

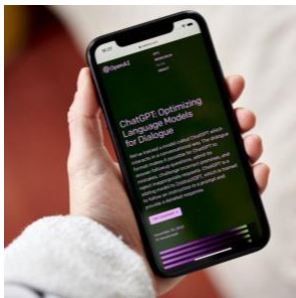


Harvard Model Congress Boston 2024

ARTIFICIAL INTELLIGENCE THREATS TO NATIONAL SECURITY

By Tova Kaplan

INTRODUCTION



The homepage of ChatGPT, an artificial intelligence chatbot launched in 2022 by the organization OpenAI

SFGATE

The phrase *artificial intelligence* (AI) may suggest futuristic images of humanoid robots shooting lasers or sleek dystopian cityscapes. However, **artificial intelligence**, defined as computer systems capable of performing tasks that normally require human intelligence, is no longer confined to the realm of science fiction. AI has emerged in recent years as a living reality impacting daily life across the globe. AI is now used for a variety of everyday tasks we take for granted, such as facial recognition technology to unlock phones, natural language processing to enable voice assistants like Siri, predictive technology personalizing our Google searches, social media feeds, and so much more (Marr, 2019). More recently, the launch of AI chatbot ChatGPT in 2022 has brought artificial intelligence to the forefront of American discourse, with the technology able to perform a stunning array of creative and analytical tasks, from writing intricate code to composing Shakespearean sonnets about how annoying it is to have to read through an entire Harvard Model Congress briefing.

But as artificial intelligence becomes more and more embedded into society, influential thinkers have begun sounding the alarm on the potential risks of such a powerful technology and the need for government intervention. Before his death, Stephen Hawking famously warned that “the development of artificial intelligence could spell the end of the human race” (Clark, 2014). Sam Altman, the CEO of OpenAI — the company behind ChatGPT and GPT-4 — testified in front of the Senate in May 2023, addressing that “if this technology goes wrong, it can go very wrong...we want to work with the government to prevent that from happening” (Duffy, 2023). Of course, not all predictions of an AI future are so dire. Yet, it is clear

that AI has the potential to change much about how the world operates, and Congress must urgently decide how to respond.

EXPLANATION OF THE ISSUE

Artificial intelligence (AI) – computer systems capable of performing tasks that normally require human intelligence.

Historical Development

Artificial intelligence is a relatively new phenomenon, reliant on increasingly advanced computing technology that emerged in the aftermath of World War II. In 1950, computer scientist Alan Turing published a paper discussing the possibility that humans could develop thinking machines and created the concept of a **Turing Test**: a machine could be classified as “thinking” if it could fool a human into believing it was having a conversation with another human. The field of artificial intelligence was officially founded at a 1956 workshop at Dartmouth College. However, limited computational power held back AI progress at the time. In more contemporary times (since the early 2000s) there has been a massive resurgence of interest in the development of AI, due to increased access to massive amounts of data to improve algorithms and processing capabilities. Machine learning techniques, such as **deep learning** (which designs algorithms to automatically learn and improve from experience) have allowed the pace of development to quickly accelerate (Council of Europe, 2023).

Deep Learning – a way to train AI algorithms through automatic learning and improving from experience, a technique that has allowed AI development to rapidly accelerate.

Theoretical Features of AI

AI is further divided into *weak* and *strong* AI. **Weak AI** is AI that focuses on a specific task with parameters defined by humans, without general intelligence or the ability to do things outside their programmed capabilities. For instance, email spam filters use weak AI to analyze the content of emails and determine whether an email contains individually valuable information. **Strong AI**, on the other hand, is a theoretical form of AI that is self-aware with intelligence comparable to a human, able to move beyond its programmed limits to achieve virtually any task a human can (IBM, 2022). When discussing policy, it is very important to note that, while *weak AI* is already widely used, *strong AI* does not currently exist, and experts can only speculate about whether it will be created in the future. Many of the most extreme predictions about AI “taking over” humanity refer to the possible development of future *strong AI* systems, not current *weak AI* capabilities. However, even the *weak AI* technology that exists can pose many national security challenges and this briefing will only discuss the implications of *weak AI* technology.

Scope of the Problem

Issues in National Defense

Data Poisoning – attempting to disable a piece of AI technology by flooding it with false information—just one of many strategies that could compromise the ability of AI technologies.

AI technology has the potential to enhance military capabilities, but that comes with challenges. One major concern is reliance on AI systems that are not fully explainable or interpretable, making it challenging to understand the decision-making process and potentially compromising trust and accountability. Furthermore, AI algorithms are susceptible to cyber-attacks from enemies of the US.

