AI FOUNDATION MODELS AND NATIONAL SECURITY: A CAREFUL BALANCE

Major Theodore H. Massey III*

* *Judge Advocate in the United States Marine Corps. The views expressed are those of the author and do not reflect the official policy or position of the United States Marine Corps, Department of Defense, or the US Government.*

INTRODUCTION

We are entering an era of technological innovation characterized by Artificial Intelligence ("AI") and machine learning ("ML") models, leading to a "new industrial era" with potentially huge economic impacts.[1] Accompanying this new era of AI industrial revolution will be the rise of AI foundation models, where deep learning neural networks are "trained on a broad spectrum of generalized and unlabeled data," allowing AI to "perform[] a wide variety of general tasks like understanding language, generating text and images, and conversing in natural language."[2] Foundation models are the "third wave"[3] of AI evolution and produce new risks.

[1] *See* OFF. OF THE DIR. NAT'L INTEL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 30 (2024), https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf (illustrating the rising importance of AI as it relates to the national security of the United States).
[2] *What Are Foundational Models?*, AMAZON WEB SERVS., https://aws.amazon.com/what-is/foundation-models/ (last visited Apr. 12, 2024).
[3] NAT'L SCI. & TECH. COUNCIL, THE NATIONAL ARTIFICIAL INTELLIGENCE RESEARCH AND DEVELOPMENT STRATEGIC PLAN 14 (2016) [hereinafter DSP 2016], https://www.nitrd.gov/pubs/national_ai_rd_strategic_plan.pdf.

While many say AI is "an under-regulated phenomenon"[4] and "there is no comprehensive federal legislation or regulations in the US that . . . specifically prohibit or restrict [its] use,"[5] this is not entirely accurate. The U.S. has enacted broad regulation in the last six years to prohibit or restrict state and non-state actors' AI use. These efforts to mitigate the national security risks associated with foreign adversaries using advanced AI systems are commendable, but the rise of AI foundation models has introduced new risks that the U.S. is not yet mitigating.

This Article addresses the national security risks associated with the advancement in AI software and algorithms, what the U.S. is doing to mitigate these risks, and where the U.S. needs to head to mitigate future risk as AI foundation models become the norm. Part I overviews AI's history and component parts and explains how advances in computing, data, and algorithms have brought us to the cusp of an AI revolution. Part I introduces the most fundamental risks AI poses to national security by detailing its use cases in intelligence activities; influence operations; CBRN and biosecurity; cybersecurity, to include critical infrastructure; military applications; and new authoritarian challenges to the global geopolitical landscape.

Part II then turns to U.S. mitigation efforts via the President's sweeping powers to control foreign access to AI foundation models through inbound and outbound investments. This Article details mitigation under the International Emergency Economic Powers Act ("IEEPA"),[6] the Foreign Investment Risk Review Modernization Act ("FIRRMA"),[7] and the Export Control Reform Act ("ECRA").[8] It also addresses actions possible under other Executive Orders ("EO"), laws, and regulations that originate from Congress's Commerce Clause[9] and

[4] Mark Findlay & Jolyon Ford, *Regulatory Insights on Artificial Intelligence: Research for Policy*, *in* REGULATORY INSIGHTS ON ARTIFICIAL INTELLIGENCE: RESEARCH FOR POLICY 1,1 (Edward Elgar Pub., 2022).
[5] *AI Watch: Global Regulatory Tracker - United States*, WHITE & CASE: INSIGHT (Mar. 31, 2025), https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states.
[6] *See* International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1710.
[7] *See* Foreign Investment Risk Review Modernization Act, 50 U.S.C. § 4565.
[8] *See* Export Control Reform Act, 50 U.S.C. §§ 4801, 4811–4852.
[9] *See* U.S. CONST. art. I, § 8, cl. 3.

the President's Treaty Clause[10] in the Constitution. These sweeping powers enable the U.S. to restrict foreign investment in U.S.-based AI companies and the export of AI systems to outside the U.S.

While the U.S. has seen some success regulating the hardware and data needed for AI, directly regulating AI algorithms and software has posed challenges. After all, the U.S. now dominates the AI industry largely because the unregulated Open Source culture of the last forty years provided a competitive advantage. Because using open-source software and code does not require a transaction, it lowers barriers to innovation and speeds technological development. But the absence of transactions circumvents inbound and outbound investment prohibitions the U.S. might place on AI software. In view of this, Part III focuses on how the U.S. could improve the current inbound and outbound investment legal framework to mitigate the risks associated with open-source AI foundation models that are currently unregulated.

I. WHAT IS ARTIFICIAL INTELLIGENCE?

AI refers to computational technologies that mimic aspects of human cognition to sense, learn, reason, and act. This section explains the core components that enabled AI's emergence—computing power, data, and algorithms—and sets the groundwork for understanding the evolution of AI that has led to the rise of AI foundation models.

A. *The Three Components of Artificial Intelligence: Computing, Data, and Algorithms*

AI can be defined as a "set of computational technologies that are inspired by—but typically operate quite differently from—the ways people use their nervous systems and bodies to sense, learn, reason, and take action."[11] The advancement of AI is attributed to its

[10] *See* U.S. CONST. art. II, § 2.

[11] PETER STONE ET AL., STANDING COMM. OF THE ONE HUNDRED YEAR STUDY OF A.I, ARTIFICIAL INTELLIGENCE AND LIFE IN 2030: ONE HUNDRED YEAR STUDY ON ARTIFICIAL INTELLIGENCE 4 (Stanford Univ. 2016), https://ai100.stanford.edu/sites/g/files/sbiybj18871/files/media/file/ai100report10032

three essential components—computing power, data, and algorithms—which have enabled the "AI revolution"[12] to flourish.

Computing power is the first component of an AI system.[13] While there is no widely agreed upon definition of computing power it can generally be defined as the processing speed of a computer.[14] In 1965 Dr. Gordon E. Moore wrote an article titled "Cramming More Components onto Integrated Circuits."[15] This article helped coin the phrase "Moore's Law,"[16] which predicts that computing power "will double every eighteen months" as nanotechnology allows more transistors and circuits to operate in smaller and smaller places.[17] While there are concerns that Moore's Law may be running up against the laws of physics,[18] the ability to package computing power in

016fnl_singles.pdf. AI is also defined by Congress under 15 U.S.C. § 9401(3): "the term "artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. Artificial intelligence systems use machine and human-based inputs to (A) perceive real and virtual environments; (B) abstract such perceptions into models through analysis in an automated manner; and (C) use model inference to formulate options for information or action." 15 U.S.C. § 9401(3).

[12] *See* ERIC SCHMIDT ET AL., NAT'L SEC. COMM'N ON A. I., FINAL REPORT 19, 26 (2021) [hereinafter NSCAI REPORT], https://sitic.org/wordpress/wp-content/uploads/Final-Report-National-Security-Commission-on-Artificial-Intelligence.pdf.

[13] Computing power is used as a metric of measurement within this paper.

[14] *See* Aadya Gupta & Adarsh Ranjan, *A Primer on Compute*, CARNEGIE ENDOWMENT FOR INT'L PEACE (Apr. 30, 2024), https://carnegieendowment.org/posts/2024/04/a-primer-on-compute?lang=en ("There is no widely agreed upon definition of compute. The term can be used interchangeably to refer to a metric of measurement, hardware, or a stack. *Compute as a metric of measurement* refers to the number of floating-point operations per second (FLOPS or flops) or calculations that a processor can do in one second. The processing speed of computers is measured in petaflops, which are equal to a thousand trillion flops (1 petaflop = 10^{15} flops).").

[15] *See generally* Gordon E. Moore, *Cramming More Components onto Integrated Circuits*, 38 ELECTRONICS 114 (1965).

[16] *See Gordon Moore Promulgates "Moore's Law*," JEREMY NORMAN'S HISTORYOFINFORMATION.COM, https://historyofinformation.com/detail.php?id=835 (last visited Apr. 13, 2025).

[17] *See* JAMES E. BAKER, THE CENTAUR'S DILEMMA 13 (Brookings Inst. Press 2021); *see also* Moore, *supra* note 15.

[18] *See* Anhan Liu et al., *The Roadmap of 2D Materials and Devices Toward Chips*, 16 NANO-MICRO LETTERS 119, 119 (2024) (discussing how nano-technology and the laws of physics are reaching its limits as it relates to Moore's Law).

progressively smaller spaces has led to supercomputers such as Stargate, OpenAI and Microsoft's supercomputer that runs ChatGPT.[19] Computing power drove the first wave of AI.

Data is the second component of an AI system, and the explosion of data and the Internet of Things is what drove the second wave of AI.[20] "Data is growing at an exponential rate, with 90% of the world's data [created] . . . in the last two years alone."[21] AI and ML "are highly dependent on access to consistent and formatted data" and data conditioning comprises approximately 80 percent of the time in developing a new AI application.[22] In order for AI to learn, it needs to train, and in order for it to train, it needs data.[23]

---

[19] *See* Erin Snodgrass, *Microsoft and OpenAI Plan to Build a $100 Billion Supercomputer to Power Artificial Intelligence: Report*, Bus. Insider (Mar. 30, 2024), https://www.businessinsider.com/microsoft-openai-plan-100-billion-supercomputer-stargate-artificial-intelligence-report-2024-3; *see also* Zachary Cavanell, *What Runs ChatGPT? Inside Microsoft's AI Supercomputer | Featuring Mark Russinovich*, MICROSOFT: MICROSOFT MECHANICS BLOG (May 24, 2023), https://techcommunity.microsoft.com/t5/microsoft-mechanics-blog/what-runs-chatgpt-inside-microsoft-s-ai-supercomputer-featuring/ba-p/3830281.

[20] *See* Lee-Lean Shu, *The Evolution of AI Progression from the Internet of Things,* Forbes (Feb. 10, 2025, 8:00 AM), https://www.forbes.com/councils/forbestechcouncil/2025/02/10/the-evolution-of-ai-progression-from-the-internet-of-things/; *see also* BAKER, *supra* note 17, at 13.

[21] *Exponential Data Growth,* REDSTOR, https://www.redstor.com/uk/use-cases/exponential-data-growth/ (last visited Apr. 13, 2025).

[22] VIJAY GADEPALLY ET. AL, AI ENABLING TECHNOLOGIES: A SURVEY 5 (Mass. Inst. Tech. 2019).

[23] Tesla's Autopilot is a great example of improving AI through training data. *See* Mark Harris, *Tesla's Autopilot Depends on a Deluge of Data: But Can a Fire-Hose Approach Solve Self-Driving's Biggest Problems?*, IEEE SPECTRUM (Aug. 4, 2022), https://spectrum.ieee.org/tesla-autopilot-data-deluge. "Most companies working on automated driving rely on a small fleet of highly instrumented test vehicles" to obtain its data. *Id.* This data is then used to train the AI model on what to do if a car approaches a stop sign, a child runs into the street, or an impending accident is about to happen. *See generally How Tesla Uses and Improves Its AI for Autonomous Driving*, AIWIRE (Mar. 8, 2023), https://www.aiwire.net/2023/03/08/how-tesla-uses-and-improves-its-ai-for-autonomous-driving/. In 2022, self-driving cars were considered one or two magnitudes below a human driver when it came to safety. *See* Mark MacCarthy, *Commentary: The Evolving Safety and Policy Challenges of Self-Driving Cars*, BROOKINGS (July 31, 2024), https://www.brookings.edu/articles/the-evolving-safety-and-policy-challenges-of-self-driving-cars/. However, in an article published in July 2024, Tesla Autopilot was considered "eight times safer than a

The third component of AI systems is algorithms. AI algorithmic and software innovations are the product of more than four decades of an open and collaborative coding culture called Open Source.[24] Indeed, many modern AI models, including OpenAI (which is not open to the public), were built on algorithmic models that were originally Open Source.[25] Open Source consists of free and open-source software, which is typically available online where others can use it for personal or public benefit.[26] Open Source "harnesses the power of distributed peer review and transparency" allowing for "higher quality, better reliability, greater flexibility, and lower costs."[27] In fact, it has become both a software development and a business model because it allows developers across the world to collaborate, reduce costs, innovate, and boost economic growth.[28] Some consider

human." *See* Brian Wang, *Tesla Autopilot, FSD and Robotaxi Safety Versus Human*, NEXTBIG FUTURE (July 8, 2024), https://www.nextbigfuture.com/2024/07/tesla-autopilot-fsd-and-robotaxi-safety-versus-human.html. Tesla was able to drastically improve its Autopilot over a few years because their customers are "training the network all the time" and "[w]hether Autopilot's on or off, the network is being trained." *See* Harris, *supra* note 23.

[24] *See generally* OPEN SOURCE LAW, POLICY AND PRACTICE (Amanda Brock, ed., Oxford Univ. Press, 2nd ed. 2022) (discussing various aspects of Open Source as it relates to, *inter alia*, the law, business practices, societal use and viewpoints, and policy).

[25] *See* Steven Vaughan-Nichols, *Open Source is Actually the Cradle of Artificial Intelligence. Here's Why*, ZDNET (Oct. 9, 2023, 11:26 AM), https://www.zdnet.com/article/why-open-source-is-the-cradle-of-artificial-intelligence/.

[26] Stephanie Susnjara & Ian Smalley, *What Is Open Source Software?*, IBM (Feb. 5, 2025), https://www.ibm.com/think/topics/open-source.

[27] *About the Open Source Initiative*, OPEN SOURCE INITIATIVE, https://opensource.org/about (last visited Sept. 15, 2024).

[28] *See id.*; Sid Sijbrandij, *How Open Source Became the Default Business Model for Software,* Forbes (July 16, 2018, 8:00 AM), https://www.forbes.com/councils/forbestechcouncil/2025/04/16/not-all-ai-agents-win-heres-how-to-pick-high-roi-bets/. *See generally* Manuel Hoffman et al., *The Value of Open Source Software* (Harv. Bus. Sch., Working Paper No. 24-038, 2024), https://www.hbs.edu/ris/Publication%20Files/24-038_51f8444f-502c-4139-8bf2-56eb4b65c58a.pdf (discussing the value of an open-sourced business model and on the economy).

it "the single-most impactful driver of innovation in the world today."[29]

B. *The Evolution of AI*

While AI concepts can be found dating back all the way to Greek mythology,[30] modern AI is attributed to the English computer scientist Alan Turing, who proposed the Turing Test in 1950.[31] The Turing Test was an experiment to test the capacity of a computer to imitate, or "to think and act like, a human."[32] Shortly after Turing proposed his test, Professor John McCarthy coined the term "artificial intelligence."[33] Now, unbeknownst to most Americans, we use AI multiple times a day, including in our personal and professional lives and our interactions with the federal government. Your smart phone, for example, uses AI algorithms for things like facial and voice recognition, GPS applications, and virtual assistants.[34] Companies use AI algorithms to produce things like buying and entertainment recommendations and summaries of web searches and reviews.[35] With

[29] Keith Bergelt, *Foreword to* OPEN SOURCE LAW, POLICY AND PRACTICE, *supra* note 24, at xvii. More recent studies conducted on open-source generative AI have shown Open Source advances research; makes GenAI more affordable, flexible, and customizable; empowers developers and fosters innovation; enables technological innovation for safety; and helps democratize AI development. *See* OPEN SOURCE LAW, POLICY AND PRACTICE, *supra* note 24 at 31; *see also See* Marcello Mariani & Yogesh K. Dwivedi, *Generative Artificial Intelligence in Innovation Management: A Preview of Future Research Developments*, J. OF BUS. RSCH., Feb. 14, 2024, at 1, 5-14.

[30] *See generally* ADRIENNE MAYOR, GODS AND ROBOTS: MYTHS, MACHINES, AND ANCIENT DREAMS OF TECHNOLOGY 1-6 (Princeton Univ. Press 2018) (discussing how ideas of artificial life were explored in Greek mythology).

[31] *See* BAKER, *supra* note 17, at 11.

[32] *Id.*

[33] *Id.*

[34] *See* GPUnet, *AI in Mobiles: Enhancing User Experience to the Next Level*, MEDIUM (Mar. 17, 2024), https://medium.com/@GPUnet/ai-in-mobiles-enhancing-user-experience-to-the-next-level-1b1806987601; Chris Phillips, *New Maps Updates: Immersive View for Routes and Other AI Features*, GOOGLE: THE KEYWORD (Oct. 26, 2023), https://blog.google/products/maps/google-maps-october-2023-update/.

[35] *See* Terry Tolentino, *Top 17 AI Trends and Applications in Media & Entertainment for 2025*, MARKETING SCOOP (Mar. 17, 2024), https://www.marketingscoop.com/ai/ai-media/; Michael Liedtke, *Google Unleashes AI in Search, Raising Hopes for Better Results and Fears About Less Web Traffic*, ASSOCIATED PRESS (May 15, 2024, 1:43 PM) https://apnews.com/article/google-search-ai-overviews-internet-traffic-ebb6bbbde17ed29a5f7b630d9e5e285b. AI

applications ranging from bank fraud protection to automated email spam filters to targeted ads, AI has become ubiquitous.[36]

C. *AI's Transformational Waves*

AI was little more than science fiction until the turn of the century when the transformative "waves" began. The first transformative wave hit in 1997 when advances in computational capacity enabled IBM's Deep Blue supercomputer to beat Gary Kasparov, the then reigning World Chess Champion.[37] This first wave of AI used computational capacity as a "blunt weapon" to beat Mr. Kasparov by weighing every possible move in response to each of Mr. Kasparov's actual and potential moves in real time.[38]

Advancements in software and algorithmic reasoning and access to big data catalyzed the second wave. The second wave "is characterized by the ascent of machine learning" where "significant[] . . . amounts of digital data" and "improved learning techniques" led to substantial advancements in AI.[39] The subfield of AI known as

models that utilize ML to create entirely new synthetic information are known as Generative AI ("GenAI"). *See* JOSH A. GOLDSTEIN ET AL., GENERATIVE LANGUAGE MODELS AND AUTOMATED INFLUENCE OPERATIONS: EMERGING THREATS AND POTENTIAL MITIGATIONS 15 (2023) (Generative AI "consist[s] of large artificial neural networks and are "trained" via a trial-and-error process over mountains of data. The neural networks are rewarded when their algorithmically generated words or images resemble the next word in a text document or a face from an image dataset. The hope is that after many rounds of trial and error, the systems will have picked up general features of the data they are trained on. After training, these generative models can be repurposed to generate entirely new synthetic artifacts.").

[36] *See generally AI in the Banking Sector: How Fraud Detection with AI Is Making Banking Safer*, INFOSYS BPM: BPM ANALYTICS, https://www.infosysbpm.com/blogs/bpm-analytics/fraud-detection-with-ai-in-banking-sector.html (last visited Apr. 19, 2025) [hereinafter *AI in the Banking Sector*]; David Emelianov, *Advanced Spam Filtering AI*, TRIMBOX (Nov. 21, 2023), https://www.trimbox.io/blog/advanced-spam-filtering-ai; Rocco Baldassarre, *How AI Is Revolutionizing Digital Advertising in 2024*, FORBES (Apr. 9, 2024, 7:30 AM), https://www.forbes.com/councils/forbesagencycouncil/2024/04/09/how-ai-is-revolutionizing-digital-advertising-in-2024/.

[37] Baker, *supra* note 17, at 2517.

[38] *See id.* (noting Deep Blue a year later went on to play and defeat Mr. Ken Jennings, the reigning *Jeopardy!* winner at that time).

