AY 2021-2022

IN AI WE TRUST, ALL OTHERS WE MODEL

ARTIFICIAL INTELLIGENCE AND SOFTWARE ENGINEERING

SEMINAR #15 (SPRING)

Dr. James "Kegs" Keagle

Dr. Michael Bartee

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

Table of Contents

Seminar 15 Student and Faculty Acknowledgement

Author Team

COL Andrii Horbenko, Ukraine Armed Forces

CDR Richard M Yates, U.S. Navy

COL Khamis Alkaabi, United Arab Emirates

LTC Richard M. Cruz, U.S. Army

LTC Daniel A. Craig, U.S. Air Force

COL Leslie D Gorman, U.S. Army

CDR Sohnwa Lee, U.S. Navy

CDR Ethan H Karp, U.S. Navy

CDR Scotty L Murphy, U.S. Navy

Ms. Michelle A Zurcher, National Security Agency

Mr. Jericho J Guzman, Defense Intelligence Agency

LTC Wayne A Sanders, U.S. Army

LtCol Matt J Beck, U.S. Marine Corps

LTC Pascal Nzaramba, Rwanda Defense Force-Army

Ms. Irene G. Johnson, Defense Contract Management Agency

Mr. Gary M. Keller, Department of the Army

Mr. Mark J Lemery, Department of Homeland Security

Instructors

Dr. James “Kegs” Keagle, National Defense University (NDU)

Dr. Michael Bartee, NDU

Methodology

The Artificial Intelligence seminar conducted research through academic and think tank publications, consultation with the National Defense University library, and through numerous conversations with leaders across government, the private sector, and academia. Substantial content for this report was adopted from individual papers written during this study.

Engagements and Speakers

5 January:	LTG Meade, Jamaican Chief of Defense
January 19:	NDU Presidential Lecture Series (PLS) – Admiral Grady, Vice Chairman Joint Chief of Staff
20 January:	Dr. Sarah Kirchberger, Asian Pacific Strategy, Kiel University
January 20:	Joint Artificial Intelligence Command (JAIC) – LTG Michael Groen, USMC
26 January:	ES CLS – Intelligence Community Panel
January 27:	Office of the Under Secretary of Defense for Research and Engineering – Dr. Jaret Riddick, Maynard Holliday, Dr. Jill Crisman
January 31:	NSO Group AI Virtual Demonstration – Shalev Hulio
3 February:	Christopher Davis PhD, Cambridge University, Russia's Defense Industrial Complex, Professorial Research Fellow, University of Oxford Senior Research Fellow
9 February:	Eisenhower Commandant Lecture Series (CLS) – Professor Eugene Gholz
10 February:	Jean-Marc Rickli, Geneva Center for Security Policy, Senior Research Professor
16-18 February:	Pittsburg Industry Travel
	Carnegie Mellon University -Shane Shaneman, Strategic Director, National Security and Defense, Adjunct Professor
	Dr. Rita Singh, PhD, Associate Research Professor Language Tech Institute
	CMU National Robotics Engineering Center (NREC) – Jeff Legault
	University of Pittsburg, Human Engineering Research Laboratories – Rory Cooper, Director

	CMU Software Engineering Institute (SEI) – Tom Longstaff, CTO
	Innovation Works, Alpha Lab and Alpha Lab Gear – Afshan Khan
24 February:	Scale AI – Mark Valentine, Head of Federal Market
2 March:	NDU PLS – Gen Richard D. Clarke, USSOCOM
2-4 March:	IBM Watson Center – George Tulevski, Doug McClure, Nancy Greco, Kush Vershney, John Rozen
11 March:	Eisenhower CLS – VADM Mewbourne, Deputy Commander USTRANSCOM
16 March:	Eisenhower CLS – Dr. Brad Roberts
17 March:	DARPA – Benjamin "Bach" Bishop, Department of the Air Force Operational Liaison to the Defense Advanced Research Projects Agency (DARPA)
21 March:	Defense Innovation Unit (DIU) – Mike Madsen, Deputy Director
22 March:	Department of Energy – Angela Sheffield
22 March:	NVIDIA GTC Keynote Watch Party – George DeLisle
23 March:	NDU PLS – Kathy Warden, Chairman, CEO, and President, Northrop Grumman
24 March:	Planet.com – Tonya Harrison, Director of Strategic Science Initiatives
20 March:	NDU PLS – Mr. Bart Gorman, Department of State, Former DCM Moscow
31 March:	Center for New American Studies – Dr. Paul Scharre (Author of *Army of None*)
4-8 April:	California Industry Travel
	Naval Postgraduate School – Jennifer Hudson and Dr. Jim Newman
	Stanford University, Gordian Knot Center, Hacking for Defense – Steve Weinstein and Joe Felter
	JABIL – Dan Gamota, Bill Yang and Sean Thompson
	HP – Tommy Gardner, Shivaun Albright, Paul Reynolds, Tom Anthony, Victor Shkolnikov, Victor Arranga

	VERSE Art of the Future - Non-Fungible Token (NFT) virtual technology exhibit
13 April:	ES CLS – Kim Zetter, Author, and award-winning investigative journalist
14 April:	Oracle – Travis Russell, Scott Nahrang, Darryl McGowan, RB Hooks, Rich Gibaldi
19 April:	Center for Security Studies (CSS) at ETH Zurich – Sophie-Charlotte Fischer
18-25 April:	Virtual Taiwan Industry Travel
	Industrial Technology Research Institute (ITRI) – Stephen Su
	Taiwan Semiconductor Industry Association / eTron – Nicky Lu
	Amazon Web Services – Robert Wang
	Microsoft AI Center – CEO Michael Chang
21 April:	John Hopkins Applied Physics Lab –
21 April:	MISI Dreamport Project – Armando Seay, John Weiler (IT-AAC.org)
22 April:	Wyss Center For Bio And Neuroengineering – Tracy Laabs
26 April:	AI Panel Discussion with National Security Agency and National Geospatial-Intelligence Agency – Dr. Josiah Dykstra, Timothy Janssen, Rachael Martin, Dr. Thomas Walcott, Dr. Jason Wang
27 April	ES CLS – Mr. Palmer Luckey, Founder, Anduril Industries
2 May:	NVIDIA – Omniverse Deep Dive – George DeLisle and Tim Woodard
4 May:	NDU PLS – Gen Jacqueline Van Ovost, USTRANSCOM

No comfortable historical reference captures the impact of artificial intelligence (AI) on national security.

AI is not a single technology breakthrough, like a bat-wing stealth bomber.

The race for AI supremacy is not like the space race to the moon.

AI is not even comparable to a general-purpose technology like electricity.

However, what Thomas Edison said of electricity encapsulates the AI future:

'It is a field of fields… it holds the secrets which will reorganize the life of the world.'

Edison's astounding assessment came from humility. All that he discovered was 'very little in comparison with the possibilities that appear.'

– National Security Commission on Artificial Intelligence (NSCAI) Final Report[1]

EXECUTIVE SUMMARY

The NSCAI explained in its 2021final report that AI is a unique human invention that is not a single event or technology. Rather, AI is like what Thomas Edison said of electricity, "It is a field of fields… it holds the secrets which will reorganize the life of the world."[2] Today, we experience AI daily. We interact directly with digital assistants like Alexa, Siri, and Watson or the IRS has our tax returns analyzed by AI to detect fraud. However, the examples today are minor advances (the tip of an iceberg) in comparison to the transformation that is coming.

This study determined that the greatest impact of AI will be on human decision making. AI can already surpass the ability of a human to process data by many thousands of times and do so at incredible speeds. Through continuous advancement in processing power and software efficiency, this advantage between AI machine and human becomes greater. Processing data is a tremendous strength of AI, but can AI create insights? More importantly, can AI be trusted to act? The answer to both these questions must be a resounding 'YES' and we must find ways to make it so.

The US military often teaches the decision-making process as a continuous loop using the acronym OODA for Observe, Orient, Decide, and Act. This process needs to account for the introduction of AI by shifting human decisions earlier in time, creating AI agents that are tested and trusted, empowering AI to act side-by-side with humans, and maintaining overall human oversight and control. We propose this modified process be called GOOD-AI for Guide, Observe, Orient, Decide, Act and Interact. A principal agent such as a commander (or civilian leader) guides the process by determining what needs to be achieved (intent) and setting the parameters, ethics, thresholds (right and left limits), etc. Key to this step, and throughout the process, is the assessment of risk impact and probability to determine when and how agents (human or machine) may act. As human-machine teams interact together solving problems, results must be fed back to the commander so that revised guidance can be fed forward. The interaction ensures continuous improvement, oversight, and the ability to terminate a system if necessary.

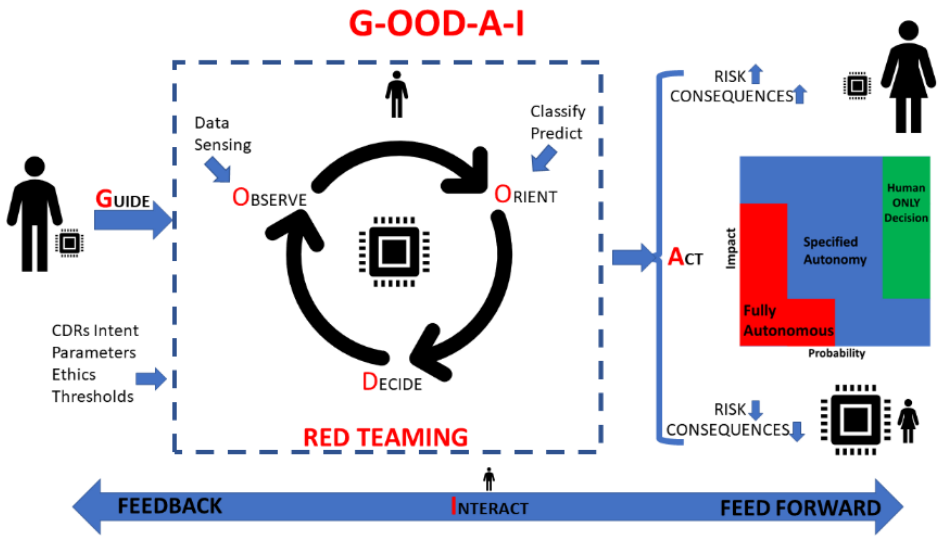

Figure 1. Adopting the OODA loop to a world with AI

Greek mythology tells of Prometheus, the Titan god, bestowing to humans the use of fire so that they could live more comfortably and prosper. The power of fire is neutral; the use of fire continues to be positive or negative based on the desires and actions of people. Today, we have created a new power, Artificial Intelligence (AI), with god-like potential. Unlike fire, AI is not simply a gift, but a tool invented by human enterprise. It is up to us to determine how we will continue to forge AI and use it to improve our lives. This study explores the development and upholding of ethics, standards, and law to ensure that the impacts of AI remain consistent with US values. To make this a reality, the US must continue to lead AI international discourse, practice, and accountability.

This study identifies three key challenges. First, the change created by AI can outpace humans. Addressing this challenge requires that we lead emerging technologies that will produce even more powerful AI, and uphold ethics, standards, and laws that are true to US values.

Second, in its final 2021 report to Congress, the NSCAI stated that presently a national AI strategy does not exist, there is insufficient organizational structure to collaborate, and inadequate resources are in place to win the global race and maintain the US's position as the leader in AI technology.[3] Recognizing these challenges, Congress took sweeping steps to deploy government agencies, enacting 20 separate provisions in the legislation of the National Defense Authorization Act 2021.[4] This study recommends that Congress' actions be considered only a start of the concerted effort necessary to increase momentum and realize the full potential of the nation's intellect, creativity and determination.

Third, human capital is the limiting factor to retaining the US's leadership position in AI and other critical technologies. Large investments into early K-12 education by the government and industry are needed to inspire generations of national security entrepreneurs and workers.

Unfortunately, the US's foremost challenger in AI, China, sees AI as critical to achieving its goal of creating a superior "world-class military".[5] China's objective is unmistakably to secure China's superpower status, as stipulated by China's ambition toward the "Great Rejuvenation."[6] Fundamentally, China's grand goal is not short-term advancement but long-term global control. It is essential to realize that AI will be the key enabler because of its ability to boost all industries. Furthermore, China's pursuit of AI objectives is outside the norms of international and US values on which international security increasingly depends. Alone, the US may be unable to outcompete China in terms of sheer numbers of investment, people, or systems. However, the US can, and must, marshal its partners and empower its people to innovate and create a freer and more prosperous world. **The US must accelerate implementation of ethical AI to secure the future - America's and the world's!**

Recommendation Summary

Change created by AI can outpace humans	
Leading Emerging Technologies	Problem – AI and quantum technologies will fundamentally change human decision making. Solution – Create a commercialization strategy for quantum that paves the way for industry and the government to accelerate out of the lab. – Adapt decision making processes to account for AI (GOOD-AI).
Upholding Ethics, Laws and Standards	Problem – Standards for ethical AI are not agreed to internationally. Solution – Reinforce ethical AI guidelines like those published by the DoD. – Require measures of the trustworthiness of AI. – Require 'red team' testing before any government or military AI is implemented. – Lead global initiatives to generate international norms and eventually law addressing the abuse of military AI. – Work towards an international body for AI cooperation and lawful use.
A national AI strategy does not exist	
Turbo-charging American Innovation	Problem – A national AI strategy does not exist. Solution – Establish a comprehensive national AI strategy to focus the US innovation system with clear priorities, measurable timeframes and goals, a shared mission, and the criticality of partnerships. • Grant the NAIIO the necessary authorities to drive national priorities. • Include state governments, industry and international partners. • Synchronize strategy across all other solutions.
Accelerating AI Adoption with Partners	Problem – Existing funding opportunities fail to identify and transition the most disruptive 'deep tech' solutions. Solution – Establish new Government Commercial Strategic Investments (GCSI) that encourage longer term startup investment in collaboration with Corporate Venture Capital. – Establish more technical Partnership Intermediary Agreements with industry for innovation centers.
Human Capital is the Limiting Factor	
Inspire a Generation of National Security Entrepreneurs and Workers	Problem: The Unites States is not educating or training enough human capital with the skills needed to meet the challenges of emerging national security technologies. Solution: A STEM Human Capital Development Plan that inspires interest at the K-12 level and incentivizes higher learning leading toward STEM careers and skill-sets needed to continue US competitive advantage. – Tuition assistance/forgiveness for critical areas such as computer science, machine learning, quantum engineering.

Introduction

What is AI?