Take, for example, **data poisoning** – when a bad actor tries to mess up an AI algorithm by feeding it misleading information (Bierbauer et al, 2022). An AI system designed to identify targets that relies on satellite imagery could be misled if an adversary introduces subtly altered images or false labels into the training data to mislead the system's ability to identify and classify targets accurately. In addition, there is danger in over-reliance on AI systems without robust fallback options, such as the loss of critical capabilities if the technology fails or is sabotaged.

Another controversial military issue involves the debate over whether AI should be integrated into weapons systems. Some experts believe that using AI to automate weapons that identify targets and fire automatically can increase accuracy, reduce civilian casualties, and increase efficiency. However, others believe that incorporating AI into weapons systems sidelines human judgment and could lead AI to escalate a situation automatically without considering the larger and long-term dangers of escalation (Coy, 2023).

Finally, there is always a risk of AI weapons technology falling into the hands of non-state actors like terrorist or militant groups, who could deploy such technology to commit acts of violence, whether that involves using AI-equipped drones to attack civilians, using AI software to break past online security and commit cyber-attacks, or more (Kreps, 2021).



AI technology scanning a military scene to identify various objects

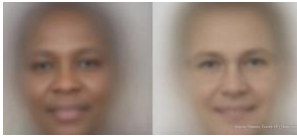
US Army/Defense Visual Information Distribution Service

Privacy Concerns

AI development has also raised significant concerns around privacy. AI systems heavily rely on vast amounts of data to train and make accurate predictions. The collection of personal data for AI purposes, especially when done without transparency or explicit consent, poses a significant privacy risk. AI algorithms have the potential to extract sensitive information from data – such as personally identifiable information (PII), financial records, medical history, or even intimate details – which can lead to privacy breaches or identity theft. In addition, the storage and security of data used by AI systems are crucial aspects to consider. As AI applications handle large volumes of sensitive information, there is an increased risk of unauthorized access, data breaches, or cyberattacks. Inadequate

security measures or vulnerabilities in AI systems can expose personal data to malicious actors, jeopardizing individuals' privacy. (Economic Times, 2023)

When applied to government, AI incorporation poses even broader ethical challenges: AI technologies enable extensive profiling and surveillance capabilities which have the potential to infringe on personal privacy. Through the analysis of individuals' online activities, facial recognition, or behavior tracking, AI algorithms can create detailed profiles, predicting personal preferences, behaviors, and even emotions. This extensive profiling raises concerns about invasion of privacy, limited personal freedoms, and the establishment of a surveillance society. Without limits on how the government can use this data, many worry that it could be used to profile people or invade the privacy of citizens (Roff, 2020).



Gender Shades, a research group at MIT, found that every AI facial recognition company that they studied performed better on recognizing male faces than female and on lighter faces over darker faces.

MIT Media Lab

Bias in AI

AI, additionally, has proven on-exempt from implicit bias. There is a major risk of AI reinforcing racial, gender, age, religious, socioeconomic, and other societal biases. For instance, some US courts used the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) algorithm to predict the chance that a defendant would re-offend and commit another crime. The model predicted double the number of false positives for reoffending for Black offenders than White offenders, which could lead to very real consequences for Black defendants (Datatron, 2023).

Even when developers and organizations aim to create fair and unbiased AI systems, unintentional biases can still emerge. Complex algorithms and intricate data interactions can make it difficult to identify and rectify biases present within AI models. Biased training data is another crucial factor contributing to biased AI systems. AI algorithms learn from historical data, which often contains societal biases and prejudices documented throughout history. If this data is not carefully curated and is not diverse and representative, the resulting AI models can perpetuate and amplify existing biases, leading to unfair outcomes and discrimination (Project Gender Shades, 2020).

The lack of diversity within AI development teams is another factor contributing to biased AI. Homogenous teams may unintentionally overlook and exclude certain biases or fail to consider the diverse perspectives necessary to identify and address potential biases in AI systems (Marr, 2022).

Biased AI raises ethical and legal concerns, as it can infringe upon individuals' rights, perpetuate discrimination, and reinforce existing societal inequalities. From an ethical standpoint, biased AI systems can compromise fairness, transparency, and accountability. Legally, it may violate regulations and anti-discrimination laws.

Disinformation

Disinformation –
false information
designed to mislead.
AI makes
disinformation much
easier to produce.