[39] DSP 2016, *supra* note 3, at 12.

machine learning ("ML"), allows a computer using algorithms, calculation, and data to learn to better perform programmed tasks and thus optimize function.[40] It is no coincidence that scientists and engineers in this space often have PhDs in cognitive neuroscience.[41] They are seeking to replicate the way that the human brain learns for AI.[42] Neural networks, an ML architecture, models the interconnectedness of the human brain.[43] Many AI foundation models use deep learning, which involves layered neural networks that process an extensive amount of data by determining the relative "weight" of each link in the network.[44] Deep learning is not necessarily better than other ML. While it can facilitate more complex tasks, it requires much more training data than other ML forms.[45] This ML-driven second wave has led to advancements in the AI that we use today on our smartphone, personal computers, and daily life.[46]

---

[40] Sara Brown, *Machine Learning, Explained*, MASS. INST. OF TECH. SLOAN SCH. OF MGMT. (Apr. 21, 2021), https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained. There are three basic subcategories of ML: (1) supervised learning uses labeled datasets to train AI, (2) unsupervised learning requires the algorithm to find patterns in unlabeled datasets, and (3) reinforcement learning uses a reward system to improve algorithmic trial and error.

[41] *See Neuroscience + Artificial Intelligence = NeuroAI: The New Field of NeuroAI Is Building Momentum at Columbia University,* COLUM., ZUCKERMAN INST. (Aug. 27, 2024), https://zuckermaninstitute.columbia.edu/neuroscience-artificial-intelligence-neuroai. (stating that the goal of NeuroAI is to "build AI systems that are as versatile and efficient as our brains"). Dr. Demis Hassabis, who has a PhD in cognitive neuroscience, is known as the "superhero of artificial intelligence." Lakshmi Varanasi & Sam Shead, *Who Is Demis Hassabis, the DeepMind Founder Who Won the Nobel Prize in Chemistry?*, BUS. INSIDER (Oct. 13, 2024), https://www.businessinsider.com/who-is-demis-hassabis-deepmind-founder-ai-google-nobel-prize-2024-10.

[42] *See id.*

[43] *What is a Neural Network*?, AMAZON WEB SERVS., https://aws.amazon.com/what-is/neural-network/ (last visited Apr. 19, 2025). Each cell in the neural network processes an input and produces an output that is sent on to additional artificial neurons, similar to how neurons and synapses process information. *See id.*

[44] *What's the Difference Between Machine Learning and Deep Learning,* AMAZON WEB SERVS., https://aws.amazon.com/compare/the-difference-between-machine-learning-and-deep-learning/ (last visited Apr. 19, 2025).

[45] *See id.*

[46] *See* THE ONE HUNDRED YEAR STUDY ON A.I. (AI100), 2021 STUDY PANEL REPORT: GATHERING STRENGTH, GATHERING STORMS 12-18 (2021); *see, e.g., AI in the Banking Sector*, *supra* note 36.

Now, AI is on the cusp of the third wave, where "AI [will] now serve[] . . . as a foundational tool with [a] myriad [of] applications across diverse domains."[47] If the second wave can be identified as statistical learning, the third wave is contextual adaptation[48] where AI can both generate an answer, as with ChatGPT,[49] *and* explain how it came to its answer.[50] Thus, this new era will move AI from a "rules-based expert system" to a system capable of generating "new multi-modal human-like content" with explainability.[51] AI development is not expected to slow, so AI will "pose a transformative relationship to all industries" in the coming years.[52]

D. *Foundation Models and the Future of AI*

While we are not yet at the third wave of AI where a single AI algorithm can serve as a foundation for various applications with explainability, foundation models[53] have launched us into the

[47] *How the 'Third Wave' of AI Is Transforming Government Operations*, FEDSCOOP (May 23, 2024), https://fedscoop.com/how-the-third-wave-of-ai-is-transforming-government-operations/ (quoting Dr. William Chappell, Vice President and Chief Technology Officer of Microsoft's Strategic Missions and Technologies Division).
[48] *See* Roey Tzezana, *Artificial Intelligence Tech Will Arrive in Three Waves*, FUTURISM: ARTIFICIAL INTELLIGENCE (May 13, 2017, 12:43 PM), https://futurism.com/artificial-intelligence-tech-will-arrive-in-three-waves.
[49] *See* Igor Mezic, *The Cybersecurity Implications of ChatGPT and Third-Wave Generative AI Models*, FORBES (May 23, 2023, 8:15 AM), https://www.forbes.com/councils/forbestechcouncil/2023/05/23/the-cybersecurity-implications-of-chatgpt-and-third-wave-generative-ai-models (noting that although ChatGPT is generative, it is still considered within the second wave).
[50] Matt Turek, Deputy Dir., Info. Innovation Off., Def. Advanced Rsch. Projects Agency, The DARPA Perspective on AI and Autonomy at the DOD (Mar. 27, 2024), https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-03/240328_Turek_DARPA_Perspective.pdf?VersionId=JAAMqItQD9Cr2ChofrR_nesqnWh73uWJ.
[51] *The Fourth AI Inflection*, FTI CONSULTING (Jun. 12, 2023), https://www.fticonsulting.com/insights/articles/fourth-ai-inflection; *see id.*
[52] *See IP and Strategic Competition with China: Part III – IP Theft, Cybersecurity, and AI: Hearing Before the H. Subcomm. on Cts., Intell. Prop., and the Internet*, 118th Cong. 2 (2023) [hereinafter *House Hearing on AI*].
[53] Foundation models inherently are a form of GenAI, which initially gained attention through Large Language Models (LLMs), such as ChatGPT, LLaMa, or BARD. *See* GOLDSTEIN ET AL., *supra* note 35, at 3517; *see* also *What is LLM (Large Language Model)?,* AMAZON WEB SERVS. https://aws.amazon.com/what-is/large-language-model/ (last visited Oct. 21, 2024) ("Large language models, also known as

transition era. "AI is undergoing a paradigm shift with the rise of [foundation] models . . . trained on broad data . . . that can be adapted to a wide range of downstream tasks."[54] By way of analogy, think of an AI foundation model as a lump of clay. You can mold the clay into a bowl or a cup to be used in kitchenware. You can turn clay into a pot or a vase to accompany your furniture. Clay can also be used in construction to build a house, or in beauty products and pharmaceuticals. While much more complex, an AI foundation model can be "molded" to seemingly any space: it can provide customer support for companies, language translation, content and image classification, or contribute to robotics, healthcare, and much more.[55] "It's faster and cheaper for data scientists to use pre-trained F[oundation] M[odel]s to develop new ML applications rather than train unique ML models from the ground up."[56]

Current AI, including foundational models, is considered "narrow" AI: AI that "perform[s] a single task very well."[57] Narrow AI systems are highly effective at performing specific, well-defined tasks, but lack the ability to generalize their knowledge or apply their skills beyond their original purpose compared to the broader adaptability of human intelligence.[58] "Artificial General Intelligence"[59] ("AGI") is a

LLMs, are very large deep learning models that are pre-trained on vast amounts of data. The underlying transformer is a set of neural networks that consist of an encoder and a decoder with self-attention capabilities. The encoder and decoder extract meanings from a sequence of text and understand the relationships between words and phrases in it.").

[54] RISHI BOMMASANI ET AL., ON THE OPPORTUNITIES AND RISKS OF FOUNDATIONAL MODELS 1 (2022).

[55] *See What Are Foundational Models?, supra* note 2.

[56] *Id.*

[57] Lisa Lacy, *There's AI, and Then There's AGI: What You Need to Know to Tell the Difference*, CNET (Feb. 17, 2020, 5:00 AM), https://www.cnet.com/tech/theres-ai-and-then-theres-agi-what-you-need-to-know-to-tell-the-difference/.

[58] *Narrow AI*, INTERACTION DESIGN FOUND., https://www.interaction-design.org/literature/topics/narrow-ai (last visited Apr. 19, 2025).

[59] For a comprehensive definition of Artificial General Intelligence, see *What is AGI (Artificial General Intelligence)?*, AMAZON WEB SERVS., https://aws.amazon.com/what-is/artificial-general-intelligence/ (last visited Apr. 19, 2025) ("Artificial general intelligence (AGI) is a field of theoretical AI research that attempts to create software with human-like intelligence and the ability to self-teach. The aim is for the software to be able to perform tasks that it is not necessarily trained or developed for. Current artificial intelligence (AI) technologies all function

field of theoretical AI research that attempts to create software with human-like intelligence and the ability to self-teach. The aim is for the software to be able to perform tasks that it is not necessarily trained or developed for.[60] Some predict that AGI is "just a few years" away.[61] "Artificial Super Intelligence" ("ASI"), AI that is smarter than humans, can in theory complete tasks better than a human can.[62] The predictions of AGI and ASI are illustrative because they show that "AI is becoming more powerful and radically cheaper by the month–what was computationally impossible, or would cost tens of millions of dollars a few years ago, is now widespread."[63] These changes are coming "faster than we can adequately prepare for" as "the most powerful" and emerging technology "is open-sourced months after creation," leading to an amplification of cutting-edge technology.[64] Any regulation of AI must consider these predicted changes, as proposed regulation in Congress may be ineffective and possibly harmful by the time the President signs it into law.

E. *Foundation Models and National Security Risks*

Foundation Models are poised to fundamentally change and augment the risks both state and non-state actors pose to U.S. national security. Because of AI's rapid evolution, new risks continually emerge

within a set of pre-determined parameters. For example, AI models trained in image recognition and generation cannot build websites. AGI is a theoretical pursuit to develop AI systems that possess autonomous self-control, a reasonable degree of self-understanding, and the ability to learn new skills. It can solve complex problems in settings and contexts that were not taught to it at the time of its creation. AGI with human abilities remains a theoretical concept and research goal.").

[60] *See What Are Foundation Models?, supra* note 2.

[61] Tristan Bove, *CEO of Google's DeepMind Says We Could be 'Just a Few Years' from A.I. That Has Human-Level Intelligence*, FORTUNE (May 3, 2023, 5:23 PM), https://fortune.com/2023/05/03/google-deepmind-ceo-agi-artificial-intelligence/.

[62] *See* Tim Mucci & Cole Stryker, *What is Artificial Superintelligence*, IBM (Dec. 18, 2023), https://www.ibm.com/think/topics/artificial-superintelligence. One survey showed that the average of predictions made by a sample of 2,778 experts in AI suggested a 50% chance that ASI would occur by 2047. *See* Will Henshall, *When Might AI Outsmart Us? It Depends Who You Ask*, TIME (Jan. 19, 2024, 1:44 PM), https://time.com/6556168/when-ai-outsmart-humans/.

[63] Mustafa Suleyman, *How the AI Revolution Will Reshape the World,* TIME (Sept. 1, 2023, 7:05 AM), https://time.com/6310115/ai-revolution-reshape-the-world/.

[64] *See id.*

as actors identify new applications. The private sector and federal government are still in the early stages of identifying and mitigating the multivarious risks associated with bad actors using AI foundation models. Open AI founders, for example, have alluded to the inherent risks of AI, raising concerns before Congress about its potential for social manipulation, cyber-attacks, and harm to children.[65] The federal government has also begun taking measures to mitigate risks associated with AI foundation models.[66] Measures include the now-revoked EO 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,"[67] which required the National Telecommunications and Information Administration ("NTIA") to

[65] *See Oversight of A.I.: Rules for Artificial Intelligence*: *Hearing Before the Subcomm. on Priv., Tech., and the L. of the S. Comm. on the Judiciary,* 118th Cong. 17-40 (2023); TOBY SHEVLANE ET AL., MODEL EVALUATION FOR EXTREME RISKS (DeepMind, 2023) (AI poses "extreme risks, such as offensive cyber capabilities or strong manipulation skills.").

[66] For a discussion of considerations by Congress regarding these measures, see *generally The Dawn of Artificial Intelligence*: *Hearing Before the Subcomm. on Space, Science, and Competitiveness of the S. Comm. on Commerce, Science, and Transportation*, 114th Cong. 28 (2016) ("With AI, we should consider safety, security, and ethics as early as possible, and start baking these into the technologies . . . that are being created today.").

[67] *See* Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023). On Jan. 20, 2025, President Trump revoked Executive Order 14,110 along with 77 other EOs and memoranda under Exec. Order 14,148, stating that these 78 actions were "unpopular, inflationary, illegal, and [involved] radical practices." *See* Exec. Order No. 14,148, 90 Fed. Reg. 8,237, 8,237 (Jan. 20, 2025). On Jan. 23,2025 President Trump published Exec. Order 14,179 requiring a working group under Section 4 to produce an AI policy for the United States to "enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security." *See* Exec. Order 14,179, 90 Fed. Reg. 8,741, 8,741 (Jan. 23, 2025). With the revocation of EO 14,110 the United States is currently evaluating policies that were established under this EO. Also of note regarding AI risk mitigation, the Biden Administration released their AI National Security Memorandum on October 24, 2024, directing the use of AI for various national security purposes within the federal government. *See generally* THE WHITE HOUSE, MEMORANDUM ON ADVANCING THE UNITED STATES' LEADERSHIP IN ARTIFICIAL INTELLIGENCE; HARNESSING ARTIFICIAL INTELLIGENCE TO FULFILL NATIONAL SECURITY OBJECTIVES; AND FOSTERING THE SAFETY, SECURITY, AND TRUSTWORTHINESS OF ARTIFICIAL INTELLIGENCE (2024), https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/.

publish a report on dual-use foundation models.[68] NTIA found that companies using advanced AI models fell on a sliding scale regarding availability of their models and model weights,[69] ranging from broad public access to access limited by information or party to no public access.[70] The report then evaluated the benefits and risks associated with these models being public and recommended circumstances in which the U.S. government should restrict broad availability of dual-use foundation models.[71] NTIA acknowledged that widely available models could (1) "bolster cyber deterrence and defense mechanisms," (2) "propel safety research and help identify safety and security vulnerabilities on future and existing models," and (3) "facilitate transparency and accountability through third party auditing mechanisms."[72] But it also noted that these models can lower the barriers to entry for nonexperts to access, design, and develop chemical, biological, radiological, and nuclear ("CBRN") weapons and facilitate offensive cyber operations by automating vulnerable discovery and exploitation.[73] The report emphasizes how each benefit has a dual risk.[74] For example, the ability of widely available models to "promote democratic values in the global AI ecosystem" poses "disinformation [and] misinformation" risks and the risk of "accelerat[ing] dual-use AI innovation in countries of concern."[75]

[68] *See* NAT'L TELECOMM. & INFO. ADMIN., DUAL-USE FOUNDATION MODELS WITH WIDELY AVAILABLE MODEL WEIGHTS (2024) [hereinafter NTIA REPORT], https://www.ntia.gov/programs-and-initiatives/artificial-intelligence/open-model-weights-report (to view the report, scroll down the page and select "Download Report").

[69] *See id.* at 10-11. *See generally* Alisdair Broshar, *What Are LLMs? An Intro into AI, Models, Tokens, Parameters, Weights, Quantization and More*, KOYEB (Apr. 25, 2024), https://www.koyeb.com/blog/what-are-large-language-models ("Weights are a subset of the parameters in a model that represent the strength of connections between variables. During training, the model adjusts these weights to optimize its performance. Weights determine how input tokens are transformed as they pass through the layers of the model.").

[70] NTIA REPORT, *supra* note 68, at 2.

[71] *Id.* at 2-3.

[72] *Id.* at 17.

[73] *Id.* at 14.

[74] *Id.* at 12-13.

[75] *Id. at* 20-25. For an example of accelerating dual-use AI innovation in countries of concern, see Washington Street Journal Podcasts, *Why the U.S. Says China Is Stealing AI Secrets to Turbocharge Spying*, WALL STREET JOURNAL (Jan. 8, 2024), https://www.wsj.com/podcasts/tech-news-briefing/why-the-us-says-china-is-

Reports have already established that "hackers from China, Iran, North Korea, and Russia are experimenting with . . . [large language models (LLMs)]", allowing hackers to enhance their capabilities "to carry out cyberattacks and produce disinformation at scale."[76]

A real-life example that illustrates the risks associated with AI foundation models is AlphaFold 3. This model, while a boon to modern day science, may carry the most significant risk to society since the creation of the nuclear bomb. The story of AlphaFold 3 starts with its creator, Dr. Demis Hassabis. Nicknamed the "superhero of artificial intelligence," Dr. Hassabis spent four years earning his PhD in cognitive neuroscience from the University College of London where he found inspiration from the human brain in designing new AI algorithms.[77] In 2010, Mr. Hassabis co-founded DeepMind aiming to "solve intelligence."[78] In 2018, DeepMind started its most significant AI system to date: AlphaFold.[79] AlphaFold was created with the goal of predicting "protein folding" within the amino acid sequence of proteins to determine "the shape of proteins by generating a [three-dimensional] model."[80] In 2021 AlphaFold 2 was released, essentially solving the protein folding problem by allowing scientists to have access to over 200 million protein predictions and predicting 98.5 percent of the three-dimensional structures for human proteins in addition to predicting structures in twenty other key organisms.[81]

---

stealing-ai-secrets-to-turbocharge-spying/d236f53a-a0a1-44bc-8f84-9717c71aedb6 (discussing China's theft of trade secrets and intellectual property as it relates to AI).

[76] Elias Groll, *State-Backed Hackers Are Experimenting with OpenAI Models*, CYBERSCOOP (Feb. 14, 2024), https://cyberscoop.com/openai-microsoft-apt-llm/.

[77] Varanasi & Shead, *supra* note 41.

[78] *Id.*

[79] Satishlokhande, *What Is the story of Alphafold?*, MEDIUM (May 30, 2024), https://medium.com/@satishlokhande5674/what-is-the-story-of-alphafold-af2025ca8bec.

[80] Tim Keary, *Google DeepMind's Achievements and Breakthroughs in AI Research*, TECHOPEDIA (Aug. 11, 2023), https://www.techopedia.com/google-deepminds-achievements-and-breakthroughs-in-ai-research; *id.* ("Despite knowing the sequence of amino acids in a protein, predicting its three-dimensional structure has been a significant challenge, commonly referred to as the "protein folding problem.").

[81] Satishlokhande, *supra* note 79; Rob Toews, *AlphaFold Is the Most Important Achievement in AI—Ever*, FORBES (Oct. 3, 2021, 7:34 PM), https://www.forbes.com/sites/robtoews/2021/10/03/alphafold-is-the-most-

In May of 2024, DeepMind announced the release of AlphaFold 3, but restricted access to the algorithmic and computational code underlying it,[82] citing "potentially unsafe applications" after consulting with "an outside biosafety expert."[83] While DeepMind didn't release what risks were associated with a full release, experts have stated that AI-assisted protein design platforms could create biological hazards and toxins, like modifying bacteria to optimize its inherent lethality in humans.[84] Bad actors could use AlphaFold to create biological weapons or the next pandemic, harming rather than advancing society.[85]

The risks associated with AlphaFold are illustrative of just how powerful foundation models can be. This section introduces the most fundamental categories of risk that AI poses to national security and how state and non-state actors pose nuanced risks.

1. National Security Threats

The modern understanding of national security can be summarized as "the safekeeping of the nation as a whole."[86] This broad

important-achievement-in-ai-ever/. The release of AlphaFold has been astronomical in accelerating biological research along with future pharmaceutical discoveries with potential applications in treating diseases such as cancer, Alzheimer's, and many others. *See id.*

[82] *See* Catherine Offord, *Limits on the Access to DeepMind's New Protein Program Trigger Backlash*, SCIENCE (May 15, 2024, 1:55 PM), https://www.science.org/content/article/limits-access-deepmind-s-new-protein-program-trigger-backlash.

