CALYPSOAI

STATE OF THE UNION 2021

EXECUTIVE SUMMARY

In the second edition of CalypsoAI's State of the Union Report, we explore four trends related to artificial intelligence (AI) and their impact on the ongoing great power competition between the United States and China. Through this report, we hope to inform policymakers, warfighters, executives, academia, and the general public of the need for rigorous testing, evaluation, verification, and validation (TEVV), which can help build trust in AI systems while addressing the challenges inherent in these trends.

TECHNICAL DEVELOPMENTS

We summarize the significant research advancements made in the field of artificial intelligence TEVV during 2021.

TREND: 01 STATE V. CITIZEN

In 2021, the use of AI-enabled surveillance tools was debated extensively as they pertain to civil liberties. This resulted from the maturation of computer vision technologies, which have accelerated the scope of control exercised by nation-states against their citizens. Significant progress was made globally to define and clarify the privacy rights afforded to citizens through the development of meaningful legislation in the U.S. and Europe. However, the Chinese Communist Party (CCP) continued to leverage AI-powered tools to increase surveillance of its citizens and target minorities. Even amid outcries from the global community about the CCP's human rights abuses, Chinese AI surveillance technology companies moved forward successfully with initial public offerings (IPOs). This troubling trend indicates that profitability may continue to drive business decisions more than ethics. Consequently, through implementing TEVV, the U.S. can build trust in AI's ability to protect civil liberties and privacy rights.

TREND: 02 ETHICAL AI REGULATION

As AI becomes more prevalent across society, ethics-related legislation has increased globally. China released its first official AI ethics framework in September 2021. Although there are parallels between the U.S. Department of Defense (DoD) and China's AI ethics principles, the CCP focuses on controlling information flow. Additionally, given China does not have property rights, the CCP does not apply regulations it places on private companies to the state. In contrast, the U.S. focuses on protecting individual rights by focusing on data privacy, responsible use, and the distinction between private and public entities. However, while many U.S. government agencies have released AI ethics frameworks, the U.S. does not yet have a single, AI ethics guidance framework. This means that with China's ethics position articulated, the U.S. now has an opportunity to work with like-minded allies and partners to promote a global standard for AI use.

TREND: 03 CHINA'S AI TALENT POOL

China's domestic talent pool is bigger than that of the U.S., but more international graduate students - particularly from China - choose to live and work in the U.S. after completing their programs. China's larger population and increased investments into talent recruitment enable more people to conduct AI research. However, the U.S. still maintains the qualitative advantage for research output. In order to strengthen its pipeline of talent and sustain its research output, the U.S. must encourage more AI PhDs to stay in academia. This way, they can ensure the U.S. does not fall behind in both quantity and quality of research, and they can train the next generation with the right skills to advance AI research and development (R&D). At the same time, with a growing workforce and no universal definition of "responsible use" for AI, the U.S. must standardize an independent testing and validation process that can be incorporated into curricula to ensure AI is deployed safely.

TREND: 04 AI IN AGRICULTURE

Within the AI competition, the agricultural sector presents an opportunity to make significant advances in TEVV, as well as to reinforce the contrast between China and the U.S. in how they develop and use AI. In making technology more accessible to farmers through its Digital Village initiative, China has simultaneously extended surveillance technologies to rural populations. In addition to monitoring its own population, the CCP has engaged in agricultural espionage, which spurred a Congressional proposal to create an intelligence-gathering office within the U.S. Department of Agriculture (USDA). In contrast, the U.S. has focused on using AI to increase crop yield and efficiency, and improve food security. Recognizing the significant investment farmers need to make to use these technologies and the nascency within the sector, the U.S. has an opportunity to promote responsible AI use through prioritizing TEVV. This will not only set a global standard, but will also enhance the confidence of U.S. farmers that AI is worth the investment.

INTRODUCTION

Artificial intelligence (AI) and associated data-driven technologies - such as machine learning (ML), deep neural networks, and quantum computing - will transform both the nature and character of war and future grey zone conflict. Knowing this, it is clear that the U.S. is in the midst of an unprecedented age of innovation that requires us to address challenges through a new lens.

Simultaneously, the race to research, develop, and deploy AI is accelerating the already intense strategic competition between the U.S. and its near-peer competitor, China. China is determined to surpass the U.S. as a technological leader and shape the global norms for how technology should be used. The Chinese Communist Party's (CCP) employment of AI as a tool for oppression domestically - and increasingly abroad - serves as a chilling indication as to how the CCP will erode global democracy and civil liberties if they are successful.

Prioritizing technical robustness, assurance, interpretability, and governability creates a strategic advantage for the U.S. in the AI competition. While China and other autocracies are leveraging AI as a tool for state-sponsored oppression, division, and discrimination[1], the U.S. has an opportunity to set the global precedent for trustworthy, transparent, and safe AI. By choosing to only deploy robust, lawful, and secure AI systems, users can have confidence that they will perform in a way that reflects U.S. democratic values.

However, achieving this state of AI is not a given; it requires prioritization of AI test, evaluation, verification, and validation (TEVV), which ensures AI/ML technologies perform as intended and are deployed at the rate of innovation. In this way, TEVV is a critical component of harnessing AI responsibly.

CalypsoAI's 2021 State of the Union Report examines four trends that demonstrate the interwoven nature of the ongoing strategic competition, AI, and the demand for robust TEVV. In this report, we unpack how powerful predictive technologies were leveraged by states against their citizenry, and discuss the explosion in ethical and responsible AI legislation that we witnessed in the last year. As states scrambled to find and maintain a skilled AI workforce in 2021, we analyze the role that AI talent demand has on China when compared to the U.S. Finally, we hone in on agricultural applications of AI to highlight how the U.S. and China differ in their approaches to developing and using AI-enabled technologies, which is emblematic of the greater competition. Through the policy recommendations for each trend offered within this report, we urge policymakers to consider implementing AI test and evaluation to confront the most pressing challenges facing America today.

[1] Paul Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority," *New York Times*, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

TECHNICAL DEVELOPMENTS

Research and development (R&D) advancements are foundational to AI progress. However, equally critical is America's ability to ensure that these powerful data-driven technologies reflect our democratic values. CalypsoAI's research suggests that the best way to ensure U.S. AI applications are trustworthy, effective, and secure is through robust TEVV that empowers end-users to deploy AI models with confidence in their performance and ability to adhere to evolving AI standards.

In 2017, Nicholas Carlini and David Wagner of the University of California, Berkeley, introduced the Carlini-Wagner attack in their seminal paper Towards Evaluating the Robustness of Neural Networks.[2] The Carlini-Wagner attack laid much of the groundwork for the modern understanding and interpretation of adversarial machine learning. Importantly, the paper introduced the standard paradigm through which most other adversarial attacks are now studied. Research in the field of machine learning robustness is still nascent when compared to the amount of AI and automation research that exists. Nevertheless, in 2021, there were significant advancements. This is notable not because of the quantity of papers, but because the methods described in the literature are feasible and increasingly accessible. To that end, CalypsoAI has captured some major research advancements in TEVV for 2021. This work will contribute to the enablement of the TEVV-related recommendations outlined in this report.

UNCERTAINTY SETS FOR IMAGE CLASSIFIERS USING CONFORMAL PREDICTION[3]

Authors: *Anastasios N. Angelopoulos, Stephen Bates, Jitendra Malik, & Michael I. Jordan of the Department of Electrical Engineering and Computer Sciences Department of Statistics University of California, Berkeley.*

Why It Matters: Published in October 2021, this research paper introduces the idea of uncertainty set predictions as a strategy to improve the likelihood of a "correct" answer. By using "conformity" functions, which use a model's past experiences to determine confidence in new predictions, end-users can quantify the uncertainty of a classifier. When making mathematical predictions, we must guarantee the validity of the outcome. Therefore, as with confidence intervals in statistics, the same conformal prediction can be embedded into machine learning. For example, given a parameter p, the model returns a set of predictions such that the likelihood of the set containing the correct label is greater than p. The paper also introduces a method to abstain from predicting altogether (i.e. the model returns an empty set) if the input does not statistically "conform" to the original training and tuning data.

