WORLD AFFAIRS COUNCIL
of Philadelphia

EXAMINING THE REGULATION OF AI AND CYBERSECURITY

Topic Background for the U.S. Senate on AI and Cybersecurity

“These commitments have the potential to shape developer norms and best practices associated with leading-edge AI models. At the same time, even less capable models are susceptible to misuse, security compromise, and proliferation risks” - Sen. Mark Warner (D - CT)

Potential of Artificial Intelligence

Photo by Chuck Ross

On September 13th, 2023, the United States Senate held a closed door meeting (picture by Chuck Ross) between Senate leadership and leading tech officials regarding the issue of Artificial Intelligence and the potential benefits and risks that it can have for the U.S. and the world.

In the field of **cybersecurity** and technology innovation, there has been optimism and discussion about the positive impacts that **Artificial Intelligence** could have in these sectors. Deputy Secretary of Defense Kathleen Hicks has welcomed the advancements in AI technology. Hicks has praised artificial intelligence for fostering “American ingenuity: our ability to innovate, change the game and, in the military sphere, to imagine, create and master the future character of warfare.” Similar praise to Artificial Intelligence has also been given by non-government officials such as former Microsoft CEO Bill Gates, who called Artificial Intelligence “the most important technological advancement in decades.”[1]

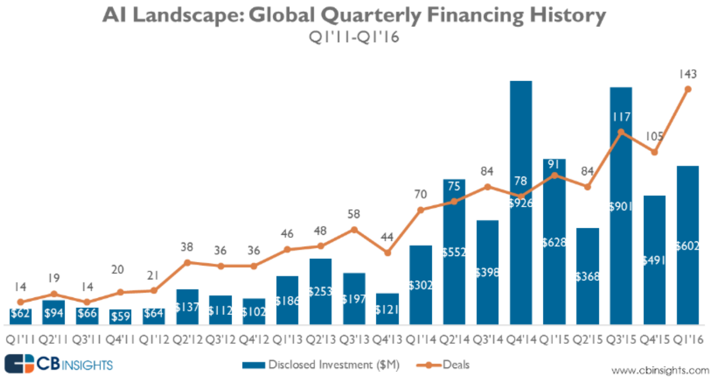
However, advancements in Artificial Intelligence have also raised significant concern over the potential threat that this new technology can pose to cybersecurity, American citizens, and the truth, if it goes unregulated. Former Google scientist and AI pioneer Geoffrey Hinton warned that the rapid growth of AI speech writing programs such as **ChatGPT** and image-altering **Deepfake** technology has the potential to create a world where people will “not be able to know what is true anymore.”[2] Concerns over the risk that AI poses to credibility and the truth have also been raised by U.S. government officials such as Senator Mark Warner of Connecticut, who believes that deepfake technology could spread misinformation during election years.

In the field of **cybersecurity**, artificial intelligence also comes with several risks. Four of these key security risks that AI poses are 1) **AI-driven malware**: computer viruses which can infect devices even faster,

[1] Hicks Discusses Replicator Initiative > U.S. Department of Defense > Defense Department News
[2] Geoffrey Hinton: AI pioneer quits Google to warn about the technology's 'dangers' | CNN Business

become larger to detect, and target more people than ever before. 2) **Vulnerable applications**: Software and machines which are not updated to deal with AI are especially vulnerable to cyber attacks. 3) **Expanded attack surface**: the use of cloud-data across multiple devices allows for AI to expand which devices and machines it can use to infiltrate systems. 4) **Constant evolution:** Artificial intelligence is always evolving, allowing for cybercriminals to learn from AI and enhance their cyber-attacks.

Benefits Artificial Intelligence



A World Economic Forum chart showing the rapid economic growth of the AI industry (weforum.org)

AI as a tool for public welfare

The U.S. Department of State has praised artificial intelligence and **quantum computing** for "providing great benefits to our social wellbeing in areas such as precision medicine, environmental sustainability, education, and public welfare."[3] Because of Artificial Intelligence, medical technologies and access to education have been made more accessible and beneficial to the public than ever before. AI has also helped break down barriers and connect the world even further through the use of language translation and voice-assisted smartphones. As a result, artificial intelligence has been a useful tool in promoting the public good.

AI as a tool for economic development

Artificial intelligence and AI-based software can greatly benefit the workforce and the economy. Through the automation of human tasks, businesses can engage more with customers through auto-response emails, automated advertisements, and feedback surveys which can improve business practices and therefore increase profits for the company. AI can also benefit worker productivity and free time. For example, the process of managing supply lines has reduced the need for larger storage facilities and workers required to staff these supply lines. This allows companies to make better use of their employees' skills and time.

AI as a tool to advance cyber security and U.S. Foreign Policy

Another prospective benefit of artificial intelligence is the ways in which it can help enhance U.S. cybersecurity efforts and promote U.S. foreign policy. Fortinet has stated that "AI tools, such as **CAPTCHA**, facial recognition, and fingerprint scanners enable organizations to automatically detect whether an attempt to log in to a service is genuine. These solutions help prevent cybercrime tactics like brute-force

[3] Artificial Intelligence (AI) - United States Department of State

attacks and **credential stuffing**, which could put an organization's entire network at risk."[4] Because of artificial intelligence technology, companies and government agencies are better able to detect potential cyber threats and act against them.