[83] Bryce Johnson, *Why AlphaFold 3 Needs to be Open Source*, ASBMBTODAY (July 7, 2024), https://www.asbmb.org/asbmb-today/opinions/070724/why-alphafold3-needs-to-be-open-source.

[84] *See* Philip Hunter, *Security Challenges by AI-Assisted Protein Design*, SCIENCE AND SOCIETY (Mar. 26, 2024), https://www.embopress.org/doi/full/10.1038/s44319-024-00124-7.

[85] *See* STERLING SAWAYA ET AL., THE POTENTIAL FOR DUAL-USE OF PROTEIN-FOLDING PREDICTION 153-66 (United Nations Interregional Crime & Just. Rsch. Inst. 2021), https://unicri.it/sites/default/files/2021-12/21_dual_use.pdf.

[86] Kim. R. Holmes, *What is National Security?*, *in* 2015 INDEX OF U.S. MILITARY STRENGTH 23 (The Heritage Found.), https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf (last visited Apr. 20, 2025).

modern framing includes everything from traditional military and intelligence aspects to "economic security; energy security; environmental security; and even health . . . and food security."[87] Because AI is poised to revolutionize every aspect of national security, it presents innumerable national security risks. Indeed, the "AI revolution will change . . . fundamental elements of national power."[88] With that said, this section focuses on the most fundamental national security risks AI poses to intelligence activities, influence operations, CBRN and biosecurity risks, cybersecurity to include critical infrastructure, military applications, and authoritarian challenges to the global geopolitical landscape.

a. Intelligence Activities

As a counterintelligence tool, AI stands unparalleled—it can help aggregate information and identify patterns in financial, physical, and digital behavior along with identifying anomalies, making "it easier for an adversary to identify a case officer or an asset not careful with his or her own electronic footprint, fingerprint, facial print, or credit trail."[89] AI software or enabled systems would be able to provide the following intelligence tasks:

- Persistent surveillance;
- Image recognition, including facial recognition;
- Link analysis;
- Voice recognition;
- Sorting;
- Aggregation, a.k.a. fusion;
- Political prediction;
- Policy modeling;
- Translation;
- Deviation and anomaly detection; and

[87] *Id*. at 19.
[88] Matthew Daniels & Ben Chang, *National Power After AI*, CTR. FOR SEC. & EMERGING TECH. iv (2021), https://cset.georgetown.edu/wp-content/uploads/CSET_Daniels_report_NATIONALPOWER_JULY2021_V2.pdf.
[89] BAKER, *supra* note 17, at 35.

- Cyber-detection, attribution, and response.[90]

While not directly linked to AI, in 2013 U.S. intelligence started to notice an alarming pattern where CIA personnel would be "rapidly and successfully identified by Chinese intelligence" in Africa and Europe.[91] Ultimately it turned out that intelligence operators in China combed through massive amounts of stolen data to identify and undercover U.S. intelligence officials.[92] With AI-enabled technology, automated systems could do the same work as Chinese intelligence operators at a fraction of the time and cost. AI's capability "to outperform humans in pattern recognition and anomaly detection" makes it the perfect tool for intelligence activities, causing both external and internal national security risks.[93] China is a worthwhile case study because, outside of the U.S., China may be the largest collector of personal information on American citizens. As I have stated in my publication *The Case for a Federal Data Privacy Law from a National Security Perspective*:[94]

[90] *Id.* at 31.
[91] Zach Dorfman, *China Used Stolen Data to Expose CIA Operatives in Africa and Europe*, FOREIGN POL'Y (Dec. 21, 2020, 6:00 AM), https://foreignpolicy.com/2020/12/21/china-stolen-us-data-exposed-cia-operatives-spy-networks/.
[92] *Id.*
[93] BAKER, *supra* note 17, at 30-31.
[94] Theodore H. Massey III, *The Case for a Federal Data Privacy Law from a National Security Perspective - What the U.S. Can Learn from Overseas*, 3 STUDENT J. INFO. PRIV. L. 17 (forthcoming May 2025).

> When considering the aggregated data of the OPM[95] and Microsoft breach, Equifax hack,[96] and bulk data sales[97] obtained by China, one can easily conceptualize the significant amount of data that China has on United States citizens. Used nefariously, this data is a significant competitive advantage for the Chinese, and a significant [external] national security risk for the United States. Once obtained by the Chinese government, there is no way to undo the damage that has been done.

By applying AI to its data troves on Americans, China can enhance its ability to track Americans on the internet and in daily life. AI also makes it easier for China to attack, harass, and surveil[98] those that speak out against the Chinese Community Party and recruit people of interest through its "Thousand Talents Program."[99]

b. Influence Operations

Influence operations are defined as "covert or deceptive efforts to influence the opinions of a target audience."[100] The goal of influence operations is to "(1) persuade[] someone of a particular viewpoint or reinforce[] an existing one, (2) distract[] them from finding or developing other ideas, or (3) distract[] them from carving out space for higher quality thought at all."[101] While influence operations are typical during armed hostilities, there is an alarming rise in peacetime foreign influence operations to spread

---

[95] MAJORITY STAFF OF H. COMM. ON OVERSIGHT AND GOV'T REFORM, 114TH CONG., THE OPM DATA BREACH: HOW THE GOVERNMENT JEOPARDIZED OUR NATIONAL SECURITY FOR MORE THAN A GENERATION (2016), https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf.

[96] Christopher Wray, Dir., Fed. Bureau of Investigation, Hudson Institute Video Event: The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States (July 7, 2020) (transcript available at https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states).

[97] *See generally* Jeff Williams, HOUSE HEARING AIRS CONCERNS ABOUT DATA BROKER PRACTICES (Aspen Publishers, Inc. 2023) (discussing the national security risks associated with the data broker industry in the United States).

[98] BAKER, *supra* note 17, at 30-31.

[99] Wray, *supra* note 96.

[100] GOLDSTEIN ET AL., *supra* note 35, at 9.

[101] *Id.* at 11.

disinformation, misinformation, and propaganda. These operations have evolved from the "art of slow-moving, highly skilled, close-range . . . psychological influence . . . [to] high-tempo, low-skilled, remote, and disjointed" influence efforts.[102]

Disinformation is inherently dangerous to democratic institutions because "disinformation corrodes the foundation of liberal democracy."[103] Americans' "ability [to] assess facts on the merits and self-correct accordingly"[104] erodes when the information received is untrue. Reduced capacity for citizens in a democratic republic to differentiate between truth and falsities, threatens the ability to self-govern.

While influence operations and disinformation are not new, AI's ability to enhance the quality and the quantity of this information is extremely troubling. A recent study found that AI will lower the cost and barriers to entry of producing disinformation and increase the ease of creating high quality, personalized content.[105] With these new technologies and internet culture, disinformation is "now . . . more active than ever before."[106] The most recent, known instance of AI-facilitated disinformation during armed hostilities was a 2022 deepfake[107] of Ukrainian President Volodymyr Zelensky urging Ukrainian soldiers to lay down their arms.[108] This example demonstrates how disinformation with AI-developed synthetic media can pose national security risks, namely:

---

[102] THOMAS RID, ACTIVE MEASURES: THE SECRET HISTORY OF DISINFORMATION AND POLITICAL WARFARE 7 (2020).
[103] *Id.* at 7-8.
[104] *Id.* at 8.
[105] RISHI BOMMASANI ET AL., *supra* note 54, at 136-37.
[106] *See id.*
[107] *See Deepfake*, MERRIAM WEBSTER, https://www.merriam-webster.com/dictionary/deepfake (last visited Oct. 24, 2024) (defining "Deepfake" as "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.").
[108] Bobby Allyn, *Deepfake Video of Zelenskyy Could be 'Tip of The Iceberg' in Info War, Experts Warn*, NPR (Mar. 16, 2022), https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.

(1) manipulating elections,[109]

(2) exacerbating social divides,[110]

(3) lowering trust in institutions and authorities,[111] and

(4) undermining journalism and trustworthy sources of information.[112]

While deepfake videos are perhaps the most discussed threat, voice cloning, deepfake images, and generative text also merit concern.[113]

c. CBRN and Biosecurity Risks

While scientists "have already made astonishing progress in fields ranging from biology and medicine to astrophysics by leveraging AI," our adversaries can also use AI to "help create precisely engineered biological agents."[114] As stated in the NCAI report, "AI may enable a pathogen to be specifically engineered for lethality or to target a genetic profile—the ultimate range and reach weapon."[115] EO 14110 had also recognized that AI-facilitated biological threats, especially from non-state actors, are a national security risk.[116] This section discusses threats posed by two types of AI that can be used for bioweapons proliferation: AI Biological Design Tools ("BDT") and LLMs.

[109] Todd C. Helmus, *Artificial Intelligence, Deepfakes, and Disinformation*, RAND CORP., July 1, 2022, at 6.
[110] *Id.*
[111] *Id.*
[112] *Id.* at 7.
[113] *Id.* at 2.
[114] NSCAI REPORT, *supra* note 12, at 8, 45.
[115] *See id.* at 52. *See generally* Jonas Sandbrink, *Chatgpt Could Make Bioterrorism Horrifyingly Easy*, VOX (Aug. 7, 2023, 7:00 AM), https://www.vox.com/future-perfect/23820331/chatgpt-bioterrorism-bioweapons-artificial-inteligence-openai-terrorism.
[116] *See* Exec. Order. No. 14,110, 88 Fed. Reg. 75,191, 75,197 (Oct. 30, 2023).

AI BDT are AI "systems that are trained on biological data and can help design proteins or other biological agents."[117] These tools "drastically expand both the capability and accessibility to biologically manipulative agents, increasing the risk of malicious actions."[118] With access to an AI BDT and the proper equipment, nefarious actors could program organisms, pathogens, and viruses to be both lethal and to spread quickly.[119] The prime example of AI's potential for bioweaponry is AlphaFold 3, discussed in the beginning of Section I.E.

While AlphaFold 3 is one example of a current foundation model that could be used to engineer the perfect bioweapon, there have been concerns that current LLMs on the market today can do the same.[120] In 2024, RAND, a global policy think tank and research institute, published a paper detailing a study it conducted in which red teams[121] used LLMs to produce a large-scale biological attack.[122] While the study showed no viable advancement in capability compared to internet searches and current LLM models, the study found that

[117] JONAS SANDBRINK, ARTIFICIAL INTELLIGENCE AND BIOLOGICAL MISUSE: DIFFERENTIATING RISKS OF LANGUAGE MODELS AND BIOLOGICAL DESIGN TOOLS (2023), https://arxiv.org/pdf/2306.13952.

[118] Renan Chaves de Lima et al., *Artificial Intelligence Challenges in the Face of Biological Threats: Emerging Catastrophic Risks for Public Health*, FRONTIERS IN ARTIFICIAL INTELLIGENCE, May 10, 2024, at 2.

[119] *See id.*

[120] One such story states that in early 2023, a little black box with a dozen test tubes was brought to the Eisenhower Executive Office Building located next to the White House. *See* Riley Griffin, *The US Government Is Worried About AI-Bioweapons*, BLOOMBERG (Aug. 6, 2024, 6:00 AM), https://www.bloomberg.com/news/newsletters/2024-08-06/ai-like-chatgpt-could-become-the-next-biosecurity-threat. Inside the box was engineered DNA. *Id.* With the right equipment and technical know-how, this DNA could be combined to create a pathogen that would start the next pandemic. *See id.* While this box was constructed by a person, not AI, allegedly an AI chatbot was the one to describe the steps needed to build this bioweapon. *See id.*

[121] "[A red team is a] group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture." *Red Team*, NAT'L INST. STANDARDS & TECH, https://csrc.nist.gov/glossary/term/red_team (last visited Oct. 24, 2024).

[122] CHRISTOPHER A MOUTON ET AL., THE OPERATIONAL RISKS OF AI IN LARGE-SCALE BIOLOGICAL ATTACKS: RESULTS OF A RED-TEAM STUDY 4 (RAND 2023), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2900/RRA2977-2/RAND_RRA2977-2.pdf.

"[g]iven more time, advanced skills, additional resources, or elevated motivations, a malign non-state actor could conceivably be spurred by an existing or future LLM to plan or wage a biological weapon attack."[123] "[W]hile not generating direct instructions for the creation of biological weapons, [LLMs] present relevant insights that could assist in the execution of these attacks."[124] Though LLMs do not have the same inherent risk that AlphaFold 3 has in creating a bioweapon, LLMs are available to everyone with an internet connection, including state and non-state actors looking to design and develop bioweapons. OpenAI and other corporations are building a blueprint in evaluating the risk that their LLMs may provide in aiding someone in creating a biological threat.[125]

d. Cybersecurity and Critical Infrastructure Protection

In 2016, it was "estimat[ed] . . . that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion."[126] In addition to economic effects, cyberattacks can affect critical infrastructure, such as power grids, gas pipelines, and water treatment plants.[127] AI foundation models will likely increase these figures and

[123] *Id*. at 17.
[124] Lima et al., *supra* note 118, at 2.
[125] *Building an Early Warning System for LLM-Aided Biological Threat Creation*, OPENAI (Jan. 31, 2024), https://openai.com/index/building-an-early-warning-system-for-llm-aided-biological-threat-creation/.
[126] COUNCIL OF ECON. ADVISERS, EXEC. OFF. OF THE PRESIDENT OF THE U.S., THE COST OF MALICIOUS CYBER ACTIVITIES TO THE U.S. ECONOMY 36 (2018).
[127] *See Director Wray's Opening Statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party*, FED. BUREAU OF INVESTIGATION, (Jan. 31, 2024), https://www.fbi.gov/news/speeches-and-testimony/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party (during a speech, FBI Direct Christopher Wray stated "PRC [People's Republic of China] hackers are targeting our critical infrastructure—our water treatment plants, our electrical grid, our oil and natural gas pipelines, our transportation systems."); *see also Protecting the Electric Grid from the Potential Threats of Solar Storms and Electromagnetic Pulse: Hearing Before the S. Comm. on Homeland Security and Governmental Affairs*, 114th Cong. 114-483 (2015) (statement of R. James Wooley, CIA Director) (stating that if the United States losses electrical power for a year, 2/3rds to 90% of the American population would die); *see, e.g.,* David E. Sanger et al., *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*, N.Y. TIMES (May 13, 2023), https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

introduce new risks because they enhance adversaries' ability to launch cyberattacks through malware, exploitation of other AI models' vulnerabilities, social engineering, and phishing schemes.[128]

AI can "automatically generate malware attacks and develop more sophisticated malware, such as viruses, ransomware, and Trojans."[129] One study found that LLMs can autonomously identify vulnerabilities on websites and extract data or introduce malware without human direction or feedback.[130] This means a foreign adversary could launch and forget an AI system until it was time to activate the malware. After all, these "AI-driven bots possess unparalleled speed and accuracy in reconnaissance, identifying vulnerabilities, and launching attacks."[131] AI-powered malware can also automatically adjust its behavior in response to defenses it encounters such that its "real-time learning and adaptation capabilities make it especially difficult to eradicate."[132] AI systems can also be used to attack other AI systems. Prompt injection, for example, can be used against generative AI systems in an attempt to bypass safeguards and obtain sensitive information.[133] Cyber criminals' access to advanced AI would also make phishing campaigns harder to detect, especially with voice cloning and synthetic media.[134] Though cyber criminals already have access to many free tools so AI foundation models may just exacerbate existing cybercrime trends, AI foundation

(discussing the Colonial Pipeline shutdown that caused President Biden to declare a national state of emergency).

[128] *See* NTIA REPORT, *supra* note 68, at 16.

[129] *Id.*

[130] *See* RICHARD FANG ET AL., LLM AGENTS CAN AUTONOMOUSLY HACK WEBSITES 1 (Feb. 16, 2024).

[131] Oluebube Princess Egbuna, *The Impact of AI on Cybersecurity: Emerging Threats and Solutions*, 2 J. SCI. & TECH. 43, 44 (2021).

[132] *Id.*

[133] *See, e.g.,* Benj Edwards, *AI-Powered Bing Chat Spills Its Secrets Via Prompt Injection Attack,* ARS TECHNICA (Feb. 10, 2023), https://arstechnica.com/information-technology/2023/02/ai-powered-bing-chat-spills-its-secrets-via-prompt-injection-attack/ (discussing the susceptibility of LLMs to prompt injection).

[134] *See* Valerie Wirtschafter, *The Implications of the AI Boom for Nonstate Armed Actors,* BROOKINGS (Jan. 16, 2024), https://www.brookings.edu/articles/the-implications-of-the-ai-boom-for-nonstate-armed-actors/.

models will certainly increase the frequency and sophistication of cyberattacks.[135]

e. Military Applications

The future of war will consist of the use of AI and robotics.[136] Former Chairman of the Joint Chiefs of Staff, Mark Milley, states that any nation that does not adapt to a fast pace of AI-powered war will be at a clear disadvantage.[137] The Department of Defense ("DoD") has identified AI as crucial to command and communications, navigation, perception, obstacle detection, and swarm behavior tactics.[138] The Intelligence Advanced Research Projects Activity ("IARPA") "concluded that AI is likely to be as transformative a military technology as aviation and nuclear weapons were before."[139]

Swarm technology, for example, has gained significant attention. Swarms are capable of being used for both offensive and defensive purposes, where Lethal Autonomous Weapon Systems ("LAWS") are used to both culminate and "swarm" on a specific target and to disburse when counterattacked.[140] Swarms are low-cost.[141] Inexpensive drones have already proven successful on the Ukrainian battlefield, demonstrating that non-state actors or cash-strapped adversaries could use this tactic to overcome the U.S.'s expensive air defense legacy systems.[142] Swarms are effective because AI-integrated drones can, without the limiting factor of human cognition, work in unison.[143] AI technology does not require unit segmentation the same

---

[135] *See* NTIA REPORT, *supra* note 68, at 26.
[136] *See generally* Mark A. Milley & Eric Schmidt, *America Isn't Ready for the Wars of the Future: And They're Already Here,* FOREIGN AFFS. (Aug. 5, 2024), https://www.foreignaffairs.com/united-states/ai-america-ready-wars-future-ukraine-israel-mark-milley-eric-schmidt.
[137] *See id.*
[138] OFF. OF THE SEC'Y OF DEF., UNMANNED SYSTEMS INTEGRATED ROADMAP: 2017-2042 18 (2018), https://www.defensedaily.com/wp-content/uploads/post_attachment/206477.pdf.
[139] BAKER, *supra* note 17, at 38.
[140] *See id.* at 39.
[141] *See* Mark A. Milley & Eric Schmidt, *supra* note 136.
[142] *See id.*
[143] A 1993 study done by a British psychologist suggests that "the maximum number of people that . . . humans can concurrently maintain stable relations with is 150."

way human soldiers do, so swarm tactics can lead to an unprecedented level of situational and domain awareness.[144] While confusion arises on the battlefield as various military units attempt to work in unison, AI technology can overcome this obstacle as its cognitive capacity will exceed any skilled and battle-hardened leader. Militaries using AI to increase awareness will have decision dominance—allowing them to "observe, orient, decide, and act faster and more effectively than their adversary."[145]

f. Authoritarian Challenges to the Global Geopolitical Landscape

AI promises tremendous economic and strategic advantages,[146] and in the world of global power competition, "the stakes for future prosperity and long-term national competitiveness are high."[147] The use of "AI is transforming almost every sector of [the] national econom[y] and is accelerating globalized competitions among digital platforms and services."[148] This has led to "intense commercial competition among the world's leading technology companies," which are mostly based in China and the U.S.[149]

We can see authoritarian challenges to global geopolitical landscape through China's social credit system. In 2014, China introduced a new social credit score to determine the trustworthiness

Tom Geraghty, *Dunbar's Number, Psychological Safety and Team Size*, PSYCH SAFETY (Oct. 21, 2022), https://psychsafety.co.uk/psychological-safety-82-dunbars-number-and-team-size/. Known as "Dunbar's Number," this theory is attributed to the size of military units, with a company existing of approximately 150 individuals. *See id.* It is important to note that human cognition only allows a limited amount of oversight, meaning that a campaigning military must coordinate between units and cannot act as a singular, conscious whole like AI.