*Fake, AI-generated
clip of CNN Anchor
Anderson Cooper
posted by Donald
Trump Jr.
Generative AI can
easily create
convincing
disinformation.*

*Screenshot, Twitter of
Donald Trump Jr.
Twitter Post*

“I’m told this is real,” wrote Donald Trump Jr., son of former US President Donald Trump, as he reposted a fake, AI-generated clip of CNN anchor Anderson Cooper making disparaging remarks (Paul, 2023). This instance showed how susceptible even high-profile Americans are to AI-generated **disinformation** (defined as false information designed to mislead). AI technology, such as generative systems like ChatGPT, make disinformation easier and cheaper to produce at a mass scale. Open AI researchers have written that AI could be used “in malicious pursuit of monetary gain, a particular political agenda, and/or a desire to create chaos or confusion” (Hsu and Thompson, 2023). Foreign actors, for instance, could use AI to mass produce convincing, fake videos of a political candidate right before an election to sway the results or create content faking evidence of voter fraud, raising baseless voter fraud claims. As generative AI technology advances to the point where it becomes indistinguishable from reality, this technology has the potential to completely upend trust in the government and spark violence and unrest based on false information.

Congressional Action

Because the issue of AI in government is so new, Congress has been slow to act, and therefore there is currently no flagship AI initiative comparable to what other countries have passed. In Europe, however, the European Union passed the AI Act to provide comprehensive legislative guidance on the implementation of AI.

So far, Congressional legislation has focused more on encouraging the US government to develop AI, such as the **National AI Initiative Act of 2020 (NAIA)**, to “ensure continued US leadership in artificial intelligence research and development”. This law and others particularly highlight the international stake in the importance of the US developing AI technology before adversaries like China and Russia (Pouget, 2023). Legislation constricting the use of AI, for instance the Algorithmic Accountability Act, which would regulate private sector AI use, have largely failed to gain momentum (Clarke, 2022).

More than legislating AI itself, Congress has attempted to improve the Executive Branch’s regulatory ability by giving Federal agencies knowledge and tools around AI, without creating specific requirements. As researchers at the Carnegie Endowment for International Peace wrote, “this sets the stage for what could be more binding regulation in the future, giving the government the tools required to identify and mitigate problems, although it is far from

clear whether this will come to pass” (O’Shaughnessy, 2023). Congress is often hesitant to act on legislating around AI because its members may feel unequipped to understand this complex issue without specialized knowledge.

Other Policy Action

In the absence of congressional legislation on how to handle AI, the Executive branch has taken center stage in directing AI policy. In 2022, the Biden administration published its **Blueprint for an AI Bill of Rights**, which set priorities for the Federal government’s policy on AI, emphasizing safe systems, data privacy, notice and explanation, and human fallback options for AI systems (The White House, 2022). The blueprint takes stronger positions than current congressional action, but it is still a voluntary document and the department that created it, the Office of Science and Technology Policy, has no direct regulatory power.

President Biden also signed an Executive Order in February 2023 directing federal agencies to work to eliminate bias in new AI technologies. The National Science Foundation also announced \$140 million in funding to launch seven new institutes to study AI across the country (The White House, 2023). However, without new and concrete legislation from Congress, Federal agencies can only control how they implement AI policy within the bound of existing legislation, which limits their ability to regulate AI.

Other countries have been more proactive in regulating AI than the United States. The European Union has advanced the **AI Act**, which includes bans on biometric surveillance, emotion recognition, and predictive policing in AI systems. The act also would require companies to conduct risk assessments of their technology with a fine of 6 percent of their global revenue if they fail to do so (European Parliament, 2023). Chinese regulators recently released new rules regulating AI companies, which would mandate that companies ensure that training data will not discriminate on the basis of ethnicity, race, and gender, will not generate false information, and, going further, won’t subvert state power and reflect socialism (Kharpal, 2023).

Private companies have also occasionally used their influence to limit AI development. Technological conglomerate Apple, for instance, delayed approval of an email app that used AI technology to generate text (Sorkin, 2023).



The Biden White House has published guidance on how the Federal government should respond to AI threats.

Mozilla Foundation

IDEOLOGICAL VIEWPOINTS



Congressman Jay Obernolte (R-CA) is one of the only lawmakers in Congress with a computer science degree, and serves on the House AI Caucus.

Wikicommons



Congressman Ted Lieu (D-CA) advocates for a general agency to regulate AI, and argues that “there is nothing inherently partisan about AI” (Mark, 2023).