[2] David Wagner and Nicholas Carlini, "Towards Evaluating the Robustness of Neural Networks," *University of California, Berkeley* (March 2017), https://arxiv.org/pdf/1608.04644.pdf.

Figure 1: See three examples of the class "fox squirrel" along with 95% prediction sets generated by this method to illustrate size changes based on the difficulty of a test image.[4]

DOCTOR: A SIMPLE METHOD FOR DETECTING MISCLASSIFICATION ERRORS[5]

Authors: *Federica Grannese of Lix, Inria, Institute Polytechnique de Paris and Sapienza University of Rome; Macro Romanelli of L2S, CentralSupelec, CNRS, University Paris Saclay; Daniele Gorla of Sapienza University of Rome; Catuscia Palamidessi of Lix, Inria, Institute Polytechnique de Paris; and Pablo Pintanida of L2S, CentraleSupelec, CNRS, University Paris Saclay.*

Why It Matters: Published in October 2021, this research paper introduces a way to predict when a deep neural network (DNN) classifier will fail with little extra computational effort. This approach effectively quantifies the uncertainty of a prediction and allows the end-user to reject any prediction that does not meet a certain criteria. While not a guaranteed strategy for solving the problem of adversarial machine learning, given confidence metrics can also be manipulated, this approach can help improve model robustness and facilitates a more graceful model failure, ensuring that end-users can accept or reject models with confidence.

[3] Anastasios N. Angelopoulos, Stephen Bates, Jitendra Malik, and Michael I. Jordan, "Uncertainty Sets for Image Classifiers Using Con formal Prediction," *University of California, Berkeley* (October 2021), https://arxiv.org/pdf/2009.14193.pdf
[4] Anastasios Angelopoulos, "conformal classification," GitHub, October 25, 2021, https://github.com/aangelopoulos/conformal_classification
[5] Federica Granese et al., "DOCTOR: A Simple Method for Detecting Misclassification Errors," *European Union Horizon Research and Innovation Program* (October, 2021), https://arxiv.org/pdf/2106.02395.pdf

WASSERSTEIN SMOOTHING: CERTIFIED ROBUSTNESS AGAINST WASSERSTEIN ADVERSARIAL ATTACKS[6]

Authors: *Alexander Levine and Soheil Feizi of the Department of Computer Science, University of Maryland, College Park.*

Why It Matters: Published in early 2021, this paper introduces a method for directly computing the robustness of an image. The paper introduces a defense against the Wasserstein Adversarial Attack (originally proposed by Wong et al in 2019) which involves slightly moving pixels in an image to create erroneous outcomes.[7] There are a few logistical considerations involved with choosing "references," and the method assumes a fairly specific representation of the input data. However, it demonstrates a way to compute a metric that has directly interpretable results. It also can be used in a similar adversarial training capacity to prior iterations that are much more ground and provable certified (i.e. the bounds here are tight where as CLEVER[8] was approximate).

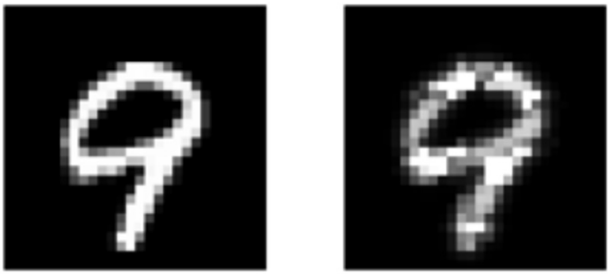

Figure 2: An illustration of the Wasserstein adversarial attack[9] against which Levine and Feizi developed a smoothing-based certifiably robust defense.

[6] Alexander Levine and Soheil Feizi, "Wasserstein Smoothing: Certified Robustness Against Wasserstein Adversarial Attacks," Proceedings of Machine Learning Research, vol. 108 (paper presented at the 23rd International Conference on AI and Statistics, Italy: August 2020), http://proceedings.mlr.press/v108/levine20a/levine20a.pdf

[7] Eric Wong, Frank R. Schmidt, and J. Ziko Kolter, "Wasserstein Adversarial Examples via Projected Sinkhorn Iterations," Proceedings of Machine Learning Research, vol. 97 (paper presented at the 36th Conference on Machine Learning, California: February 2019), https://arxiv.org/abs/1902.07906.

[8] Tsui-Wei Weng et al., "Evaluating the Robustness of Neural Networks: An Extreme Value Theory Approach," (paper presented at 6th International Conference on Learning Representations, Vancouver: Canada, January 2018), https://arxiv.org/pdf/1801.10578.pdf.

[9] Wong, Schmidt, and Kolter, "Wasserstein Adversarial Examples via Projected Sinkhorn Iterations."

TREND: 01 STATE V. CITIZEN

The year 2021 ushered in the next era of the debate on civil liberties, particularly one's right to privacy. Although laws differ depending on the entity's role within the national security ecosystem, analytics enhanced by AI can help officials process and decipher massive amounts of data, enabling rapid threat detection. However, within the context of aggregating citizens' personal data, state use of biometric AI (i.e. AI systems that analyze data related to a person's voice, face, DNA, fingerprints, etc.) raises several concerns and challenges concerning privacy, civil liberties, and civil rights.[10] When used improperly, AI technologies offer governments powerful ways to collect and process information, track citizens' behavior and movements, and act on computer-generated analyses.[11]

Throughout 2021, techno-authoritarian governance continued to gain traction internationally as regimes exploited these emerging technological capabilities that underpin large-scale surveillance, with techniques for image classification,[12] face recognition,[13] video analysis,[14] and voice ID[15] expanding exponentially over the last year.[16]

Private sector entities in the U.S. did not avoid controversy either, as the public observed cases where automated technology infringed on their right to privacy during 2021.

These questions of privacy and civil liberties have arisen with the maturation of computer vision technologies, which have enabled immense progress in tasks such as object-detection frameworks for analysis from videos, and synthetic image generation.[17] Accelerated by deep learning-based algorithms and the use of increased computation and larger datasets, image recognition has emerged as an inexpensive, easy to deploy, and increasingly ubiquitous technology. In fact, recent advancements in computer vision have surpassed human levels of performance on some restricted visual tasks such as early detection of cancer,[18] and have enabled the acceleration of security applications, including satellite image analysis and surveillance.

[10] Jonathan Hillman, "China is Watching You," The Atlantic, October 18, 2021, https://www.theatlantic.com/ideas/archive/2021/10/china-america-surveillance-hikvision/620404/.
[11] Nicole Kobie, "The complicated truth about China's social credit system," WIRED, July 6, 2019, https://www.wired.co.uk/article/china-social-credit-system-explained.
[12] Andre Ye, "5 Exciting Deep Learning Advancements to Keep an Eye on in 2021," Towards Data Science, January 10, 2021, https://towardsdatascience.com/5-exciting-deep-learning-advancements-to-keep-your-eye-on-in-2021-6f6a9b6d2406.
[13] Alan L. Yuille and Chenxi Liu, "Deep Nets: What have They Ever Done for Vision," International Journal of Computer Vision, 129: 781-802 (2021), https://doi.org/10.1007/s11263-020-01405-z.
[14] Stepan Tulyakov et al., "Time Lens: Event-based Video Frame Interpolation" (paper presented at the IEEE Conference on Computer Vision and Pattern Recognition, Nashville: 2021), http://rpg.ifi.uzh.ch/docs/CVPR21_Gehrig.pdf.
[15] Markets and Markets, Speech and Voice Recognition Market with COVID-19 Impact Analysis by Delivery Method, Deployment Mode, Technology, Vertical, and Geography-Global Forecast to 2026, report ID: 5415408 (August 2021), https://www.researchandmarkets.com/reports/5415408/speech-and-voice-recognition-market-with-covid
[16] Mozur, "One Month, 500,000 Face Scans: How China is Using A.I. to Profile a Minority."
[17] Adam Coates, Honglak Lee, Andrew Y. Ng, "An Analysis of Single Layer Networks in Unsupervised Feature Learning," (presented at the 14th International Conference on Artificial Intelligence and Statistics, Florida, 2011) , https://cs.stanford.edu/~acoates/stl10/.
[18] Rachael Gordon, "Robust artificial intelligence tools to predict future cancer," Massachusetts Institute of Technology News, January 28, 2021, https://news.mit.edu/2021/robust-artificial-intelligence-tools-predict-future-cancer-0128.

