest, Brian G Gladstone, Laura A Hildreth, and Miranda G Seitz-McLeese. "Evaluating and Predicting Contract Performance Using Machine Learning: A Feasibility Study," n.d.

[31] Breaking Defense. "Pentagon Should Experiment with AIs like ChatGPT — but Don't Trust Them yet: DoD's Ex-AI Chiefs." Accessed April 28, 2023. https://breakingdefense.sites.breakingmedia.com/2023/04/dods-ex-ai-chiefs-pentagon-should-experiment-with-ais-like-chatgpt-but-dont-trust-them-yet/.

[32] Ashley Andreou, "Generative AI Could Help Solve the US Mental Health Crisis." Psychology Today, Sussex Publishers, March 9, 2023, https://www.psychologytoday.com/us/blog/the-doctor-of-the-future/202303/generative-ai-could-help-solve-the-us-mental-health-crisis.

[33] Andreau.

[34] Amelia Fiske, Peter Henningsen, and Alena Buyx, "Your Robot Therapist Will See You Now: Ethical Implications of Embodied Artificial Intelligence in Psychiatry, Psychology, and Psychotherapy" *Journal of Medical Internet Research*, no. 5 (2019).

[35] Fiske, Henningsen, and Buyx.

[36] Robin C. Feldman, Ehrik Aldana, and Kara Sein, "Artificial Intelligence In The Health Care Space: How We Can Trust What We Cannot Know," *Stanford Law & Policy Review* 30, 400.

[37] Margaret C. Wilmoth and Jeffrey Phillips, "Nurses are in critically short supply in the Defense Department -will Congress act?" The Hill, February 15, 2023, accessed April 17, 2023, https://thehill.com/opinion/healthcare/3856126-nurses-are-in-critically-short-supply-in-the-defense-department-will-congress-act/.

[38] "Health and Healthcare," World Economic Forum, assessed April 19, 2023, https://www.weforum.org/agenda/2020/01/future-of-artificial-intelligence-healthcare-delivery/.

[39] IBM, "How AI Is Impacting Healthcare: Watson Health: IBM," IBM Watson Health, August 10, 2021, https://www.ibm.com/resources/watson-health/artificial-intelligence-impacting-healthcare/.

[40] Karin Kelly, "How AI and Data Science is Changing the Role of Radiologists," Simplilearn, assessed April 19, 2023, https://www.simplilearn.com/how-ai-and-data-science-is-changing-the-role-of-radiologists-article.

[41] Kelly.

[42] Hassan A. Tetteh, "Joint Artificial Intelligence Center (JAIC) and the Warfighter Health Mission," *CADO*, February 26, 2020, assessed April 21, 2023, https://www.ai.mil/blog_02_26_20-jaic_warfighter_health.html.

[43] "Health and Healthcare," World Economic Forum, assessed April 19, 2023, https://www.weforum.org/agenda/2020/01/future-of-artificial-intelligence-healthcare-delivery/.

[44] Artificial Intelligence Industry Study Field Visits, April 10-14, 2023.

[45] Neil Thompson, Shunning Ge, and Gabriel Manso, "The Importance of (Exponentially More) Computing Power," DeepAI, June 28, 2022, 1-2, https://arxiv.org/pdf/2206.14007v1.pdf.

[46] Thompson, Ge and Manso, 1-3.

[47] Thompson, Ge and Manso, 5.

[48] Thompson, Ge and Manso, 6.

[49] Gordon Moore, "Cramming More Components onto Integrated Circuits," *Electronics* 38, no. 8 (April 1965), http://www.monolithic3d.com/uploads/6/0/5/5/6055488/gordon_moore_1965_ article.pdf.

[50] Mark LaPedus and Ed Sperling, "Making Chips at 3nm and Beyond," Semiconductor Engineering, April 16, 2020, https://semiengineering.com/making-chips-at-3nm-and-beyond/.

[51] Scott Morgan, "TSMC Cleared to Build New Factory in Southern Taiwan," *Taiwan News*, December 20, 2018, https://www.taiwannews.com.tw/en/news/3600724.

[52] Emna Amor, "4 CNN Networks Every Machine Learning Engineer Should Know," Top Bots, https://www.topbots.com/important-cnn-architectures/.

[53] "AI and Compute," OpenAI, May 16, 2018, https://openai.com/research/ai-and-compute.