Wikicommons

Conservative View

Conservatives generally prioritize limited government intervention and regulation. Some conservatives may have concerns about excessive regulation of AI technology stifling innovation and impeding free market dynamics. Particularly, conservatives tend to express concern that, if the United States regulates AI too strictly, our foreign adversaries will develop AI technology faster than us, creating a significant developmental advantage. For instance, President Trump made an Executive Order arguing that “continued American leadership in AI is of paramount importance to maintaining economic and national security” (Donald Trump, 2020). They may favor a more hands-off approach to AI regulation, with a focus on voluntary industry standards and self-regulation.

Conservatives generally emphasize the positive economic impact of AI, such as increased productivity and innovation. They may view AI as a driver of economic growth and job creation in various sectors with the potential to offset any short-term job displacement. Also, conservatives generally tend to be skeptical of spending too much money on any initiatives and may prefer targeted investments in AI research and development, often with a focus on national security and defense applications. They may prioritize funding mechanisms that promote private-sector innovation and competition. Some conservatives may also support the use of AI technologies for defense applications, including autonomous systems and surveillance, with a focus on maintaining a strong military advantage.

Liberal View

Liberals, on the other hand, tend to emphasize the need for robust regulation and oversight to address potential risks and societal implications of AI. They may advocate for stricter regulations to ensure ethical AI development, protect individual privacy, prevent algorithmic bias, and promote fairness and accountability. Liberals often emphasize social justice and equality and may advocate for accountability to ensure that AI benefits society and minimizes harm. Liberals may also have concerns about the potential negative impact of AI on income inequality. They may prioritize policies such as retraining programs, job guarantees, and social safety nets to mitigate the potential adverse effects of AI-driven automation on workers. Liberals may advocate for increased government funding in AI research, development, and literacy to ensure that the technology holistically benefits society, particularly in areas such as AI ethics, fairness, and social impact research.

Liberals may also prioritize diplomacy and international coordination with other countries on AI, particularly with military issues, rather than focusing only on developing US AI technology in competition with other countries.

However, it is important to keep in mind that most action on AI regulation has been bipartisan, and there is considerable overlap between political ideologies on this issue.

AREAS OF DEBATE

Establishing a Federal Agency to Regulate and Study AI

One common solution for dealing with AI is for Congress to establish a federal agency to license and regulate AI development. Congressman Ted Lieu (D-CA) argued to the Washington Post that having a “general agency do regulations” would be a more effective policy than regulating AI in every discrete instance in which it is used” (Mark, 2023). Sam Altman, the founder of Open AI, suggested that this agency could be made up of a group of scientists to test AI products and force companies to address safety risks (Fung, 2023). In a report, the US Government Accountability Office urged Congress to establish an agency to “issue guidance that defines outcomes and monitors accountability for AI-related activities”. In addition to regulating AI, this agency could conduct research on AI technology and its impacts. Many lawmakers feel that they have historically failed to regulate social media companies, another technology whose sudden rise many feel is analogous to that of AI, and so they want to make up for their previous failure by proactively moving to regulate AI through establishing a federal agency (Howley, 2023). However, other lawmakers, such as Congressman Obernolte (R-CA), believe that instead of creating a federal agency, Congress should instead create legislation on a case-by-case basis (Mark, 2023).

Political Perspectives on this Solution

AI is a rapidly evolving field, and excessive or premature regulation could stifle innovation. It is crucial to strike a delicate balance between encouraging technological advancements and ensuring adequate safeguards to protect public interest. In addition, if the US too harshly regulates AI, it could develop its AI technology slower than other countries like China and lose its current advantage in AI development (Morrison, 2023). Also, some conservatives

“The Industrial Revolution was all about replacing the physical power of humans. AI is about replacing humans’ cognitive power”

- Tom Wheeler,
Center for
Technology
and
Innovation



Sam Altman, CEO of Open AI, testifying before Congress. Altman has advocated for increasing regulation on AI.

CNN

Regulatory capture – when regulatory agencies tasked with protecting the public interest, become too controlled by the industries that they are supposed to regulate, which leads to rules that favor the industry important term means.

express concerns that leaders in AI skew liberal, so they may be wary of an AI regulatory agency that they believe has too much democratic influence.