CHINA'S USE OF SURVEILLANCE TECHNOLOGIES

Advances in computer vision technology have created new opportunities, as well as threats when levied by states against their own citizens. For instance, the Chinese state exercises an astonishing level of surveillance over its citizens, generating massive databases used to punish people for even minor deviations from expected norms of behavior.[19] The ideological rigidity embraced by the regime of Chinese President Xi Jinping includes an unprecedented level of control over its population.

China's use of technology on a vast scale to monitor and score the Chinese population, especially specific subgroups,[20] is at odds with democratic values by undermining human dignity, autonomy, non-discrimination, and individual rights to freedom of expression. One company that enables the surveillance of minorities is China's SenseTime, a $12 billion facial recognition software company that filed to list on the Hong Kong stock exchange in April 2021.[21]

Although SenseTime was blacklisted by the U.S. government in 2019 for powering the surveillance technology in Uighur Muslim detainment camps,[22] the company still generated $525 million of revenue in 2020, and is often regarded as the most valuable of China's "four AI dragons" as it moves forward with its IPO.[23] The SenseTime IPO indicates a troubling trend, since the economic benefit of the company going public seems to outweigh the moral tenet that all people should be treated fairly.

As Chinese institutions dominate research in smart cities, observers similarly worry this success is synonymous with accelerated government surveillance.[24] Generally, smart cities deploy a host of technologies, such as 5G mobile telecoms, sensors, and AI that automate data mining and facial recognition. Electronic, thermal, and LIDAR sensors for the basis of the smart grid do everything from operating streetlights to detecting house fires and crime. Recently, Shanghai installed Alibaba's City Brain public surveillance system, which oversees the collection of over 20 million images a day from a slew of fixed cameras, drones, and satellites. In parallel, citizen credit cards, metro, and bus cards are traced in real time.[25] Consequently, privacy does not exist for Chinese citizens.

[19] Anna Mitchell and Larry Diamond, "China's Surveillance State Should Scare Everyone," The Atlantic, February 2, 2018, https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/.
[20] Chris Buckley and Paul Mozur, "How China Uses High-Tech Surveillance to Subdue Minorities," New York Times, May 22, 2019, https://www.nytimes.com/2019/05/22/world/asia/china-surveillance-xinjiang.html.
[21] Zeyi Yang, "SenseTime IPO: Everything You Need To Know About The SenseTime IPO," Protocol, August 31, 2021, https://www.protocol.com/china/sensetime-ipo.
[22] Sherisse Pham, "The United States Strikes a Blow to China's AI Ambitions," CNN, October 10, 2019, https://www.cnn.com/2019/10/09/tech/hikvision-sensetime-blacklist/index.html.
[23] Yvonne Lau, "SenseTime's Hong Kong IPO could be a boon for China's controversial 'A.I. dragons,'" Fortune, August 30, 2021, https://fortune.com/2021/08/30/sensetime-hong-kong-ipo-ai-dragons-china-us-blacklist/.
[24] Katherine Atha et al., China's Smart Cities Development, (Reston, Virginia: SOS International LLC, January 2020), https://www.uscc.gov/sites/default/files/2020-04/China_Smart_Cities_Development.pdf.
[25] Yusho Cho, "Shanghai district installs comprehensive surveillance system," Nikkei Asia, May 7, 2019, https://asia.nikkei.com/Business/China-tech/Shanghai-district-installs-comprehensive-surveillance-system

As part of China's Belt and Road Initiative - President Xi Jinping's project to invest in overseas infrastructure - the Chinese-made technology that underpins smart cities is being exported to Latin America, Africa, and other parts of Asia to enable what some call "digital authoritarianism."[26] Accelerated by the Chinese economy, the exportation of advanced technologies to developing countries enables the adoption of the Chinese worldview in these nations as well. While smart cities are generally described in benign terms with the promise of greener energy solutions and safer streets, there are growing concerns about the ways in which personal data collected through surveillance is encroaching on free speech and privacy.

THE U.S. PRIVACY DEBATE

Outside of China, surveillance technologies received public backlash in North America and Western Europe throughout 2021 in response to the pervasive collection, retention, and misuse of personal data by law enforcement agencies and private companies. As we discussed in last year's 2020 State of the Union Report, facial recognition technologies are notoriously inaccurate when evaluating race and gender.

In the two years since San Francisco banned facial recognition technologies, 13 other U.S. cities have followed suit, naming racial bias and discrimination as a key factor.[27] Domestically, private sector collection and aggregation of personal data received heightened attention for security concerns throughout 2021.

For instance, in April, the data of over 500 million Facebook users and 500 million LinkedIn users were scraped and aggregated by bad actors selling the massive datasets to scammers.[28]

While China has leveraged facial recognition technology to surveil its citizenry for years, in 2021, the debate around facial recognition technology finally escalated around the world. In the U.S., examples include the Commonwealth of Virginia[29], which ended one controversial policing facial recognition system, and Microsoft and Amazon, which banned sales of their facial recognition software to police until further regulation is in place.[30] In early November 2021, Facebook announced plans to shutter its decade-old facial recognition system that has been the subject of a class-action lawsuit and government investigations, and has fueled privacy concerns for the over one billion users whose face scan data lives within Facebook's repository.[31]

[26] Paul Mozur, Jonah M. Kessel, and Melissa Chan, "Made in China, Exported to the World: The Surveillance State," New York Times, April 24, 2019,
[27] Shannon Flynn, "13 Cities Where Police Are Banned From Using Facial Recognition Tech," Innovation & tech today, November 18, 2021, https://innotechtoday.com/13-cities-where-police-are-banned-from-using-facial-recognition-tech/.
[28] Jonathan Vanian, "Why Facebook and LinkedIn's data scraping fiascos are a huge security problem for their users," Fortune, April 17, 2021, https://fortune.com/2021/04/17/facebook-linkedin-data-scraping-security-problem-social-media-cybersecurity/.
[29] Justin Jouvenal, "D.C.-area facial recognition system to identify Lafayette Square protester to be halted," Washington Post, May 18, 2021, https://www.washingtonpost.com/local/public-safety/facial-recognition-system-halted/2021/05/18/af2d19e2-b737-11eb-a6b1-81296da0339b_story.html.
[30] Jay Greene, "Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM," Washington Post, June 11, 2021, https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/
[31] Kashmir Hill and Ryan Mac, "Facebook Citing Societal Concerns, Plans to Shut Down Facial Recognition Systems," New York Times, November 2, 2021, https://www-nytimes-com.cdn.ampproject.org/c/s/www.nytimes.com/2021/11/02/technology/facebook-facial-recognition.amp.html

In light of recent domestic debates on the proper use and scope of facial recognition technologies in society, it is promising to see the private sector make forward strides in the development of responsible AI policies.[32] However, since there is still much work to do, it will be important to develop algorithmic testing and validation standards that protect individuals' data while enabling companies to leverage technologies like these that can have positive benefits if used properly.