AI is "The theory, development, and simulation of computer systems able to perform tasks normally requiring human intelligence."[7] Other AI definitions are more context-specific and worth noting. In particular, the National Intelligence Council's (NIC) *Global Trends 2040* report differentiates between 'artificial narrow intelligence' (ANI) and 'artificial general intelligence'. "Artificial Intelligence (AI) is the demonstration of cognition and creative problem solving by machines rather than humans or animals, ranging from narrow AI, designed to solve specific problems, to Artificial General Intelligence (AGI), a system that in the future may match a human being's understanding and learning capacity."[8] The Congressional Research Service also follows the ANI and AGI definition model: "a computer system capable of human-level cognition."[9]

AI is often cited for its impact. According to industry analysts, the technology's prospective economic implications and potential benefits are universally venerated. For instance, Accenture Consulting estimated that AI could double annual economic growth rates in the 12 largest industrialized economies by 2035 by raising labor productivity and creating a new virtual workforce.[10] Price Waterhouse Coopers further corroborated this, which assessed that the adoption and application of AI would enhance global gross domestic product (GDP) by 14% ($16 trillion) by 2030.[11]

How does AI work?

AI has been a significant development activity since 1956 and an idea among philosophers long before that.[12] The Defense Advanced Research Projects Agency (DARPA) currently describes three waves of AI – (1) handcrafted knowledge, (2) statistical learning, and (3) contextual reasoning.[13]

A simple example of the first wave, handcrafted knowledge, is a basic telephone help service. With handcrafted AI, the developer, in collaboration with subject matter experts, programs the system to conduct predictable steps – *If this input is received, then do that*.[14] These systems are still very much in use today and can be extraordinarily capable and useful for complex tasks from tax preparation to missile guidance systems.[15] Since handcrafted knowledge AI is dependable and traceable, they will always be in use, but they are labor-intensive and costly to design and maintain.

The current wave that DARPA describes as statistical learning, also called machine learning, was enabled by the vast amount of data available from the internet, advances in computer processing and cloud computing, and better tools.[16] Machine learning involves providing large data sets to an algorithm to train it to learn to complete a task and become better at the job over time. Training can follow multiple paths:

1) Supervised – provided data sets labeled by humans
2) Unsupervised – provided un-labeled data that the algorithm sorts for patterns
3) Semi-supervised – a combination of supervised and unsupervised
4) Reinforcement learning – the AI collects data from its environment (real or simulated) and receives a reward in the form of feedback input when a task is successful.[17]

From supervised to reinforcement learning, the predictability of the training method decreases. However, each training method has important applications. An important type of algorithm called neural network (or deep learning) is modeled on biological neurons. One can train neural network algorithms using the same methods already described, but they have a unique characteristic. It isn't easy to understand or even show the decision steps that resulted in the output. This characteristic may limit such algorithms to non-critical tasks until they are better understood and more transparent[18] Ironically, scientists still do not know how human brains make many decisions.[19]

Machine learning AI has provided incredible abilities to analyze imagery, recognize language, and identify patterns in business data. While powerful, it performs best given a narrow set of tasks, even within the same general task category.

Industry Analysis

This study group conducted analysis of six specific corporations leading in the AI and software industry – Amazon Web Services (AWS), IBM, Microsoft, and NVIDIA from the US and Huawei and Tencent from China. The study also engaged startups and small business through engagements with the incubator Innovation Works, and a model of small business success, Scale AI. Also, any industry study would be incomplete without input from academia, the US government (USG), and foreign partners. The study will provide its analysis in the context of Michael Porter's Competitive Advantage of Nations framework, also known as Porter's Diamond.[20]

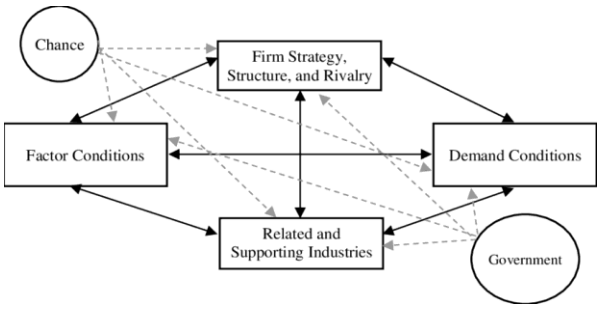

Figure 2. Porter's Diamond

Related and Supporting Industries

The explosive growth of AI is the result of advancements in several supporting industries. Integrated circuits (IC), the internet, information and communications technology (ICT), data storage, and cloud computing all provide access to AI's key ingredient – data. And as every source for this study stated repeatedly, 'It is ALL about the DATA'. W. Edwards Deming, an American statistician and management theorist, is widely attributed as saying it best, "In God we trust. All others must bring data."[21]

NVIDIA, founded in 1993, invested heavily in the development of graphics processing IC and invented the Graphics Processing Unit (GPU) allowing parallel processing of data. In 2006, NVIDIA released Compute-Unified Device Architecture (CUDA) to enable the most

efficient use of its GPUs. CUDA became, and remains through continuous evolution, one of the most powerful tools accelerating development and implementation of AI.[22] In 2012, the cost of a giga-FLOP of computing power fell below one dollar ($1).[23] This was the result of the fierce competition in the graphics processing industry. Without these technical advancements and cost reductions, AI would have remained a tool of limited use that was only available to organizations with the most resources.

Earlier wireless standard implementations such as 3G and 4G were based significantly on vendor hardware solutions that made it difficult to obtain the data needed to support AI. In contrast, 5G is software centric with data centers built on cloud computing. Cloud Infrastructure as a Service (IaaS) is a computing service that offers essential compute, storage, and networking resources on-demand, on a pay-as-you-go basis.[24] Within this market, the customer does not have to have many skills or existing hardware beyond using a computer or smartphone and having a broadband internet connection. As a customer's business grows, they can rapidly scale the type and size of the services they purchase from an IaaS provider. 5G provides better communication support to cloud services and enables movement of the vast amounts of data created by the Internet of Things (IoT). Data from the IoT will provide many AI opportunities.[25] Future 6G+ standards are in development to make the 'intelligentization' of the IoT and other systems possible (smart manufacturing, smart energy, smart building, smart logistics, etc.)[26]

Demand Conditions

Providers of IaaS, including all five of this study's focus corporations, now include access to AI algorithms, implementation tools, and even data to differentiate themselves from competitors. This means that AI is accessible to anyone, from a single individual to a small business to an international mega-corporation. In today's extremely competitive global economies, every player needs to become as efficient as possible, and AI provides an opportunity to find and implement efficiencies before competitors and often in real-time through machine learning. The demand for AI is very high and is expected to grow rapidly with AI software revenue reaching $126B by 2025.[27] This is especially true in fields favored by current technologies and with increasing availability of data including business and finance, image processing, language, and biology.[28]

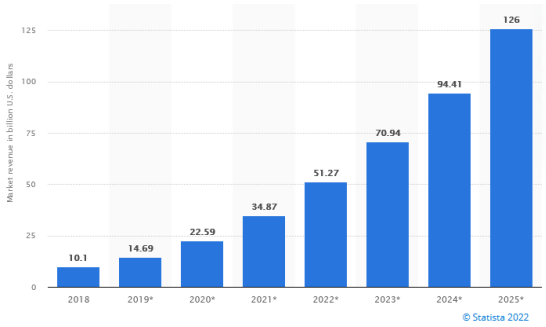

Figure 3. Revenues from AI software market worldwide

An area where demand has lagged has been in implementation within the USG at all levels. Since 2020, the number of AI efforts have risen sharply, especially within research institutions and the Department of Defense (DOD). However, they remain low in other areas[29] and surprisingly low compared to the private sector. This may be attributed to numerous barriers to the government adopting AI and preventing industry from providing AI services.

Government

Industry initiated AI development through a Rockefeller grant to Dartmouth University in 1956. However, it was the USG that provided significant early basic research funding through what is now the Defense Advanced Research Project Agency (DARPA) and National Science Foundation (NSF). The government also played a significant role in providing the stable, long-term investment that allowed AI development to continue through several 'winters' during which private interest waned due to a lack of immediate results. Today, the amount of funding from the private sector greatly surpasses that of the USG as companies race to benefit financially from AI. While federal AI research and development spending will likely exceed $6B in 2021,[30] private investment in the US was nearly $53B.[31]

Though the USG needs to continue investing in AI, it must understand that it cannot outpace the volume of demand or amount of funding from world-wide commercial markets. In AI, the USG is an adopter of commercial technology, not a driver. At the same time, the USG still has significant power, especially through policy and legislation. The USG can and should influence industry in the areas of basic research, ensuring ethical and lawful AI, and ensuring that the nation has the right people with the right skills to implement AI better than anyone else.

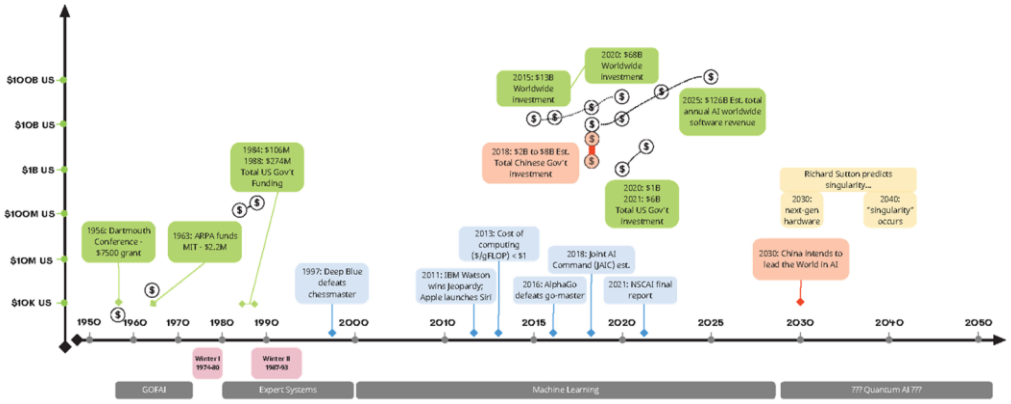

Figure 4. AI Timeline with key events and scale of funding examples

Firm Strategy, Structure and Rivalry

Quite simply, the AI marketplace is extremely competitive and changing very rapidly. Many companies of all sizes can purchase AI resources to develop unique capabilities, arrive at novel insights, and sell services to others. This vibrant community is driving much of the innovation and revenue that is attributable to AI. A small number of large international corporations, including those focused on in this study, dominate the underlying AI infrastructure. The number of AI infrastructure suppliers may decline further over time. Price competition is high, it is becoming increasingly difficult for companies to differentiate their offerings, and customers are increasingly capable of moving between suppliers. Consolidation among AI infrastructure should be monitored for possible government intervention since a trend towards monopoly will increase costs, reduce innovation, and may present a national security risk.

Factor Conditions and Chance

The basic resources required for AI include the natural resources needed to manufacture data storage, collection, and processing equipment. It also includes the complex, international supply chains that provide the necessary components and end-user devices, especially ICs. Competition for these resources is very high and the chance introduction of the 2019 COVID pandemic has revealed the true vulnerability of US supply chains.

Competition with China (and other adversaries)

China's objective is unmistakable. The goal is to secure China's superpower status, as stipulated by China's ambition toward the "Great Rejuvenation."[32] **Fundamentally, China's grand goal is not short-term advancement but long-term global control.** It is essential to realize that AI will be the key enabler because of its ability to boost all industries.

China's government support for business and institutions is astonishing and continues to increase. Launched from its 'Made in China 2025' plan, it intends to commit $1.68 trillion to transform its economy and dominate key industries, including artificial intelligence, advanced information technology, and the critical infrastructure to support it.[33] In effect, Made in China 2025 is an operational plan strategically aligned to a grander scheme to lead AI by 2030.

The COVID pandemic revealed significant US vulnerabilities to the current international supply chain structure. While the US still leads in the development and supply of the best IC designs, the IC industry is dangerously dependent on rare-earth materials almost exclusively mined in or by China.[34] Further, more than 50% ICs are manufactured by Taiwan Semiconductor Manufacturing Corporation (TSMC).[35] China maintains that Taiwan has always been part of China and that control of Taiwan will be restored. Because of US dependence on TSMC, the loss, damage, or destruction of TSMC facilities would be catastrophic. The US increase its independence through efforts that support domestic IC manufacturing such as the Chips for America and FABS Act.[36]

The US is also in competition with China for people with technical knowledge and skills. A 2018 report underscored that China had at least 4.7 million recent Science, Technology, Engineering and Math (STEM) graduates. The US had 568,000.[37] American universities and research institutions educate many of the Chinese students. Presumptive People's Liberation Army (PLA) officers learn about advanced and emerging technologies such as AI, quantum computing and hypersonics, then take their education back to China, feeding their military expansion.[38]

While other adversaries such as Russia, Iran and North Korea do not stand out as major investors in basic research and development of AI, this does not mean they do not pose a threat. The democratization of technology may allow them to weaponize technology, especially unconstrained application of AI to autonomous systems, with profoundly negative impacts on the world.[39] The most important mitigation against risks from China and other adversaries is to strengthen America's ability to adapt to every challenge.

Turbo-charging American Innovation

The foundation of the United States' innovation system traces to the end of World War 2 and Dr. Vannevar Bush, the Director of the Office of Scientific Research and Development. In a letter to Dr. Bush, President Franklin D. Roosevelt praised the work of the Office of Scientific Research and Development for "coordinating scientific research and in applying existing scientific knowledge to the solution of the technical problems paramount in war."[40] The letter's purpose was to obtain a plan from Dr. Bush to apply the "same vision, boldness, and drive with which we have waged this war" to create a "fuller and more fruitful life."[41] The response, titled *Science, The Endless Frontier*, laid the foundation for key institutions and processes that enabled the US to prosper through the cold war, multiple wars in the middle east and into the present day. These institutions include the National Science Foundation (NSF), national laboratories, defense service research laboratories, DARPA, University Affiliated Research Centers (UARCs) and Federally Funded Research and Development Centers (FFRDCs). These institutions have served the nation well, but in the face of extreme and unbalanced competition from China, improvements are needed. The core problem to solve is how to reduce the time and increase the success rate of a technology's transition from development to implementation, often referred to as 'crossing the valley of death'.