[144] *See generally* Robert M. Ryder, *Domain Awareness Superiority Is the Future of Military Intelligence*, MIL.REV. 69-73 (2021) (describing how AI is enabling the realization of domain awareness).

[145] *Id.* at 69.

[146] *See id.* at 71.

[147] Eric Schmidt, *AI, Great Power Competition & National Security*, 151 AI & SOC'Y 288, 288 (2022).

[148] *Id.*

[149] *Id.*

of its citizens.[150] Through the social credit system, China constantly monitors its citizens' online and offline activity. China has complete control of what their citizens post, what websites they visit, and how they interact with others in cyberspace, in what is known as "IT-backed authoritarianism."[151] China also tracks their citizens' offline activity through internet-based AI facial recognition algorithms.[152] In Beijing alone, there are 800,000 CCTV cameras that China uses to track its citizens and their daily lives, including things as minor as jaywalking infractions, which can make up a citizen's social credit score.[153] This Orwellian social credit system could not be maintained without AI-enabled technologies, as expressed in China's 2017 *Next Generation Artificial Intelligence Development Plan* ("China's AI Plan").[154] China utilizes AI-enabled technologies, for example, to surveil and track "the movements and associations of its ethnic minority and largely Muslim Uighur population outside of the Uighur Autonomous Region."[155] Through empowered AI-enabled facial recognition software, China can track both minority groups like the Uighurs and citizens of interest in real time as they move throughout China.

While initially it may seem that China's social credit score may not have a direct link to the U.S. and national security, China, along with other authoritarian regimes, have been outsourcing their authoritarian-backed technology to the rest of the world.[156] Indeed,

---

[150] Claire Seungeun Lee, *Datafication, Dataveillance, and the Social Credit System as China's New Normal*, 43 ONLINE INFO. REV. 952, 953 (2019).
[151] *See id.* at 952.
[152] BAKER, *supra* note 17, at 31.
[153] *Id.*
[154] *See generally* 新一代人工智能发展规划 [Notice of the State Council on Issuing the Development Plan for the New Generation of Artificial Intelligence], Guofa [2017] No. 35(China), *translated in* Webster et al., *A Next Generation Artificial Intelligence Development Plan*, CHINA COPYRIGHT & MEDIA (Aug. 1, 2017), https://chinacopyrightandmedia.wordpress.com/2017/07/20/a-next-generation-artificial-intelligence-development-plan/ [hereinafter *China's Plan*].
[155] BAKER, *supra* note 17, at 31.
[156] *See* Adrian Shahbaz, *The Rise of Digital Authoritarianism: Fake News, Data Collection, and the Challenge to Democracy*, FREEDOM HOUSE, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism (last visited Apr. 21, 2025) ("[A] cohort of countries is moving toward digital authoritarianism by embracing the Chinese model of extensive censorship and

China has demonstrated both the desire and capability to export its authoritarian-backed AI.[157] The convergence of AI, great power competition, and national security creates opportunities for adversaries like China and Russia and to upend the global geopolitical regime and is discussed in more detail in the nation state actors subsection within the next section.[158]

2. Actor-Based Threats

National security threats associated with AI foundation models can be categorially divided into two classes: (1) threats posed by nation-state actors, whose access to AI foundation models may exacerbate authoritarian challenges to the global geopolitical landscape, and (2) non-state actors.

a. Nation State Actors

Public statements suggest that the Russian government prioritizes the use of AI to support its information and cyber operations. [159] While the Global AI Index, the most comprehensive effort to date on evaluating AI advancement in nation states,[160] ranked Russia in thirty-first place,[161] "Russian President Vladimir Putin signed a "40-page decree to update the national strategy of developing AI."[162] Like plans enacted in the U.S., Russia's plan is to develop a

automated surveillance systems. As a result of these trends, global internet freedom declined for the eighth consecutive year in 2018.").

[157] *See* VALENTIN WEBER, DATA-CENTRIC AUTHORITARIANISM: HOW CHINA'S DEVELOPMENT OF FRONTIER TECHNOLOGIES COULD GLOBALIZE REPRESSION 4-7 (Nat'l Endowment for Democracy & Int'l Forum for Democratic Studs., 2025), https://www.ned.org/wp-content/uploads/2025/02/NED_FORUM-China-Emerging-Technologies-Report.pdf.

[158] *See* Schmidt, *supra* note 147, at 288-89.

[159] Samuel Bendett, *The Role of AI in Russia's Confrontation with the West*, CTR. NEW AM. SEC. (May 3, 2024), https://www.cnas.org/publications/reports/the-role-of-ai-in-russias-confrontation-with-the-west.

[160] Schmidt, *supra* note 147, at 291.

[161] *The Global AI Index,* TORTOISE, https://www.tortoisemedia.com/data/global-ai (last visited Apr. 21, 2025) (select "Rankings" from the options at the top of the page).

[162] Jeremy Werner, *Russia Updates National AI Strategy*, BABL (Mar. 1, 2024), https://babl.ai/russia-updates-national-ai-strategy/.

robust AI system by 2030 focused on AI infrastructure, economic growth, talent management, and research and development.[163] Much of this is spurred on by Russia's "concern about falling behind" in the technological competition between great powers.[164] After all, Russian President Vladimir Putin believes AI "is the future, not only for Russia, but for all mankind . . . [w]hoever becomes the leader in this sphere will become the ruler of the world."[165] It is not "hard to imagine Russian cyber and disinformation activities in Ukraine or elsewhere in Europe becoming more effective, persistent, and influential with AI."[166] Nor is it hard to imagine Russian interference, like its conduct during the 2016 U.S. election,[167] increasing in scope and effectiveness.

Digital platforms and services lead an AI-centric, globalized economic competition, mainly between China and the U.S.[168] The U.S. currently ranks first in the AI Global Index, exceeding China, ranked second, by more than five times in the talent category.[169] In one strategy, China outlined its ambition to lead in AI by 2030.[170] An examination of the three components of AI reveals that China may present a legitimate threat to U.S. dominance in this space.

---

[163] *See id.*

[164] SAMUEL BENDETT, THE ROLE OF AI IN RUSSIA'S CONFRONTATION WITH THE WEST 3 (Ctr. New Am. Sec., 2024), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Russia-AI_2024-final.pdf (Russia is also concerned with building its capacity to leverage AI for information and cyber operations).

[165] James Vincent, *Putin Says the Nation That Leads in AI 'Will be the Ruler of the World'*, THE VERGE (Sept. 4, 2017, 4:53 AM), https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world.

[166] Schmidt, *supra* note 147, at 294.

[167] *See, e.g., Russian Interference in 2016 U.S. Elections*, FBI: MOST WANTED, https://www.fbi.gov/wanted/cyber/russian-interference-in-2016-u-s-elections (last visited May 7, 2025).

[168] *See id.* at 288, 290.

[169] *The Global AI Index, supra* note 161.

[170] *See China's Plan*, *supra* note 154, § II.(3). China hit the first milestone of this plan in 2020 when it produced the most AI research papers, highly cited AI papers, and AI patents worldwide. *See* Ricardo Tellez, *China A.I. Plan for 2030*, THE CONSTRUCT (Dec. 11, 2021), https://www.theconstruct.ai/98-chinas-ai-plan-for-2030/.

First, the most pressing advantage is China's access to vast amounts of data that can be used for training AI models.[171] This is partly because of China's vast population[172] and "partly due to . . . [the fact China] monitors everything from birth: facial recognition is so widespread you can be picked up for jaywalking and stopped from stealing tissue at the Temple of Heaven in Beijing."[173] China collects data not only on its population, but on manufacturing, internet usage, medical data, the economy, on smart cities, and more.[174] Second, China is catching up to the U.S.'s computing lead in some areas, though it is still generally "two years" behind global leaders when it comes to the design of logic chips for AI applications.[175] China is actively seeking to become self-reliant on the computing aspect of AI and has received a high level of patents related to this technology.[176] Third, as it relates to algorithmic innovation, "China is rapidly narrowing the algorithmic gap,"[177] especially by partnering with U.S. academics and stealing U.S. AI software innovations.[178]

China has weaknesses that cause it to lag in computing and algorithmic innovations, including shortages in (1) "cutting-edge talent for AI" at scientific research institutions and universities; (2) "major original results" and knowledge in semiconductors innovation, AI technical standards, and software frameworks and platforms; and (3) fruitful interactions between institutions and

[171] *See* Steve Hsu, *FT Podcasts on US-China Competition and AI,* INFO. PROCESSING – STEVE HSU, https://stevehsu.substack.com/p/ft-podcasts-on-us-china-competition-and-ai (noting that "access to vast amounts of data may prove to be China's secret weapon).

[172] *See*, *U.S. and World Population*, U.S. CENSUS BUREAU, https://www.census.gov/popclock/world?intcmp=w_200x402 (last visited Apr. 21, 2025).

[173] Louise Lucas & Richard Waters, *China and US Compete to Dominate Big Data,* FIN. TIMES (May 1, 2018), https://www.ft.com/content/e33a6994-447e-11e8-93cf-67ac3a6482fd.

[174] *Id.*

[175] STEPHEN EZELL, HOW INNOVATIVE IS CHINA IN SEMICONDUCTORS?, 1 (Info. Tech. & Innovation Found., 2024), https://www2.itif.org/2024-china-semiconductors.pdf.

[176] *See id.* at 1, 3, 6, 25 (discussing the recent activity of China as it relates to patents and AI technology).

[177] Lucas & Waters, *supra* note 173.

[178] *House Hearing on AI, supra* note 52, at 16 (statement of Dr. William Hannas, Lead Analyst, Ctr. for Sec. & Emerging Tech., Georgetown Univ.).

enterprises.[179] But China plans to shore up these weaknesses through industrial espionage and foreign technology transfer. Indeed, "China has not shied from acquiring AI technology from abroad" and has pursued foreign technology transfer regimes since 1956.[180] China acquires technology through illegal, legal, and extralegal transfers,[181] and without U.S. mitigation, China could achieve technology dominance over the U.S.

b. Non-State Actors

AI foundation models increase the risks non-state actors pose because they lower the barriers to entry for national security risks historically relegated to well-funded, sophisticated state actors. For example, "AI could lower the technical threshold required to commit destabilizing attacks on critical infrastructure, like hospitals or electric grids."[182] This means incidents like the Colonial Pipeline ransomware attack[183] are likely to occur more frequently, with AI to automate steps in the process (e.g., find and exploit vulnerabilities). Additionally, non-state actors—particularly organized crime syndicates and state-sponsored non-state actors—are increasingly stealing data and leveraging it to surveil and manipulate individuals.[184]

---

[179] *See China's Plan*, *supra* note 154, § I.

[180] *See House Hearing on AI*, *supra* note 52, at 7-8 (statement of Dr. William Hannas, Lead Analyst, Ctr. for Sec. & Emerging Tech., Georgetown Univ.).

[181] *Id.* at 11-13 (discussing in detail how China for decades has had a strategy of IP and technology theft)*; see also The China Threat: Chinese Talent Plans Encourage Trade Secret Theft, Economic Espionage*, FED. BUREAU INV., https://www.fbi.gov/investigate/counterintelligence/the-china-threat/chinese-talent-plans?ref=americanpurpose.com (last visited Apr. 21, 2025) (discussing the FBI's perspective on the unique threat China poses to national security and technology theft); Christopher Burgess, *China's Thousand Talents Program Harvests U.S. Technology and a Guilty Verdict*, CLEARANCEJOBS: NEWS & CAREER ADVICE (May 1, 2023), https://news.clearancejobs.com/2023/05/01/chinas-thousand-talents-program-harvests-u-s-technology/.

[182] Wirtschafter, *supra* note 134.

[183] Zachary Cohen et al., *What We Know About the Pipeline Ransomware Attack: How it Happened, Who is Responsible and More*, CNN POLITICS (May 10, 2021, 4:45 PM), https://www.cnn.com/2021/05/10/politics/colonial-ransomware-attack-explainer/index.html.

[184] *See* THE WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY 2-3 (2023), https://bidenwhitehouse.archives.gov/wp-content/uploads/2023/03/National-

Many non-state actors, such as extremist groups, could use the generative capabilities of AI foundation models to maliciously spread disinformation and extremist views. For example, the Islamic State of Iraq and Syria ("ISIS") was unique because of the global influence it had on many Muslim youths.[185] ISIS exerted global influence on Muslim youths by using social media to rapidly and broadly spread extremist messaging and ISIS propaganda.[186] ISIS even developed a Twitter app accessible on the Google Play store that had a timing mechanism to avoid algorithmic detection.[187] This app enabled the posting of almost 40,000 tweets before it was taken down.[188] Although AI foundation models were not used by ISIS, the technology can enhance a non-state actor's influence operations by bolstering disinformation, recruitment, and intelligence efforts.[189] Non-state actors could also use deepfake technology to create convincing "evidence" of wrongdoings through synthetic image, voice, and video generation.[190] So, AI foundation models could improve the quantity and quality of non-state actors' propaganda.

AI foundation models also lower the expertise and monetary barriers to developing bioweapons, potentially such that making current international prevention methods ineffective at preventing

Cybersecurity-Strategy-2023.pdf. *See generally* Evan Morgan, *Eroding Global Stability: The Cybersecurity Strategies of China, Russia, North Korea, and Iran*, IRREGULAR WARFARE INITIATIVE (Aug. 1, 2024), https://irregularwarfare.org/articles/eroding-global-stability-the-cybersecurity-strategies-of-china-russia-north-korea-and-iran/ (discussing the use of proxy organizations loosely associated with authoritarian regimes that are utilized by said regimes to undermine democratic institutions such as the United States).

[185] *See generally* Jamil Walli, The Psychology of Detachment and Hyperreality: Analysing ISIL's Propaganda 1, 98 (June 30, 2015) (B. thesis, Linnaeus University).

[186] *See* Dylan Gerstel, *ISIS and Innovative Propaganda: Confronting Extremism in the Digital Age*, 1 SWARTHMORE INT'L RELS. J. 1, 1-2 (2017).

[187] *See id.* at 4.

[188] *See id.*

[189] Wirtschafter, *supra* note 134.

[190] *Id*; *see* ELLA BUSCH & JACOB WARE, THE WEAPONISATION OF DEEPFAKES: DIGITAL DECEPTION BY THE FAR-RIGHT 5-7 (Int'l Centre for Counter-Terrorism, 2023), https://www.icct.nl/sites/default/files/2023-12/The%20Weaponisation%20of%20Deepfakes.pdf.

even low-funded non-state actors from bioweapons proliferation.[191] The use of biological weapons by non-state actors is not new, although their use has not yet successfully caused more than minimal harm.[192] History has proven that organizations like ISIS, Al-Qaeda, and Aum Shinrikyo, along with domestic terrorists,[193] would use bioweapons for their own nefarious purposes.[194] AI foundation models that lower the barrier to entry for creating bioweapons would substantially increase the likelihood of success of future significant harm.[195]

The use of "[l]ow-cost, commercial off-the-shelf AI" coupled with cheap, easily accessible drone technology could "destabilize existing state-nonstate power dynamics on the battlefield."[196] Non-state actors have already used semi-autonomous drones on the battlefield, showing how, even with limited funds, the use of inexpensive hardware can stand completely against a nation states' far costlier and more sophisticated weaponry.[197] State actors have not openly deployed LAWS without human oversight because of the potential to violate (1) the law of armed conflict, (2) international customary law, and (3) treaty obligations, in addition to the *jus cogens*

[191] *See* Shravishtha Ajaykumar, *Pathogen Peril: Non-State Access to Bioweapons*, OBSERVER RSCH. FOUND. (Jul. 2, 2024), https://www.orfonline.org/expert-speak/pathogen-peril-non-state-access-to-bioweapons.
[192] *See generally Biological Weapons Nonproliferation: Module 3: Bioterrorism*, JAMES MARTIN CTR. FOR NONPROLIFERATION STUDIES, MONTEREY INST. OF INT'L STUDS, https://tutorials.nti.org/biological-weapons-nonproliferation/bioterrorism/ (last visited Apr. 21, 2024) (click individual drop-down options for text) (illustrating examples of non-state actors and their attempts to use biological weapons).
[193] There is also the additional concern of domestic terrorism applications. There have already been multiple examples of domestic terrorists using biological agents for nefarious purposes. *See id.* (click drop-down option 2. and select "Start exploring") (illustrating that biological weapons have been used by domestic terrorists and not only foreign terrorists).
[194] *See id.*
[195] *See id.* (illustrating the desire of non-state actors to use biological weapons).
[196] *See generally* SARAH KREPS, DEMOCRATIZING HARM: ARTIFICIAL INTELLIGENCE IN THE HANDS OF NONSTATE ACTORS 1, 6 (Brookings Inst., 2021), https://www.brookings.edu/wpcontent/uploads/2021/11/FP_20211122_ai_nonstate_actors_kreps.pdf (discussing the use of AI and drone technology to overcome legacy defense systems).
[197] *See id.* at 2.

implications of their use.[198] Hostile non-state actors, however, do not share these concerns, thus creating an asymmetric advantage compared to traditional nation state legacy systems.[199] Using open-source AI and commercial drones, a non-state actor can create makeshift LAWS at a fraction of the cost.[200] These tactics have already been used against Russian bases in Syria.[201] Using these tactics, automated systems that increase quantity and lethality would be even easier to employ for non-state actors like the Houthis and Hamas, groups already using drones in their attacks.[202]

[198] *Id.* at 5 ("This machine learning process could result in devastating false positives (identifying a civilian as a combatant) or false negatives (identifying a combatant as a civilian). The more controversial outcome is the former, because it means innocent people being killed by a machine."). AI-led attacks could possibly implicate *jus cogens*, for example, if incidental civilian casualties were egregious enough to implicate a violation of the right to life. *See* Karen Parker & Lyn Beth Neylon, *Jus Cogens: Compelling the Law of Human Rights*, 12 HASTINGS INT'L & COMP. L. REV. 411, 431 (1989).

[199] Mark A. Milley & Eric Schmidt, *supra* note 136 ("Beijing is already deploying AI-powered surveillance and electronic warfare systems that could give it a defensive advantage over the United States in the entire Indo-Pacific. In the air, the capable but costly F-35 might struggle against swarms of cheap drones. So might the heavily armored Abrams and Bradley tanks on the ground. Given these unfortunate facts, U.S. military planners are right to have concluded that the era of "shock and awe" campaigns—in which Washington could decimate its adversaries with overwhelming firepower—is finished."); *see also id.* at 5 (discussing asymmetries involved with non-state actors' use of AI.)