A LOOK AHEAD AT GLOBAL AI SURVEILLANCE TECHNOLOGY STANDARDS

Similarly, in April 2021, the European Union (EU) proposed a comprehensive ban on biometric mass surveillance.[33] Under the proposal, mandatory requirements are attached to the "high risk" category of AI applications that are deemed a safety risk or threaten to impede EU fundamental rights. The parliament has also called for a ban on private facial recognition databases,[34] and said predictive policing based on behavioral data should be outlawed.[35]

To respect privacy and human dignity, in early October 2021, the European Parliament adopted a resolution that takes aim at algorithmic bias, calling for human supervision and strong legal powers to prevent discrimination by AI. Further, the legislation requires that human operators make the final decision when leveraging the insights of AI-powered systems.[36]

In contrast to the U.S. and EU, which have both prioritized the protection of individual rights, China's Personal Information Protection Law (PIPL) that went into effect in November 2021 was notably aimed at both the private and public sector, but not applicable to the Chinese government.[37] This gives the Chinese government access to data that enables their mass surveillance practices and accelerates their AI-enabled technology.

The personal privacy law mirrors many aspects of Europe's all-encompassing General Data Protection Regulation (GDPR) and California's Consumer Privacy Act (CCPA).

[32] Jerome Pesenti, "Facebook's five pillars of Responsible AI," Facebook, Blog, June 22, 2021, https://ai.facebook.com/blog/facebooks-five-pillars-of-responsible-ai/.
[33] European Commission, Proposal for a Regulation of the European Parliament and of the Council: Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts, Explanatory Memorandum, COM/2021/206 (April, 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.
[34] Zack Whittaker, "Clearview AI ruled 'illegal' by Canadian privacy authorities," TechCrunch, February 3, 2021, https://techcrunch.com/2021/02/03/clearview-ai-ruled-illegal-by-canadian-privacy-authorities/.
[35] Committee on Civil Liberties, Justice, and Home Affairs, Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, European Parliament, Plenary sitting, A9-0232/2021 (July 13, 2021), https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.pdf.
[36] European Parliament, Use of artificial intelligence by the police MEPs, propose mass surveillance, European Parliament News, Press release from Plenary session (June 10, 2021), https://www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance.
[37] Graham Webster, Personal Information Protection Law (California: Stanford University, DigiChina project, October 2021), https://digichina.stanford.edu/work/knowledge-base-personal-information-protection-law/.

For example, the laws articulate rights for citizens to access what information is held about them, update or delete the information, and withhold consent for the information to be handled by a company. Both EU and Chinese regulations appear in agreement with respect to consumer rights; the systems must not implicitly manipulate consumer behavior, and consumers must be alerted when they are interacting with the AI system. However, PIPL does not prevent the state itself from accessing its citizens' personal information. Instead, Chinese e-commerce giants and social networks appear to be at the center of a regulatory crackdown, and the law may in fact signal a desire to reduce the economic power of big tech companies.

In the U.S., there is still no federal law protecting consumer data privacy. The Algorithmic Accountability Act was proposed in 2019 and required companies to study and fix flaws in algorithms that result in inaccurate, unfair, biased, or discriminatory decisions impacting Americans.[38] The bill was not adopted, and since then, the U.S. has not seen a comprehensive national AI regulation or consumer data privacy law.

Existing federal laws are fragmented, partially covering data in specific domains like health, credit, and education. Some laws, like those on surveillance, are outdated and ill-suited to the modern internet.

Meanwhile, the vast majority of data, including third-party data, remains unregulated. A regulatory framework for data privacy in the U.S. must encourage federal agencies to independently manage their data, ensuring extensive regulatory barriers are avoided, while emphasizing our nation's democratic values. For instance, the White House Office of Science and Technology Policy (OSTP) is developing an "AI Bill of Rights" to guard Americans against AI-powered technologies.[39] The OSTP proposes enumerated guarantees that powerful technologies, such as biometric recognition systems, are required to respect democratic values and abide by the central tenet that everyone should be treated fairly.

"The White House Office of Science and Technology Policy (OSTP) is developing an "AI Bill of Rights" to guard Americans against AI-powered technologies.[39]"

[38] U.S. Senate Committee on Commerce, Science, and Transportation, A bill to direct the Federal Trade Commission to require entities that use, store, or share personal information to conduct automated decision system impact assessments and data protection impact assessments, 116th Cong., 1st sess. (April 10, 2019), https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf.

[39] Eric Lander and Alondra Nelson, "Americans Need a Bill of Rights for an AI-Powered World," WIRED, October 8, 2021, https://www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/.

CONCLUSION

As machine learning technologies evolve based on changing data and interactions with other models, AI systems require continuous TEVV to ensure that AI-enabled tools function as intended and clearly define the parameters for human and machine analysis.[40] Powerful technologies that surveil, identify individuals, and make inferences based on their attributes must adhere to the same values enumerated within our democratic society.

To ensure those systems are equitable to all citizens, the machine learning models that underpin such technologies must be validated and verified through a robust TEVV ecosystem. Further, the public requires international cooperation on TEVV policy around AI development, with fielding in these high-risk technologies as a cornerstone of future collaboration.

[40] Michèle A. Flournoy, Avril Haines, and Gabrielle Chefitz, Building Trust Through Testing, (Washington, DC: Center for Emerging Technology and Security, October 2020), https://cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf.

POLICY RECOMMENDATIONS: STATE V. CITIZEN

- ***In parallel with their AI Bill of Rights, OSTP should develop an approach to TEVV*** to ensure these enumerated rights are protected.
- ***NIST should tailor and develop quantitative TEVV standards and performance metrics*** to measure AI for transparency, bias, and efficacy. As AI increases the potential scale of bias, any flaw could harm millions of citizens. Clear, quantitative metrics would enable a standardized assessment of the trustworthiness of AI systems.
- ***Third-party AI testing requirements for high-stakes systems should be mandatory*** to ensure the efficacy and validity of machine learning technologies. Third-party testing provides federal agencies and other highly regulated industries the opportunity to hone expertise in AI TEVV regulations and overcome in-house limitations while ensuring their AI is effective, unbiased, and secure from adversarial attack.

TREND: 02 ETHICAL AI REGULATION

Artificial intelligence will continue to impact every aspect of our lives. Knowing this, the question becomes: how do we ensure it performs in a way that aligns with our values? Considering 68% of respondents to a 2021 Pew Research Center poll said they did not believe ethical principles focused on the public good would be incorporated into AI systems by 2030, it is unsurprising that over the past few years, this challenge has become an increasing topic of interest for academia, government, and industry stakeholders alike.[41]

For example, between 2015 to 2019 alone, research paper submissions to AI conferences focused on ethics increased from less than 20 papers to 70.[42]

Similarly, between 2015 and 2020, 117 documents on AI principles were published worldwide, jumping from 2 in 2015 to a high of 45 in 2018.[43] The trend of ethical AI-related guidance continued in 2021, when U.S. federal agencies such as the U.S. Department of Defense (DoD) and the U.S. Department of Veterans Affairs (VA), and international organizations such as the World Health Organization and UNESCO, all released documents focused on ethical use. Even the White House recognized the necessity when it launched an effort to develop an AI "Bill of Rights" to "ensure that data-driven technologies reflect, and respect, our democratic values."[44] Therefore, assessing AI ethics informs how each country will use AI, and in doing so, how they will approach AI security.

[41] Lee Rainie, Janna Anderson, and Emily A. Vogels, Experts Doubt Ethical AI Design Will Be Broadly Adopted as the Norm Within the Next Decade (Pew Research Center, June 2021), https://www.pewresearch.org/internet/2021/06/16/experts-doubt-ethical-ai-design-will-be-broadly-adopted-as-the-norm-within-the-next-decade/.
[42] Daniel Zhang et al., "The AI Index Report 2021," AI Index Steering Committee, Human-Centered AI Institute, Stanford University, Stanford: California, pg 133, (March 2021), https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf.
[43] Ibid., pg 130.
[44] Lander and Nelson, "Americans Need a Bill of Rights for an AI-Powered World."