In terms of helping U.S. foreign policy, the United States Department of State has asserted that AI technology can help "both further our scientific and technological capabilities and promote democracy and human rights by working together to identify and seize the opportunities while meeting the challenges by promoting shared norms and agreements on the responsible use of AI." In other words, properly regulated AI could help advance U.S. partnerships and promote democracy and human rights across the globe.

Challenges posed by Artificial Intelligence

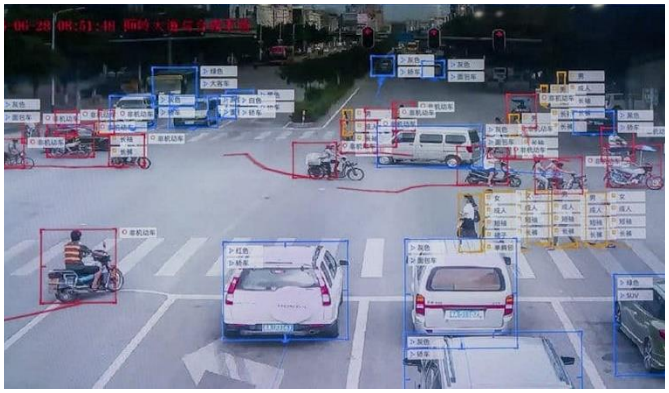
Challenges to Civil Rights

Corrine Yu, a top figure within the Leadership Conference on Civil and Human Rights, has warned that automated systems such as Artificial Intelligence can marginalize people based on their race, ethnicity, gender identity, or citizenship status. With AI algorithms typically created by humans, they are often subject to the same implicit biases and sampling biases that people have. **Implicit bias** is a bias that people hold which they might not even be aware of, and this can result in the bias being programmed into an AI's algorithm. **Sampling bias** refers to an error in which some members are represented in data more than others. Therefore, AI created by people with implicit biases could result in sampling biases in the AI they create.

A report from Joy Buolamwini of TIMES magazine has found that AI has been less likely to recognize the faces of minorities and women when compared to their white male counterparts. This shortcoming could undermine inclusivity and civil rights within society through the unintentional promotion of exclusion. Given the rapid expansion of Artificial Intelligence in society, it is crucial that such technologies are accessible to all members of society regardless of factors such as skin color or gender.

Challenges to Civil Liberties

Another big challenge posed by Artificial Intelligence is the threat it can pose to **civil liberties** in the United States. Civil liberties, such as freedom of speech and protection from unreasonable searches, help guarantee that citizens have rights which are protected from government interference. However, in other countries, the rise of AI technology has been utilized to crack down on political freedom and civil liberties. For example, it has been reported that in authoritarian countries such as China that artificial intelligence technology has been used to spy on citizens and to monitor their activity. Mareike Ohlberg, a surveillance



Artificial Intelligence technology being utilized on surveillance cameras to monitor street traffic in China, photo by BBC News

[4] AI-Driven Security Operations (SOC) | Fortinet

expert at the German Marshall Fund, warned that artificial intelligence surveillance "is a way of sorting information that makes it easier to track individuals.” Given these incidents, it is clear that artificial intelligence poses some risk towards democracy and civil liberties and this could present a problem to the American public as AI technology continues to advance.

Challenges to personal security

As discussed by Forbes, Artificial Intelligence technologies can be used by cybercriminals to increase the scale and effectiveness of their social engineering cyber-attacks. **Social engineering** in the context of cybersecurity refers to the manipulation of human error to gain access to personal information, private servers, and other valuables. According to Statistia, the average cyber-attack cost the U.S. 9.48 million dollars per attack in 2023 alone.[5] With Artificial Intelligence having the capabilities to increase the frequencies of these attacks, the financial damages and security risk can only grow higher. As a result, this is an issue which will only continue to grow with time unless significant regulatory actions are taken.

Potential Solutions

Updating United States Government Procedures for AI and Cybersecurity

The U.S. Department of Homeland Security (pictured) has taken precautions on AI (dhs.gov)

While Artificial Intelligence and its implications can cause many problems regarding cybersecurity, responsible use of AI technology can help decrease cybersecurity risks. For instance, artificial intelligence can perform the repetitive tasks needed to minimize errors in our cybersecurity systems. In many U.S. government agencies, there have already been steps taken to set **proper rules, procedures, and regulations** for Artificial Intelligence in order to maximize its potential. In November 2023, the U.S. Department of Homeland Security’s (DHS) Cybersecurity and Infrastructure Security Agency (CISA) revealed its inaugural plan to regulate Artificial Intelligence as

[5] Types of AI-enabled cyberattacks 2021 | Statista

supported by the Biden administration.