Also, the role of tech companies in developing AI regulations needs to be considered. If tech companies have too much influence over regulations, there is a risk of **regulatory capture** — when regulatory agencies tasked with protecting the public interest, are controlled by the industries that they are supposed to regulate, leading to the enforcement of rules that favor the industry. On the other hand, some AI companies may not want to be regulated. Tech company Alphabet’s CEO Sundar Pichai, for instance, lobbied against facial-recognition regulations, arguing that “we aren’t anti-regulation, but we’d want smart regulation” (Sorkin, 2023).

International Treaty

Some believe that international coordination is the best way to resolve AI issues. On May 30, 2023, over 350 AI executives signed a letter arguing that “mitigating [AI risk] should be a global priority alongside other societal-scale risks, such as pandemics and nuclear war” (Roose, 2023). An article written by the leaders of Open AI urged the creation of an international organization on par with the International Atomic Energy Agency (which regulates nuclear weapons) that could “inspect systems, require audits, and test for compliance” (Altman et al, 2023). An international agency or treaty on AI could promote global cooperation and coordination in addressing the risks associated with AI. It could facilitate the sharing of best practices, information, and expertise among nations, leading to consistently enforced standards and regulations for AI development and deployment. As AI-related challenges are not confined within national borders, an international treaty could provide a platform to address these transnational issues effectively, fostering international cooperation and mutual assistance. As French President Emmanuel Macron remarked, “who can claim to be sovereign, on their own, in the face of the digital giants?” (Kane and Wallach, 2022).

However, this might prove difficult as negotiating an international treaty requires aligning the interests and priorities of participating nations. Given the diversity of nations’ concerns and agendas, it might be challenging to reach a consensus on the provisions and enforcement mechanisms of the treaty.

Furthermore, ensuring enforcement and compliance with an international treaty can be complex, especially when nations have differing legal systems and levels of commitment to the treaty. The effectiveness of the treaty would largely depend on the willingness of participating nations to enforce its provisions and the availability of mechanisms to monitor compliance.

“Who can claim to be sovereign, on their own, in the face of the digital giants?”
French President Emmanuel Macron

Political Perspectives on this Solution

While the idea of international cooperation on AI draws bipartisan support, liberals generally tend to be more supportive of diplomacy as a resolution to international issues, while conservatives tend to be more skeptical. Congressional Republicans may worry that other countries could find ways to secretly avoid fulfilling a treaty's provisions, causing the US to fall behind in the AI race.

There are also many ways to go about an international treaty on AI, each of which may draw varying levels of support from each political party. The US could pursue a comprehensive AI treaty, aiming to address a wide range of issues related to AI including ethical principles, human rights safeguards, data security, limits on the use of AI in military weapons, and more. On the other hand, instead of covering all aspects of AI, the US could pursue specific issue-focused treaties to address specific areas, for instance, autonomous weapons systems. The treaty could also be either binding (the countries who sign are legally required to fulfill their commitments, with consequences for failing to do so) or non-binding (voluntary goals countries set without punishment for not achieving them).

Mandated Disclosure for AI Systems

One major goal in AI regulation is to increase transparency in AI technology so that people know when they are interacting with AI and can see how AI algorithms come to their decisions. Without transparency in AI algorithms, it is easier for people to be misled or succumb to false information. AI systems are known to fabricate information or come to false conclusions, a phenomenon known as **hallucinating**, so many contend that it is crucial that people using AI have the right to understand how it came to produce a certain result (Metz and Weise, 2023). One of the primary advantages of mandating transparency in AI technology is the enhancement of accountability and trust. By requiring AI systems to disclose their underlying algorithms and data sources, users can better understand how decisions are being made. This transparency enables individuals and organizations to systematically hold AI systems accountable for biased or discriminatory outcomes, promoting fairness and avoiding potential harm.

hallucinating – the tendency for generative AI systems to occasionally make up information, highlighting the need for systems to disclose their data sources and algorithms.

Some have proposed a requirement of disclosing when material has been generated by AI. For instance, if someone is talking to a chatbot instead of a human, they should have the right to know and have the option to switch to a human instead. This has the advantage

of allowing people to opt out of AI technology if they chose and would give consumers more power to make decisions.

However, mandating that AI systems identify themselves might make them less effective. For example, a recent study found that sales performance dropped by 80% when a chatbot was forced to identify itself as AI instead of a human (Engler, 2020). Another significant drawback of mandating transparency in AI technology relates to intellectual property (IP) concerns. Requiring companies to reveal their proprietary algorithms and datasets may discourage innovation and limit companies' ability to protect their trade secrets and successes.