[54] John Roach, "How Microsoft's Bet on Azure Unlocked an AI Revolution," Microsoft, March 13, 2023, https://news.microsoft.com/source/features/ai/how-microsofts-bet-on-azure-unlocked-an-ai-revolution/.

[55] Artificial Intelligence Industry Study Field Visits, April 10-14, 2023.

[56] Artificial Intelligence Industry Study Field Visits, April 10-14, 2023.

[57] J.P. Buntinx, "The Surge in ChatGPT's Popularity Drives Nvidia H100 GPU Prices Skyward," Cryptomode, April 17, 2023, https://cryptomode.com/the-surge-in-chatgpts-popularity-drives-nvidia-h100-gpu-prices-skyward/.

[58] Will Knight, "OpenAI's CEO Says the Age of Giant A.I. Models is Already Over," *Wired*, April 17, 2023, https://www.wired.com/story/openai-ceo-sam-altman-the-age-of-giant-ai-models-is-already-over/.

[59] Andrew Lohn and Micah Musser, *AI and Compute: How Much Longer can Computing Power Drive Artificial Intelligence Progress,* Center for Security and Emerging Technology, January 2023, https://cset.georgetown.edu/publication/ai-and-compute/.

[60] Carol-Jean Wu et al., "Sustainable AI: Environmental Implications, Challenges and Opportunities," Meta Research, January 9, 2022, 1-7, https://research.facebook.com/publications/sustainable-ai-environmental-implications-challenges-and-opportunities/.

[61] Wu et al., 1-7.

[62] Note: GPT-3 utilized 285,000 CPU cores, 10,000 Nvidia V100 GPUs, and 400 gigabits per second of network connectivity per GPU server. (Source: Nefi Alarcon, "OpenAI Presents GPT-3, a 175 Billion Parameter Language Model," Nvidia Technical Blog, July 7, 2020, https://developer.nvidia.com/blog/openai-presents-gpt-3-a-175-billion-parameters-language-model/).

[63] Nestor Maslej et al., *The A.I. Index 2023 Annual Report* (Stanford, CA: A.I. Index Steering Committee, Institute for Human-Centered A.I., April 2023), 120, https://aiindex.stanford.edu/ wp-content/uploads/2023/04/HAI_AI-Index-Report_2023.pdf.

[64] Pengfei Li, Jianyi Yang, Mohammad Islam, and Shaolei Ren, *Making AI Less 'Thirsty': Uncovering and Addressing the Secret Water Footprint of AI Models*, April 6, 2023, *arXiv* (preprint), 2304.03271, 1-3, https://arxiv.org/pdf/2304.03271.pdf.

[65] Wu et al., 1-7.

[66] Kasper Groes Albin Ludvigsen, "ChatGPT's Electricity Consumption," *Medium*, March 1, 2023, https://towardsdatascience.com/chatgpts-electricity-consumption-7873483feac4.

[67] Li, Yang, Islam, and Ren.

[68] James Ang et al., *Decadal Plan for Semiconductors: Full Report* (Durham, NC: Semiconductor Research Corporation, January 2021), 122-146, https://www.src.org/about/decadal-plan/.

[69] Note: this paper does not address the computing and environmental impacts of blockchain technology, which are, to date, worse than that of A.I.

[70] Artificial Intelligence Industry Study Field Visits, April 10-14, 2023.

[71] Kathryn Ross, "Creating Sustainable A.I.: An Interview with Blumind's Niraj Mathur," VentureLAB, October 12, 2021, https://www.venturelab.ca/news/creating-sustainable-ai-an-interview-with-bluminds-niraj-mathur.

[72] Charles Q. Choi, "Brain-Inspired Chips Good for More than AI, Study Says," *IEEE Spectrum*, February 16, 2022, https://spectrum.ieee.org/neuromorphic-computing-more-than-ai.

[73] Michael Palmer, "Data is the New Oil," *ANA Marketing Maestros*, November 3, 2006, accessed May 19, 2023, https://ana.blogs.com/maestros/2006/11/data_is_the_new.html.

[74] Department of Defense, *Executive Summary: DoD Data Strategy*, September 30, 2022, https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

[75] "About Us," Federal CDO Council, accessed May 18, 2023, https://www.cdo.gov/about-us/.