As stated by CISA director Jen Easterly, “Artificial intelligence holds immense promise in enhancing our nation’s cybersecurity, but as the most powerful technology of our lifetimes, it also presents enormous risks.”[6] The United States Senate could examine these policies taken by various U.S. Government Departments and model potential legislation on those department policies.

Working with private companies to enhance AI regulations

As artificial intelligence has become a more prominent issue in the United States, there has been increasing collaboration between the private sector and government officials to work towards regulating the industry. Many of the country’s prominent tech companies and their CEOs have shared similar concerns that U.S. Senators have surrounding threats posed by AI. However, there remains a lack of common consensus among tech leaders and Senators on how much regulation should be done and what specifically about AI needs to be regulated. Therefore, it may be beneficial for Senators to reapproach and work with private companies to determine a lasting solution to regulate AI.

Taking inspiration from already existing AI policies on the state level

On September 20th, 2023, the Pennsylvania Governor Josh Shapiro signed an **executive order** to establish a framework for responsibly regulating AI and AI technologies in the Commonwealth of Pennsylvania. According to Governor Shapiro, “this new Executive Order will help us responsibly integrate this emerging technology into some of our government operations so we can move at the speed of business and better serve Pennsylvanians.”[7] Pennsylvania is not the only state to have passed legislation and executive orders regarding Artificial Intelligence. In addition, California consulted AI experts before passing AI regulations[8]. The United States Senate could learn from such state-level actions and model a potential resolution on them.

Subcommittee Charge

The United States Senate is tasked with the oversight, regulation, funding, and lawmaking of nearly all aspects of life in the United States. From food safety to military contracts and space exploration, the United States Senate is tasked with ensuring that U.S. policy is aligned to their, and their constitutions, policy preferences. In order to distribute this massive responsibility, the Senate is split into distinct Committees with broad responsibilities, and then subcommittees with more specific jurisdiction. Each of the 100 members of the United States Senate is assigned to one or more committees where the majority of legislative debate, discussion and review occur. For a bill to become a law, it must be approved in its respective committee before being elevated to the Senate floor.

The regulation and investigation of AI is under the jurisdiction of the **Committee on Commerce, Science and Transportation**, and more specifically, the **Subcommittee on Consumer Protection, Product Safety and Data Security**. The subcommittee has a number of policy avenues to explore in relation to the

[6] CISA turns 5 and looks to the future - Nextgov/FCW
[7] Governor Josh Shapiro (pa.gov)
[8] Governor Newsom Signs Executive Order to Prepare California for the Progress of Artificial Intelligence | California Governor

regulation and oversight of AI and Cybersecurity. Committee members can focus on legislative proposals, regulation utilized by private companies, or investigating the current use of AI algorithms among other topics.

Expert Witnesses will provide opening testimony for the committee, and then will be available for questioning from the Senators. Through the testimony and questioning of expert witnesses, along with speeches and debate between Senators, the committee is charged with crafting a policy proposal aimed at solving persistent issues plaguing AI and Cyber Security regulations.

Questions to Consider

1. What are the four key security risks that AI impacts cyber security? How does each one affect cybersecurity and the public?

2. In what ways has AI technology benefited the general public?

3. What AI tools currently used to prevent cyber-attacks and cybercrimes do you feel is most at risk? Why?

4. What are the implications that AI may affect civil liberties in the United States? Use examples

5. What do you believe poses the biggest challenge to AI regulation in terms of cyber security?

Glossary of Terms

Term	Description
Cybersecurity	the state of being protected against the criminal or unauthorized use of electronic data, or the measures taken to achieve this:
Artificial Intelligence	the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and language translation.
ChatGPT	An AI-powered service that allows for people to generate paragraphs and writing based on prompts given
Deepfake	an image or recording that has been convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said
AI-driven malware	AI-supported computer viruses which can infect devices even faster, become larger to detect, and target more people than ever before
Vulnerable applications	Software and machines which are not updated to deal with AI and thus especially vulnerable to cyber attacks
Expanded attack surface	the areas of technology in which artificial intelligence malware is able to attack, such as cloud-data systems across multiple devices.
Constant evolution	the constantly changing nature of artificial intelligence
Quantum computing	computing that makes use of the quantum states of subatomic particles to store information.

Helpful Resources

- **The Rise of AI in Cybersecurity | Insight**
  This infographic includes a visual map with benefits and risks of AI technology.

- ***'Watch out': Senate Intelligence chair cautions on AI 'deep fakes' ahead of 2024 election (msn.com)***
  A helpful news article detailing how AI's potential could impact the Senate and other United States elections.

- **What's in the US 'AI Bill of Rights' - and what isn't | World Economic Forum (weforum.org)**
  This World Economic Forum helps highlight the policy and regulatory goals of the Biden Administration's 'AI Bill of Rights' and could be a useful reference point when determining the Senate's course of action.

- **12 Risks and Dangers of Artificial Intelligence (AI) | Built In**
  This article provides meaningful insight into AI and potential risks associated with it.

The Advancement of Civics Education Youth Initiative is made possible by

Connelly
Foundation