Furthermore, transparency requirements for AI systems could raise security risks. If companies are compelled to disclose sensitive information about their AI technologies, it could expose exploitable vulnerabilities. Releasing detailed information on algorithms and data sources could enable reverse engineering or facilitate attacks on the systems themselves, potentially undermining privacy and system security.

The global AI market size is expected to increase ninefold between 2020 and 28 (Kane, 2022)

Political Perspectives on this Solution

Conservatives would likely prioritize limited government intervention and the protection of free-market principles over a regulatory approach. From a conservative perspective, mandating AI disclosure could be seen as excessive government regulation that stifles innovation and hampers economic growth. They might argue that businesses should have the freedom to protect their intellectual property, maintain trade secrets, and compete in the marketplace without burdensome requirements. Conservative thinkers may also emphasize the potential security risks associated with disclosing sensitive information, highlighting the need to safeguard algorithms from malicious actors. Finally, conservatives may worry that requiring US companies to disclose their algorithms would advantage foreign adversaries, who could unfairly incorporate aspects of US AI technology and benefit from US-funded research.

From a liberal perspective, mandating AI disclosure aligns with liberal principles of transparency, accountability, and fairness. Liberals may argue that requiring transparency promotes ethical decision-making, prevents discrimination, and ensures that AI systems do not perpetuate biases and/or harm marginalized communities. Liberals might view AI as having significant societal impacts and argue that the public should have access to information about the algorithms and data that drive these systems. They may also advocate for transparency to enable independent audits and assessments of AI technologies to uncover potential biases or discrimination. Finally, although many AI companies have called for regulation, some may be against enforced disclosure requirements

from Congress. As very few Congresspeople have experience with AI or understand the technology, they may not know how to best enforce requirements like transparency and may make rules that are overly difficult for companies to follow. Complying with transparency mandates may impose significant costs and administrative burdens on corporations. This could divert valuable resources away from other critical activities such as research, development, and innovation of new AI technology. Corporations may assert that the additional compliance burdens could hinder their ability to adapt and compete in a rapidly evolving technological landscape.



*Asad Ramzanali,
Chief of Staff for the
White House Office
of Science and
Technology Policy,
who oversaw a
\$140 million
increase in funding
for AI research.*

The White House

Investing in AI Safety Research and Training

Another category of proposals focuses on improving research around AI safety and educating lawmakers and government officials about the risks associated with AI. Investing in AI safety research today can yield significant long-term benefits. By proactively addressing potential risks, we can avoid the negative consequences that may emerge as AI technology becomes more prevalent and powerful. Much is still unknown about AI and its impacts on society, so investing funding in research can help us better adapt to its challenges.

In addition, there is currently a lack of lawmakers who understand AI technology, with the US government needing 400,000 additional cybersecurity-trained people (National Counterintelligence and Security Center, 2020). AI research could focus on improving knowledge of AI in government, so that officials can feel empowered to create better AI policy in the future.

Political Perspectives on this Solution

Increasing funding for researching AI safety requires diverting resources from other areas of research and development. Critics may argue that these resources could be better utilized for other pressing issues, such as healthcare, education, or climate change. Prioritization and delegation become key considerations, as allocating more funding to AI safety may mean sacrificing investment in other critical areas. In addition, the outcomes of increased funding for AI safety research are not guaranteed, so critics may question the effectiveness of pouring more resources into a field that is still evolving and may not deliver immediate tangible results. Measuring the impact and determining the return on investment in AI safety research can be challenging.

BUDGETARY CONSIDERATIONS

When developing bills, keep in mind the various associated costs for your proposals. Establishing any government agency or allocating people in charge of regulating AI would cost money to pay for salaries, infrastructure, and administrative costs. Other proposals, such as investing in AI research, would also carry a monetary cost. Furthermore, regulation may have an indirect cost of limiting innovation and the growth of the rapidly expanding AI sector of the economy. Each situation is different but be sure to consider these costs and explicitly incorporate them into your bills.

CONCLUSION

*“AI is one of the most powerful technologies of our time, but in order to seize the opportunities it presents, we must first mitigate its risks”
(Biden Administration Briefing, May 4, 2023)*

Artificial intelligence will change much about our world, impacting all aspects of life, from the economy to the military, to communication, to education, and so much more. Our government must decide how to act now, balancing the complex push-and-pull between international competition and cooperation, private companies and public interests, and innovation and regulation. The exciting thing about this topic is that because it is so new and most lawmakers have little expertise on it, your ideas, even as high schoolers, can be as innovative as those currently floating around Congress. Feel encouraged to develop your own thoughts and solutions, even those not discussed in this briefing. You will be able to watch the issues you discuss now play out in real-time on the world stage. Together, we can imagine ways to create a world with artificial intelligence that is safe, equitable, and beneficial to all.