[200] *See id.* at 1, 4 (discussing how the use of commercial AI and drones has lowered the cost for barriers to entry on their use).

[201] *See* Charlie D'Agata, *Russian Military Base in Syria Attacked by Mysterious Drone Swarm*, CBS NEWS (Jan. 11, 2018), https://www.cbsnews.com/news/russian-military-base-in-syria-attacked-by-mysterious-drone-swarm/.

[202] *See id.*; *see also Evolution of UAVs Employed by Houthi Forces in Yemen*, CONFLICT ARMAMENT RSCH., https://storymaps.arcgis.com/stories/46283842630243379f0504ece90a821f (last visited Apr. 21, 2025); *Israel-Hamas War Latest: Hezbollah Says it Launched a Drone Attack on Northern Israel*, ASSOCIATED PRESS (Aug. 5, 2024; 5:32 PM), https://apnews.com/article/israel-hamas-war-latest-5-august-2024-631cf209427743bfa105516d52c1556d.

II. CURRENT LEGAL FRAMEWORK INVOLVING NATIONAL SECURITY RISKS OF AI FOUNDATION MODELS

Since 2018, the U.S. has implemented broad export and import controls to mitigate national security risks by restricting the use of U.S.-developed AI technologies by both state and non-state foreign adversaries. By implementing the Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA")[203] and the Export Control Act of 2018 ("ECRA")[204] through the John S. McCaine National Defense Authorization Act ("NDAA") of 2019,[205] the U.S. has focused on curbing access by foreign adversaries to "critical," "emerging," and "foundational" technologies[206] involving both inbound and outbound investments. This section summarizes the constitutional, statutory, and regulatory laws and directives the U.S. currently has in place to curtail access to AI through both inbound and outbound investment, and then overviews the current regulations that limit access to AI foundation models outside of the inbound and outbound investment scope.

A. *AI and Inbound & Outbound Investment*

Congress and the President's power to regulate economic activity with foreign entities stems directly from the Commerce Clause and the Treaty Clause of the Constitution.[207] These clauses grant sweeping powers to regulate foreign and domestic commerce within the U.S. and, when it relates to ECRA, extraterritorially. This allows the U.S. to regulate transactions involving U.S.-based AI foundation models and foreign entities, thus mitigating national security risks that may stem from these transactions.

The Commerce Clause specifically gives Congress the power to "regulate Commerce with foreign Nations."[208] Under this authority,

---

[203] *See* Foreign Investment Risk Review Modernization Act, 50 U.S.C. § 4565.
[204] *See* Export Control Reform Act, 50 U.S.C. §§ 4801, 4811–4852.
[205] *See* John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, §§ 1701, 1767, 132 Stat. 1635, 2174, 2233 (2018).
[206] *See* 50 U.S.C. §§ 4565(a)(6), 4817.
[207] *See* U.S. CONST. art. I, § 8, cl. 3; *id.* art. II, § 2, cl. 2.
[208] *Id.* art. I, § 8, cl. 3.

Congress can place comprehensive internal and external foreign controls on both outbound and inbound investment under "interstate commerce," which itself has been incorporated as a requirement as it applies to both FIRRMA and ECRA.[209] This clause grants sweeping powers,[210] including over local commerce so long as the activity was part of a continuous "current" of commerce that involved interstate goods and services.[211]

The Treaty Clause states that the President "shall have the Power, by and with the Advice and Consent of the Senate, to make Treaties."[212] The Supreme Court determined in *U.S. v. Curtiss-Wright* that "the President alone has the power to speak or listen as a representative of the nation,"[213] and to conduct foreign affairs.[214] The Treaty clause is important for two reasons. First, it may confer to the President constitutional authority, beyond what is congressionally bestowed, to regulate foreign commerce as it relates to foreign affairs.[215] Second, the President may act in contradiction to Congress if Congress encroaches on the Presidents' foreign affairs powers.[216]

[209] *See id.* art. I, § 8, cl. 3; Foreign Investment Risk Review Modernization Act, 50 U.S.C. § 4565(a)(13); Export Control Reform Act, 50 U.S.C. §§ 4842(a)(1).
[210] *See, e.g.*, Gonzales v. Raich, 545 U.S. 1, 2 (2005) (reaffirming Congress' commerce clause power was "firmly established" to regulate purely local activities that are a part of a "class of activities" with a substantial effect on interstate commerce under the rationale that local use affected supply and demand of national markets, making regulation of intrastate use "essential" to regulating the national market).
[211] *See* Gibbons v. Ogden, 22 U.S. 1, 196, 211 (1824) (holding that Congress has the power to "regulate commerce" and that federal law takes precedence over state laws); Swift & Co. v. United States, 196 U.S. 375, 398-99 (1905) (holding that interstate commerce included actions that were part of the "stream of commerce" where the stream was clearly interstate in character).
[212] U.S. CONST. art. II, § 2, cl. 2.
[213] United States. v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 319 (1936).
[214] *See generally id.* (discussing that the power to regulate foreign affairs solely rests with the President of the United States).
[215] *Id.* at 319-20.
[216] *See* Zivotofsky v. Kerry, 576 U.S. 1, 56 (2015); Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579 (1952) (In *Zivotofsky v. Kerry*, Congress specifically passed a law requiring American citizens born in Jerusalem to have their passports labeled as being born in "Israel" instead of "Jerusalem." The President directed the Department of State to continue to label passports of individuals born in Jerusalem as "Jerusalem." The Supreme Court determined that it was an inherent power within

The current U.S. framework uses a combination of Executive Branch regulatory bodies and statutes to oversee foreign investments in AI through FIRRMA, ECRA, and IEEPA.

1. The Committee on Foreign Investment in the United States

The Committee on Foreign Investment in the United States ("CFIUS") regulates the access of AI by foreign adversaries within the U.S.[217] *CFIUS* originally had no decision-making authority; it simply monitored the impact of foreign investment in the U.S., but it has since evolved.[218] Based on concerns involving new technologies, investment schemes, and the rise of Chinese civil-military fusion and technological theft, Congress enacted CFIUS's current version through FIRRMA in 2018.

CFIUS's mission under 50 U.S.C. § 4565 is to review and investigate "covered transactions" into a U.S. business to evaluate national security concerns and take necessary mitigating steps.[219] A "covered transaction"[220] is generally an investment by a foreign entity

---

the constitution for the President to determine if they recognized foreign nations or not, thus passing the strict scrutiny standard as determined in *Youngstown*.).

[217] *See* Heath P. Tarbert, *Modernizing CFIUS*, 88 GEO. WASH. L. REV. 1477, 1483 (2020).

[218] *Id.* at 1479-1503.

[219] *See* 31 C.F.R. §§ 800.101(a), 802.101(a).

[220] A covered transaction is generally defined as "Any merger, acquisition, or takeover . . . by or with any foreign person that could result in foreign control of any United States business, including such a merger, acquisition, or takeover carried out through a joint venture." 50 U.S.C. § 4565(a)(4)(B)(ii) (Another covered transaction is the purchase or lease of specific real estate based on its proximity to a U.S. national security interest. 50 U.S.C. § 4565(a)(4)(B)(ii). Further, a covered transactions are those that meet criteria set by CFIUS under regulation, which includes – a covered investment from a non-excepted investor in a business involving critical technology, critical infrastructure, or sensitive personal data (TID) which would allow a foreign person access to any material nonpublic technical information, membership or observer rights on the board of directors or equivalent, or involvement in substantial decision making; a change in rights by a foreign person in a U.S. business that would result in a covered control transaction; or any other arrangement meant to evade or circumvent 50 US.C. § 4565(a)(4)(B)(ii)(III); For examples of criteria set by CFIUS, see 31 C.F.R. § 800.219 (an excepted investor is a national from an excepted state: Australia, Canada, New Zealand, UK, and Northern Ireland); 31 C.F.R. §§ 800.219,

into a U.S. business that provides the foreign entity control of the U.S. business or nonpublic access in a U.S. business involving critical technology or infrastructure or sensitive personal data (i.e., a TID business). A U.S. business is any business within U.S. jurisdiction, whether foreign or domestically controlled.[221] Control means power, direct or indirect, whether or not exercised, to determine, direct, or decide important matters affecting an entity.[222] CFIUS monitors transactions itself but also receives declarations and notifications from foreign entities. Declarations and notifications typically occur in four ways:

(1) A party may make a declaration;[223]

(2) a declaration may be mandatory when there exists a substantial interest in a TID business;

(3) a party may make a notification, which requires more information and a filing fee when compared to a declaration;[224] or

(4) the committee may unilaterally request the foreign person to file a notification either without or after a declaration if there is a covered transaction.[225]

Though most CFIUS transactions do not require notification to CFIUS, many foreign entities choose to file a declaration or notification even when it is not mandatory.[226] This is because CFIUS

802.215; 31 C.F.R §§ 800.211, 800.213, 800.248, 802.211 (any other investment in a TID business). Any change in rights that can give a foreign person control of a U.S. business is also a covered transaction. 50 U.S.C. § 4565(a)(4)(B)(iv). ((Finally, any other transaction, transfer, agreement, or arrangement that would circumvent 50 U.S.C. § 4565 may also be considered a covered transaction. 50 U.S.C. § 4565(a)(4)(B)(v). *See generally* 50 U.S.C. § 4565. CFIUS regulations interpreting these provisions are complex. For a more detailed description of CFIUS regulations regarding covered transactions, see generally 50 U.S.C. § 4565; 31 C.F.R. §§ 800).

[221] 31 C.F.R. § 800.252.

[222] *See* 31 C.F.R. §§ 800.208, 802.208.

[223] 50 U.S.C. § 4565(b)(1)(C)(v).

[224] 50 U.S.C. § 4565(b)(1)(C).

[225] 50 U.S.C. § 4565(b)(1)(C)(v)(III).

[226] *CFIUS Overview*, U.S. DEP'T OF THE TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-

will grant safe harbor so long as the declaration or notification is accurate and not misleading and a material change to control or TID business classification does not occur.[227]

If a national security risk arises as a result of the risk-based analysis from a covered transaction, CFIUS can suspend or mitigate the covered transaction so long as the whole committee adopts it.[228] During an investigation, the Director of National Intelligence will conduct a thorough analysis—with input from the rest of the Committee—of the potential national security threats the transaction poses.[229] CFIUS can only impose suspension or mitigation based on a risk-based analysis of the following elements: (1) threat from foreign interest, (2) vulnerability caused by the transaction, and (3) consequence of the transaction.[230] If any of the three elements has zero risk, then no risk exists. If risk does exist, CFIUS can enter into mitigation agreements with foreign entities to mitigate the identified risks.[231] A lead agency monitors the mitigation agreement for breach or substantial changes that would create a security risk.[232] If a substantial change occurs, a new mitigation agreement can be reached, and if a breach occurs, additional investigation or referral to the President can occur.[233]

Under 50 U.S.C. § 4565(f), the President, based on credible evidence that a covered transaction might threaten or impair national security, can suspend, prohibit, and even reverse a covered transaction.[234] Section (f) lists eleven factors, and while most of these factors could be a consideration for foreign investment in a U.S.

---

cfius/cfius-overview (last visited Apr. 21, 2025) (The process remains largely voluntary, where parties may submit a short-form declaration notifying CFIUS of a covered transaction in order to receive a potential "safe harbor" letter "which limits CFIUS from subsequently initiating a review of a transaction except in certain limited circumstances").

[227] 31 C.F.R. § 800.701; 50 U.S.C. § 4565(b)(1)(D).

[228] *See* 50 U.S.C. § 4565(l)(1), (l)(3)(A), (l)(4)(A), (l)(4)(B); (detailing the procedural steps that are created through the U.S.C. as it relates to *CFIUS*).

[229] 50 U.S.C. §§ 4565(b)(4), (k).

[230] 50 U.S.C. § 4565(l)(4).

[231] 50 U.S.C. § 4564(l)(3).

[232] *See* 50 U.S.C. § 4564(l)(3).

[233] *See* 50 U.S.C. § 4564(l)(3); *see also* 50 U.S.C. § 4565(b)(1)(D).

[234] 50 U.S.C. § 4565(l)(d)-(f).

business focused on AI foundation models, four directly correlate to national security risks involving AI foundation models.[235] These are factors five (the potential effects of the proposed or pending transaction on U.S. international technological leadership in areas affecting U.S. national security), six and seven (the potential national security-related effects on critical technologies and infrastructure), and eleven (such other facts as the President may deem appropriate).

CFIUS also defines critical technologies for itself and ECRA[236] under 50 U.S.C. § 4565(a)(6), which includes the U.S. Munitions List ("UMLS") under the International Traffic in Arms Regulation ("ITAR"), Commerce Control List ("CCL"), various nuclear equipment, facilities, and material, select agents and toxins under 7 C.F.R. § 331, and "[e]merging and foundational technologies" under *ECRA*, which is yet to be defined.[237] In 2022, former President Biden issued EO 14083 under his 50 U.S.C. § 4565(f)(11) authority to consider "evolving national security risks" as they relate to CFIUS's risk-based analysis involving foreign investment.[238] Here, the former President directed CFIUS to consider "technologies that are fundamental to national security, including . . . artificial intelligence."[239]

CFIUS does an excellent job suspending, prohibiting, and reversing foreign investments into U.S.-based AI foundation models that may result in a national security risk. For example, the Biden administration forced a Saudi Aramco venture capital firm to sell its shares in a Silicon Valley AI chip startup backed by OpenAI.[240] The venture capital firm had direct ties to China, so the President, through

[235] 50 U.S.C. § 4565(f).
[236] *See* 50 U.S.C. § 4817(a).
[237] 50 U.S.C. § 4565(a)(6); *see also Emerging Technologies*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., https://www.bis.gov/emerging-technologies (last visited Apr. 21, 2025).
[238] *See generally* Exec. Order 14,083, 87 Fed. Reg. 57,369 (Sept. 15, 2022) (discussing the evolving national security risks that CFIUS should take into consideration).
[239] *Id*. at 57,370.
[240] Jane Lanhee Lee, *US Compels Saudi Fund to Exit AI Chip Startup Backed by Altman*, BLOOMBERG (Nov. 30, 2023, 10:53 PM), https://www.bloomberg.com/news/articles/2023-11-30/us-compels-saudi-fund-to-exit-ai-chip-startup-backed-by-altman.

CFIUS, forced the firm to sell its shares.[241] This is a clear example of CFIUS successfully protecting against potential technology theft by China, which is an ongoing national security risk.

While CFIUS stops foreign direct investments that may implicate national security risk, CFIUS draws the line when investment is done by a U.S. national or involves a greenfield.[242] For example, while CFIUS is known for its involvement in its negotiations with TikTok and ByteDance,[243] it determined it lacked jurisdiction over Elon Musk's purchase of Twitter, which included a Saudi Prince as a foreign investor, because Elon Musk is a U.S. citizen.[244] CFIUS narrowly construed its reach even though both TikTok and Twitter share similar national security concerns: the use of Americans' personal data by foreign adversaries. One can imagine a similar scenario occurring with an investment in OpenAI, Google, or another AI pioneer. So, if a foreign adversary had enough capital to invest into a greenfield within the U.S. and then recruited local talent, CFIUS would not have jurisdiction.

2. Export Control Reform Act

While CFIUS protects against foreign adversaries investing within the U.S.,[245] ECRA protects against the export of "critical," "foundational," and "emerging" technology that may put U.S. "leadership in . . . science, technology, engineering, and manufacturing sectors, including foundational technology that is essential to innovation," at risk.[246] Unlike CFIUS, which considers "covered

[241] *See id.*
[242] *See generally* 50 U.S.C. § 4565; 31 C.F.R. §§ 800, 802 (nowhere in the statute or regulations does *CFIUS* draw the authority to review greenfield investments in the United States).
[243] *See* Fatima Hussein & Sally Ho, *How a Little-Known Agency Holds Power Over TikTok's Future*, ASSOCIATED PRESS (Mar. 31, 2023), https://apnews.com/article/tiktok-ban-china-cfius-national-security-a7f59032a6a68c67470a0746d560e411.
[244] Jeff Stein, *U.S. Government Is Not Investigating Elon Musk's Twitter Purchase*, THE WASHINGTON POST (Feb. 6, 2023), https://www.washingtonpost.com/us-policy/2023/02/06/twitter-musk-treasury-cfius/.
[245] *See generally* U.S.C. § 4565(a)(6).
[246] Export Control Reform Act, 50 U.S.C. §§ 4811(3), 4817.

transactions" on a case-by-case basis, ECRA is based on "quantitative restrictions and export bans."[247] For most of U.S. history, export controls were limited to times of armed conflict.[248] But in 1949, Congress enacted the Export Control Act for three reasons: (1) "to protect the domestic economy," (2) "to further the foreign policy of the United States", and (3) "to exercise the necessary vigilance over exports from the standpoint of their significance to the national security."[249] This "three-prong approach" underlies the current export policy of the U.S.[250] "Realizing that export controls with foreign policy and national security goals would be ineffective without multilateral coordination," the U.S. and its major allies entered into multilateral export control regimes starting during the Cold War; these regimes persist in four major multilateral control regimes today.[251] The Wassenaar Arrangement is one of the four multilateral control regimes focused on "Conventional Arms and Dual-Use Goods and Technologies" and fits within the ECRA paradigm.[252] The Wassenaar Arrangement is a treaty with forty-two nation-state signatories, and while there are additional multilateral control regimes that exist, AI foundation models would most likely fall under this agreement.[253]

ECRA is implemented through the Export Administration Regulations ("EAR")[254] which "set[] forth licensing policy for goods and destinations, the application process used by exporters, and the [Commerce Control List ("CCL"),] . . . which is the list of specific commodities, technologies, and software controlled by the EAR."[255]

---

[247] PAUL K. KERR & CHRISTOPHER A. CASEY, CONG. RSCH. SERV., R46814, THE U.S. EXPORT CONTROL SYSTEM AND THE EXPORT CONTROL REFORM ACT OF 2018 (2021) [hereinafter CRS ECRA REPORT].

[248] *See, e.g.,* Trading with the Enemy Act, Pub. L. No. 65-91, 40 Stat. 411 (1917).

[249] CRS ECRA REPORT, *supra* note 247, at 4 (quoting Export Control Act of 1949, Pub. L. 81-11, 63 Stat. 7 (1949)).

[250] *Id.* Up until *ECRA*, all export control laws had an expiration date. For example, the Export Administrative Act of 1979, Pub. L. 96-72 (1979), expired in 2001. *Id.* at 5. However, Presidents continued to enforce this act under IEEPA until *ECRA* was enacted in 2018. *See, e.g.* Exec. Order No. 13,222, 66 Fed. Reg. 44,025 (Aug. 17, 2001). *See generally* Export Control Reform Act, 50 U.S.C. §§ 4801, 4811–4852.

[251] CRS ECRA REPORT, *supra* note 247, at 3, 16.

[252] *Id*. at 16.

[253] *See id*. at 17.

[254] 15 C.F.R. § 730.2.

[255] CRS ECRA REPORT, *supra* note 247, at 6.