U.S. AI ETHICS PRINCIPLES

Although there is not yet a single, ethical AI framework for the U.S. Government, DoD's ethical principles were one of the first released in the U.S., which means they can serve as a model for other agencies that are in the midst of establishing ethical principles. The following principles were issued in 2020 and reaffirmed in the Deputy Secretary of Defense's Memorandum, "Implementing Responsible Artificial Intelligence in the Department of Defense," dated May 26, 2021[45] :

1. Responsible
2. Equitable
3. Traceable
4. Reliable
5. Governable
6. Improving ethical quality

CHINA'S AI ETHICS PRINCIPLES

China's approach to AI ethics is captured in its first official AI ethical principles document, titled "New Generation Artificial Intelligence Ethics Specifications." This guidance was issued in September 2021 and identifies six principles[46]:

1. Promoting human well-being
2. Promoting fairness and justice
3. Protecting privacy and security
4. Ensuring controllability and credibility
5. Strengthening accountability
6. Improving ethical quality

These build upon China's 2017 New Generation Artificial Intelligence Plan, which called for China to establish ethical norms by 2025, as well as the 2019 AI Governance Principles.[47]

COMPARISON

Comparing the U.S. and China AI ethics principles shows similarities, which are depicted in Figure 1:

United States	China
1. Resonsible	6. Improving ethical quality
2. Equitable	1. Promoting human well-being 2. Promoting fairness and justive
3. Traceable 4. Reliable	5. Strengthening accountability
5. Governable	3. Protecting privacy and security

Figure 1

However, analyzing the intent behind these principles reveals key differences between Chinese and Western approaches to AI. Whereas Western society seeks to make AI compatible with democracy and the rules-based order, China's approach to AI ethics supports its authoritarian way of governing. It is important to note China's first ethical principle, "Promoting Human Well-Being," because it reveals an important distinction. In the Western context, this means protecting individual rights, and separates private entities from the state.

[45] U.S. Deputy Secretary of Defense, Kathleen Hicks, "Implementing Responsible Artificial Intelligence in the Department of Defense," Memorandum for Senior Pentagon Leadership, Commanders of the Combatant Commands, Defense Agency and the DOD Field Activity Directors (Washington, Pentagon: Department of Defense, May 26, 2021), https://media.defense.gov/2021/May/27/2002730593/-1/-1/0/IMPLEMENTING-RESPONSIBLE-ARTIFICIAL-INTELLIGENCE-IN-THE-DEPARTMENT-OF-DEFENSE.PDF.

[46] Yi Zeng, "The Ethical Norms for the New Generation Artificial Intelligence, China," International Research Center for AI Ethics and Governance, September 27, 2021, https://ai-ethics-and-governance.institute/2021/09/27/the-ethical-norms-for-the-new-generation-artificial-intelligence-china/

[47] Rebecca Arcesati, Lofty principles, conflicting incentives: AI ethics and governance in China, (Berlin: Mercator Institute for China Studies, June 2021), https://merics.org/en/report/lofty-principles-conflicting-incentives-ai-ethics-and-governance-china.

In contrast, while China's principles may appear to give individual users better control of their AI, as the China-focused European think tank MERICS notes, the CCP frames ethical questions around collective society.[48] In viewing itself as the only legitimate representative of the collective, the government exempts itself from the restrictions it imposes on companies to use an individual's data, which creates the concerns discussed in the section of this report titled, "Citizen v. State." As a result, the race to define ethical AI use has intensified the U.S.-China competition of worldviews because the winner will set the standard for AI use globally.

For the CCP, ethical principle number 4, "Ensuring Controllability and Credibility" is a means to extend control over its population. In 2021, this was most clearly demonstrated through the CCP's attempt to crack down on big tech organizations that depend upon recommendation algorithms.

The CCP views recommendation algorithms as a threat because they can influence public opinion, which therefore inhibits the CCP's ability to control messaging and information flow.[49] Consequently, in an effort to reclaim control, the CCP has drafted regulations that would require companies to submit their algorithms to the Chinese government for approval.[50] This slows company innovation and decreases the value of AI for business purposes. Additionally, the proposed regulations further diminish the power of private companies by requiring measures for improved algorithm explainability, as well as an option for users to opt out of recommendations if they feel their rights have been violated.[51]

While controversies have also arisen in the U.S. around big technology organizations and their use of AI, the U.S. has focused on strengthening protection of individual data privacy and freedom of speech, as well as improving inherent algorithmic bias. In this way, the U.S. focus on protecting the individual poses a clear contrast to the CCP, which prioritizes the interests of the state in its quest to control messaging.

The CCP views recommendation algorithms as a threat because they can influence public opinion, which therefore inhibits the CCP's ability to control messaging and information flow.[49]

[48] Ibid.
[49] Spandana Singh, "What we can learn from China's proposed AI regulations," VentureBeat, October 3, 2021, https://venturebeat.com/2021/10/03/what-we-can-learn-from-chinas-proposed-ai-regulations/.
[50] Arijit Sengupta, "China's new proposed law could strangle development of AI," Fast Company, September 15, 2021, https://www.fastcompany.com/90676516/china-ai-law-problems.
[51] Singh, "What we can learn from China's proposed AI regulations."

CONCLUSION

China's decision to produce its first written guidance on how it views ethical AI use makes 2021 an inflection point in the race for AI. With China's approach articulated, the U.S. now has the opportunity to shape AI governance in a way that clearly contrasts with the CCP's authoritarian approach. Since the U.S. does not yet have a singular document that conveys its approach to ethical AI, the U.S. can focus on developing policies that prioritize the protection of individual user rights targeted at each part of the AI development process. The U.S. can also draw the important distinction between the roles of private and public entities that China does not define. In doing so, the U.S. should work closely with like-minded allies and partners who will adopt this approach to AI as well.

In order to shape AI governance with an eye to individual user rights and clearly-defined parameters between public and private entities, it will be essential to build AI models with independent TEVV capabilities that ensure data privacy and security thresholds are met both prior to and after AI deployment. These tests will provide the accountability and visibility necessary to give users confidence in the accuracy, privacy compliance, and safety of their model's performance. As a result, with proper validation measures in place, the U.S. can protect innovation and use AI safely without overly regulating private companies.

POLICY RECOMMENDATIONS: ETHICAL AI REGULATION

- ***Conduct a full review of Department-level ethical AI frameworks*** to determine where policies align. Use these frameworks to inform national-level standards that can be implemented across Departments for testing, evaluating, verifying, and validating AI systems to ensure data privacy and security.
- ***Instead of imposing regulations, create a public-private sector working group*** that continuously monitors data privacy and security concerns and can address them in a timely manner with new or updated tests. Ensure companies of all sizes and federal agencies are represented.
- ***Conduct a review of the AI development process*** that includes a range of end users to create a process that is accepted by all of society.
- ***Incentivize companies that can prove they have independently tested and verified their AI models with additional funding*** to encourage best practices and innovation. This may support acquisition reform efforts to speed up the process safely.

TREND: 03 CHINA'S AI TALENT POOL

In the race for AI, there is one vital component to success: a strong workforce. Without a large pool of talent, innovation can only go so far. To avoid an outcome that erodes the U.S. advantage, the U.S must prioritize progress by building its talent pipeline. A look at the state of the U.S.-China talent competition in 2021 reinforces the urgency.

China has been vocal about its intentions for bolstering science and technology (S&T) skills among its population. Building upon its emphasis to modernize and increase education enrollment in the 1990s, China's strategy has focused on three fundamental pillars for S&T:

1. Improving domestic education;
2. Attracting overseas Chinese talent; and
3. Attracting foreign talent.[52]

To realize these goals, the Chinese government has increased spending into research and development of technologies such as AI to achieve "sustainability" by 2025.[53]

Additionally, during the Fourth Session of the 13th National People's Congress held in February 2021, the Chinese government committed to building more national AI labs over the next five years.[54]

As recently as September 2021, Chinese President Xi Jinping reinforced his prioritization of skill development at a conference when he said, "At the end of the day, the country's overall competitiveness is the competitiveness of its skilled personnel ... National development depends on talent, and national rejuvenation depends on talent."[55]

Understanding China's approach to accelerating educational efforts helps to assess the regime's progress in realizing its goals. Although China's efforts to improve its workforce capabilities extend beyond AI, this report focuses on how China has applied its S&T strategy to building its AI talent pipeline because whoever learns to harness AI best will significantly influence how it is used globally.