[76] Chief Data Officer's Data Sharing Working Group, *Data Sharing Working Group Findings and Recommendations*, Federal CDO Council, accessed May 17, 2023, https://resources.data.gov/assets/documents/2021_DSWG_Recommendations_and_Findings_508.pdf.

[77] The Office of the Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information Officer, *Department of Defense Information Sharing Implementation Plan*, April 2009, https://dodcio.defense.gov/portals/0/documents/ise/dod%20isip%20-%20apr%202009_approved.pdf, 2.

[78] Lloyd J. Austin III, *2022 National Defense Strategy* (Washington, DC: The Pentagon, October 2022), 19.

[79] Joseph R. Biden Jr., *National Security Strategy* (Washington, DC: The White House, October 2022), 46.

[80] National Security Strategy, 33.

[81] Rachel Lilly, "Quality Data and Validation are Critical for AI: The DOD's chief digital and AI officer answers the question: How do we get data right?" May 3, 2023, https://www.afcea.org/signal-media/defense-operations/quality-data-and-validation-are-critical-ai.

[82] "Data Governance," Principal Deputy, Acquisition Data and Analytics, accessed May 19, 2023, https://www.acq.osd.mil/asda/ae/ada/pd-ada.html.

[83] Sean O'Donnell, Acting Inspector General, *Fiscal Year 2023 Top DoD Management Challenges*, October 14, 2022, https://media.defense.gov/2022/Nov/16/2003115791/-1/-1/1/MANAGEMENT%20CHALLENGES%20FY2023.PDF, 49-51.

[84] "2022 State of Data Science," *Anaconda*, accessed April 15, 2023, https://www.anaconda.com/resources/whitepapers/state-of-data-science-report-2022/.

[85] *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, Public Law No. 117-263, 117th Cong., December 23, 2022, Sec 7226.

[86] World Economic Forum, *Future of Jobs Report 2023* (Geneva, Switzerland: World Economic Forum, May 2023), 5-6, https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf.

[87] "Generative AI Could Raise Global GDP by 7%," Goldman Sachs, April 5, 2023, https://www.goldmansachs.com/intelligence/pages/generative-ai-could-raise-global-gdp-by-7-percent.html.

[88] Goldman Sachs, "Generative AI Could Raise Global GDP by 7%."

[89] David Kiron, Elizabeth J. Altman, and Christoph Riedl, "Workforce Ecosystems and AI," *Brookings Institution*, April 13, 2023, https://www.brookings.edu/research/workforce-ecosystems-and-ai/#:~:text=AI%20supports%20individual%20performance%20within,safety%20in%20some%20workplace%20environments.

[90] Kai-Fu Lee, *AI Superpowers: China, Silicon Valley, and the New World Order* (New York: Harper Business, 2018), 146.

[91] World Economic Forum, *Future of Jobs Report 2023* (Geneva, Switzerland: World Economic Forum, May 2023), 6, https://www3.weforum.org/docs/WEF_Future_of_Jobs_2023.pdf.

[92] World Economic Forum, Future of Jobs Report 2023, 42-44.

[93] World Economic Forum, Future of Jobs Report 2023, 44.

[94] Jamie Birt, "5 of the Highest-Paid Apprenticeships (Plus 5 More Programs)," *Indeed.com*, March 10, 2023, https://www.indeed.com/career-advice/finding-a-job/highest-paid-apprenticeships.

[95] Eric Schmidt, Robert Work, *Final Report: National Security Commission on Artificial Intelligence*, March 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[96] "The State of U.S. Science and Engineering 2022," National Science Foundation accessed May 6, 2023, https://ncses.nsf.gov/pubs/nsb20221/u-s-and-global-stem-education-and-labor-force.

[97] "The State of U.S. Science and Engineering 2022."

[98] Heather B. Gonzalez and Jeffrey J. Kuenzi, "Science Technology, Engineering, and Mathematics (STEM) Education: A Primer," n.d.

[99] Gonzalez and Kuenzi.

[100] Joe McKendrick, "Beyond STEM: Why AI Demands Higher-Level Skills," Forbes, accessed May 10, 2023, https://www.forbes.com/sites/joemckendrick/2018/09/20/beyond-stem-why-ai-demands-higher-level-skills/?sh=6b19893f2c0f.

[101] World Economic Forum, Future of Jobs Report 2023.