"Nearly all U.S.-origin items are subject to the EAR."[256] Even when a good is subject to a license, it can either be shipped to a destination with no license required, or it may be eligible for a license exception where the exporter has to agree to certain terms or conditions to export.[257] In actuality, very few exports require a license and the exports that do require a license mostly get approved.[258]

ECRA is also far-reaching, affecting the "export, reexport, and in-country transfer of items subject to the jurisdiction of the United States, whether by United States persons or by foreign persons",[259] along with the "activities of United States persons, wherever located, relating to . . . nuclear explosive devices; . . . missiles; . . . chemical or biological weapons; . . . whole plants for chemical weapons and precursors; foreign maritime nuclear projects; and . . . foreign military, security, or intelligence services."[260] ECRA's extraterritoriality is unique because it applies not only to the export of U.S. goods to a foreign country, but also to the "reexport" of a U.S. good. A reexport is defined as "shipment or transmission of . . . [an] item from a foreign country to another foreign country," to include "release or transfer of technology or source code."[261] For example, if a good is exported to Germany and does not require a license, and then is "reexported" from Germany to Cuba, which does require an export license,[262] the original export would require a license because it is "reexported" to Cuba.[263] This is the same case for "in-country" transfers, where a good would be shipped to Germany and then transferred "in-country" from a German entity to a Cuban entity.[264] Export laws would also apply

[256] *Id.* at 17 (In 2019 "[a]pproximately 83.3% of U.S. exports (by value) were subject to the EAR." Licensing requirements are imposed on a much smaller number, only "13.7% of the value of U.S. exports (by value) fall on the [CCL] requiring a license to some destinations.").
[257] *Id.*
[258] *See id.* (Noting "[o]nly 0.4% of total exports valued at $6.3 billion required . . . an export license in 2019" and out of the licenses that are applied for, approximately 85% get approved).
[259] 50 U.S.C. § 4812(a)(1).
[260] 50 U.S.C.§ 4812(a)(2).
[261] 50 U.S.C. § 4801(9).
[262] *Id.*
[263] *See* 50 U.S.C. § 4801(a)(9).
[264] *See* 50 U.S.C. § 4801(6).

within the U.S., under a "deemed export"[265] as described in the EAR. Here, an entity within the U.S. (whether a foreign or U.S. entity), "releases" a controlled technology to a foreign person, which would be subject to the EAR and potentially require a license.[266] The governmental agency that oversees the CCL and EAR, states that "[t]ypical organizations using 'deemed' export licenses include universities, high technology research and development institutions, bio-chemical firms, as well as the medical and computer sectors."[267]

For a U.S. person, ECRA is far reaching because it allows the President to regulate activities of U.S. persons if they fall under at least one of the six categories of ECRA § 4812(a)(2). It is not difficult to draw a correlation between AI foundation models and these six categories because AI can facilitate and further chemical or biological weapons proliferation and foreign military, security, or intelligence activities, among other things. This is important because, if the President deems activity falls within one of the six categories, he or she can invoke *ECRA* § 4812(a)(2) and regulate, prohibit, or curtail a U.S. person's activities involving AI foundation models.

While not listed in *ECRA*, the Foreign Direct Product Rule ("FDPR") under the EAR expand export controls' scope even further.[268] The FDPR states:

> Foreign-produced items located outside the United States are subject to the EAR when they are a "direct product" of specified "technology" or "software," or are produced by a complete plant or 'major component' of a plant that itself is a "direct product" of specified "technology" or "software." If a foreign-produced item is subject to the EAR, then you should separately determine the license requirements that apply to that foreign-produced item.[269]

The FDPR is quite broad because if a direct U.S. export is a component, technology, or software that is used to make a foreign-

[265] 15 C.F.R. § 734.13(b).
[266] 15 C.F.R. § 734.13(a)(2).
[267] *See Deemed Exports*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports (last visited Apr. 21, 2025).
[268] 15 C.F.R. § 734.9.
[269] 15 C.F.R. § 734.9.

produced item subject to the EAR, then that component will fall under the same export and licensing scheme as if the exporter was exporting the foreign-product from the U.S.

The U.S. government's amended dual-use export controls covering AI applications in geospatial imagery can inform how ECRA, EAR, CCL, and the FDPR apply to AI foundation models.[270] In early 2020, the Bureau of Industry and Security ("BIS"), which enforces the EAR, [271] released an interim final rule implementing export restrictions on AI applications in geospatial imagery, adding in "software specially designed to automate the analysis of geospatial imagery."[272] This interim rule modified the EAR under 15 C.F.R. § 744 and updated the CCL, under Export Control Classification Number ("ECCN") 0Y521, "specifically under ECCN 0D521."[273] ECCN 05D21 "covers geospatial imagery software specially designed for training a Deep Convolutional Neural Network ("DCNN") to automate the analysis of geospatial imagery and point clouds."[274] EAR export controls are very technical because ECCNs are based on concise, technical information. ECCNs and their related controls can have major implications. Companies working on AI foundation models in image recognition now have to account for if their product falls under the ECCN 0D521 classification. An AI foundation model may also become a "component" under FDPR. If that occurred, the company must also monitor non-U.S. investments that may trigger mandatory filing requirements as a TID U.S. business under CFIUS.[275] As it relates to ECCN 0D521, "geospatial imagery software specially designed for training a Deep Convolutional Neural Networks to automate the

[270] Kara M. Bombach et al., *U.S. Export License Now Required for AI Software Related to Geospatial Imagery*, NAT'L L. REV. (Jan. 16, 2020), https://natlawreview.com/article/us-export-license-now-required-ai-software-related-to-geospatial-imagery.
[271] *See generally* 50 U.S.C. § 4813; *Bureau of Industry and Security*, BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM., https://www.bis.gov/ (last visited Apr. 21, 2025).
[272] Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521, 85 Fed. Reg. 459, 459 (Jan. 6, 2020).
[273] *Id*. at 460.
[274] Bombach et al., *supra* note 270.
[275] *See* 50 U.S.C. § 4565(a)(4)(iii).

analysis of geospatial imagery"[276] "has a crucial role in clearing the path ahead for autonomous vehicles."[277] With ECCN 0D521's new addition by the associated interim rule, carmakers like Tesla, which may be using AI systems to train self-driving cars, will have to use due diligence when considering exporting their vehicles or obtaining non-U.S. investment.

ECRA also requires the President to set up an interagency process to identify and license emerging and foundational technologies that are "essential to the national security of the United States" and are not covered as "critical technologies" under FIRRMA.[278] Per this requirement, BIS published an advanced notice of proposed rulemaking ("ANPRM") seeking "public comment on criteria for identifying emerging technologies that are essential to . . . U.S. national security."[279] Within this ANPRM, BIS specifically called out AI and ML as potential emerging technologies essential to national security.[280] Then, in 2020, BIS published a ANPRM for "foundational technologies."[281] This ANPRM did not mention categories of technology similar to the emerging technologies ANPRM.[282] BIS did, however, seek public guidance on the control of "foundational technologies," which it described as "those that may warrant stricter controls if a present or potential application or capability of that technology poses a national security threat to the United States."[283] So, BIS has clearly identified AI as an emerging technology but has not yet clearly identified it as a foundational technology. Neither types of technologies, emerging and foundational, have been defined.

[276] Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521, 85 Fed. Reg. at 460.
[277] *See Self-Driving Cars and the Role of GIS in Transportation's Future,* USCDORNSIFE (June 2, 2021), https://gis.usc.edu/blog/self-driving-cars-and-the-role-of-gis-in-future-transportation/.
[278] 50 U.S.C. § 4817(a)(1)(A).
[279] Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201, 58,201 (Nov. 19, 2018).
[280] *Id.* at 58,202.
[281] *See generally* Identification and Review of Controls for Certain Foundational Technologies, 85 Fed. Reg. 52,934 (Aug. 27, 2020).
[282] *See id.*
[283] *Id.* at 52,934.

Despite the lack of definitions, BIS had, by 2022, established thirty-eight emerging technologies, each as a modified, subparagraph, or a new ECCN.[284] Most of the ECCNs were established through the Wassenaar Agreement or the Australia Group, which is one of the other multilateral export regimes.[285] Many of the ECCNs correlate to AI foundation models, including ECCNs for software to be used by law enforcement to analyze communications, to circumvent authentication or authorization mechanisms, to extract raw data, and in geospatial imagery.[286] While other published emerging technologies may not utilize AI directly in the items listed on the ECCN, AI may still be used under the FDPR, causing exporters concern regarding how foreign entities might use their AI foundation models.[287]

While identifying thirty-eight emerging technologies ECCNs is a step in the right direction, some believe it is not enough. In June 2021, the U.S.-China Economic and Security Review Commission issued a congressional advisory criticizing the lack of speed in BIS defining emerging and foundational technologies.[288] This advisory stated that Department of Commerce ("DoC") had failed in its

[284] TONGELE N. TONGELE, U.S. DEP'T OF COM., EMERGING AND FOUNDATIONAL TECHNOLOGY CONTROLS 23 (2022), https://researchservices.upenn.edu/wp-content/uploads/2022/04/Emerging-and-Foundational-tech.pdf.
[285] *See id.* at 10.
[286] *See* Implementation of Certain New Controls on Emerging Technologies Agreed at Wassenaar Arrangement 2019 Plenary, 85 Fed. Reg. 62,583, 62,584 (Oct. 5, 2020) (to be codified at 15 C.F.R. pts. 740, 772, 774) (ECCNs 5D001, 5A004, 5D002, and 5E002); Addition of Software Specially Designed to Automate the Analysis of Geospatial Imagery to the Export Control Classification Number 0Y521, 85 Fed. Reg. 459, 459 (Jan. 6, 2020).
[287] *See, e.g., BIS Accounces New Regulatory Framework for AI and Controls on Advanced Computing Technology and AI Models*, WILEY (Jan. 17, 2025), https://www.wiley.law/alert-BIS-Announces-New-Regulatory-Framework-for-AI-and-Controls-on-Advanced-Computing-Technology-and-AI-Models (describing concerns of U.S. allies and AI industry leaders in the U.S. "that the new rules may weaken global competitiveness and undermine AI innovation.").
[288] *See* EMMA RAFAELOF, UNFINISHED BUSINESS: EXPORT CONTROL AND FOREIGN INVESTMENT REFORMS 4-6 (U.S.-China Econ. & Sec. Rev. Comm'n, 2021). *See generally* Section 1758 Technology Export Controls on Instruments for the Automated Chemical Synthesis of Peptides, 88 Fed. Reg. 24,341 (proposed Apr. 20, 2023) (to be codified at 15 C.F.R. pt. 774) (Section 1758 technologies are interchangeable with foundational and emerging technologies because, originally, foundational and emerging technologies were found in § 1758 of the code).

responsibilities to publish a list of 1758 technologies,[289] which impedes CFIUS's ability to review such technologies and causes additional national security risks.[290] Following this advisory, five Senators sent a letter to the Secretary of Commerce in late November, 2021, urging BIS to define 1758 technologies. Specifically, the senators stated that "the Office of the Director of National Intelligence (ODNI) recently identified five technology areas key to America's strategic competition with China: artificial intelligence (AI), quantum computing, semiconductors, biotechnology, and autonomous systems."[291] The letter noted how "only eight percent of the 273 companies" supplying AI equipment to the People's Liberation Army are on the Entity List ("EL") and the "remaining [ninety-two percent] of Chinese AI companies are free to purchase key U.S. technology for use in military applications."[292] These numbers are quite concerning. They indicate that the U.S. has a robust system to prohibit the export of AI foundation models to state and non-state actors, but that enforcement is starkly lacking, even in the face of the national security risks these models pose.

ECRA and the EAR determine licensing requirements and prohibitions based upon "end-use" and "end-user."[293] This means certain uses of ECCNs on the EAR, such as general microprocessors used for military weapons, are prohibited.[294] End-users, like certain

[289] Emerging and foundational technologies are also referred to as 1758 technologies because they originally fell under 1758 of the 2018 version of the *ECRA*. *See BIS's New Approach to Identifying "Emerging and Foundational Technologies,"* TORRES TRADE L. (July 1, 2022), https://www.torrestradelaw.com/posts/BIS%E2%80%99s-New-Approach-to-Identifying-%E2%80%9CEmerging-and-Foundational-Technologies%E2%80%9D/285. *See generally* 50 U.S.C. § 1758 (2018).
[290] RAFAELOF, *supra* note 288, at 1.
[291] *See* Letter from Tom Cotton, U.S. Sen., to Gina Raimondo, Sec'y, U.S. Dep't Com. (Nov. 15, 2021), https://www.cotton.senate.gov/imo/media/doc/commerce_bis_letter.pdf.
[292] *Id*. at 1.
[293] *See generally* 15 C.F.R. § 744 (2024); 50 U.S.C. §§ 4801-4852.
[294] *See* 15 C.F.R. §§ 736, 744.17 (2024); *see also* 15 C.F.R. § 744 (2003) ("Examples of military end-uses (as described in § 744.17 (d) of this part) of general-purpose microprocessors classified as ECCN 3A991.a.1 includes employing such microprocessors in the 'use', 'development', 'production', or deployment of: (1) Cruise missiles; (2) Electronic suites of military aircraft and helicopters; (3) Radar for searching, targeting, or tracking systems; (4)

foreign adversaries, would require a license and are most likely prohibited from export.[295]

The EAR also lists foreign entities—government, business, or person—that are subject to specific licensing requirements in what is known as the Entity List ("EL").[296] For example, BIS added an additional 68 non-U.S. Huawei affiliates on August 20, 2020, to the EL as Huawei posed significant risks to national security or foreign policy after allegations of criminal violations of U.S. law.[297] While those on the EL require a license for specific items on the CCL, most additions to the EL have a license review policy of "presumption of denial".[298] A recent NPRM aims to expand restrictions on military and intelligence end-use and end-users and implement control over activities by U.S. persons supporting certain foreign military and intelligence entities, an ECRA authority that Congress expanded in the 2022 NDAA.[299]

While BIS has left 1758 technologies undefined, one of the avenues the EAR can potentially obtain export controls over AI foundation models is through ECCN 4D993, which includes "software" allowing the automatic generation of "source codes" or through ECCN 4A004 and its subsequent FDPR, which establishes control over "neural computers" that "are computational devices designed or modified to mimic the behaviour of a neuron or a

Command/control/communications or navigation systems; (5) Unmanned aerial vehicles capable of performing military reconnaissance, surveillance, or combat support; (6) Rocket or missile systems; (7) Electronic or information warfare systems; or (8) Intelligence, reconnaissance, or surveillance systems suitable for supporting military operations.").

[295] *See* 15 C.F.R. § 744 (2021) (subjecting software that can generate its own source code to Military End User License Requirement); 15 C.F.R. § 744 (2024); *see also* 15 C.F.R. § 736 (2024).

[296] 15 C.F.R. § 744 (2025).

[297] *See generally* Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule), 85 Fed. Reg. 51,596 (Aug. 20, 2020) (to be codified 15 C.F.R. pts. 736, 744, 762).

[298] *See id.* at 51,597.

[299] *See* End-Use and End-User Based Export Controls, Including U.S. Persons Activities Controls: Military and Intelligence End Uses and End Users, 89 Fed. Reg. 60,985, 60,986 (Jul. 29, 2024).

collection of neurons."[300] While ECCN 4D993 does not have any country listed as requiring a license under anti-terrorism, ECCN 4A004 requires a license for all countries for reasons of national security or country groups D:1, 4, and 5, for regional stability reasons, although an exception can be made for notified advanced computing.[301] Under ECCN 4A004, China and Russia among other foreign adversaries fall under the licensing requirement, allowing BIS to prohibit the exportation of AI foundation models to foreign state adversaries if it falls under the FDPR.[302] While ECCN 4D993 does not have a licensing requirement listed directly within the CCL, if an entity is added to the EL, then any exportation of ECCN 4D993, or other items on the CCL, would be met with a license requirement and a presumption of denial.

Because AI foundation models use ML that writes its own source code,[303] presumably any entity added to the EL would be barred from these software and algorithms. Through the EAR and CCL prohibitions and adding entities to the EL, the U.S. can prohibit transactions of AI foundation models to both known state actors and non-state actors through export.[304] While the U.S. does an excellent job prohibiting the hardware that provides the computing power necessary to run AI foundation models, the U.S. is not as restrictive with the software and algorithms necessary to run AI foundation

[300] 15 C.F.R. § 744 (2003).
[301] 15 C.F.R. §§ 738 (2024), 740 (1996), 744 (2003).
[302] 15 C.F.R. §§ 738 (2024), 740 (1996), 744 (2003).
[303] *See* Chizaram Ken, *What is AI Code Generation and How Does it Work?,* LogRocket (Apr. 10, 2025), https://blog.logrocket.com/ai-code-generation/#what-is-ai-code-generation.
[304] *See, e.g.*, Karen Freifeld & Doina Chiacu, *Chinese Firms Helping Military Get AI Chips Added to US Export Blacklist*, REUTERS (Apr. 11, 2024, 4:14 AM), https://www.reuters.com/business/us-restricts-trade-with-11-entities-russia-china-uae-government-notice-says-2024-04-10/ (discussing how four Chinese firms are added to the EL as they were used to circumvent *ECRA* in an attempt to get AI chips for the Chinse military); *see also* Emily S. Weinstein & Kevin Wolf, *For Export Controls on AI, Don't Forget the "Catch-All" Basics*, CENTER FOR SEC. AND EMERGING TECH. (Jul. 5, 2023), https://cset.georgetown.edu/article/dont-forget-the-catch-all-basics-ai-export-controls/ (discussing how the United States is able to prohibit exportation of AI algorithms and software).

models.[305] The most likely reason why AI foundation model software is not prohibited is because much of this code is available through Open Source, which does not involve a transaction.[306] ECRA not only contemplates restriction of exports based on national security risks and foreign policy, but also the effects prohibition would have on global access.[307] So, practically speaking, a ban on exporting open-source software would have a minimal effect on access to that software.[308]

3. International Emergency Economic Powers Act

While FIRRMA and *ECRA* are excellent controls on investment risks involving AI foundation models, the President has another mechanism to institute investment controls. The 1977 International Emergency Economic Powers Act ("IEEPA") gives the President broad powers to regulate, license, investigate, prevent, or prohibit a foreign transaction subject to U.S. jurisdiction when the President declares a national emergency for any "unusual and extraordinary threat."[309] As of March 2022, "[p]residents had declared 67 national emergencies invoking IEEPA, 37 of which are still ongoing."[310] EO 13873, Securing the Information and

[305] Of note, BIS released an interim final rule on January 13, 2025, adding a new control on AI model weights for certain advanced closed-weight dual-use AI models. While this is a step in the right direction in regulating AI, this policy does not regulate open-sourced AI models, to include open-sourced AI foundational models. *See* 80 Fed. Reg. 4,544, 4,554 (Jan. 15, 2025) (discussing new export control); Michael C. Horowitz, *What to Know About the New U.S. AI Diffusion Policy and Export Controls*, COUNCIL ON FOREIGN RELS. (Jan. 13, 2025 3:19 PM), https://www.cfr.org/blog/what-know-about-new-us-ai-diffusion-policy-and-export-controls ("Finally, the policy does not control open-source models. Instead, state of the art open-source models will serve as the basis of future determinations regarding the scale of closed-weight models the policy regulates. Once a good open-source model exists at a certain computational level, controls on the model and weights will no longer succeed. So as open-source models improve, more powerful close-weight AI models will be available without restrictions.").

[306] *See* Susnjara & Smalley, *supra* note 26.

[307] *See generally* CRS ECRA REPORT, *supra* note 247.