[52] Remco Zwetsloot, China's approach to tech talent competition, (Washington, DC: Brookings Institution, April 2020), https://www.brookings.edu/research/chinas-approach-to-tech-talent-competition/.
[53] Eduardo Baptista, "Xi Jinping stresses need for China to expand its talent pool, attract science and tech professionals," South China Morning Post, 29 September, 2021, https://www.scmp.com/news/china/politics/article/3150493/xi-jinping-stresses-need-china-expand-its-talent-pool-attract.
[54] Reuters, "China ramps up tech commitment in 5-year plan, eyes 7% boost in R&D spend," March 4, 2021, https://www.reuters.com/article/us-china-parliament-technology/china-ramps-up-tech-commitment-in-5-year-plan-eyes-7-boost-in-rd-spend-idUSKBN2AX055
[55] Baptista, "Xi Jinping stresses need for China to expand its talent pool, attract science and tech professionals."

IMPROVING DOMESTIC EDUCATION

Of the three pillars, China has by far made the most significant progress on improving domestic education for AI. Looking back to the 1980s confirms this assessment, as China did not report publishing any AI papers. This is expected, given China's educational modernization push took place in the 1990s and Deng Xiaoping only "opened up" China in 1978.[56] However, as educational modernization spurred efforts into AI research, China increased its paper output from 1,086 in 1997 to 37,343 in 2017, catapulting it to become the world leader by sheer number.[57] In 2021, China maintained that title, as well as one for the most AI journal citations.[58] China's progress is supported by the number of AI courses increasing across the country, coupled with China's large population and access to data due to its policy of "military-civil" fusion.

Not only has China's quantitative output improved, but also its qualitative ability. In recent years, a number of Chinese research labs and universities have climbed into the top 15 ranking list of papers published in top AI conferences.[59] This is partially due to China's large population of 1.4 billion, which far exceeds the U.S. population of 332.4 million.[60]

While the U.S. still holds the top spot, it is important to recognize current trends that will have longer term impacts if unaddressed. For example, both the number of U.S. students participating in an introductory level AI course and the number of U.S. AI PhD professors entering academia have dropped, from about 50% to 21% between the 2018-19 and 2019-20 academic years and by 44% between 2010-19, respectively.[61] In contrast, China's number of STEM PhDs will be twice that of the U.S. annually by 2025. [62]

These PhD trends must be monitored for two reasons. First, without PhD students entering academia, the U.S. may lose its advantage in research output, which will stymie technological advancement. Second, without strong professors to teach the next generation, the U.S. risks the ability to grow and sustain the workforce it is hoping to build beyond the private sector, where academia mainly goes to work. Lack of knowledge about AI in academia will only perpetuate the threats to AI use because graduates will not be adequately prepared to recognize vulnerabilities that their AI may face. In the absence of trained talent, the importance of a simple TEVV process is heightened for using AI safely and effectively. Consequently, TEVV must be a central component of all artificial intelligence curricula, particularly for those who will become AI users for critical systems.

[56] Zwetsloot, China's approach to tech talent competition.
[57] Daitian Li, Tony W. Tong, and Yangao Xiao, "Is China Emerging as the Global Leader in AI?" Harvard Business Review, February 18, 2021, https://hbr.org/2021/02/is-china-emerging-as-the-global-leader-in-ai.
[58] Zhang et al., "The AI Index Report 2021."
[59] "ChinAI: The Talent," Paulson Institute: MacroPolo, Digital Report, https://macropolo.org/digital-projects/chinai/the-talent/.
[60] Shashank Jacob, "Chinese AI Research and Business is Booming, but America is Still King," Bezinga, October 12, 2021, https://www.yahoo.com/now/chinese-ai-research-business-booming-135519057.html; United States Census Bureau, "U.S. and World Population Clock," https://www.census.gov/popclock/.
[61] Zhang et al., "The AI Index Report 2021."
[62] Ibid.; Graham Allison, "America needs a 'Million Talents Program' now," The Hill, September 28, 2021, https://thehill.com/opinion/technology/574160-america-needs-a-million-talents-program-now

ATTRACTING OVERSEAS CHINESE TALENT

Despite the progress China has made in growing its AI talent pool, it performs poorly on its second pillar "attracting overseas Chinese talent." Even with significant investment into recruitment programs such as the Thousand Talents Plan, China struggles to retain its talent because individuals often choose to live in other places, such as the United States. In fact, many of the top Chinese AI researchers and PhDs work for American companies. This diverse talent pool benefits AI advancement in the U.S. by strengthening the size of the U.S. AI workforce. However, a growing U.S. AI workforce does not immediately make AI safer to deploy; different experiences with AI creates varied conceptions across the workforce about what constitutes "responsible use", which may lead to undetected vulnerabilities. Consequently, instituting a standard process to independently test and validate algorithms will maximize the U.S. AI workforce's talent while protecting everyone from vulnerabilities that they may not identify under their own conception of "responsible use."

ATTRACTING FOREIGN TALENT

Likewise, China struggles to attract foreign talent. As the Center for Security and Emerging Technology (CSET) notes, few students choose to live in China after graduating from AI programs, with less than 20% coming from the United States.[63] Of the foreign students that are in China, 65% come from Belt and Road countries.[64] Looking at the numbers and patterns, this is less concerning for the U.S. than protecting its AI-related intellectual property and systems against potential attacks.

> **Few students choose to live in China after graduating from AI programs, with less than 20% coming from the United States.[63]**

[63] Remco Zwetsloot, James Dunham, Zachary Arnold, and Tina Huang, Keeping Top AI Talent in the US (Washington, DC: CSET, January 2018), https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf.
[64] Zwetsloot, China's approach to tech talent competition.

CONCLUSION

While 2021 revealed concerning trends for Chinese AI talent development, the U.S. still maintains the advantage in that many top researchers study and choose to live in the U.S. long-term, rather than return to China, including about 90% of international AI PhDs.[65] However, with President Xi Jinping's continued investments in talent and AI research and development (R&D) efforts, the U.S. must think about how to grow its domestic talent pool while protecting its systems. The U.S. must also increase its government spending to attract and retain talent. Efforts in 2021 such as the establishment of the U.S. Digital Corps and the Central Intelligence Agency's (CIA) Technology Fellows program are commendable starts, but much more must be done. With AI accelerating globally, adversarial tactics will only become more sophisticated. Therefore, the U.S. must train talent that is agile enough to recognize emerging and existing vulnerabilities, and that can produce the research needed to develop testing methods that keep pace with these threats. By maintaining TEVV research output, the U.S. will ultimately reach a point whereby it can automate TEVV processes. This will be critical to continued AI progress because existing brainpower can focus on development, as opposed to implementing manual security checks.

[65] Zwetsloot, Dunham, Arnold, and Huang, Keeping Top AI Talent in the US

POLICY RECOMMENDATIONS: CHINA'S AI TALENT POOL

- ***Increase federal funding*** for AI talent growth. Specifically, provide additional funding to universities that increase participation in introductory AI courses.
- ***Create a federal scholarship program*** for pursuing a degree in an AI-related field and guarantee a first job working on improving AI TEVV for the federal government.
- ***Create an international student program*** to facilitate a dialogue on AI collaboration and shaping AI security best practices.
- ***Allocate additional funding for federally funded research and development centers (FFRDCs)*** to specifically research new TEVV methods.
- ***Create more private-public partnership programs*** to increase academic and private sector participation in government.