[102] "US Markets Stock Ticker - Insider," *Business Insider*, accessed May 10, 2023, https://embed.businessinsider.com/render-embed/live-updates#amp=1.

[103] "US Markets Stock Ticker - Insider."

[104] "The State of U.S. Science and Engineering 2022."

[105] Eric Schmidt, "To Compete With China on Tech, America Needs to Fix Its Immigration System." *Foreign Affairs*, May 16, 2023. https://www.foreignaffairs.com/united-states/eric-schmidt-compete-china-tech-america-needs-fix-its-immigration-system.

[106] Schmidt.

[107] Ashley Gold, "OpenAI CEO in 'Historic' Move Calls for Regulation before Congress," Axios, May 16, 2023, https://www.axios.com/2023/05/16/openai-ceo-sam-altman-artificial-intelligence-congress.

[108] Gold.

[109] "Discrimination by Proxy," AI Blindspot, https://aiblindspot.media.mit.edu/discrimination_by_proxy.html.

[110] Ziad Obermeyer et al., "Dissecting Racial Bias in an Algorithm Used to Manage the Health of Populations," *Science* 366, no. 6464 (October 25, 2019): 447–53, https://doi.org/10.1126/science.aax2342.

[111] Jesse Damiani, "A Voice Deepfake Was Used To Scam A CEO Out Of $243,000," Forbes, accessed April 8, 2023, https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/.

[112] Pranshu Verma, "They Thought Loved Ones Were Calling for Help. It Was an AI Scam.," *Washington Post*, March 10, 2023, https://www.washingtonpost.com/technology/2023/03/05/ai-voice-scam/.

[113] Lou Blouin, "AI's Mysterious 'Black Box' Problem, Explained | University of Michigan-Dearborn," accessed April 29, 2023, https://umdearborn.edu/news/ais-mysterious-black-box-problem-explained.

[114] Artificial Intelligence Industry Study Speaker Series, Eisenhower School, 2023.

[115] "IDF Unit 8200 commander reveals cyber use to target Hamas commander." The Jerusalem Post. February 13, 2023.

[116] Exec. Order No. 12333, 3 C.F.R. (1981).

[117] "Ethics and Autonomous Weapon Systems: An Ethical Basis for Human Control?" Arms Control Association, August 2018, accessed February 18, 2023, https://www.armscontrol.org/act/2018-07/features/document-ethics-autonomous-weapon-systems-ethical-basis-human-control.

[118] Gina M. Raimondo, Secretary and Laurie E. Locascio, U.S. Department of Commerce, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, January 2023, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf, 7.

[119] Department of Defense, *Autonomy in Weapon Systems*, DoDD 3000.09, January 25, 2023.

[120] Joint Chiefs of Staff, "Joint Publication 3-16 Multinational Operations" (United States Department of Defense, March 1, 2019), III–12, accessed March 12, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_16.pdf.

[121] United States Marine Corps, *Law of War/Introduction to Rules of Engagement*, accessed March 25, 2023, https://usmcofficer.com/wp-content/uploads/2014/01/Law-of-War-and-Introduction-to-Rules-of-Engagement-ROE.pdf.

[122] National Security Strategy, 9.

[123] National Security Strategy, 15.

[124] National Security Strategy, 15.

[125] Gina M. Raimondo, Secretary and Laurie E. Locascio, U.S. Department of Commerce, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, January 2023, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf, 7.

[126] National Security Strategy, 10.

[127] National Security Strategy, 11.

[128] Megan Lamberth and Paul Scharre, "Arms Control for Artificial Intelligence," *Texas National Security Review* 6, no. 2, Spring 2023, https://tnsr.org/2023/05/arms-control-for-artificial-intelligence/.

[129] "China's Xi Vows Victory in Tech Battle After U.S. Chip Curbs," *Bloomberg News*, October 16, 2022, https://www.bloomberg.com/news/articles/2022-10-16/china-s-xi-pledges-victory-in-tech-battle-after-us-chip-curbs.

[130] Eric Schmidt et al., *National Security Commission on Artificial Intelligence Final Report,* 2021, accessed February 17, 2023, https://www.nscai.gov/2021-final-report/.

[131] Schmidt et al.

[132] James Ang et al., *Decadal Plan for Semiconductors: Full Report* (Durham, NC: Semiconductor Research Corporation, January 2021), https://www.src.org/about/decadal-plan, 122-146.