With the impetus of renewed great power competition, improvements to the US innovation system aimed at the valley of death have been growing in number (Figure 5). Defense Innovation Unit - Experimental (DIU-x) was established in 2015 by then-Secretary of Defense Ashton Carter to engage America's technology companies As of DIU's 2021 annual report, it has delivered 35 capabilities,[42] transitioning an average of six technologies per year.[43]

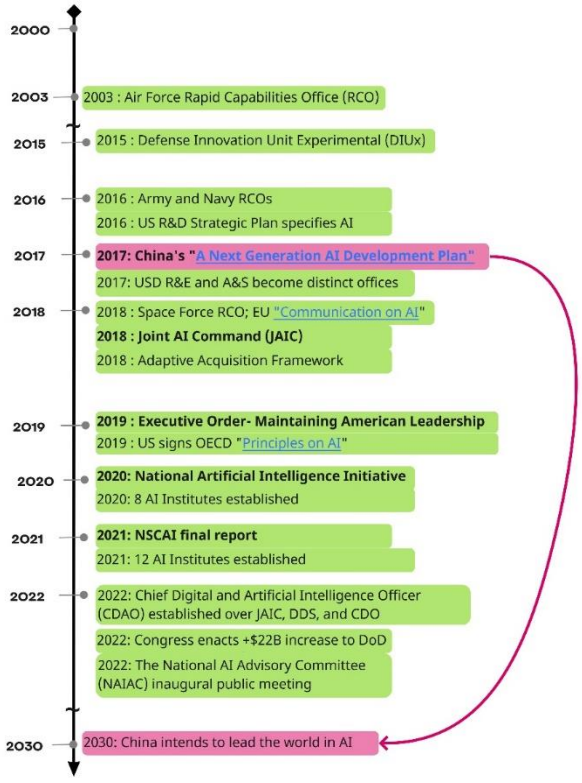

Figure 5. Timeline of improvements to US innovation system

There is also no shortage of leaders advocating for delivering "performance at the speed of relevance."[44] Ms. Ellen Lord, Undersecretary of Defense for Acquisition & Sustainment (USD A&S) from 2017 to 2020, stated that the Adaptive Acquisition Framework (AAF) she approved in the revised Department of Defense Instruction (DoDI) 5000.02 was "the most transformational change to acquisition policy in decades."[45] The current Deputy Secretary of Defense, Ms. Kathleen Hicks, is working on expanding the AAF further[46] and accelerating capabilities with a Rapid Defense Experimentation Reserve (RDER).[47] In the 2017 NDAA, Congress established the distinct offices of the USD A&S and USD Research and & Engineering (USD R&E) with the

clear expectation that OUSD R&E "would take risks, press the technology envelope, test, and experiment, and have the latitude to fail, as appropriate."[48] The current USD R&E, Ms. Heidi Shyu, has energized her department to do this by focusing on 14 critical technology areas,[49] approving 32 proposals to be funded by RDER and declaring her belief that Congress is "on board with Pentagon tech priorities" and will continue increases like the $22 billion increase to the 2022 NDAA.[50] Based on the National Artificial Intelligence Initiative Act of 2020, 18 National AI Institutes and two Agency AI Institutes have been established (Annex B: AI Institutes).[51] These new institutes augment the Software Engineering Institute lead by Carnegie Mellon University to advance DOD's understanding and use of software including AI since 1984.[52] During this study an industry partner stated, "At least the Government is self-aware that it needs to catch up" and based on the number of its initiatives it is certainly striving to do so.

Despite the number and diversity of these initiatives, in its final 2021 report to Congress, the National Security Commission on AI stated that presently a national AI strategy does not exist. Further it states that there is insufficient organizational structure to collaborate, and inadequate resources are in place to win the global race and maintain the US position as the leader in AI technology.[53] In contrast, China is rated superior in government strategy, digital infrastructure, and operational ecosystem for future innovation.[54] Clearly, China is unmistakably determined and focused on overtaking the U.S.

Recommendations

This study recommends that the US establish a comprehensive national strategy for organizing, aligning, cooperating, and supporting efforts to achieve a national whole-of-government and society approach to AI. Additionally, the US needs to expand the recently established National AI Initiative Office (NAIIO) beyond federal interagency cooperation by granting the NAIIO the necessary authorities to drive national priorities. Moreover, the NAIIO should increase its interface to include participation with state governments to establish a more complete whole-of-government effort and enhance public-private sector participation across all levels of government.

China may have more people and the political ability to direct its people towards a goal. However, China cannot match the quality, diversity, and independent thought (creativity) of a free people focused on common goals. In directing its people to produce innovation, China accomplished creating 63 percent more publications than the US in 2021. However, the same study notes that with fewer publications, the US maintained "a dominate lead among major AI powers in the number of AI conference and repository citations."[55] This suggests that the US produces quality of work over mere quantity. Establishing a comprehensive national AI strategy will turbo-charge the US innovation system by establishing clear priorities, measurable timeframes and goals, and reinforcing shared mission and the criticality of partnerships.

Leading Emerging Technologies

"If quantum mechanics hasn't profoundly shocked you, you haven't understood it yet."

– Niels Bohr

The world is creating 2.5 exabytes (2.5 billion gigabytes) of data every day.[56] Quantum computing could provide the capability to process that amount of data in a useful and timely manner. Therefore, conditions are set for emerging technologies to advance, if only the amount of data that traverses the internet alone is considered. Internet data doubles every year due to the increase in users, growth in bandwidth availability, and improved connectivity. By 2024, annual internet data alone is estimated to reach almost 150 zetabytes (Figure 6).[57] These trend lines indicate astounding rates of data growth that no human could possibly process even with the aid of human – AI machine teaming. Advances in quantum computing hold the promise to further increase AI capabilities and address this challenge.

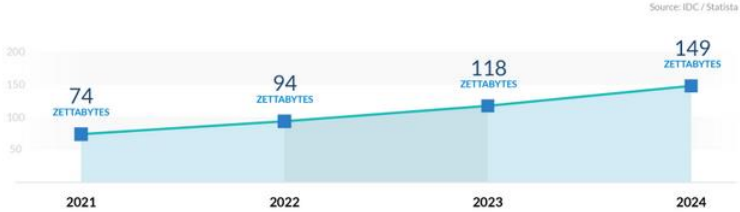

Figure 6. Estimated Internet Data Growth

In 2018, the USG established the National Quantum Initiative Act to provide a solid foundation for quantum R&D. However, the USG must formalize a strategy for quantum focused on building a quantum-ready workforce, experimental development efforts through R&D partnerships with industry and committing to a long-term commercialization strategy. Aggressive pursuit of a national quantum strategy will help offset human displacement or being outpaced by our Great Power competitor, China, as quantum technologies and science advance into the future.

What is Quantum Computing (QC)?

Quantum computers are devices that use the fundamental laws of quantum mechanics to process information. "Instead of using bits of 0s and 1s, as all classical computers do, quantum computers' quantum bits – or qubits – represented in combinations, or superpositions, of states of 0 or 1. Superposition gives quantum computers the potential for exponentially growing compute states," says Bob Sutor, vice-president of IBM Q Strategy & Ecosystem. Quantum machines can look at information in innumerable simultaneous states, store many more variables in a much smaller space, and they can have greater processing speeds.[58] QC can be over 100 million times faster than the most sophisticated supercomputer we have today. It is so powerful that QC can do in four minutes what it would take a traditional supercomputer 10,000 years to accomplish. QC is orders of magnitude more powerful than traditional computers, with potential applications in pharmaceuticals, finance, transportation, and beyond.

Applications for Commercial and Government Use

QCs are especially good for optimizing problems and are designed to explore all possibilities and evaluate those that are most probable for success. Examples of applications include optimizing data flow through a network, supporting air traffic controllers for congested airports, or evaluating war game scenarios for military engagements. QCs will enable advances in machine learning for pattern recognition and target identification, in turn, enabling the development of more accurate lethal autonomous weapon systems.[59] QCs are most known for their potential ability to build and break current encryption algorithms.

IBM remains at the forefront of industry research for quantum computing. Citing QC as the most disruptive technology since the transistor, IBM believes the world is entering the 'Quantum Decade' and is rapidly advancing from a prototype QC to a system with 127 stable qubits and cloud technology communications. IBM developed a Quantum System One network and partnered with four international organizations to establish a research and development system to prepare for the Quantum Decade.[60]

Government Policy and Funding to Advance QC

While the US historically played a leading role in developing quantum technologies, QIS related technologies are now a global field. China is second to the US in quantum capabilities and rapidly closing the technology gap. China incorporated QC into its 15-year science and technology development plan with annual funding of over $250 million per year. Additionally, China is building a multi-billion-dollar quantum computing mega-project. If the US is to maintain its leadership position, more resources will be needed.[61]

The National Quantum Initiative Act provides a coordinated federal program to accelerate quantum R&D.[62] While mostly providing a broad umbrella for the direction of quantum R&D, the creation of some specific quantum entities such as the National Quantum Coordination Office (NQCO), the Subcommittee on Quantum Information Science (SCQIS), the Subcommittee on the Economic and Security Implications of Quantum Science (ESIX), and the National Quantum Initiative Advisory Committee (NQIAC) play significant roles in pursuit of Quantum Information Science (QIS).[63] These are important organizational steps to advance QIS.

The US also committed to a five-year investment of $1.2 billion in quantum information research and has expanded collaboration with allies and partners. The French government announced a five-year €1.8 billion strategy to boost research in quantum technologies, specifically quantum computers. Other nations such as Japan, South Korea, and Germany, also made significant contributions to QC.[64] Collectively these contributions by the US and its partners are imperative to accelerating technology advancements, establishing global standardization for QC, and countering China's goal of dominating this uncharted opportunity.

Impact of AI (and Quantum) on Decision-Making

When describing plans to develop and field human and AI machine pilot teams, the Secretary of the Air Force, Frank Kendall, recently stated "There is no question in my mind that

machines are going to be better at this than people. They are going to be faster. They are not going to get tired, and they will push the envelope further to the limits of the aircraft."[65] We further project that Kendall's pronouncement will apply not just to aviation, but to every aspect of our lives. Use of AI is rapidly decreasing what the military refers to as 'time to decision'. With the future prospect of combining AI and QC, this time reduction will apply to ever more complex problems. Optimal solutions supporting decisions may be determined in seconds, vice hours or days using classical computers. We need to understand and remain in control of how AI effects our decision making.

The US military often teaches the decision-making process as a continuous loop using the acronym OODA for Observe, Orient, Decide, and Act. This process needs to account for the introduction of AI by shifting human decisions earlier in time, creating AI agents that are tested and trusted, empowering AI to act side-by-side with humans, and maintaining overall human oversight and control. We propose this modified process be called **GOOD-AI** for Guide, Observe, Orient, Decide, Act and Interact.

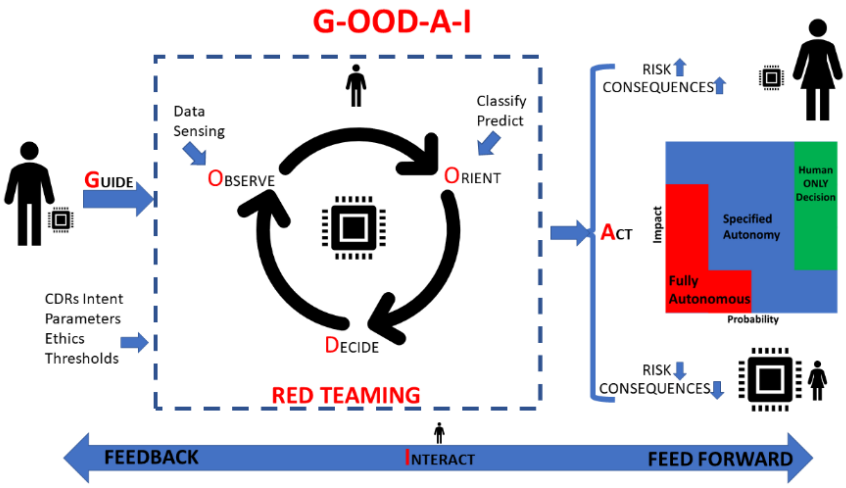

Figure 7. Adopting the OODA loop to a world with AI

A principal agent such as a commander (or civilian leader) guides the process by determining what needs to be achieved (intent) and setting the parameters, ethics, thresholds (right and left limits), etc. Key to this step, and throughout the process, is the assessment of risk impact and probability to determine when and how agents (human or machine) may act. As human-machine teams interact together solving problems, results must be fed back to the commander so that revised guidance can be fed forward. The interaction ensures continuous improvement, oversight, and the ability to terminate a system if necessary.

AI can be designed to perform in three different ways. The first and most common AI method is *human in the loop* or *human only decision*. This method leverages AI to identify patterns in complex data and provide them as an output for a decision-maker.[66] Human in the loop is often preferred because it defaults to a human making the decision. This method should remain the default for high negative impact/high probability of occurrence applications. However, the downside is that humans add significant time and within some use cases such time may not be available.

The second AI method is known as *human on the loop* or *specified autonomy*. With this method, the human operator has complete oversight and override authority, but the AI has a certain threshold for making specific decisions.[67] Some people are comfortable with this model,

and some are not. One senior military leader who believes human on the loop is the future is Air Force General Timothy O'Shaughnessy, the Command of North American Aerospace Defense Command (NORAD). He believes that "what we have to get away from is … 'human in the loop,' or sometimes 'the human is the loop.'"[68] GEN O'Shaughnessy believes that the only way to keep up with advanced technologies, such as hypersonic missiles, is to cede some control to autonomous AI systems that can react quickly enough to adapt. Human on the loop may be applicable when probability of occurrence and risk impact are moderate, as well as when risks are largely knowable and limits on AI decision making can be expected to function well.

The third and most advanced AI method is human *out of the loop* or *fully autonomous*. This method cedes almost complete control for decision-making to the AI construct.[69] This method is appropriate when risk is low such as in the controlled environment of a factory. However, it may also be necessary to move beyond current human capability and speed. One of the most prevalent examples of the *human out of the loop* model is self-driving vehicles. People can just turn on their car, enter an address, and then allow the car to get them to their destination. The user is 'out of the loop' during that drive. The car decides when to accelerate, when to brake, and when to change lanes. All decisions have been left to a trusted AI model in these circumstances.[70] However, it has taken a long time and massive amounts of data to reduce risk sufficiently for some humans to trust self-driving cars. In many cases, they still don't.

The Guide step in GOOD-AI reflects the human portion of future decision making moving far to the left of when and how real-time decisions will be made. This guidance must determine which form of AI will be implemented given the risk probabilities and impacts of an application since it is integral to the design and construction of AI systems.

Recommendations

A US **commercialization strategy** for quantum should be established to pave the way for industry and the government to accelerate out of the lab.

- Invest in targeted, time-limited quantum R&D programs to achieve concrete, measurable objectives.
- Monitor the quantum field closely to evaluate the outcome of federal QIS investments and quickly adapt programs to take advantage of technological breakthroughs.
- Maintain stable and sustained core QIS programs that can be enhanced as new opportunities appear and restructured as quantum impediments evolve.
- Pursue partnerships to build a quantum-ready workforce.
- Lead global establishment of quantum computing standards and regulation through representation in the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) and other technology governance bodies.

The US must recognize that **AI will have profound impacts on decision-making** processes. Current processes must be adapted to account for this (GOOD-AI) and these processes must be taught widely and implemented whenever AI is part of a solution.