GUIDE TO FURTHER RESEARCH

Although research into modern AI technology is relatively new, there is a wealth of information online. For one, the US government has commissioned many reports on AI and its significance for US national security (some of which are cited in this briefing’s bibliography). I suggest looking into the White House AI Commission, House AI Caucus, and the National AI Initiative (AI.gov).

To step outside the government bubble, I also recommend reading articles from AI experts at think tanks (research institutes) to gain a more comprehensive background on the issue. Try to investigate think tanks from diverse ideological perspectives to further understand how political leanings can influence policy

recommendations. Liberal-leaning think tanks to research include the Center for American Progress, Economic Policy Institute, and Human Rights Watch, while some conservative-leaning think tanks include the American Enterprise Institute, Heritage Foundation, and Cato Institute. Pew Research, Brookings Institution, and the Carnegie Endowment for International Peace are regarded as nonpartisan (Georgetown University Library, 2023).

Finally, play around with AI technology yourself! The best way to understand the capabilities of these technologies is to engage with them, whether that's testing prompts on ChatGPT, generating images on DALL-E, or just generally probing the limits and capabilities of AI. Many new programs will likely be created even between the publication of this briefing and our HMC conference, so get creative exploring them and charting the exciting future of AI technology.

GLOSSARY

Artificial intelligence (AI) – computer systems capable of performing tasks that normally require human intelligence

Deep Learning – a way to train AI algorithms through automatic learning and improving from experience, a technique that has allowed AI development to rapidly accelerate

Data Poisoning – attempting to disable a piece of AI technology by flooding it with false information— just one of many strategies that could compromise the ability of AI technologies

Disinformation – false information designed to mislead. AI makes disinformation much easier to produce

Regulatory capture – when regulatory agencies tasked with protecting the public interest, become too controlled by the industries that they are supposed to regulate, which leads to rules that favor the industry

Hallucinating – the tendency for generative AI systems to occasionally make up information, highlighting the need for systems to disclose their data sources and algorithms

BIBLIOGRAPHY

- Marr, Bernard. "The 10 Best Examples of How AI Is Already Used in Our Everyday Life." Forbes, 16 Dec. 2019, www.forbes.com/sites/bernardmarr/2019/12/16/the-10-best-examples-of-how-ai-is-already-used-in-our-everyday-life/?sh=3c13b3081171.
- Gibney, Elizabeth. "Stephen Hawking to Enable Injured Astronaut to Communicate via Brainwaves." The Guardian, 2 Dec. 2014, www.theguardian.com/science/2014/dec/02/stephen-hawking-intel-communication-system-astrophysicist-software-predictive-text-type.
- "Artificial intelligence, deep learning, and machine learning: What do they mean and how do they relate?" IBM, www.ibm.com/topics/strong-ai.
- "History of AI." Council of Europe, www.coe.int/en/web/artificial-intelligence/history-of-ai.
- "Democratizing harm: Artificial intelligence in the hands of non-state actors." Brookings, www.brookings.edu/research/democratizing-harm-artificial-intelligence-in-the-hands-of-non-state-actors/.
- Gohel, Sajjan. "Artificial Intelligence: Real Risks, Understanding and Mitigating Vulnerabilities in the Military Use of AI." Modern War Institute at West Point, mwi.usma.edu/artificial-intelligence-real-risks-understanding-and-mitigating-vulnerabilities-in-the-military-use-of-ai/.
- "Artificial Intelligence: Real Risks, Understanding and Mitigating Vulnerabilities in the Military Use of AI." Brookings, www.brookings.edu/research/what-is-artificial-intelligence/.
- "How Machine Learning is Revolutionizing Everyday Life." Georgetown University Library, guides.library.georgetown.edu/c.php?g=933266&p=6727039.
- "The Rise of AI: How Artificial Intelligence Is Changing Our Lives." Apple News, apple.news/Ak7PYypw2RUWV-e_PfjywfA.
- "Artificial Intelligence and Machine Learning in Healthcare." Apple News, apple.news/A9OCloigON5OkAzWawF7Oyw.

No author. "AI and Nuclear Weapons Are a Troubling Combination." The New York Times, 19 May 2023, www.nytimes.com/2023/05/19/opinion/artificial-intelligence-military-nuclear.html?smid=nytcore-ios-share&referringSource=articleShare.