[308] *See* Horowitz, *supra* note 305.

[309] *See* International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1702.

[310] CHRISTOPHER A. CASEY & JENNIFER K. ELSEA, CONG. RSCH. SERV., R45618, THE INTERNATIONAL EMERGENCY ECONOMIC POWERS ACT: ORIGINS, EVOLUTION, AND USE (2022).

Communications Technology and Services Supply Chain, invokes IEEPA and forbids transactions through DoC.[311] These transactions involve information and communications technologies or services by foreign adversaries that pose undue risk of sabotage or subversion, "catastrophic effects on the security or resiliency of [U.S.] critical infrastructure," or the national security of the U.S.[312] Per this EO, the DoC published regulations that expanded inbound investment principles, forbidding access to information and communications technology or services—including those that may fall within the AI foundation model scope—when unacceptable risk exists with foreign adversaries.[313]

IEEPA was also invoked in 2023 to enact EO 14105, "Addressing United States Investments in Certain National Security Technologies and Products in Countries of Concern", which some call an "Outbound CFIUS" regime.[314] This EO addresses the threats to the U.S. posed by certain countries of concern that seek to develop and exploit sensitive or advanced technologies or products critical to military, intelligence, surveillance, or cyber-enabled capabilities.[315] This EO is meant to fill the gap involving outbound investment created by ECRA. EO 14105 regulates exports of AI foundation models to state and non-state actors[316] but does not regulate financial investment by a U.S. entity into an overseas foreign entity that may produce an AI foundation model.

The EO directs the Department of Treasury ("DoT") to establish a program to prohibit or require notification of certain types of outbound investments to China, specifically three categories of national security technologies—semiconductors and microelectronics, quantum information technologies, and AI.[317] DoT's 2024 final rule sets forth regulations that require either U.S.

[311] *See* Exec. Order No. 13,873, 84 Fed. Reg. 22,689, 22,689-90 (May 15, 2019).
[312] *See id.*
[313] *See* 15 C.F.R. § 791.4 (2024) (specifying the following foreign adversaries: China, Cuba, Iran, North Korea, Russia, and the Venezuelan Maduro Regime.
[314] *See* Exec. Order No. 14,105, 88 Fed. Reg. 54,867 (Aug. 9, 2023).
[315] *See* Exec. Order No. 14,105;88 Fed. Reg. at 54,867. 54,872.
[316] *See generally id.* at 54,869-70.
[317] *Id.* at 54,868, 54,870.

persons (including foreigners within the U.S.) to notify DoT of such transactions, or authorizes DoT to prohibit a transaction.[318] Of note, the final rule expands the scope of covered investments of AI systems to include technical specifications and establishes the Office of Global Transactions within the Office of Investment Security, which is a part of DoT, to manage the program established under 31 C.F.R. § 850.[319] In the preceding NPRM, DoT notes that it is concerned with "AI systems that enable the military modernization of countries of concern—including weapons, intelligence, and surveillance capabilities—including those that have applications in areas such as cybersecurity and robotics."[320]

Like *CFIUS*, EO 14105 defines both a "covered foreign person" and a "covered investment;" however, unlike *CFIUS*, EO 14105 also covers greenfield and brownfield[321] investments.[322] The EO covers "[n]otifiable transaction[s]" involving AI models:

(1) A "covered transaction . . . in which the relevant covered foreign person"

(2) "[d]evelops any AI system that is not described" as a prohibited transaction

[318] Provisions Pertaining to U.S. Investments in Certain Security Technologies and Products in Countries of Concern, 89 Fed. Reg. 90,398,90,399 (Nov. 15, 2024).
[319] *See generally* OFF. OF INV. SEC., U.S. DEP'T OF TREASURY, ADDITIONAL INFORMATION ON FINAL REGULATIONS IMPLEMENTING OUTBOUND INVESTMENT EXECUTIVE ORDER (E.O. 14105) (2024);Press Release, U.S. Dep't of the Treasury, Treasury Issues Regulations to Implement Executive Order Addressing U.S. Investments in Certain National Security Technologies and Products in Countries of Concern (Oct. 28, 2024); *see also* 31 C.F.R. § 850 (2024).
[320] 31 C.F.R. § 850.202 (2024).
[321] "In economics, a brownfield investment (BI) is a type of foreign direct investment (FDI) where a company invests in an existing facility to start its operations in the foreign country. In other words, a brownfield investment is the lease or purchase of a pre-existing facility in a foreign country." *Brownfield Investment*, CFI, https://corporatefinanceinstitute.com/resources/management/brownfield-investment (last visited Apr. 21, 2025).
[322] *See* Provisions Pertaining to U.S. Investments in Certain Security Technologies and Products in Countries of Concern, 89 Fed. Reg. at 90,415, 90,418, 90,422.

(3) that is "[d]esigned to be used for any military end use;" and

(4) intended for "[c]ybersecurity applications," "digital forensic tools," "penetration testing tools," "control of robotic systems;" or "[t]rained using a quantity of computing power greater than 10^23 computational operations."[323]

"Prohibited transaction[s]" under 31 C.F.R. § 850.224 include "a covered transaction in which the relevant covered foreign person . . . [d]evelops any AI system that is" either (1) intended for or "designed to be exclusively used for" military or "government intelligence or mass-surveillance end use" or (2) "trained using a quantity of computing power" that exceeds "10^25 computational operations" or "10^24 computational operations [if] using primarily biological sequence data."[324]

While chaired by the DoT, the committee established by EO 14105 includes "Departments of State, Defense, Justice, Commerce, Energy, and Homeland Security, the Office of the United States Trade Representative, the Office of Science and Technology Policy, the Office of the Director of National Intelligence, the Office of the National Cyber Director" and others when appropriate.[325] Ten excepted transactions are provided by 31 C.F.R. § 850 and are not considered covered transactions, including a national interest catch-all exception.[326] Like CFIUS, 31 C.F.R. § 850 provides procedures for notification, penalties like fines and imprisonment, and a confidentiality provision.[327] While a final rule has been published and went into effect on January 2, 2025, its efficacy is yet to be seen.[328]

B. *AI and Other Legal Methods of Control*

While inbound and outbound investment in AI foundation models in the U.S. is expansive, there is a gap in federal legislation

[323] 31. C.F.R. § 850.217.
[324] 31 C.F.R. § 850.224.
[325] 31 C.F.R. § 850.226.
[326] 31 C.F.R. §§ 850.501-.502.
[327] 31 C.F.R. §§ 850.401-.406, 850.601-704, 850.801.
[328] Provisions Pertaining to U.S. Investments in Certain Security Technologies and Products in Countries of Concern, 89 Fed. Reg. 90,398, 90,398 (Nov. 15, 2024).

when it comes to investment in AI within the bounds of the U.S. that does not involve a transaction with a foreign entity.[329] While Congress has proposed the National AI Initiative Act of 2020, which calls for a coordinated program across the entire federal government to accelerate AI research and application for the Nation's economic prosperity and national security, this act does not directly address the national security risks AI foundation models pose.[330] In 2024, thirty-one states and two territories adopted resolutions or enacted legislation for AI.[331] None of these resolutions or enacted legislation specifically protect against national security threats from state or non-state actors.

While Congress has not passed a comprehensive law, former President Biden issued EO 14110 in 2023, building upon President Trump's prior EOs 13859 and 13960.[332] The EO required that companies developing, or intending to develop, dual-use AI foundation models report on model training, testing, and data ownership, and "entities that acquire, develop, or possess" large computing infrastructure to report the location and amount of computing power to the U.S. government under the DPA.[333] BIS was tasked with providing the technical standards for the minimal computational threshold that would require reporting, which it provided in a 2024 NPRM, although no final rule was established.[334]

---

[329] *See generally,* Hope Anderson et al., *AI Watch: Global Regulatory Tracker – United States*, JDSUPRA (Dec. 20, 2024) (tracking existing AI-related laws and regulations).

[330] *See generally* National Artificial Intelligence Initiative Act of 2020, H.R. 6216, 116th Cong. (2020).

[331] For example, Colorado enacted "comprehensive AI legislation requiring developers and deployers of high-risk AI systems to use reasonable care to avoid algorithmic discrimination and requir[ing] . . . disclosures to consumers." *Artificial Intelligence 2024*, NAT'L CONF. OF STATE LEGISLATURES (Sept. 9, 2024), https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation.

[332] *See* Exec. Order 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023); Exec. Order 13,859, 84 Fed. Reg. 3967 (Feb. 11, 2019); Exec. Order 13960, 85 Fed. Reg. 78,939 (Dec. 3, 2020).

[333] Exec. Order No. 14110, 88 Fed. Reg. at 75197.

[334] *See id.* at 75,191.BIS suggested the following technical standards in addition to those in EO 14110:

But in 2025, President Trump revoked EO 14110 along with seventy-seven other EO's, stating they "embedded deeply unpopular, inflationary, illegal, and radical practices" and improper "'diversity equity, and inclusion'".[335] Following this revocation, President Trump issued EO 14179, "Removing Barriers to American Leadership in Artificial Intelligence", which required a new working group to provide the President with an action plan within 180 days "to sustain and enhance America's global AI dominance in order to promote human flourishing, economic competitiveness, and national security."[336] With the revocation of EO 14110 and publication of EO 14179, the U.S.'s ability to track dual-use foundation models is fettered until a new EO is published. It is unclear whether NTIA's report on the risks, benefits, and policy and regulatory mechanisms applicable to dual-use foundation models will be rescinded or revised under the new EO because the EO requires the SoC to "identify any actions taken

"A dual-use foundation model training run triggers reporting requirements if it utilizes more than 10^26 computational operations (e.g., integer or floating-point operations). Models trained on primarily biological sequence data, but at the lower threshold of 10^23 computational operations, as specified by section 4.2(b) of E.O. 14110, will be addressed in a separate survey.

Large-scale computing clusters are defined as clusters having a set of machines transitively connected by networking of over 300 Gbit/s and having a theoretical maximum performance greater than 10^20 computational operations (e.g., integer or floating-point operations) per second (OP/s) for AI training, without sparsity."

Establishment of Reporting Requirements for the Development of Advanced Artificial Intelligence Models and Computing Clusters, 89 Fed. Reg. 73612, 73615 (proposed Sept. 11, 2024) (to be codified at 15 C.F.R. § 702). These standards were proposed in addition to those in EO 14110, which provided other safeguards such as reporting when foreign persons use cloud services to train AI systems, evaluate and assess potential risks related to critical infrastructure adoption and use of AI, best practices for financial sectors to manage AI-specific cybersecurity risks, incorporating an AI Risk Management Framework into critical infrastructure owner and operators, developing advanced cybersecurity program to develop AI tools, evaluating potential for AI to be used for CBRN threats, and detecting AI-created synthetic media. *See generally* Exec. Order 14,110, 88 Fed. Reg. 75191.

[335] Exec. Order 14,148, 90 Fed. Reg. 8237, 8237 (Jan. 28, 2025).

[336] Exec. Order 14,179, 90 Fed. Reg. 8741, 8741 (Jan. 31, 2025).

pursuant to Executive Order 14110 that are or may be inconsistent with, or present obstacles to, the [new EO's] policy."[337]

C. *What Remains Unregulated*

While CFIUS, ECRA, IEEPA, and EO 14105 are powerful tools for mitigating the national security risks associated with AI foundation models, there are still national security risks that remain unregulated. The current frameworks prohibit certain outbound transactions, but they do not mitigate the risk of U.S. entities allowing state or non-state actors to use AI foundation models without an investment or transaction. While the U.S. can control state and non-state actors' access to AI foundation models through inbound and outbound investments, these regulatory schemes do not address the Open Source culture behind software and algorithmic development that has led to AI foundation models.

For example, Hugging Face (headquartered in NYC) is "the leading open platform of AI builders" and maintains open-source libraries that include transformers for individuals to publish models and collaborate.[338] If a company that is already on the EL, like Huawei, wished to download a Hugging Face Transformer to build an AI foundation model, CFIUS, ECRA, and IEEPA would not prohibit this. A scenario akin to this has already occurred with the Chinese firm Pythium, which was added to the EL in April 2021, "for the firm's role in China's hypersonic weapons program."[339] After Pythium was added to the EL, BIS was unable to "restrict Pythium's and other PRC firms' use of U.S. open source technology platforms and U.S. software tools to design and test advanced chips for China's strategic advanced computing programs."[340] Allowing this area to remain unregulated poses major risks associated with state and non-state foreign adversaries building and obtaining AI foundation models using open-source software. Advocates both in the public and private sectors have

---

[337] *Id.* at 8741; *see generally* NTIA REPORT, *supra* note 68.
[338] *Hugging Face is the Leading Open Platform for AI Builders*, BUILT IN NYC, https://www.builtinnyc.com/company/hugging-face (last visited Apr. 21, 2025).
[339] KAREN M. SUTTER & CHRISTOPHER A. CASEY, CONG. RSCH. SERV., IF 11627, U.S. EXPORT CONTROLS AND CHINA 2 (2022).
[340] *Id.*

urged regulators to step in.[341] Thus, the question is not *whether* AI should be regulated outside of the inbound and outbound foreign investment scheme, but *how* it should be regulated.

III. RECOMMENDATIONS FOR REGULATING AI: A CAREFUL BALANCE

While the U.S.'s current inbound and outbound investment regulatory scheme does a good job in mitigating national security risks that arise from foreign investment in U.S.-based AI companies, Congress can improve this regulatory framework by defining "foundational" and "emerging" technology under *ECRA* and expanding *CFIUS* jurisdiction to include greenfields and brownfields for "emerging" technology. Congress should also regulate AI foundation models through an AI Agency and create an inter-governmental AI Committee to determine on a sliding scale how open- or closed-source new AI foundation models should be.

A. *Inbound and Outbound Investment Regulations*

While the U.S. has done an excellent job in the past six years establishing the mechanisms to regulate AI through CFIUS, ECRA, and IEEPA, there remains a critical gap in the protections the current framework offers. DoC must define "foundational and emerging technologies" because the lack of definitions is a critical vulnerability to both inbound CFIUS transactions and outbound ECRA exports.

While BIS has been the lead agency on defining foundational and emerging technologies, the Emerging Technology and Research Advisory Committee ("ETRAC") under 50 U.S.C. § 4817(f) should be realigned to the National Institute of Standards and Technology ("NIST") for the limited role of defining these technologies under ECRA.[342] NIST is the "lead national laboratory for providing the measurements, calibrations, and quality assurance techniques which underpin United States commerce, technological progress, improved

[341] *See* Blair Levin & Larry Downes, *Who Is Going to Regulate AI?*, HARV. BUS. REV. (May 19, 2023), https://hbr.org/2023/05/who-is-going-to-regulate-ai.
[342] *See* 50 U.S.C. § 4817(f).

product reliability and manufacturing processes, and public safety."[343] NIST routinely cooperates with the industry to "overcome technical barriers to commercialization of emerging technologies."[344] Because NIST already has the technical expertise to understand emerging technologies, NIST is in the best position to identify these technologies as they develop.

AI advancement has been increasing at an accelerated pace, and with NIST at the forefront of technology and innovation, NIST is better positioned to keep pace than BIS. NIST's focus on technical standards would also help it identify foundational technologies that arise and the associated national security risks. So, NIST should develop an emerging and foundational technology list ("EFL") to supplement the CCL. With NIST developing an EFL, AI foundation models and future AI could be better regulated through inbound CFIUS and outbound ECRA mechanisms. BIS should publish the new EFL through interim final rules or use the "good cause" exception clause under the Administrative Procedures Act ("APA") to publish a final rule without publishing a proposed rule. The APA "good cause" exception should apply because the notice-and-comment process for cutting-edge technology would be "impracticable, unnecessary, or contrary to the public interest."[345] The latter avenue would likely be better because it would allow BIS to update the EFL at a pace that could match swift changes in technology. Congress should do what it can to allow NIST to define 1758 technologies as quickly as possible because "AI is becoming more powerful and radically cheaper by the month—what was computationally impossible, or would cost tens of millions of dollars a few years ago, is now widespread."[346]

Congress should also require NIST to review the EFL on an ongoing basis as "emerging" technologies fall off the list or become foundational, and current "foundational" technologies become obsolete. AI will continue to evolve as AI foundation models are initially classified as emerging, followed by foundational, as AI

[343] 15 U.S.C. § 271(b)(1).
[344] EMILY G. BLEVINS., CONG. RSCH. SERV., R43908, THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY: AN APPROPRIATIONS OVERVIEW 1 (Sept. 26, 2022).
[345] 5 U.S.C. § 553(b)(4)(B).
[346] Suleyman, *supra* note 63.

foundation models become more of the societal norm. AI foundation models may become so commonplace in the future that they will not be considered critical, emerging, or foundational at all, a trajectory that might mirror modern smartphone technology. Congress, therefore, should facilitate continuous review and boost spending and support to ETRAC because the 2020 ETRAC charter only provides an annual operating cost of $37,861 and an "estimated 0.3 person-year of staff support."[347] The lack of support for ETRAC is concerning, especially with the stock the U.S. puts into its technological dominance as a reason for its national power.[348] Congress should sufficiently invest in ETRAC so it can keep the EFL current with evolving cutting-edge technology like AI foundation models.

ECRA and EO 14105 already contemplate greenfields and brownfields, regulating outbound investment into start-up AI companies that may act as shell companies for state or non-state foreign adversaries. CFIUS should add greenfields and brownfields as a covered entity and include "emerging" technology as a covered transaction. CFIUS's ability to review greenfields and brownfields in "emerging" technologies is important because of the exponential growth that has occurred in the AI economy. In 2022, the AI market was worth $86.9 billion, and its estimated 2027 worth is $470 billion.[349] From 2013 until 2023, 5,509 AI startup companies launched in the U.S., and this number is expected to grow.[350] Under the current regime, any foreign transaction in an U.S.-based AI startup would not be a covered by CFIUS unless Congress were to expand the scope of

[347] *See* BUREAU OF INDUS. & SEC., U.S. DEP'T OF COM. EMERGING TECHNOLOGY TECH. ADVISORY COMM., CHARTER ¶ 7 (2020).
[348] *See* James Andrew Lewis, *Technology and the Shifting Balance of Power*, CTR. FOR STRAT. & INT'L STUD. (Apr. 19, 2022), https://www.csis.org/analysis/technology-and-shifting-balance-power.
[349] Benjamin Stratton, *AI Industry Growth Statistics: Exploring Key Metrics Driving Growth of AI (Updated for 2025)*, BLUE TREE, https://bluetree.digital/ai-industry-growth-metrics/#:~:text=The%20AI%20market%20is%20expected,%2486.9%20billion%20revenue%20in%202022 (last visited Apr. 17, 2025).
[350] Marcus Lu, *Mapped: The Number of AI Startups by Country*, VISUAL CAPITALIST (May 6, 2024), https://www.visualcapitalist.com/mapped-the-number-of-ai-startups-by-country/.

FIRRMA to include covered transactions in greenfield or brownfield investments.

As with any regulation, there are both positive and negative effects of expanding the scope of FIRRMA. Reviewing greenfield investments would raise the barrier to entry for foreign investment and would cause investors to look elsewhere. This negative effect, however, would be far outweighed by ensuring the U.S. reviews investments in "emerging" technology to protect against technology theft and promote U.S. technological dominance. Additionally, focusing on reviewing greenfield and brownfield "emerging" technology as listed in the EFL would minimize negative effects on foreign investment compared to a blanket greenfield and brownfield review of all investment within the U.S. Currently, if a foreign adversary were to invest in a startup that builds an AI foundation model and the company grew to be as prominent as OpenAI, CFIUS would not be able to review the transaction even if the company was controlled by the foreign adversary. By allowing CFIUS to review greenfield and brownfield investments in "emerging" technology, CFIUS and the President can mitigate potential national security risks by stopping the initial covered transaction.