Applying Standards, Ethics, and Laws

Increasing demand for AI-led technology underpins US economic prosperity and national security but has sparked debates on the inherent moral, ethical, and legal dilemmas associated with delegating life-and-death decisions to machines.[71] Unlike the US and its businesses bent on ethos and fair market competition, Chinese companies are legally obligated to promote the Chinese Communist Party (CCP) great power competition ideology and socialist economic market.[72] As stated by Ms. Gina Raimondo, Secretary of Commerce, "The greatest issue of our time is the struggle between democracy and autocracy," and that AI is at the center of this with massive potential for both good and bad.[73] The US must lead the world in ethical implementation of trusted AI through domestic policy and laws and leadership on international standards.

Standards Build Trust

Trust is a component of ethics and values that must be understood to increase adoption and deepen acceptance of AI. Establishing standards and implementing those standards will create and increase trust. The ability to explain the specific AI/ML solution (referred to as explainability) is the most relatable trust attribute to stakeholders and the workforce. When technology is explainable, the result is an understanding of the technology, which provides the opportunity to build trust and create trustworthy AI solutions.

Through research and evaluation of various industry trust frameworks, the finding of this study is that the *DOD 5 Principles for AI Ethics* are well suited to assess trustworthiness.[74] The sum of the five ethical elements creates trust within the Department of Defense. The following descriptions from the *DOD 5 Principles for AI Ethics* are adapted to articulate the association to trust elements and the vernacular from the conference paper of Toreini et al. shown in parentheses.[75]

- **Responsible** – the appropriate amount of human involvement in the AI's output. The AI produces the intended result. (Safety and Accuracy).
- **Equitable** - unintended biases are removed and managed through feedback. (Fairness).
- **Traceable** - a proper understanding of the technology, development processes, and operational methods applicable to AI capabilities, including transparent and auditable methodologies, data sources, and design procedures and documentation. (Auditable/Explainable)
- **Reliable** - explicit, well-defined uses and the safety, security, and effectiveness of such capabilities are subject to testing and assurance within those defined uses across their entire life cycles. (Security and Resiliency)
- **Governable** - fulfill the AI intended functions while capable of detecting and avoiding unintended consequences and disengaging or deactivating deployed systems that demonstrate unintended behavior. (Auditable)

The DOD also has a model it uses to measure the maturity and readiness of a technology to be adopted and deployed into an operational state called Technology Readiness Level (TRL).

A certain amount of trust is associated with the TRL assessment. Trust is measurable and can be demonstrated/proven. As AI implementation grows, an improved DOD TRL, or similar assessment that measures the trustworthiness of AI, should be required of all AI systems.

Ensuring trust is planned and captured in the technology requirements prior to development is known as the Chain of Trust.[76] Researcher at IBM in New York and author of *Trustworthy Machine Learning*, Kush R. Varshney, provides valuable insight and practical methods for addressing data and AI bias. According to Kush, from the Chain of Trust perspective, data collection, data preparation, and inference (model construction) are the steps when bias occurs. Below are the types of biases that must be addressed early in the lifecycle. Continual monitoring, assessments, and corrective actions must be taken throughout an AI product's lifecyle to mitigate unacceptable biases.

Social – implicit biases that result in systematic disadvantages to the underprivileged

Representation – a population that should be included in the data set is not

Temporal –unbalanced collection of data that occurs when sampling versus using a complete set of data.

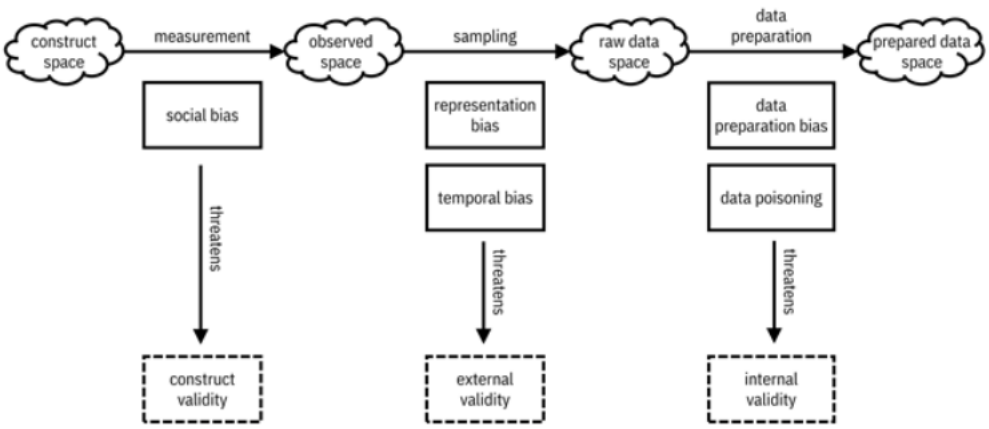

Figure 8. A mental model of spaces, validities, and biases[73]

Data preparation – data cleaning, enrichment, aggregation, and augmentation can each introduce biases. The method to handle 'null' values could also introduce biases.

Data poisoning (or polluting) – a malicious actor can introduce unwanted biases into a dataset through data injection or manipulation. Data injection is adding additional data points with characteristics desired by the adversary. Data manipulation is altering the data points already in the dataset.[77]

Red-Teaming and Cybersecurity

One of the best ways to identify and remove data bias, ensure ethical AI, and strengthen a system is by 'red teaming' the model. Red teaming is a common technique among military and corporate organizations to provide better defense against technological attacks. For example, many corporate firms pay penetration testers to attempt to break into their computer networks so that they can identify any vulnerabilities within their network defense.[78] Once identified, the firms can harden their networks before a hacker takes advantage of the weaknesses. The intent is to look at the AI system from an adversary's point of view and then try and manipulate the

system to their advantage. Another key red teaming activity is to challenge when oversight by a user may be too lax. The red team can introduce scenarios that may generate AI decision-making that crosses ethical boundaries that the programmers have yet to consider. Identifying and fixing such issues will increase trust in AI systems and could save lives. By bringing in a red team, who constantly thinks as the 'devil's advocate,' the programmer can create an even better system.[79]

Another key red teaming activity is ensuring strong cybersecurity. The low barrier of entry into cyberspace operations means that adversaries can pose a significant threat in this domain. Tools for cybersecurity require the ability to detect and respond at the speed of computers which now means that these technologies must be powered by AI.

International Standards and Laws

There are no explicit conventions or laws on a global scale that define the limits of how Lethal Autonomous Weapons (LAWs) can be used. The only legal guidance restricting the use of LAWS is in Article 36 of the UN Convention on Certain Conventional Weapons (CCW) requiring the military to consider whether LAWS or -not should be prohibited.[80] In his *China's New AI Governance Initiatives Shouldn't be Ignored*, article Sheehan Matt said that AI systems are intertwined profoundly into the fabrics of militaries around the world, and governments want to ensure that those systems are robust, reliable, and controllable for the sake of international stability.[81] The challenge remains on how to manage the proliferation of military AI as the risk of tolerance of adversaries' capability to make and use military AI is profoundly high. A global treaty prohibiting the development and deployment, or use of AI-enabled LAWS would offer hope, but NSCAI says that the treaty is not currently in the interest of U.S. or international security.[82] The US currently abides by existing International Humanitarian Law on distinguishing between combatants and civilians, and the U.S. DoD directive on ethical military AI capable of independently selecting and discriminating targets.[83] China has established AI ethics that resonate with the UN standards, but the truth is that given the Chinese hands-on approach to AI, their efforts do not translate into AI ethical realities.

Although garnering international consensus will be challenging, the US must lead global initiatives to generate an international norm addressing the abuse of military AI. If the objection to such action is the inability to verify compliance, then the US should lead creation of an international body for this purpose. The same need existed for nuclear weapons and resulted in the International Atomic Energy Agency (IAEA). After all, these actions should really go together since there is no point in a standard or law that cannot be verified. If the US does not lead the world towards a set of international standards and eventually law regarding AI, then it will simply be allowing China and others to misuse AI at will.

Recommendations

The US should continue to reinforce ethical AI guidelines like those published by the DoD. As a standard, all AI developments should be required to provide an improved DOD TRL, or similar, assessment that measures the trustworthiness of AI. Red team requirements should be

developed with industry and remain as non-specific to DoD as possible to provide a larger pool of qualified testers, and increased innovation and competition. These red teams should be applied to test the following areas before any AI system is implemented by the government or the military:

1. Process – whether human 'in the loop,' 'on the loop,' or 'out of the loop,' identify gaps that may lead to unsafe, inaccurate, or biased decisions and behavior.
2. Counter-Intelligence (CI) Threat – verify that access to AI system modification is limited to only those authorized to do so.
3. Cybersecurity – search for network vulnerabilities inside and external to the network. This should be an annual requirement or any time that there is a significant system upgrade.
4. Data Training – challenge the variables and parameters of the training model to increase pattern recognition confidence and identify errors that may lead to unsafe, inaccurate or biased decisions and behavior.

The US must lead global initiatives to generate international norms and eventually law addressing the abuse of military AI. Further the US should work towards an international body for AI cooperation and lawful use that is like the IAEA. AI is a tool, although capable, that can only derive its morality from human beings. The US must help define this morality.

Developing A National Security Human Capital Development Plan

In October 1957, "the world had a novel word—Sputnik—and the United States a new mission: to close the gap in the race for space with the Soviet Union. That urgent sense of mission triggered a revolution spurred by the desire to win the space race and get a generation of young Americans excited about and educated in science, technology, engineering, and mathematics."[84] The interstellar competition was not only one of prestige but underpinned the Cold War relationship between the U.S. and USSR. Science and Technology excitement driving competition against a true nation-state adversary was short-lived.

Following the Cold War, the United States became the lone superpower, with a noticeable drop in technological competition. While America was engaged in two wars in the Middle East following the September 11, 2001 terrorist attacks, China rose to contest American innovation and high-tech hegemony. Other state and non-state adversaries also threaten and undermine US hegemony primarily in the cyber and information domains. Emerging technology such as AI that is reinforced with a talent pool rich with high technology-trained human capital is critical to combat these threats.

The Obama Administration launched initiatives such as the Defense Digital Service in 2015 to recruit private-sector technology workers to serve in DoD to address these challenges.[85] Similarly, Deputy Secretary of Defense Dr. Kathleen Hicks created a Chief Artificial Intelligence Officer position with duties such as leading an AI Training Corps. These initiatives may not be enough to instill a sense of purpose for potential human capital for AI growth. The government at echelon needs to develop policy that utilizes the talents of our private sector and shapes the behavior necessary to address the STEM shortfall. AI and STEM educated human capital is the critical component for AI advancement. Unfortunately, there are critical limitations in the current U.S. education system, policies, and a remarkable absence of high-tech entrepreneur interest in DoD deep-tech and AI strategic initiatives.

Human Capital Conundrum

US academic institutions and major companies willingly acknowledge that human capital is their primary concern and are grappling with how to mitigate the issue. Our near-peer competitors, namely China, Russia, and India, are investing heavily into their workforces and developing capabilities to compete with the US. These nations often use American higher education centers in science, technology, engineering, and math (STEM) to build their skilled labor force with the desired skillsets.

Meanwhile, the lack of technology skill sets and failure to emphasize STEM in the American education systems continues to put the American worker behind our competitors and potential adversaries in critical domains. The American education system must take immediate actions such as instituting STEM-centric education initiatives in public schools for early childhood or pre-Kindergarten children. Early exposure to math and science is critical for future innovative outcomes.[86] Additionally, studies show that early STEM education positively impacts

language and literacy in children.[87] By instituting a STEM curriculum and education glide path that extends from early childhood through high school graduation, students will be indoctrinated into the mathematics and sciences required for advanced education opportunities in AI and deep technologies.

A December 2018 White House report, “Charting a Course for Success: America’s Strategy for STEM Education," underscored a continuous year over year low enrollment in STEM courses and dismal scores in the STEM-related courses, with 24 percent of fourth-graders, 32 percent of eighth graders, and 40 percent of twelfth graders were rated “below basic” for their grade levels.[88] Furthermore, reported effects of the COVID pandemic indicate students may have lost up to a year of learning in math.[89] The absence of collaboration and experiential learning, inherent activities to STEM skills proficiency were limited or non-existent in many school systems due to COVID restrictions. To mitigate education gaps during the pandemic, Federal policy needs to address STEM requirements in elementary education now. A Purdue University study showed that exposing students to STEM at an early age goes a long way in capturing their imagination and interest in science, technology, engineering, and math for future careers.[90]

Government policy, such as EO 13859, must buttress the initiatives of academic institutions, educate the American workforce on emergent technologies, and build a human capital development plan that supports a national strategy to recruit, educate and train the workforce with the skill sets we need to meet the increasingly demanding emerging technologies vital to our national security and economic prosperity.

AI-The Fourth Industrial Revolution Is Here

Today’s Defense Department and other leading experts agree that the future of America’s defense will rely on advanced technologies such as AI, cyber, quantum, robotics, directed energy and hypersonic weapons, and even 3-D printing.[91] However, the American workforce and society writ large is behind the technology curve. Most Americans lack a basic understanding of AI, how the interconnected Internet of Things ecosystem works, and the vulnerabilities presented. Norton, the leading Anti-virus software company, estimates over 21 billion interconnected devices by 2025.[92]

Many businesses and employers found productivity options using emerging technologies during the COVID-19 pandemic; AI integration enhances telework capabilities. “AI can vastly improve work-from-home environments, bringing much-needed support to communications, collaboration, workflow management.”[93] This virtual work environment and social media also serve as grounds for adversaries to undermine the United States and all rules-based democratic valued nations through misinformation and disinformation campaigns. In 2020 alone, Facebook removed 5.8 billion inauthentic accounts using a combination of machine learning-enabled detection technology Center for Security and Emerging Technology and human threat-hunting teams. Despite those efforts, fake profiles—a portion of them linked to disinformation campaigns—continue to make up around 5 percent of monthly users, or approximately 90

million accounts.[94] Therefore, it is not only critical to have skilled workers capable of developing advanced technology to combat these despicable campaigns but educate and alert the American society that these actions are occurring. In fact, government emphasis on STEM education and careers is overwhelmingly needed in the underserved urban and rural communities of America.

Include Everyone

Underserved communities are not seeing themselves in these high-tech career fields, nor do they have access to or education to compete. Patti Rote, a Robotics professor at Carnegie Mellon and co-founder of a K-12 robotics education group, Girls of Steel, echoed the same concerns. "CMU's campus does not represent a cross-cut of American society." Ms. Rote, with assistance from the Build Back Better plan, is targeting underserved communities to educate and train a resource into a needed sector that pays well beyond a living wage. According to the Bureau of Labor Statistics website, the inner-city populations, primarily African American and Latino, make up most blue-collar jobs such as automotive repair, construction, and manufacturing. Ms. Rote notes, these skill sets potentially translate seamlessly into building the robots, drones, and emerging capabilities of the future.[95] However, it is not just urban and communities of color that underrepresent academic and employment in high-tech fields.