"The Problem with Biased AIs and How to Make AI Better." Forbes, 30 Sept. 2022, www.forbes.com/sites/bernardmarr/2022/09/30/the-problem-with-biased-ais-and-how-to-make-ai-better/?sh=65f5def44770.

"Uncomfortable Ground Truths: The Impact of Artificial Intelligence and Automation on Human Rights." Brookings, www.brookings.edu/research/uncomfortable-ground-truths/.

"AI and Privacy: The Privacy Concerns Surrounding AI & Its Potential Impact on Personal Data." The Economic Times, 7 Oct. 2021, economictimes.indiatimes.com/news/how-to/ai-and-privacy-the-privacy-concerns-surrounding-ai-its-potential-impact-on-personal-data/articleshow/99738234.cms.

"Real-Life Examples of Discriminating Artificial Intelligence." Datatron, datatron.com/real-life-examples-of-discriminating-artificial-intelligence/#:~:text=Arguably%20the%20most%20notable%20example,defendant%20would%20become%20a%20recidivist.

"Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." MIT Media Lab, www.media.mit.edu/projects/gender-shades/overview/.

"AI Chatbots and Disinformation: How Artificial Intelligence is Used for Misinformation." The New York Times, 8 Feb. 2023, www.nytimes.com/2023/02/08/technology/ai-chatbots-disinformation.html.

Paul, Andrew. "Trump Shares AI-altered Fake Clip of Anderson Cooper." Popular Science, 17 May 2023. <https://apple.news/ACQDNZx6ET5-jxiEaLMsiWA>

"Carnegie Endowment for International Peace." Carnegie Endowment for International Peace, 3 May 2023, carnegieendowment.org/2023/05/03/reconciling-u.s.-approach-to-ai-pub-89674.

- "Text - H.R.6580 - 117th Congress (2021-2022): Artificial Intelligence in Government Act of 2022." Congress.gov, Library of Congress, www.congress.gov/bill/117th-congress/house-bill/6580/text.
- "Lawmakers Look to Implement AI Regulations." DealBook, The New York Times, 3 Mar. 2023, www.nytimes.com/2023/03/03/business/dealbook/lawmakers-ai-regulations.html.
- "Executive Order on Further Advancing Racial Equity and Support for Underserved Communities Through the Federal Government." The White House, 16 Feb. 2023, www.whitehouse.gov/briefing-room/presidential-actions/2023/02/16/executive-order-on-further-advancing-racial-equity-and-support-for-underserved-communities-through-the-federal-government/.
- "AI Act: A Step Closer to the First Rules on Artificial Intelligence." European Parliament, 5 May 2023, www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence.
- "China Releases Rules for Generative AI like ChatGPT after Alibaba Launch." CNBC, 11 Apr. 2023, www.cnbc.com/2023/04/11/china-releases-rules-for-generative-ai-like-chatgpt-after-alibaba-launch.html.
- "Maintaining American Leadership in Artificial Intelligence." Federal Register, 14 Feb. 2019, www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence.
- "The U.S. Lags Behind China in AI, but Does It Matter?" Apple News, AwzwUMZLmTMOrodZjTfslsg.
- "Artificial Intelligence: GAO-22-105834." U.S. Government Accountability Office, www.gao.gov/products/gao-22-105834#summary_recommend.
- "Lawmakers seek to regulate AI use." Apple News, AHgD25mn6SmyhCLvyh3cdfA.
- Rey, Jason. "The AI industry needs Washington to do its homework." Vox, 11 May 2023, www.vox.com/technology/2023/5/11/23717408/ai-dc-laws-congress-google-microsoft.

Dwoskin, Elizabeth. "Tech Companies Pour Millions into Lobbying as They Face Threats to Their Power." The Washington Post, 17 May 2023, www.washingtonpost.com/technology/2023/05/17/ai-congress-obernalte/.

"Artificial intelligence is already upending geopolitics." TechCrunch, 6 Apr. 2022, techcrunch.com/2022/04/06/artificial-intelligence-is-already-upending-geopolitics/.

"AI chatbots are having hallucinations, and it's a bigger problem than you think." The New York Times, 1 May 2023, www.nytimes.com/2023/05/01/business/ai-chatbots-hallucination.html.

Singer, Peter W., and Peter W. Singer. "The Case for AI Transparency Requirements." Brookings Institution, 3 Mar. 2023, www.brookings.edu/research/the-case-for-ai-transparency-requirements/.