TREND: 04 AI IN AGRICULTURE

The landscape of AI supporting critical industries evolved substantially in 2021, including applications in cybersecurity, supply chain resiliency, and medical care. While these verticals received significant press attention due to an increase in cyberattacks and continued efforts to address COVID-19 disruptions and improve treatments, AI advancements extended to other key areas that, with heightened attention and investment, have the potential to accelerate the ability of the U.S. to adopt AI at scale.

Notably, in 2021, we witnessed the expansion of the AI market in agriculture; from agricultural robotics to soil and crop monitoring to predictive analytics, AI is becoming an integral part of the fight to feed the future.[66] If done effectively, AI in agriculture also has the potential to address many of the supply chain issues and labor shortages caused by the COVID-19 pandemic, which is why adoption is increasing quickly in a typically slow-to-change industry. As a result, since AI in agriculture advancements are still nascent, they create a high reward opportunity to effectively build, refine, and measure an AI testing ecosystem.

Artificial intelligence in agriculture also presents a clear, practical example of how the U.S. and China differ in their approaches to AI. Whereas the U.S. prioritizes safety and resiliency in its deployments of AI in agriculture, the CCP is strengthening its surveillance efforts.

For example, in 2021, 87% of executives in the U.S. agricultural sector report AI use in their business, which is up from 74% in 2020. Of these executives, 90% also reported that they believe implementing ethical standards in the development of their AI technologies can represent a competitive advantage for their business.[67] In contrast, the CCP has used its Digital Village initiative to aggressively deploy frontier technologies like AI to rural communities, where 25% of the Chinese population lives and works on farms.[68] Although this initiative presents an opportunity to improve agrarian practices in China, the CCP has used it to simultaneously expand its public security surveillance efforts over its population through providing new technologies that perform activities such as facial recognition and motion detection.[69]

At the same time, the CCP is engaging in agricultural espionage to accelerate their progress. According to the FBI, Chinese espionage targeting U.S. agricultural technologies have increased by over 1,300% in recent years,[70] in what is reportedly the most expansive heist in farming history.[71] Lawmakers are also concerned about China's control of the food supply, given China has increased its investment into foreign farmland over the last decade such that it now owns 192,000 acres in the U.S. worth $1.9B, as of the beginning of 2020.[72] The clear contrast between how China and the U.S. use AI and accelerate their technological development presents an opportunity for the U.S. to use TEVV as a means to promote responsible AI use, as well as to protect its technological advancements in the AI competition.

[66] Konstantina Spanaki et al., "Disruptive technologies in agricultural operations: a systemic review of AI-drive Agritech research," Annals of Operations Research (2021), https://doi.org/10.1007/s10479-020-03922-z.
[67] RELX, 2021 RELX Emerging Tech Executive Report - Executive Summary (RELX: 4th edition, 2021), https://www.relx.com/~/media/Files/R/RELX-Group/documents/press-releases/2021/2021-relx-emerging-tech-exec-summary.pdf.
[68] Line Heidenheim Hule, "How tech is transforming agriculture in China," China Experience: Insights for future business, May 6, 2021, https://www.china-experience.com/china-experience-insights/how-tech-is-transforming-agriculture-in-china.
[69] GetNews, "China Mobile's Peaceful Village Initiative tends to make China's rural area safer by intelligent monitoring facilities," Digital Journal, December 3, 2020, https://www.digitaljournal.com/pr/4901553.
[70] Gina Heeb," FBI Says It Opens New Espionage Investigation into China 'Every 10 Hours,'" Forbes, April 14, 2021, https://www.forbes.com/sites/gina-heeb/2021/04/14/fbi-says-it-opens-new-espionage-investigation-into-china-every-10-hours/?sh=1b82b6457a5d.
[71] Chris Bennett, "While America Slept, China Stole the Farm," AgWeb, June 8, 2021, https://www.agweb.com/news/business/technology/while-america-slept-china-stole-farm.
[72] Ryan Morgan, "China is buying billions in US farmland and lawmakers are scrambling to try to stop them," American Military News, July 20, 2021, https://americanmilitarynews.com/2021/07/china-is-buying-billions-in-us-farmland-and-lawmakers-are-scrambling-to-try-to-stop-them/.

U.S. TECHNICAL ADVANCEMENTS IN THE AGRICULTURAL SECTOR

Food and agriculture account for one-quarter of the world's greenhouse gas emissions,[73] while livestock account for an additional 14.5% - a figure that is projected to increase in parallel with the ballooning global population.[74] According to United Nations (UN) projections, the global population will increase by over two billion people by 2050, and in turn, food production must increase by 60%.[75] Consequently, by unlocking the efficiency and scale at which farmers and manufacturers can produce and deliver food, AI can be leveraged to test, iterate, and scale agricultural production at a pace not previously achievable.[76]

To support the healthy growth of crops and ensure higher yields, AI-enabled drones can obtain aerial views of cultivated fields, and generate 3D maps to monitor the health of crops or check soil conditions through geosensing. Compared with manual operations, the real-time monitoring of crop growth by computer vision technology enables the detection of subtle changes in crops due to malnutrition much earlier than human monitoring.[77] Farmers can leverage deep learning paired with satellite imagery to efficiently gather information on soil conditions, nitrogen levels, moisture, and a crop's historical yield data to accurately predict annual yields.[78]

AI-enabled drones are capable of monitoring infected crops and spraying pesticides to prevent insects and pests through computer vision technology that enables the drones to precisely detect the infected crops and spray the pesticides accordingly. Artificial intelligence can similarly be used to sort good crops from bad crops and determine which will be stable for longer shipments and which will go bad first and must be shipped to local markets.[79]

In each use case, computer vision technology is applied to aspects of the agricultural production management lifecycle to solve food production challenges and improve the performance of agricultural systems. AI-powered solutions enable farmers to improve efficiencies in crop production while improving the quantity and ensuring a faster go-to-market for crops.[80] However, while these examples clearly demonstrate the power of AI, a key component of effective deployment is ensuring computer vision models correctly classify images. Machine learning systems, like the ones used in agriculture, have an increased potential for failure, such as bias due to a distribution shift in data, or model drift which occurs when the accuracy of predictions produced from new input values skews away from a model's performance during the training period. As a result, it will be important to implement robust TEVV in agricultural systems to ensure they are performing as intended.

[73] Hannah Ritchie and Max Roser, Environmental Impacts of Food Production, (England: University of Oxford - Our World in Data, January 2020), https://ourworldindata.org/environmental-impacts-of-food.
[74] Maarten Elferink and Florian Schierhorn, "Global Demand For Food Is Rising: Can We Meet It?" Harvard Business Review, April 7, 2016, https://hbr.org/2016/04/global-demand-for-food-is-rising-can-we-meet-it.
[75] United Nations, Growing at a slower pace, world population is expected to reach 97 billion in 2050 and could peak at nearly 11 billion around 2100 (New York: United Nations, June 2019) https://www.un.org/development/desa/en/news/population/world-population-prospects-2019.html.
[76] Louis Columbus, "10 Ways AI Has The Potential To Improve Agriculture in 2021," Forbes, February 17, 2021, https://www.forbes.com/sites/louiscolumbus/2021/02/17/10-ways-ai-has-the-potential-to-improve-agriculture-in-2021/?sh=713b09967f3b.
[77] Hongkun Tian et al., "Computer vision technology in agricultural automation- A Review," Information Processing in Agriculture, vol. 7, issue 1 (March 2020): 1-19, https://doi.org/10.1016/j.inpa.2019.09.006.
[78] Saeed Khaki and Lizhi Wang, "Crop Yield Prediction Using Deep Neural Networks," Frontiers in Plant Science (May 2019), https://doi.org/10.3389/fpls.2019.00621.
[79] Tian et al., "Computer vision technology in agricultural automation- A Review."
[80] Ibid.