Rural America is another societal sector currently underserved in the national security and high-tech commercial/private career fields. BLS.gov states that rural America comprises nearly one-third of American households. Education and training targeting this demographic could tap a new resource in coding and programming. Shivan Albright, Chief Technologist of Print Security at HP, expressed concerns that as hacking becomes more prolific, we need more ethical hackers and penetration testers to stay ahead of the adversary.[96] Both robotics and coding are fields that pay workers, even at entry levels, more than a living wage, and neither requires an advanced degree. However, access and education take partnerships at the local, state, and federal levels. Especially since only the largest or most profitable companies and academic institutions can justify the funding for these types of initiatives. The U.S. education system cannot be singularly focused on developing STEM and AI talent in the university system. Vocational technical schools and junior colleges must expand curriculum for STEM training and computer science at low or no cost to encourage the underserved or students who desire to take the vocational path, coding in computer languages, software, and hardware development.

Currently, some states offer free community college. However, the United States is yet to increase the skill sets needed or address the disparity in lower economic and gender divisions. The current graduating class at the University of Maryland with a Computer Science or similar technical degree is only 8% female and 7% African American.[97]

National Security Readiness Shortfalls

Deputy Secretary of Defense Hicks wrote in a May 05, 2021, memorandum to all DOD leadership, **"Data is essential to preserving military advantage, supporting our people, and serving the public."**[98] The Pentagon is focused on man-machine teaming, emphasizing how AI

can help users make more informed decisions. Artificial Intelligence allows analysts to evaluate vast amounts of data, an unachievable feat prior to machine partnerships. However, the number of qualified personnel to build AI algorithms or maintain and analyze data is not growing sufficiently to keep up with the growth of information. Honorable Hicks actively meets with companies and academic centers, collaborating on a tech-centric human capital plan. Unfortunately, the issue is two-fold, complex, and primarily due to the lack of a workforce with the technical skills needed to keep pace with emerging technologies and a lack of a cohesive executable strategy to correct the shortfall.

Over the past forty years, the number of American college students doubled while students graduating with STEM degrees remained virtually the same over the same period.[99] Additionally, the White House report, "Charting a Course for Success: America's Strategy for STEM Education," underscored that China had at least 4.7 million recent STEM graduates, and India had 2.6 million. The US had 568,000.[100] Meanwhile, near-peer competitors, namely China, challenge US leadership in STEM fields. As previously stated, American universities and research institutions educate these Chinese students. Presumptive PLA officers learn about advanced and emerging technologies such as quantum computing and hypersonic, then take their education back to China, potentially feeding their military expansion.[101] According to the Center for Security and Emerging Technology in 2019, there were 112,000 Chinese students in the U.S. seeking STEM degrees; 36,000 were PhD candidates. The Great Power Competition's reach into academia has long-term implications on AI industry and the national security of our nation.[102]

Many of the country's finest academic institutions are implementing strategies while seeking government assistance to target a future workforce for advanced tech careers and national security endeavors. For example, Stanford University offers programs targeting dual-use skill sets. The Gordian Knot Center for National Security Innovation, in partnership with a local venture capitalist, Silicon Valley, and DoD, bring together and attempt to interconnect innovation, coding, policy, and workforce development with the goal of scale and speed to compete with not only our GPC competitors but also with allies that compete in this shared space such as Israel and the United Kingdom.[103]

Workforce Reluctance Towards STEM

The American workers that qualified in a STEM career field increasingly have no interest in joining the military or federal government. This challenge is juxtaposed to the labor issues today. The workforce gap today is not due to the number of available workers, it is the lack of a sufficiently skilled and qualified labor market to meet requirements to compete in a technologically changing landscape that is the issue. Additionally, the younger generations feeding the workforce, Millennial and Generation Z, who are much more tech-savvy than prior generations with technology, are not selecting STEM skills or careers at levels needed to keep pace with emerging technology.[104] "They want to work from home with flexible hours and to learn skills to start their own business."[105] The disinterest to not only pursue STEM education

and jobs, or federal defense careers is troubling at the national level. "In 2020, there were more than 430,000 open computer science jobs in the United States, while only 71,000 new computer scientists graduate from American universities each year."[106] China continues to top the list of countries sending 348,992 students to the United States"[107] With most of these students getting advanced degrees in engineering, artificial intelligence, and computer science, then departing the United States to go back and work for the Chinese government this causes a brain drain of talent in technical jobs while allowing the Chinese government to close the knowledge gap between the two countries.

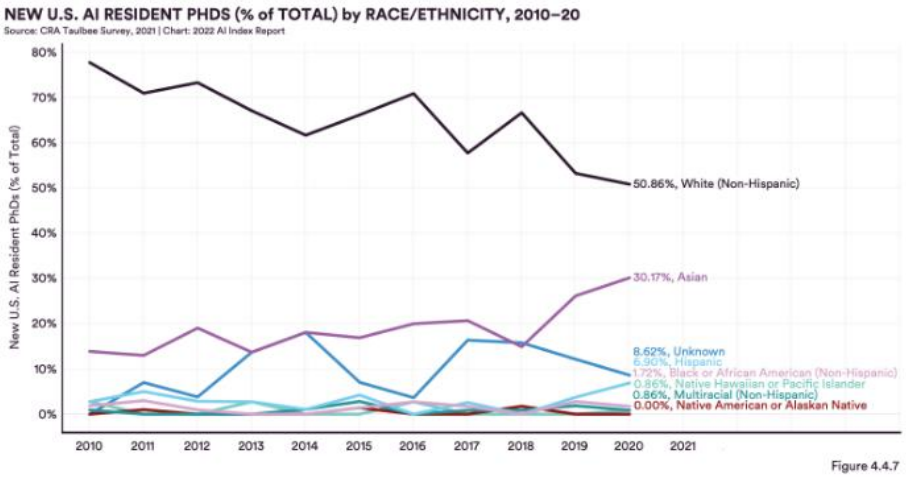

Figure 9. US AI PHD Candidates Don't Fully Represent America[53]

National security agencies need more digital experts now, or they will remain unprepared to buy, build, and use AI and its associated technologies. Digital expertise is the most important requirement for government modernization. The continued competition for talent is detrimental to National Security. The best and brightest are tempted away from cash-rich tech firms' governmental work. The government will continue to lose talent to big business and other state actors due to the lack of incentive and policy to promote and keep the required AI skills. Retaining the required talent is just one step to increasing National Security with AI.

Reports indicate that DOD and the defense industry also face challenges when recruiting and retaining personnel with expertise in AI due to research funding and salaries that significantly lag commercial companies.[108] This sentiment echoes the findings of the National Security Commission on Artificial Intelligence, which notes that “AI experts would be willing to serve in government if officials could create a more compelling sense of purpose and a technical environment within the government that would maximize their talents.”[109] Regardless, observers note probable AI application delays, such as “deficient, or lacking in appropriate safeguards and testing," if DOD and the defense industry cannot recruit and retain the appropriate experts.[110] The competition between government agencies and the private sector for the nation’s AI best and brightest sways increasingly toward the commercial/private sector. Job searches advertise the flexibility to do innovative work from the comfort of home or anywhere with a network connection; an incredibly attractive option for many compared to working on national security issues out of a government facility.

Policy Change and STEM Human Capital

EO 13859 highlights a change in the battlespace. Adversaries and rogue nations are creating advanced technology that will require countering with US AI-enabled intelligence, surveillance, and reconnaissance platforms, and indication and warning (I&W) systems[111] A computer and global connectivity revolution brought about interconnected networks. Along with it came emerging technologies such as AI and a new competitive space. The report also highlighted a critical need "to recruit more science and technology experts into the intelligence community and aggressively pursue security clearance reform."[112] Further highlighting the need for STEM-trained workforce that can obtain security clearance credentials for working on emergent technologies for the USG. These defense sectors impact our national security and economic prosperity but could be course corrected with a skilled workforce and government partnering with U.S. corporate sector on cultivating deep and advanced technology development in AI.

Recommendations

Shaping Skillsets with Policy. Artificial intelligence (AI) and emerging technologies of the Fourth Industrial Revolution are achieving breakthroughs. The USG must take the lead and utilize its unique capabilities to **shape the skillsets for future human capital while adapting governance structures to accompany the beneficial uses of these technologies and avoid their malicious uses**.[113] Policy is needed for USG **emphasis on academic institution initiatives with specific provisions directed at underserved, inner-city, and rural communities** while tapping into currently available private-sector STEM talent. To improve STEM career recruitment for state and federal government, the USG should advocate grade-specific STEM exposure highlighting how STEM careers support national security, economic growth, and personal prosperity. Consider Defense Production Act, Title III Program (50 U.S.C. App. § 2091 et seq.) funding for workforce development in sectors that support national objectives.

Educate the American Public on Technologies. **The USG must increase scrutiny on which foreign nations utilize US higher education.** Finally, government policy and public education efforts must be employed, ensuring all Americans understand the capabilities, interconnectedness, and vulnerabilities of AI and IoT devices that can be exploited by nation-state adversaries. *STEM Career Broadening Opportunities.* Establish an education and career broadening opportunity program at the federal and state levels for students pursuing an education in AI and other deep technologies. The education program must include student loan forgiveness in exchange for civil or military service in their specific field for 3-5 years. Additionally, the USG should consider establishing an AI career track that works with private industry and academia to offer broadening opportunities. This program would support AI workforce transitions among civil service, jobs with private industry, and teaching to afford diverse work opportunities.

Implementing AI with Partners

A prime AI growth area impacting industry and the USG is dual-use technology. Dual-use is technology that has "a significant government application and a private sector application, especially as the government application pertains to national security."[114] Dual-use technology also encompasses deep technology (deep tech) that provides disruptive solutions built around unique, proprietary, and hard-to-reproduce technological or scientific advances.[115] The government application of deep tech (e.g., weaponization of AI married with neurotechnology[116]) is attractive to governments for national security and military superiority. The same deep-tech phenomenon is simultaneously occurring with our Great Power Competitors, so the USG needs an effective strategic investment policy to better capitalize on deep tech.

Shortfalls of Venture Capital, SBIR, and IQT

Although the venture capital (VC) market has been an engine of innovation, the VC investment model has limitations. First, the higher risks in investing in tech start-up companies have led venture capitalists to create a more selective investment profile targeting firms with lower risks. The structure of VC investment has drawn venture capitalists to investment opportunities where they can rapidly commercialize and cash out ideas within a short period.[117] Second, the disproportionate influence of a few deep-pocketed investors on investment decisions has widened the valley of death.[118] Increasingly, deep-pocketed investors' business decisions have shifted the VC industry to creating unicorns – start-ups whose valuations exceed a billion dollars even though some firms fail to generate a profit.[119] Consequently, a small group of leading venture capitalists can predetermine winners and push potentially promising start-ups into the valley of death. Therefore, the shortfalls of the VC investment model hinder deep tech innovation. Although private investments in deep tech start-ups have increased from $4.5 billion in 2016 to $11.2 billion in 2020,[120] VC has overwhelmingly targeted synthetic biology with more than 60% of its funding because of its potential to produce tangible commercial products and low market risks.[121] Concurrently, their overwhelming focus on commercial demand overlooks the military application of deep tech. Additionally, venture capitalists' risk-adverseness and myopic vision are unfit for deep tech ventures and the emerging technology innovation ecosystem because venture capitalists tend to be financial-oriented with a target return on investment.[122]

In parallel to the VC industry, the USG investment programs have also revealed their impediments to deep tech innovations. In the case of the Small Business Innovation Research (SBIR), its ability to foster the deep tech innovation ecosystem is limited. First, the program exclusively focuses on providing financial aid for ventures that do not need to purchase expensive research and testing equipment and can commercialize a developed technology on their own with minimal risk in Phase III.[123] Second, it is incredibly selective and artificially competitive. In recent years, about 13% of phase I applications resulted in an award, and fewer than 6% of the Phase I awardees resulted in a Phase II award.[124] Additionally, less than 50% of the accepted Phase II applications were successful.[125] Thus, less than 1% of the total applicants

successfully completed the program. Third, the program's three-phase process lasts approximately three years.[126] As a result, the program is short-lived for deep tech ventures that require ten years or more. Therefore, the SBIR is ineffective in helping early-stage deep tech ventures avoid the valley of death.

Even though In-Q-Tel (IQT) has performed better than SBIR, its hybrid structure of venture capital and strategic investment poses obstacles that resemble the limitations of the VC model. First, it primarily focuses on late-stage tech entrepreneurs ready to present a prototype demonstration in a relevant environment, a prototype in an operational environment, a complete system through test and demonstration, and an actual proven system through mission operations. An IQT program objective is generating prototypes specifically valuable for the USG more than the marketability and profitability of a final product for a firm and prefers firms with low demand risks.[127] Its preference for firms specializing in the government application of deep tech is great for the USG, but the pool of available start-ups is insignificant because most start-ups aim at commercial markets for high profitability. Second, IQT's influence on portfolio companies through investments and its definition of successful investments – a transition of prototypes from the work program to operational use and the private capital market process of generating investment liquidity – can make IQT prone to preferential investments in particular technologies.[128] Such investment practice can also condone the risk-averse culture. Third, a shortage of personnel with the organizational knowledge or breadth of expertise to assimilate all potential customer needs makes IQT's mission challenging because IQT relies on a government-private sector interface function.[129] Thus, even though the USG has tried to adapt and respond to changes in the innovation ecosystem by adopting the VC investment model, the government investment programs are fragmented, share limitations similar to private VC's and remain less attractive to commercial companies due to the higher cost than the benefit of entry to the relatively small defense market.

A Better Option

The USG must have a better option available to attract deep tech and AI entrepreneurs to strategic defense portfolios. Another initiative, the Government-Corporate Strategic Investment (GCSI) offers an attractive alternative.