B. *Federally Regulate AI Foundation Models*

While regulation could stifle innovation, open-source AI software carries national security risks and should be regulated. The question becomes how to balance national security risk mitigation while not threatening U.S. AI technological supremacy. "In an open global economy, countries may confront a trade-off between competitiveness of domestic firms and the stringency of domestic rules . . . [as] tight rules make production more expensive."[351] In other words, there is a direct correlation between regulatory stringency and economic competitiveness.[352] The European Union ("EU") for example, has implemented a comprehensive law regulating AI

[351] DANIEL MÜGGE, Regulatory Interdependence in AI, *in* HANDBOOK ON PUBLIC POLICY AND ARTIFICIAL 250 (Regine Paul, Emma Carmel, & Jennifer Cobbe eds., 2024).
[352] *See id.* at 252.

through the AI Act.[353] While the AI Act is quite thorough in addressing risks as it relates to EU citizens, there have been many concerns that it stifles innovation.[354]

Even still, many of the leaders in AI technology have embraced the idea of regulating AI. Sundar Pichai, Google's CEO, stated "AI is too important not to regulate and too important not to regulate well."[355] Sam Altman, OpenAI's CEO, stated the government should form "a new agency that licenses any effort above a certain scale of capabilities and could take that license away and ensure compliance with safety standards."[356] Tom Wheeler, former Chairman of the Federal Communications Commission, illustrates why licensing may not be the answer as "a license is inherently an anti-competitive, anti-innovative vehicle for incumbent enrichment."[357] Mr. Wheeler states:

> As a regulatory tool . . . licensing turned out to be a blunt instrument that prioritized the rights of licensees, as opposed to providing a tool for meaningful oversight of their behavior . . . The federal licensing activity I witnessed was anti-competitive because only the chosen could participate, anti-innovative because of the lack of competition,

[353] *See* Regulation 2024/1689 (EU) (regulation of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence and amending, Regulation 300/2008 (EU), Regulation 167/2013 (EU), Regulation 168/2013 (EU), Regulation 2018/858 (EU), Regulation 2018/1139 (EU), Regulation 2019/2144 (EU), Council Directive 2014/90/EU, Council Directive 2016/797 (EU), and Council Directive 2020/1828 (EU) (Artificial Intelligence Act).

[354] *See, e.g.*, Pascale Davies, *'Potentially Disastrous' for Innovation: Tech Sector Reacts to the EU AI Act Saying It Goes Too Far*, EURO NEWS (Dec. 15, 2024), https://www.euronews.com/next/2023/12/15/potentially-disastrous-for-innovation-tech-sector-says-eu-ai-act-goes-too-far; Daniel Castro, *The EU's AI Act Creates Regulatory Complexity for Open-Source AI*, CTR. FOR DATA INNOVATION (Mar. 4, 2024), https://datainnovation.org/2024/03/the-eus-ai-act-creates-regulatory-complexity-for-open-source-ai/; Javier Espinoza & Leila Abboud, *EU's New AI Act Risks Hampering Innovation, Warns Emmanuel Macron*, FIN. TIMES (Dec. 11, 2023), https://www.ft.com/content/9339d104-7b0c-42b8-9316-72226dd4e4c0.

[355] Tom Wheeler, *Licensing AI Is Not the answer – But It Contains the Answers*, BROOKINGS (Feb. 12, 2024), https://www.brookings.edu/articles/licensing-ai-is-not-the-answer-but-it-contains-the-answers/ (internal quotations omitted).

[356] *Id.* (internal quotations omitted).

[357] *Id.*

> and incumbent-enriching through the creation of quasi-monopolies.[358]

A licensing structure for AI foundation models could lead to the downfall of U.S. AI technological supremacy. While a license would be an easy way to control access of AI foundation models by state and non-state foreign adversaries, it would push the U.S. too far into regulation stringency, making innovation suffer. While companies like OpenAI and some members of Congress advocate for AI model regulation,[359] any regulatory consideration must also consider the negative consequences of limiting public access to AI models.

The regulation of AI foundation models will unavoidably suppress some of the benefits of open-source AI models, but the national security risks associated with a completely unregulated system outweigh the costs. Take China as an example risk vector. The New York Times published an article in July 2024 that discussed how Chinese AI systems are now "catching up" to U.S. AI systems.[360] While the U.S. has limited China's access to AI chips, China has been able to fix the hardware deficit by leveraging open-source AI software from the U.S.[361] The New York Times reported that "a dozen technologists and researchers at Chinese tech companies said open-source technologies were a key reason that China's A.I. development has advanced so quickly."[362] Indeed, on January 20, 2025, a small lab in China released DeepSeek, an advanced AI assistant to rival LLM's like ChatGPT.[363] DeepSeek's version 3 allegedly took only two months to

---

[358] *Id.*

[359] *See* Cecilia Kang, *OpenAI's Sam Altman Urges A.I. Regulation in Senate Hearing*, N.Y. TIMES (May 16, 2023), https://www.nytimes.com/2023/05/16/technology/openai-altman-artificial-intelligence-regulation.html.

[360] Meaghan Tobin & Cade Metz, *China Is Closing the A.I. Gap With the United States*, N.Y. TIMES (July 25, 2024), https://www.nytimes.com/2024/07/25/technology/china-open-source-ai.html.

[361] Angela Yang & Jasmine Cui, *A New AI Assistant from China Has Silicon Valley Talking*, NBC NEWS (Jan. 27, 2025), https://www.nbcnews.com/tech/tech-news/china-ai-assistant-deepseek-rcna189385.

[362] Tobin & Metz, *supra* note 360.

[363] Kelly Ng. et al., *DeepSeek: The Chinese AI App That Has the World Talking*, BBC (Jan. 28, 2025), https://www.bbc.com/news/articles/c5yv5976z9po.

develop and $6 million to build while U.S. technology companies have invested billions of dollars into AI technology.[364] Meta's Chief AI Scientist, Yann LeCun, commented on DeepSeek, stating it was clear evidence that "open source models are surpassing proprietary ones."[365] This new revelation is deeply concerning to the U.S., as DeepSeek has shown that, at minimal cost, it is possible to develop an AI foundation model that outperforms top proprietary U.S. models.[366]

One route to mitigate these risks is for Congress to limit the availability of open-source AI models in view of the U.S.'s competition against China. But limiting open-source software would stifle innovation and advancement in AI and may directly contribute to the U.S. losing the AI race to China. Moreover, China has started to build its own open-source ecosystem,[367] and by the U.S. prohibiting open-source AI models, U.S. developers may start relying on Chinese open-source if it remains readily available.[368] Many research and development labs and universities in the U.S. also rely on openness and foreign-originating talent: "74% of full time electrical engineering graduate students and 72% of those in computer and information sciences are foreign nationals" who bring talent and innovation to the U.S.[369] Another route, suggested in a 2024 bill, would be to expand the scope of ECRA to cover "artificial intelligence systems" as it relates to "the design, development, production, use, operation, installation, maintenance, repair, overhaul, or refurbishing of, or for the performance of services relating to [AI]."[370] If Congress were to pass

[364] *Id.*
[365] Katie Balevic & Lakshmi Varanasi, *Meta's Chief AI Scientist Says DeepSeek's Success Shows That 'Open Source Models Are Surpassing Proprietary Ones'*, BUS. INSIDER (Jan. 25, 2025), https://www.businessinsider.com/meta-ai-yann-lecun-deepseek-open-source-openai-2025-1 (internal quotations omitted).
[366] *Id.*
[367] Zeyi Yang, *Why Chinese Companies Are Betting on Open-Source AI*, MASS. INST. OF TECH. TECH. REV. (Jul. 24, 2024), https://www.technologyreview.com/2024/07/24/1095239/chinese-companies-open-source-ai/.
[368] Tobin & Metz, *supra* note 360.
[369] John Villasenor, *The Tension Between AI Export Control and U.S. AI Innovation*, BROOKINGS (Sep. 24, 2024), https://www.brookings.edu/articles/the-tension-between-ai-export-control-and-u-s-ai-innovation/.
[370] ENFORCE Act, H.R. 8315, 118th Cong. (2024).

this act, a foreign national attending a university, who is then allowed to work on an AI system would be a deemed export, requiring a license and potentially prohibiting their access to that AI system. While these routes are viable options, they may overly restrict innovation.

A better route would be for Congress to codify the national security sections of EO 14110 and provide additional authorities to the President to regulate AI foundation models. Congress should establish a new federal agency (AI Agency) under DoC to regulate covered AI models outside of the existing ECRA and FIRRMA scope. EO 14110 identified "dual-use foundational models" as an area of concern and tasked BIS through DoC with developing the minimum computational threshold for determining a covered AI model and computing infrastructure.[371] While the revocation of EO 14110 stopped BIS's determination of a covered AI model, the Center for Security and Emerging Technologies ("CSET") suggests that a covered AI model is:

(1) "[T]rained using a quantity of computing power greater than 10^26 integer or floating-point operations, or using primarily biological sequence data and using a quantity of computing power greater than 10^23";

(2) Cost more than $100,000 to train;

(3) Contain more than 10 billion parameters ("smaller models are currently becoming more capable");

(4) Achieve high "performance on one or more standardized capabilities evaluations or evaluations focused specifically on risk levels than current models"; and

(5) Produce "highly realistic synthetic media images, audio and video."[372]

[371] Exec. Order No. 14,110 88 Fed. Reg. 75,191, 75,197 (Nov. 1, 2023).
[372] David Evan Harris, *How to Regulate Unsecured "Open-Source" AI: No Exemptions*, TECH POL'Y (Dec. 3, 2023),

Using CSETs covered AI model would cover most of the AI foundation models that would present national security risks, while not being overly burdensome. While CSETs model would be appropriate as a starting point, the AI Agency would need to evaluate its definition of an AI covered model on an annual basis, with a report to Congress in case this definition requires change in the future.

Not only should the AI Agency be the reporting agency under this new law, but it should also regulate AI foundation models based on their inherent national security risks. This regulation would have to be carefully balanced to mitigate the most serious national security risks associated with AI foundation models while minimizing the negative effects to Open Source innovation. For example, while older open-sourced LLMs such as LLaMa 1 can enhance nefarious actors capability to create malware and phishing campaigns, the value of having LLaMa 1 open-sourced as a tool for economic progress and future innovation outweighs risks associated with LLaMa 1.[373] On the

https://www.techpolicy.press/how-to-regulate-unsecured-opensource-ai-no-exemptions/; Helen Toner & Timothy Fist, *Regulating the AI Frontier: Design Choices and Constraints*, CTR SEC. AND EMERGING TECH. (Oct. 26, 2023), https://cset.georgetown.edu/article/regulating-the-ai-frontier-design-choices-and-constraints.

[373] On February 24, 2023, Meta introduced LLaMa 1, an LLM foundation model with 65-billion-parameters, which was leaked on 4chan after its release. *See* Mark Zuckerberg, *Open Source AI Is the Path Forward*, META: NEWSROOM (Jul. 23, 2024), https://about.fb.com/news/2024/07/open-source-ai-is-the-path-forward/ (discussing the release of LLaMa 1); Arvind Narayanan & Sayash Kapoor, *The LLaMA Is Out of The Bag. Should We Expect a Tidal Wave of Disinformation?*, KNIGHT FIRST AMEND. INST. COLUMBIA UNIV. (Mar. 6, 2023), https://knightcolumbia.org/blog/the-llama-is-out-of-the-bag-should-we-expect-a-tidal-wave-of-disinformation; Anirudh VK, *Meta's LLaMA Leaked to the Public, Thanks to 4chan*, AIM (Mar. 7, 2023), https://analyticsindiamag.com/ai-origins-evolution/metas-llama-leaked-to-the-public-thanks-to-4chan/. While it has been touted that LLaMa 1 could be misused to create malware and phishing campaigns, financial fraud, obscene content involving children, and other crimes, its accessibility allows for researchers and developers to freely access, use, and modify the model, fostering community-driven innovation and customization for various applications. *See generally* Letter from Richard Blumenthal & Josh Hawley, U.S. Sens., to Mark Zuckerberg, CEO Meta (Jun. 6, 2023), https://www.blumenthal.senate.gov/imo/media/doc/06062023metallamamodelleakletter.pdf (describing the two Senators concerns over the release of LlaMa); Zuckerberg, *supra* note 373 (discussing the benefits and reasonings behind Meta's AI open-source model).

other hand, when looking at AlphaFold 3, the biosecurity risks associated with that AI foundation model would justify prohibiting the release of the underlying algorithmic and computational code. Congress should create an interagency Committee (AI Committee) chaired by DoC and run by the new AI Agency. Nearly all agencies should have a seat at the table because AI is interdisciplinary and will touch various, sometimes overlapping, spheres of agency authority and missions.[374]

Congress should also codify "dual-use foundational models" as a covered AI foundation model while the AI Agency defines the minimal computational threshold. Covered entities should consist of any entity, foreign or domestic, within U.S. jurisdiction, with Congress's authority to regulate AI foundation models stemming from the Commerce Clause.[375]

Congress should also require the AI Committee to make a risk-based analysis of any covered AI model and consider specific elements like CFIUS's risk-based analysis, which includes both the risks the specific AI model poses to national security and the benefits the open-source AI model would have on society. Based on its risk analysis, the AI Committee would regulate on a sliding scale to what extent an AI foundation model is open- or closed-source.

The President should also have the power, on exceptionally rare occasions, to forbid the use of a specific model, especially if it (1) has criminal implications, such as synthetic media related to child sexual abuse material, or (2) could pose such a significant national security risk that no manner of mitigation could outweigh the risk. Owners of AI foundation models should also have the ability after a set number of years to apply to have their models open-sourced. As technology and cutting-edge AI models change over time, the risks

[374] At a minimum, the Department of State, Treasury, Justice, Labor, Defense, Health and Human Services, Transportation, Energy, Homeland Security should be permanent members of the AI Committee with other agencies when necessary and invited.

[375] For examples of cases that illustrate the extent of Congress' Commerce Clause powers see Gibbons v. Ogden, 22 U.S. 1 (1824); Swift & Co. v. United States,196 U.S. 375 (1905); Gonzales v. Raich, 545 U.S. 1 (2005).

associated with the regulated models will disappear and the benefits of an open-source model will outweigh the costs. For example, an AI foundation model that could be used to penetrate cyber defenses of critical infrastructure may initially be identified as a national security risk that needs regulation; however, with the development of cyber defense tools over the years, that same AI foundation model may later pose minimal risks.

Effectively regulating AI foundation models will require constant evaluation of what is a covered AI model and what factors will go into the risked-based analysis of open-sourced models. Congress should require an annual or biennial report from the SoC, produced by the AI Committee so that Congress can determine if the federal AI regulation law needs to be amended and the definition of "covered AI model" updated. CFIUS provides a similar, detailed requirement under 50 U.S.C. § 4565(m) that allows Congress to determine national security risk trends, funding requirements, and other statistical information to gauge whether FIRRMA needs amending.[376] The AI Committee's report will also serve to inform Congress of required amendments to the risk-based analysis methodology as AI technology continues to change, especially as we approach an age of AGI. Without updating the law and the regulatory schemes, the U.S. may negatively impede innovation and the economy by keeping an AI foundation model from being open-sourced, or it may allow a model to be open-sourced that carries new, emerging national security risks that the AI Committee did not consider.

CONCLUSION

The promise of AI can transform our lives in a way that no other technology has done before. Like fire, the wheel, and electricity, AI will launch civilization into a new era because "[t]hese [technological] waves followed a similar trajectory," states Mustafa Suleyman, CEO of Microsoft AI.[377] "[B]reakthrough technologies were invented, delivered huge value, and so they proliferated, became more

[376] *See* Foreign Investment Risk Review Modernization Act, 50 U.S.C. § 4565(m).
[377] Suleyman, *supra* note 63.

effective, cheaper, more widespread and were absorbed into the normal, ever-evolving fabric of human life."[378]

While critics have stated AI is "an under-regulated phenomenon,"[379] they are wrong. Through FIRRMA, ECRA, IEEPA, EO 14083, EO 13873, and EO 14105 the U.S. can limit and prohibit access to AI foundation models by both inbound and outbound investment mechanisms. As it relates to inbound investments, EO 13873, CFIUS, and the additional guidance provided in EO 14083, are excellent tools in mitigating or prohibiting investment by state and non-state actors whose access to AI foundation models would be a national security risk.

Congress should modify FIRRMA by allowing CFIUS to expand its definition of a covered investment to include greenfields and brownfields for "emerging" technology and therefore reach emerging AI foundation models. In relation to outbound investments, ECRA, CCL, EAR, and EO 14105, provide a robust avenue to mitigate or prohibit a transaction with state and non-state actors, along with prohibiting U.S. persons from certain acts globally that pose national security risks or are in contradiction to foreign policy.

ECRA could better control the export of software and algorithms associated with AI foundation models with appropriate classifications through an EFL.[380] While ECRA is a good mechanism for execution of outbound investment, (1) realigning ETRAC under NIST; (2) boosting ETRAC's budget, and (3) creating an EFL that is provided to BIS for publication in the CCL with a focus on emerging and foundational technology, such as AI foundation models and its progeny, would help enhance ECRA to mitigate the risks associated with AI foundation models and outbound investments. NIST should also define 1758 technology to help CFIUS and ECRA respond to current and future AI foundation models risks relating to inbound and outbound investment.

---

[378] *Id.*

[379] Findlay & Ford, *supra* note 4, at 1.

[380] *See* 15 C.F.R. § 744 (Supp. 1(a)(4)) (including "command/control/communication or navigation systems" in definition of military end-uses of microprocessors).

Some consider "Open Source software[as] the single-most impactful driver of innovation in the world today,"[381] but the inherent risks associated with AI foundation models in the hands of state and non-state foreign adversaries should give both enthusiasts and regulators pause. Despite Open Source creating the AI we see today, we must be cautious with continuing this practice without regulation as it relates to AI foundation models that could be considered "dual-use foundational models." Any regulation on Open Source cannot be a one-size-fits-all methodology; some AI systems like synthetic media may have national security risks that can be mitigated with time, while other models like AI BDT's may not.

Congress should codify the national security sections of EO 14110 and establish a new AI Agency and AI Committee in a similar fashion as CFIUS to regulate AI foundation models. The AI Committee should weigh the benefits of allowing covered AI foundation models to stay open-source against the national security risks that arise, and then determine what mitigation, if any, should occur to restrict access to these AI foundation models. On rare occasions, the AI Committee should refer AI foundation models to the President to prohibit an AI foundation model when it is vital to national security. The AI Committee should, on a regular basis, report to Congress so that appropriate updates to law and regulation keep pace with exponentially advancing AI technologies.

This Article focused on current and recommended laws to mitigate national security risks related to AI foundation models, yet it is important that the U.S. take a holistic approach. The U.S. must mitigate AI algorithms and software risks, especially those posed by AI foundation models, while learning to safely, ethically, and securely implement these new technologies into government, the private sector, and society.

[381] Bergelt, *supra* note 29, at 28.