The GCSI is an adaptive investment policy based on the strategically oriented business-unit-led model and establishes a framework for a trilateral relationship between the government, corporations, and entrepreneurs. Corporate Venture Capital (CVC) funds associated with sponsoring corporate entities as the primary funder are less financial return-driven than VC funds and tend to pursue strategic investments.[130] The USG defines the vision for

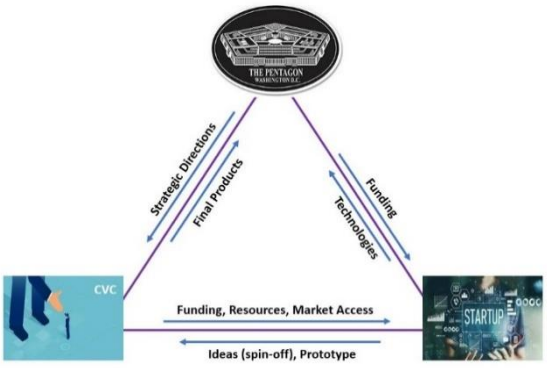

Figure 10. Government-Corporate Strategic Investment Initiative Framework

the joint investment team, sets an annual technology development budget after negotiations with the corporate leadership, and provides guidance for critical projects. The USG and CVC partners share the funding for the initiative based on negotiations on the ownership of final products, intellectual property rights, production rights, profit sharing, and other conditions. The GCSI framework conceptualizes a deep tech innovation ecosystem that enables the actors to exchange strategic, economic, and technological elements necessary for achieving their military, economic and technological objectives. More importantly, new joint investment opportunities allow the government to focus on disruptive innovations that weaponize disruptive technologies to stay ahead of its adversaries. Moreover, military innovations can have spill-over effects on the commercial sector by creating new markets for commercial use.

Recommendations

Promote deep tech innovation through Government-Corporate Strategic Investment (GCSI) Initiative. Investing in disruptive deep technologies demands a creative investment strategy to break the prejudice that big companies and start-ups cannot join forces at an operational level. The primary purpose of the GCSI policy is to advance the military application of deep tech, the economic externalities of military innovations also matter for national economic welfare, and technological advancement as demonstrated in the effects of the internet and the global positioning system on the national and global economies. The GCSI offers agility and autonomy which is absent when rigid, overly bureaucratic organizational structure and close supervision fail to cultivate a culture of innovation. An agile and independent organization of individuals with the required expertise in deep tech, business management, and the defense acquisition program is necessary for the success of the innovation ecosystem.

Establish more technical Partnership Intermediary Agreements with industry for the establishment of innovation centers. A prime example is the DreamPort facility, a partnered opportunity between a not-for-profit organization, MISI (Maryland Innovation Security Institute) and USCYBERCOM. The primary mission for these centers should be to incubate and accelerate AI efforts under the Pentagon's Office of Small Business Programs *(OSBP)* to work with universities, Historically Black Colleges and Universities (HBCUs), universities, small businesses, and AI industry.

Conclusion

AI is ubiquitous and rapidly proliferating around the world, even into virtual instantiations such as the Metaverse. China intends to secure its superpower status and their grand goal is not for short-term advancement but for long-term global control. It is essential to realize that AI will be the key enabler because of its ability to boost all industries. Furthermore, China's pursuit of AI objectives is outside the norms of international and US values on which international security increasingly depends. Unfortunately, during this research effort significant gaps were identified in the USG and DoD's efforts to operationalize AI solutions. The USG and DoD would best take cues from AI industry and partner with them to turbo-charge growth in AI innovation for the defense of our nation. This study identifies three key challenges:

First, the change created by AI can outpace humans. Addressing this challenge requires we lead emerging technologies that will produce even more powerful AI and uphold ethics, standards, and laws that are true to U.S. values. New human decision processes are needed.

Second, in its final 2021 report to Congress, the NSCAI stated that presently a national AI strategy does not exist. An overarching national AI strategy must be thoughtfully and aggressively implemented to place the USG and DoD left of the AI boom, now. The recently formed National Artificial Intelligence Initiative Office (NAIIO) is best postured to orchestrate partnership building efforts between USG and AI industry while setting the conditions for federal and state collaboration efforts on deep technology growth and AI. As part of this strategy, new Government Commercial Strategic Investments (GCSI) should be pursued that encourage longer-term investments into emerging technology such as quantum computing with potential to further expand AI. This will foster economic growth and strengthen government-private industry partnerships while reducing the acquisition process timeline to better support rapid fielding of AI and software solutions for the DoD.

Third, human capital is the limiting factor to retaining the U.S.'s leadership position in AI and other critical technologies. A holistic STEM Human Capital Development Plan must be implemented at the federal and state levels. Research identified a strong demand for STEM education initiatives to start at the pre-school age with continuous emphasis into secondary school for skillset proficiency. Early STEM education is foundational for instilling a technology-enriched learning culture while advancing interest in academics and career development for vocational and university schooling alike. To capitalize on these efforts, collaboration between the USG, AI industry, and academia to establish technology centers akin to Pittsburgh, Pennsylvania help identify STEM talent in underserved communities which level the playing field.

Alone, the US may be unable to outcompete China in terms of sheer numbers of investment, people, or systems. However, the US can, and must, marshal its partners and empower its people to innovate and create a freer and more prosperous world. **The US must accelerate implementation of ethical AI to secure the future - America's and the world's!**

Annex A: Russo-Ukraine, 20th Century Doctrine in a 21st Century Conflict

The nature of warfare is changing; it spans an unprecedented theater that stretches from the heavens to cyberspace and far into the oceans' depths. That demands new thinking and new action ...We must redouble our efforts to work together — with allies and partners... It is always easier to stamp out a small ember than to put out a raging fire.

- U.S. Defense Secretary, Lloyd J. Austin III[131]

The role of non-military means of achieving political and strategic goals has grown and, in many cases, they have exceeded the power of force of weapons in their effectiveness… All this is supplemented by military means of a concealed character.

- Chief of the General Staff of the Russian Armed Forces, Valery Gerasimov[132]

Russia is demonstrating to the world that it is fighting a 21st century conflict against Ukraine using 20th century land warfare concepts and capabilities akin to the Cold War era. By all appearances, Russia is not following the same tactics or playbook it employed against Ukraine in 2014. Russia's 'Gerasimov Doctrine,' a 21st century digital battle plan that embodies 'hybrid' warfare by employing a whole-of-government approach of hard and soft power in conflict, short of war was used to annex Crimea.[133] In contrast, Ukraine learned valuable lessons from 2014 and is employing every tool at hand and those provided from European and international partners. Of note, Ukraine has been very successful engaging and receiving support from international businesses to leverage commercial dual-use technologies.

In response to Russia's egregious attack on Ukraine, AI research groups and security think tanks immediately posited – will this conflict be a key proving ground for artificial intelligence, for better or for worse? War is devastating but it plays a pivotal role in advancing technology. New AI technologies are being utilized during the current conflict, such as the facial recognition application provided by Clearview AI, a U.S. AI startup, to identify the deceased.[134] Ukraine is using AI-based speech transcription, translation, and natural language processing against intercepted Russian radio transmissions to support intelligence operations.[135] Other examples of AI in action are the employment of UKROPTOSS, AI software used for battle tracking the conflict in Ukraine and an AI model to detect misinformation on the Russia-Ukraine war (Ukr.ai). While these AI enablers are facilitating intelligence and humanitarian efforts in Ukraine, there are additional AI capabilities the U.S. and allied partners must consider integrating into the Ukraine fight against Russia:

- Employ the DoD Defense Innovation Unit's (DIU) xView2 to assess battle damage to Ukrainian cities and infrastructure using satellite imagery and AI-generated vision algorithms. XView2 employs xBD, a significantly comprehensive database of high-resolution imagery which is then measured

against the Joint Damage Scale of 'before' and 'after' disaster events within 48 hours.[136]

- Assist in detecting and responding with machine learning, cyber threat attacks against malware and malicious network intrusions. The Ukrainian internet penetration rate is projected to be over 85 percent in 2022, a staggering problem for the Ukrainian society at large.[137]
- Assist Ukraine's Ministry of Digital Transformation (MoDT) with creating an AI-enabled, fully digital Ukraine. Pre-conflict, the MoDT established the Diia tool to reinvent how individual Ukrainian citizens and businesses interact with the state. Diia is the cornerstone to Ukraine's emerging digital ecosystem. Currently, 13 million Ukrainians use Diia for managing official documents and over seventy online public services for Ukrainian citizens and businesses.[138]
- Leverage Project Convergence for deploying AI-enabled Unmanned Aerial Systems (UAS)[139] into Ukraine. Fielded and prototype aircraft would be used for targeting and reconnaissance against Russian artillery and missile systems, humanitarian relief delivery, rescue operations, and front-line logistics resupply efforts.
- Help the Ukraine establish an augmented reality, virtual world to rebuild its historical and cultural sites or structures that Russia destroyed. According to UNESCO, as of April 2022, over fifty cultural sites which include museums, monuments, buildings, and religious sites have been destroyed by the Russians.[140]

Ukraine's expansion of its IT (information technology) sector is another milestone for the country's path to becoming a digitalized country. More than 200,000 highly qualified professionals work in Ukraine's IT sector accounting for around 4% of the country's GDP and about a quarter of Ukrainian service exports.[141] The branch experiences consistent annual growth, owing primarily to exports. Ukraine ranked 12th among the world's major exporters of IT services in 2019.[142] The global demand for digitalization of corporate operations has been the key driving force behind the industry's development in Ukraine.[143]

The Ukraine established the Institute of Artificial Intelligence Problems (IAIP) through the Ministry of Education and Science of Ukraine and the National Academy of Sciences of Ukraine.[144] The IAIP's major goal is to make effective use of scientific and technological potential in the search for and resolution of urgent problems in the creation of intelligent systems, new information and communication technologies, intelligent robotic systems, and a thorough study of artificial intelligence systems with the goal of integration in various areas of society. Additionally, Ukraine established the Ministry of Digital Transformation who produced an AI Concept for Development plan through 2024 that leverages both Ukrainian government, industry, and academia.[145]

Ideally, the US and allied partners will continue to support Ukraine's efforts to become a major IT center in Eastern Europe. The Ukrainian government has taken several actions to set the

conditions for IT growth. In cooperation with private sectors and other like-minded partners, the U.S. government should consider providing AI-related solutions to Ukraine. This would not only aid Ukraine in its fight against Russia, U.S.-developed AI warfare technologies would accelerate and mature while enhancing operations. Ukraine would potentially prevail over Russia and restore its economy faster. The U.S. would receive tested AI capabilities in real warfare AI technologies and a reliable partner to protect the Eastern border of allied European countries.

UKRAINE'S CONCEPT FOR DEVELOPMENT OF ARTIFICIAL INTELLIGENCE 2021-2024[146]

Application fields	**Tasks**
Science	- Fostering AI research and its use - Scientific cooperation with international research centers
Information security	- Creation of a protected national information space - Identification, prevention and neutralization of informational threats (violence, brutality, pornography, manipulation of consciousness, dissemination of inaccurate information)
Cyber security	- Improvement of legislation and creation of a modern legal framework - Development of innovative systems - Creation of national informational products that will be used by government bodies
Justice	- Development of technologies in the field of justice (unified judicial information and telecommunication system, electronic court, unified register of pre-trial investigations, etc) - Implementing Al-based advisory programs - Prevention of social hazards through Al-powered data analytics - Determination of resocialization measures for convicts using AI - AI-assisted adjudication in cases of minor complexity (by mutual agreement of the parties)
Economy	- Motivating entrepreneurs to adopt AI technologies - Development of a roadmap for retraining employees whose work can be automated in the next 5-10 years agreement of the parties - Introduction of government orders on the AI system - Stimulating partnership between the state and business in the field of relevant projects, improving legislation
Legal regulation and ethics	- Harmonization of the principles of using Al in Ukrainian legislation with European norms

	- Determining the legal and ethical boundaries of the application of Al systems to provide legal aid - Support for initiatives to create organizational forms for cooperation of legal entities and individuals in the field of AI
Education	GENERAL HIGH SCHOOL EDUCATION - AI courses for educators - Digital literacy among school students COLLEGE EDUCATION - Development of specialized educational programs - Involvement of IT specialists in the development of educational programs and certification of applicants for higher education - Professional development and professional retraining Providing social protection for specialists, obtaining additional education in the field of AI
Defense	USING AI TECHNOLOGIES IN SUCH SYSTEMS AS: - Command and control - Collection and analysis of information during hostilities - Countering cyber defense threats - Simulation of combat situations - Troop capabilities analysis
Public administration	Creation of a list of administrative services with automatic decisions APPLICATION OF AI TECHNOLOGIES - For digital identification and verification of persons In the field of healthcare - For analysis, forecasting and modeling of public administration performance indicators - To detect unlawful interference in the activities of the electronic system of public procurement and other systems - To identify unfair activities by officials

Annex B: AI Institutes

Inception Year	Type	Name	Theme	Gov't Lead(s)	Primary Org	Description	Website
2021	AI Institute for	Edge Computering Leveraging Next-Generation Networks (Athena)	AI in Computer and Network Systems	DHS NSF	Duke University	Develop edge computing with groundbreaking AI functionality while keeping complexity and costs under control.	https://athena.duke.edu/
2021	AI Institute for	Future Edge Networks and Distributed Intelligence (AI-EDGE)	AI in Computer and Network Systems	DHS NSF	Ohio State University	Establish U.S. leadership in next-generation edge networks and distributed AI	https://aiedge.osu.edu/
2021	AI Institute for	Advances in Optimization (AI4Opt)	AI for Advances in Optimization	NSF	Georgia Institute of Technology	Revolutionize decision making on a large scale by fusing AI and mathematical optimization into intelligent systems.	https://www.ai4opt.org/
2021	AI Institute for	Learning-Enabled Optimization at Scale (TILOS)	AI for Advances in Optimization	NSF	University of California, San Diego	Aim to "make impossible optimizations possible" by addressing the fundamental challenges of scale and complexity.	https://tilos.ucsd.edu
2021	AI Institute for	Intelligent Cyberinfrastructure with Computational Learning in the Environment (ICICLE)	AI and Advanced Cyberinfrastructure	NSF	Ohio State University	Build the next generation of cyberinfrastructure that will make AI easy for scientists to use and promote its further democratization.	https://icicle.osu.edu/
2021	AI Institute for	Adult Learning and Online Education (ALOE)	AI-Augmented Learning	NSF	Georgia Research Alliance	Lead the country and the world in the development of novel AI theories and techniques for enhancing the quality of adult online education, making this mode of learning comparable to that of in-person education in STEM disciplines.	https://aialoe.org/
2021	AI Institute for	Engaged Learning	AI-Augmented Learning	NSF	North Carolina State University	Advance natural language processing, computer vision and machine learning to engage learners in AI-driven narrative-centered learning environments.	https://www.aiengage.org/
2020	AI Institute for	Student–AI Teaming	AI-Augmented Learning	NSF	University of Colorado, Boulder	Develop groundbreaking AI that helps both students and teachers to work and learn together more effectively, and equitably, while helping educators focus on what they do best: inspiring and teaching students.	https://www.colorado.edu/research/ai-institute/
2020	AI Institute for	Future Agricultural Resilience, Management, and Sustainability (AI-FARMS)	AI-Driven Innovation in Agriculture and the Food System	USDA-NIFA	University of Illinois, Urbana-Champaign	Advance AI research to solve major agricultural challenges including labor shortages, efficiency and animal welfare.	https://digitalag.illinois.edu/research/aifarms/
2020	AI Institute for	Next-Generation Food Systems (AIFS)	AI-Driven Innovation in Agriculture and the Food System	USDA-NIFA	University of California, Davis	Integrate a holistic view of the food system with AI and bioinformatics.	https://aifs.ucdavis.edu/
2021	AI Institute for	Resilient Agriculture (AIIRA)	AI-Driven Innovation in Agriculture and the Food System	USDA-NIFA	Iowa State University	Transform agriculture through innovative AI-driven digital twins that model plants at an unprecedented scale.	https://aiira.iastate.edu/
2021	AI Institute for	Agricultural AI for Transforming Workforce and Decision Support (AgAID)□	AI-Driven Innovation in Agriculture and the Food System	USDA-NIFA	Washington State University	Integrate AI methods into agriculture operations for prediction, decision support, and robotics-enabled agriculture to address complex agricultural challenges. This Institute uses a unique adopt-adapt-amplify approach to develop and deliver AI solutions to agriculture that address pressing challenges related to labor, water, weather and climate change.	https://agaid.wsu.edu/
2020	AI Institute for	Molecular Discovery, Synthetic Strategy, and Manufacturing (Molecule Maker Lab)	AI for Accelerating Molecular Synthesis and Manufacturing	NSF	University of Illinois, Urbana-Champaign	Develop new AI-enabled tools to accelerate automated chemical synthesis and advance the discovery and manufacture of novel materials and bioactive compounds.	https://moleculemaker.org/
2020	AI Institute for	Artificial Intelligence and Fundamental Interactions	AI for Discovery in Physics	NSF	MIT	Develop AI methods that integrate the laws of physics as a guiding framework to advance physics knowledge.	https://iaifi.org/
2021	AI Institute for	Dynamic Systems	AI in Dynamic Systems	DHS NSF	University of Washington	Enable innovative research and education in fundamental AI and machine learning theory, algorithms and applications specifically for safe, real-time learning and control of complex dynamic systems.	http://dynamicsai.org/
2020	AI Institute for	Foundations of Machine Learning	Foundations of Machine Learning	NSF	University of Texas, Austin	Address major theoretical challenges in AI, including next-generation algorithms for deep learning, neural architecture optimization, and efficient robust statistics.	https://www.ifml.institute/

Annex B: AI Institutes Continued

Inception Year	Type	Name	Theme	Gov't Lead(s)	Primary Org	Description	Website
2021	AI Institute for	Collaborative Assistance and Responsive Interaction for Networked Groups (AI-CARING)	Human-AI Interaction and Collaboration	NSF	Georgia Institute of Technology	Seek to create a vibrant, fully developed discipline focused on personalized, longitudinal (over months and years) collaborative AI systems that learn individual models of human behavior and how they change over time and use that knowledge to better collaborate and communicate in caregiving environments.	http://ai-caring.org/
2021	AI Institute for	Research on Trustworthy AI in Weather, Climate, and Coastal Oceanography (Artificial Intelligence for Environmental Sciences, AI2ES)	Trustworthy AI	NSF	University of Oklahoma, Norman Campus	Develop user-driven trustworthy AI that addresses pressing concerns in weather, climate, and coastal oceanography and coastal hazards prediction.	https://www.ai2es.org/
2020	Other Agency Institute	DAF-MIT Accelerator		USAF	MIT	conducting fundamental research to enable rapid prototyping, scaling, and the ethical application of AI algorithms and systems.	https://aia.mit.edu/
2020	Other Agency Institute	Veterans Affairs National AI Institute	R&D Focus on Veterans	VA		Develop AI research and development capabilities in the VA.	https://www.research.va.gov/naii/
1984	FFRDC	Software Engineering Institute	Software	DOD	Carnegie Mellon University	Support national security by advancing and transitioning the science, technologies, and practices needed to make software a strategic advantage for the DoD.	https://www.sei.cmu.edu/

Notes

[1] "Final Report" (The National Security Commission on Artificial Intelligence, March 19, 2021), 7, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[2] "NSCAI 2021 Final Report."

[3] "NSCAI 2021 Final Report."

[4] "Summary of AI Provisions from the National Defense Authorization Act 2021," Stanford Institute for Human-Centered Artificial Intelligence, accessed April 26, 2022, https://hai.stanford.edu/policy/policy-resources/summary-ai-provisions-national-defense-authorization-act-2021.

[5] "Military-Civil Fusion and the People's Republic of China" (US State Department, May 2020), https://www.state.gov/wp-content/uploads/2020/05/What-is-MCF-One-Pager.pdf.

[6] "Chasing the Chinese Dream," *The Economist*, n.d., http://www.economist.com/briefing/2013/05/04/chasing-the-chinese-dream.

[7] "Final Report" (Cyberspace Solarium Commission, March 2020), 130, https://www.solarium.gov/.

[8] "Global Trends 2040, A More Contested World" (National Intelligence Council, March 2021), 58, https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf.

[9] Kelley M. Sayler, "Emerging Military Technologies: Background and Issues for Congress" (Congressional Research Service, April 6, 2022), 2, https://sgp.fas.org/crs/natsec/R46458.pdf.

[10] "AI Poised to Double Annual Economic Growth Rate," Accenture, September 28, 2016, https://newsroom.accenture.com/news/artificial-intelligence-poised-to-double-annual-economic-growth-rate-in-12-developed-economies-and-boost-labor-productivity-by-up-to-40-percent-by-2035-according-to-new-research-by-accenture.htm.

[11] "The Macroeconomic Impact of Artificial Intelligence" (Price Waterhouse Coopers, February 2018), 3, https://www.pwc.co.uk/economic-services/assets/macroeconomic-impact-of-ai-technical-report-feb-18.pdf.

[12] Tanya Lewis, "A Brief History of Artificial Intelligence," livescience.com, December 4, 2014, https://www.livescience.com/49007-history-of-artificial-intelligence.html.

[13] "AI Next Campaign," accessed December 5, 2021, https://www.darpa.mil/work-with-us/ai-next-campaign.

[14] Greg Allen, "Understanding AI Technology - AI Guide for DoD Leaders" (Joint Artificial Intelligence Center (JAIC), Department of Defense, April 2020), 6, https://www.ai.mil/references.html.

[15] Allen, 6.

[16] Allen, 9–10.

[17] Allen, 11–15.

[18] Allen, 16–17.

[19] Discussion with Tracy Laabs, Wyss Center for Bio and Neuroengineering, April 22, 2022.

[20] Michael Porter, "The Competitive Advantage of Nations," *Harvard Business Review,* April 1990, https://hbr.org/1990/03/the-competitive-advantage-of-nations.

[21] Susan Ratcliffe, "Oxford Essential Quotations, W. Edwards Deming," in *Oxford Reference*, 2018, https://www.oxfordreference.com/view/10.1093/acref/9780191866692.001.0001/q-oro-ed6-00019739.

[22] "NVIDIA Company History: Innovations Over the Years," NVIDIA, accessed May 7, 2022, https://www.nvidia.com/en-us/about-nvidia/corporate-timeline/.

[23] Korem, "The Challenges of Operationalizing AI Models With Real-Time Business Data," accessed May 6, 2022, https://blog.worldsummit.ai/challenges-of-operationalizing-ai-models.

[24] "What Is IaaS? Infrastructure as a Service | Microsoft Azure," accessed February 19, 2022, https://azure.microsoft.com/en-us/overview/what-is-iaas/.

[25] Discussion with Oracle personnel, April 14, 2022.

[26] Stephen Su, Discussion with Industrial Technology Research Institute (ITRI), April 18, 2022.

[27] "Artificial Intelligence Software Market to Reach $126.0 Billion in Annual Worldwide Revenue by 2025," *Edge AI and Vision Alliance* (blog), January 7, 2020, https://www.edge-ai-vision.com/2020/01/artificial-intelligence-software-market-to-reach-126-0-billion-in-annual-worldwide-revenue-by-2025/.

[28] Meetings with John Hopkins University, Applied Physics Laboratory (JHU APL), April 21, 2021.

[29] "Free Summary, Federal Artificial Intelligence Landscape, 2022" (Deltek, Inc.), 19, accessed May 6, 2022, https://info.deltek.com/Federal-Artificial-Intelligence-2022.

[30] "Federal AI Spending to Top $6 Billion," accessed May 6, 2022, https://www.nationaldefensemagazine.org/articles/2021/2/10/federal-ai-spending-to-top-$6-billion.

[31] Matt Asay, "AI Investments Soared in 2021, but Big Problems Remain," TechRepublic, March 25, 2022, https://www.techrepublic.com/article/ai-investments-soared-2021-big-problems-remain/.

[32] "Chasing the Chinese Dream."

[33] Takashi Kawakami, "China to Pump $1.6tn into Tech Infrastructure through 2025," Nikkei Asia, January 21, 2021, https://asia.nikkei.com/Business/China-tech/China-to-pump-1.6tn-into-tech-infrastructure-through-2025.

[34] Gustavo Ferreira and Jamie Critelli, "China's Global Monopoly on Rare-Earth Elements.," *Parameters: U.S. Army War College* 52, no. 1 (2022): 57–58.

[35] Prableen Bajpai, "An Overview of the Top 5 Semiconductor Foundry Companies," n.d., https://www.nasdaq.com/articles/an-overview-of-the-top-5-semiconductor-foundry-companies-2021-10-01.

[36] Sarah Ravi, "CHIPS for America Act & FABS Act," Semiconductor Industry Association, February 26, 2021, https://www.semiconductors.org/chips/.

[37] Alexis Nicols, "STEM Education Statistics 2019 – How the US Ranks," Parentology, n.d., https://parentology.com/stem-education-statistics-2019-how-the-u-s-ranks/.

[38] Alex Joske, "Picking Flowers, Making Honey," Australian Strategic Policy Institute, October 3, 2018, http://www.aspi.org.au/report/picking-flowers-making-honey.

[39] Jean-Marc Rickli and Marcello Ienca, "The Security and Military Implications of Neurotechnology and Artificial Intelligence," 2021, 204–5, https://doi.org/10.1007/978-3-030-64590-8_15.

[40] Vannevar Bush, *Science--the Endless Frontier: A Report to the President on a Program for Postwar Scientific Research* (National Science Foundation, 1990), 3.

[41] Bush, 4.

[42] "DIU FY 2021 Annual Report," n.d., 3, https://www.diu.mil/latest/diu-fy-2021-annual-report-a-preview-into-fy-2022.

[43] "DIU Report," 7.

[44] "Summary of the 2018 National Defense Strategy of the United States of America" (Department of Defense, January 19, 2018),

https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

[45] Dr. William A. Schleckser, "Adaptive Acquisition Framework — Ready, Set, Contract?," May 29, 2020, https://www.nationaldefensemagazine.org/articles/2020/5/29/adaptive-acquisition-framework-ready-set-contract.

[46] Jackson Barnett, "Pentagon Chief Hicks Pursuing Workarounds to Fast-Track Military Tech Acquisition - FedScoop," June 8, 2021, https://www.fedscoop.com/acquisition-reform-kathleen-hicks/.

[47] Sydney J. Freedberg Jr, "Hicks Seeks To Unify Service Experiments With New 'Raider' Fund," Breaking Defense, June 21, 2021, https://breakingdefense.sites.breakingmedia.com/2021/06/hicks-seeks-to-unify-service-experiments-with-new-raider-fund/.

[48] Marcy E. Gallo, "Defense Primer: Under Secretary of Defense for Research and Engineering" (Congressional Research Service, December 20, 2021), 1, https://crsreports.congress.gov/product/pdf/IF/IF10834.

[49] Ronald O'Rourke, "Renewed Great Power Competition: Implications for Defense—Issues for Congress" (Congressional Research Service, March 10, 2022), 20, https://crsreports.congress.gov/product/pdf/R/R43838.

[50] Patrick Tucker, "Impressed by 2022's Record Research Budget? Wait 'Til Next Year, DOD Undersecretary Says," Defense One, January 13, 2022, https://www.defenseone.com/technology/2022/01/impressed-2022s-record-research-budget-wait-til-next-year-dod-undersecretary-says/360754/.

[51] "The Networking & Information Technology R&D Program and the National Artificial Intelligence Initiative Office SUPPLEMENT TO THE PRESIDENT'S FY2022 BUDGET" (Subcommittee on Networking & Information Technology Research & Development and National Artificial Intelligence Initiative Office, December 2021), 61–73, https://www.nitrd.gov/pubs/FY2022-NITRD-NAIIO-Supplement.pdf.

[52] "History of Innovation at the SEI," Software Engineering Institute, n.d., https://www.sei.cmu.edu/about/history-of-innovation-at-the-sei/index.cfm.

[53] "NSCAI 2021 Final Report."

[54] Alexandra Mousavizadeh, Bijal Mehta, and Kim Darrah, "AI Boom Time," Tortoise, December 2, 2021, https://www.tortoisemedia.com/2021/12/02/ai-boom-time/.

[55] "AI Index 2022," Stanford Institute for Human-Centered Artificial Intelligence, May 15, 2022, https://hai.stanford.edu/research/ai-index-2022.

[56] Wise, "How Much Data Is Created Every Day in 2022?," *Earthweb* (blog), May 15, 2022, https://earthweb.com/how-much-data-is-created-every-day/.

[57] "53 Important Statistics About How Much Data Is Created Every Day," Financesonline.com, June 15, 2021, https://financesonline.com/how-much-data-is-created-every-day/.

[58] Adam Stone, "What Is Quantum Computing and How It's Changing Government," December 5, 2019, https://fedtechmagazine.com/article/2019/12/what-quantum-computing-and-how-can-it-help-feds-perfcon.

[59] Kelley M. Sayler, "Defense Primer: Quantum Technology" (Congressional Research Service, May 6, 2022), https://crsreports.congress.gov/product/pdf/IF/IF11836.

[60] "IBM Quantum System One," IBM Quantum System One, March 12, 2018, https://research.ibm.com/ibm-q/qed/index.html.

[61] *Quantum Computing: Progress and Prospects* (Washington, DC: National Academies of Sciences, Engineering, and Medicine, 2019), https://doi.org/10.17226/25196.

[62] 115th Congress, "H.R.6227 - National Quantum Initiative Act" (US Congress, December 21, 2018), 2017/2018, https://www.congress.gov/bill/115th-congress/house-bill/6227/text.

[63] "About," National Quantum Coordination Office, accessed April 2, 2022, https://www.quantum.gov/about/.

[64] Market Trends, "Top Government's Budget for Quantum Computing in 2022," Analytics Insight, March 2, 2022, https://www.analyticsinsight.net/top-governments-budget-for-quantum-computing-in-2022/.

[65] "Opinion | The Pentagon Plans Anew to Head off an Old Worry: Nuclear War," *Washington Post*, accessed May 1, 2022, https://www.washingtonpost.com/opinions/2022/04/28/russia-ukraine-nuclear-pentagon-budget/.

[66] "Human in the Loop: Accelerating the AI Lifecycle," CloudFactory, n.d., https://www.cloudfactory.com/human-in-the-loop.

[67] Jackson Barnett, "AI Needs Humans 'on the Loop' Not 'in the Loop' for Nuke Detection, General Says," *FedScoop*, February 14, 2020, https://www.fedscoop.com/ai-should-have-human-on-the-loop-not-in-the-loop-when-it-comes-to-nuke-detection-general-says/.

[68] Barnett.

[69] Dr. Michael B. Cowen and Captain (ret.) Rick Williams, "Is Human-On-the-Loop the Best Answer for Rapid Relevant Responses? -," Joint Air Power Competence Centre, May 2021,

https://www.japcc.org/essays/is-human-on-the-loop-the-best-answer-for-rapid-relevant-responses/.

[70] Eliot, "Human In-The-Loop Vs. Out-of-The-Loop in AI Systems: The Case of AI Self-Driving Cars," AI Trends, April 9, 2019, https://www.aitrends.com/ai-insider/human-in-the-loop-vs-out-of-the-loop-in-ai-systems-the-case-of-ai-self-driving-cars/.

[71] Campbell Kwan, "Is There Room for Ethics and the Law in Military AI?," *TechRepublic*, April 10, 2019, https://www.techrepublic.com/article/is-there-room-for-ethics-and-the-law-in-military-ai/#:~:text=The%20state%20of%20military%20AI,autonomous%20weapons%20can%20be%20used.

[72] Hu Jintao, "Companies Law of the People's Republic of China, No. 42" (President of the People's Republic of China, October 27, 2005), https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/92643/108008/F-186401967/CHN92643%20Eng.pdf.

[73] *The National AI Advisory Committee (NAIAC) Meeting #1*, 2022, https://www.ai.gov/naiac/.

[74] "DOD Adopts 5 Principles of Artificial Intelligence Ethics," U.S. Department of Defense, February 25, 2020, https://www.defense.gov/News/News-Stories/Article/Article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/.

[75] Ehsan Toreini et al., "The Relationship between Trust in AI and Trustworthy Machine Learning Technologies" (FAT '20: Conference on Fairness, Accountability, and Transparency, Barcelona, Spain: Association for Computing Machinery, 2020), 272–83, https://doi.org/DOI: 10.1145/3351095.3372834.

[76] Toreini et al., 276.

[77] Kush R. Varshney, *Trustworthy Machine Learning* (Independently Published, 2022), 46, www.trustworthymachinelearning.com.

[78] "What Is Penetration Testing?," Contrast Security, accessed April 26, 2022, https://www.contrastsecurity.com/knowledge-hub/glossary/penetration-testing.

[79] "5 Things Every Red Team Needs to Optimize Operations," NetSPI, accessed April 26, 2022, https://www.netspi.com/resources/tip-sheets/5-things-every-red-team-needs-to-optimize-operations/.

[80] Vincent C. Müller, "Ethics of Artificial Intelligence and Robotics," in *The Stanford Encyclopedia of Philosophy*, ed. Edward N. Zalta, Summer 2021 (Metaphysics Research Lab, Stanford University, 2021), https://plato.stanford.edu/archives/sum2021/entries/ethics-ai/.

[81] Matt Sheehan, "China's New AI Governance Initiatives Shouldn't Be Ignored," Carnegie Endowment for International Peace, January 4, 2022, https://carnegieendowment.org/2022/01/04/china-s-new-ai-governance-initiatives-shouldn-t-be-ignored-pub-86127.

[82] Sheehan.

[83] "Directive 3000.09, Autonomy in Weapon Systems" (Department of Defense, May 1, 2017), https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf.

[84] Arthur Herman, "America's STEM Crisis Threatens Our National Security," *American Affairs Journal* (blog), February 20, 2019, https://americanaffairsjournal.org/2019/02/americas-stem-crisis-threatens-our-national-security/.

[85] Steven Levy, "Inside the Obama Tech Surge as It Hacks the Pentagon and VA," *Wired*, July 19, 2016, https://www.wired.com/2016/07/inside-the-obama-tech-surge-as-it-hacks-the-pentagon-and-va/.

[86] Elisabeth McClure, "More Than a Foundation: Young Children Are Capable STEM Learners," NAEYC, May 12, 2022, https://www.naeyc.org/resources/pubs/yc/nov2017/STEM-learners.

[87] Greg Duncan and Katherine Magnuson, "The Nature and Impact of Early Achievement Skills, Attention Skills, and Behavior Problems," in *Whither Opportunity?: Rising Inequality, Schools, and Children's Life Chances*, 2011, 47–69.

[88] Herman, "America's STEM Crisis Threatens Our National Security."

[89] Susan Rotermund and Amy Burke, "Elementary and Secondary STEM Education," National Science Foundation - National Science Foundation, July 8, 2021, https://ncses.nsf.gov/pubs/nsb20211/.

[90] "Little Bits, Early Exposure to STEM and Its Impact on the Future of Work" (Purdue University, n.d.), https://gems.education.purdue.edu/wp-content/uploads/2019/02/STEM_in_Schools_v1-2.pdf.

[91] Herman, "America's STEM Crisis Threatens Our National Security."

[92] Steve Manovich, "The Future of IoT: 10 Predictions about the Internet of Things," Norton, August 28, 2019, https://us.norton.com/internetsecurity-iot-5-predictions-for-the-future-of-iot.html.

[93] Arthur Cole, "How AI Will Drive the Hybrid Work Environment," *VentureBeat* (blog), January 16, 2022, https://venturebeat.com/2022/01/16/how-ai-will-drive-the-hybrid-work-environment/.

[94] Will Hurd and Robin L. Kelly, "Rise of the Machines: Artificial Intelligence and Its Growing Impact on U.S. Policy" (United States. Congress. House. Committee on Oversight and Government Reform (2007-), September 2018), https://www.hsdl.org/?abstract&did=816362.

[95] Patti Rote and Ethan Karp, Discussion of issues with underserved communities in robotics, March 5, 2022.

[96] Shivaun Albright and Ethan Karp, Discussion of the need for more ethical hackers, April 7, 2022.

[97] Ming Lin and Ethan Karp, Discussion regarding percentages of female and African American graduates, University of Maryland Computer Science Department, January 15, 2022.

[98] Katherine Hicks, "Memorandum for Senior Pentagon Leadership, Creating Data Advantage" (Deputy Secretary of Defense, May 2021), https://media.defense.gov/2021/May/10/2002638551/-1/-1/0/deputy-secretary-of-defense-memorandum.pdf.

[99] Herman, "America's STEM Crisis Threatens Our National Security."

[100] Nicols, "STEM Education Statistics 2019."

[101] Joske, "Picking Flowers, Making Honey."

[102] Jacob Feldgoise and Remco Zwetsloot, "Estimating the Number of Chinese STEM Students in the United States," *Center for Security and Emerging Technology* (blog), October 2020, https://cset.georgetown.edu/publication/estimating-the-number-of-chinese-stem-students-in-the-united-states/.

[103] "The Gordian Knot Center for National Security Innovation," Stanford University, accessed May 19, 2022, https://gordianknot.stanford.edu/.

[104] Catherine Armstrong, "What Kind of Jobs Did People Have in the 1930s?," *Career Trend*, 2018, https://careertrend.com/info-8254157-kind-jobs-did-people-1930s.html.

[105] Armstrong.

[106] "The Data Army," *Praxis* (blog), April 9, 2021, https://praxis.ac.in/the-data-army/.

[107] "All Countries of Citizenship by Number of Active Student & Exchange Visitor Information System (SEVIS) Records" (US Immigration and Customs Enforcement, 2021), https://www.ice.gov/doclib/sevis/pdf/data-CitizenshipActiveStudents_2021.pdf.

[108] COL Chris H. Bachmann, "Mobilizing in the Twenty-First Century," *Army University Press,* April 2021, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/March-April-2021/Bachmann-Mobilization/.

[109] Kelley M. Sayler, "Artificial Intelligence and National Security" (Congressional Research Service, November 10, 2020), https://crsreports.congress.gov/product/details?prodcode=R45178.

[110] Sayler.

[111] "NSCAI 2021 Final Report," 109.

[112] "NSCAI 2021 Final Report."

[113] Jean-Marc Rickli, "Containing Emerging Technologies' Impact on International Security" (Transatlantic Leadership Forum, April 2020), https://frivarld.se/wp-content/uploads/2019/12/rickli.pdf.

[114] The National Academies of Sciences Engineering Medicine, "Dual-Use Technologies and National Security," *International Friction and Cooperation in High-Technology Development and Trade: Papers and Proceedings,* The National Academies Press, 1997, https://nap.nationalacademies.org/read/5902/chapter/16#131.

[115] Nicolas Harle, et al., "What Deep-tech Startups Want From Corporate Partners," The Boston Consulting Group, April 2017, https://image-src.bcg.com/Images/BCG-What-Deep-Tech-Startups-Want-from-Corporate-Partners-Apr-2017_tcm9-150440.pdf.

[116] Jean-Marc Rickli and Marcello Ienca, "The Security and Military Implications of Neurotechnology and Artificial Intelligence," *Clinical Neurotechnology Meets Artificial Intelligence, Philosophical Ethical, Legal and Social Implications* (March 2021): 197, https://www.researchgate.net/publication/349772511_The_Security_and_Military_Implications_of_Neurotechnology_and_Artificial_Intelligence.

[117] Josh Lerner and Ramana Nanda, "Venture Capital's Role in Financing Innovation: What We Know and How Much We Still Need to Learn," *Journal of Economic Perspectives,* Vol. 34, No. 3 (Summer 2020): 246.

[118] Josh Lerner and Ramana Nanda, "Venture Capital's Role in Financing Innovation: What We Know and How Much We Still Need to Learn," *Journal of Economic Perspectives,* Vol. 34, No. 3 (Summer 2020): 249.

[119] Charles Duhigg, "How Venture Capitalists Are Deforming Capitalism," *The New Yorker,* November 23, 2020, https://www.newyorker.com/magazine/2020/11/30/how-venture-capitalists-are-deforming-capitalism.

[120] Nicolas Goeldel et al., "Deep Tech: The Great Wave of Innovation" (The Boston Consulting Group, January 2021), https://hello-tomorrow.org/wp-content/uploads/2021/01/BCG_Hello_Tomorrow_Great-Wave.pdf.

[121] Mossimo Portincaso et al., "The Deep Tech Investment Paradox: A Call To Redesign The Investor Model" (The Boston Consulting Group, May 2021), https://hello-tomorrow.org/wp-content/uploads/2021/05/Deep-Tech-Investment-Paradox-BCG.pdf.

[122] Portincaso et al.

[123] Ellen Chang, "DoD, Investment, Dual Use, Acceleration!," *Medium* (blog), October 30, 2019, https://syndicate708.medium.com/dod-investment-dual-use-acceleration-8ec5c9f9183b.

[124] Chang.

[125] Chang.

[126] Karmjot Grewal, "SBIR and STTR 101" (Office of Community and Economic Development, December 9, 2015), https://www.slideshare.net/MystyRusk/sbir-101-overview.

[127] Tim Webb et al., "Venture Capital and Strategic Investment for Developing Government Mission Capabilities" (RAND, 2014), https://www.rand.org/content/dam/rand/pubs/research_reports/RR100/RR176/RAND_RR176.sum.pdf.

[128] Webb et al.

[129] Webb et al.

[130] Jonathan Miller, "Who's Your Ally?," *Medium*, August 10, 2020, https://medium.com/@iamjmill/whos-your-ally-e2ff6068cd3a.

[131] Lloyd J. Austin III, "Opinion | The Pentagon Must Prepare for a Much Bigger Theater of War," *Washington Post*, May 5, 2021, https://www.washingtonpost.com/opinions/lloyd-austin-us-deter-threat-war/2021/05/05/bed8af58-add9-11eb-b476-c3b287e52a01_story.html.

[132] Valery Gerasimov, "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and of Carrying Out Combat Operations," trans. Robert Coalson, Military-*Industrial Kurier*, 27 February 2013, *Military Review*, February 2016, 23–29.

[133] Eugene Rumer, "The Primakov (Not Gerasimov) Doctrine in Action," Carnegie Endowment for International Peace, 2019, https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.

[134] James Clayton, "How Facial Recognition Is Identifying the Dead in Ukraine," *BBC*, April 13, 2022, https://www.bbc.com/news/technology-61055319.

[135] Will Knight, "As Russia Plots Its Next Move, an AI Listens to the Chatter," *Wired*, April 4, 2022, https://www.wired.com/story/russia-ukraine-war-ai-surveillance/.

[136] Ritwik Gupta et al., "XBD: A Dataset for Assessing Building Damage from Satellite Imagery" (arXiv, November 21, 2019), https://doi.org/10.48550/arXiv.1911.09296.

[137] "Ukraine: Internet Penetration 2023," Statista, accessed May 20, 2022, https://www.statista.com/statistics/1023197/ukraine-internet-penetration/.

[138] Mykhailo Fedorov, "Ukraine's Digital Revolution Is Gaining Momentum," *Atlantic Council* (blog), September 7, 2021, https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-digital-revolution-is-gaining-momentum/.

[139] Jen Judson, "US Army to Demo Offensive Drone Swarms in next Project Convergence," C4ISRNet, March 1, 2022, https://www.c4isrnet.com/unmanned/2022/03/01/us-army-to-demo-offensive-drone-swarms-in-next-project-convergence/.

[140] Deepa Shivaram, "UNESCO Says 53 Cultural Sites in Ukraine Have Been Damaged since the Russian Invasion," *NPR*, April 2, 2022, sec. World, unesco, https://www.npr.org/2022/04/02/1090475172/unesco-ukraine-cultural-sites-damage.

[141] Huileng Tan, "Ukraine's 285,000 IT Specialists," Business Insider, April 8, 2022, https://www.businessinsider.com/ukraine-it-specialists-still-working-through-war-2022-4.

[142] "Digital Country," Official website of Ukraine, accessed May 20, 2022, https://ukraine.ua/invest-trade/digitalization/.

[143] "Digital Country."

[144] "History of the Institute | Інститут Проблем Штучного Інтелекту (Київ, Україна)," accessed April 23, 2022, http://www.ipai.net.ua/en/history.

[145] Denys Shmyhal, "Concept of Artificial Intelligence Development in Ukraine for 2021-2024," Legislation of Ukraine, May 12, 2021, https://zakon.rada.gov.ua/go/438-2021-%D1%80.

[146] Shmyhal.