Despite their benefits, farmers may be deterred from investing in AI systems due to their cost and the need for a technical user. Consequently, in order for these technologies to perform tasks such as yielding healthier crops, controlling pests, monitoring soil and growing conditions, organizing data for farmers, helping with workload, and improving tasks across the entire food supply chain, they must be easy to use and have interpretable metrics. One key way to do this will be to improve TEVV such that this process can be automated, or achieved through user-friendly third-party testing. This capability is currently growing within the space of AI TEVV, meaning that the agricultural sector presents a great way to advance TEVV R&D efforts. In doing so, the U.S. can continue to improve its practices such that it can apply TEVV to other critical sectors, including those mentioned at the beginning of this section, and can impact significant national security-related outcomes, such as improving food security for military members whose nutrition is linked to their overall readiness.[81]

CHINA'S UNETHICAL USE OF AI IN THE AGRICULTURAL SECTOR

China is similarly leveraging AI to rapidly advance their agricultural industry. A 2017 McKinsey report made clear that farming was one of China's industries left furthest behind in smart technologies, but also has the widest margin for growth.[82]

A decade ago, the CCP announced a new farmland projection for the cultivation of an additional 132 million acres in 10 years, turning acreage outsizing the state of California into high standard farmland.

As of 2021, they have expanded their farmland to roughly the size of Ireland and have used the Belt and Road Initiative as a way to secure food supply for China's population of 1.4 billion.[83] Just as alarming as the Belt and Road Initiative is the CCP's Made in China 2025, which outlines the CCP's plan for domination of 10 high-tech sectors by 2025, and notably includes agricultural technology.[84]

"As of 2021, they have expanded their farmland to roughly the size of Ireland and have used the Belt and Road Initiative as a way to secure food supply for China's population of 1.4 billion.[83]"

[81] "Terri Moon Cronk, "Defense Official Says Food Insecurity Is a Readiness, National Security Issue," DOD News, U.S. Department of Defense, July 27, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2709598/defense-official-says-food-insecurity-is-a-readiness-national-security-issue/.

[82] Jonathan Woetzel et al., Digital China: Powering the Economy to Global Competitiveness (New York: McKinsey & Company, December 2017), https://www.mckinsey.com/featured-insights/china/digital-china-powering-the-economy-to-global-competitiveness.

[83] Andrew Chatzky and James McBride, China's Massive Belt and Road Initiative (New York: Council on Foreign Relations, January 2020), https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

[84] Craig Moran, "China is Spearheading the Future of Agriculture," RealClearScience, June 30, 2018, https://www.realclearscience.com/articles/2018/06/30/china_is_spearheading_the_future_of_agriculture.html.

In the last decade, the CCP has invested heavily in technology solutions for agriculture. For example, as of September 2021, China established 18 unmanned pilot agricultural zones for 14 types of crops in 12 provinces, where self-driving agricultural machinery saved up to 30% in pesticides and 50% of labor costs.[85]

Tech giants Huawei, Alibaba, and Jd.com also developed surveillance systems for pigs and cows to help farmers monitor and manage livestock, and equipped chickens with internet of things (IoT) devices that store information like how many steps the chicken ran before it became a consumer's Tuesday night dinner.[86]

In 2021, the CCP accelerated its experiments using a combination of AI, big data, drones and autonomous agricultural machinery. For example, an AI-assisted team of researchers recently beat traditional farmers in a strawberry growing competition where Chinese researchers demonstrated the efficacy of intelligent sensors, data analysis and fully digital greenhouse automation to produce 196% more strawberries than traditional farmers.[87]

Alibaba Cloud debuted its proprietary ET Agricultural Brain initiative, and results were instant. Tequ Group, a Sichuan-based pig farming enterprise, used Alibaba's Cloud Intelligence platform to induce pigs to give birth to three additional newborns each year. Similarly, Chinese produce company, Haisheng Group, saved $3 million USD per apple farm last year using Alibaba's technology.

Importantly, in parallel with the deployment of AI-enabled agricultural technologies, a 2021 report detailed how the digitization of rural communities has accelerated state surveillance outside of major cities in China.[88]

Sharp Eyes, for example, is one of the CCP's technological surveillance projects for small, rural villages and contributes to the 200 million security cameras installed across China used to surveil citizens.[89]

[85] "Intelligent technologies drive China's agricultural modernization," Xinhua Net, 1 January, 2021, http://www.xinhuanet.com/english/2021-01/01/c_139635020.htm.

[86] Rita Liao, "Alibaba gets into farming - without getting its hand dirty," Tech in Asia, 7 June, 2018, https://www.techinasia.com/alibaba-ai-et-brain-agriculture.

[87] Winston Ma, "AI strawberries and blockchain chicken: how digital agriculture could rescue global food security," World Economic Forum, 26 January, 2021, https://www.weforum.org/agenda/2021/01/china-digital-agriculture-global-food-security/.

[88] Dave Gershgorn, "China's 'Sharp Eyes' Program Aims to Surveil 100% of Public Space," One Zero, March 2, 2021, https://onezero.medium.com/chinas-sharp-eyes-program-aims-to-surveil-100-of-public-space-ddc22d63e015.

[89] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame, and Lots of Cameras," New York Times, July 8, 2018, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

As part of the CCP's 2016 five-year plan, Sharp Eyes was set to achieve 100% coverage of China's rural communities by 2020 and publicly available reports suggest the CCP has gotten very close to hitting their goal.[90]

The problem with these advancements in agricultural AI are two-fold: they are not solely due to Chinese innovation, given the CCP is investing in economic espionage to pilfer technological advancements abroad; and they extend the overreach of the state. According to a recent report by the FBI, a new China-related counterintelligence case opens every 10 hours. Of the cases that involve gaining access to sophisticated U.S. technology, China demonstrates a keen interest in the latest advances in the agriculture industry.[91]

Chinese espionage and trade secret theft against biotechnology and agricultural companies is on the rise, with the CCP targeting U.S. companies, universities, and government research facilities for agricultural information concerning plant genome, new variety development, and advanced manufacturing processes.[92]

As part of the CCP's espionage efforts, the People's Liberation Army (PLA) uses the saying, 'Picking flowers in foreign lands to make honey in China.'[93]

For example, in 2011, the FBI began a multi-year investigation into the U.S. director of international business for Beijing Dabeinong Technology Group after he was spotted crawling through Iowa corn rows.[94] The FBI ultimately found that he was smuggling hundreds of seed samples back to China. Similarly, a Chinese Kansas State University student recently gained access to a climate-controlled seed room and stole samples representing $75 million in research.[95]

Additionally, a Chinese scientist working for Monsanto was recently stopped at a U.S. airport with a micro SD card copy of a proprietary algorithm tagged the Nutrient Optimizer. The scientist's case, ruled in the Eastern District Court of Missouri in October 2021, ultimately found evidence that China is currently conducting a historical, mass raid of the American farm. [96]

Promisingly, the Agricultural Intelligence Measures (AIM) Act proposed the creation of an intelligence-gathering office within the U.S. Department of Agriculture (USDA) so that the U.S. can "focus on understanding foreign efforts to steal U.S. agriculture knowledge and technology." This signifies an important acknowledgement and step forward to ensuring the security of critical emerging U.S. technologies.[97]

[90] Charles Rollet, "China Public Video Surveillance Guide: From Skynet to Sharp Eyes," IPVM, June 14, 2018, https://ipvm.com/reports/sharpeyes.
[91] Christopher Wray, "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States, Federal Bureau of Investigation, Remarks as delivered (Washington, DC: Hudson Institute, July 7, 2020), 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
[92] Federal Bureau of Investigation, "Agricultural Economic Espionage, A Growing Threat," U.S. Department of Justice (2017), https://ucr.fbi.gov/investigate/counterintelligence/agricultural-economic-espionage-brochure.
[93] Alex Joske, Picking flowers, making honey: The Chinese military's collaboration with foreign universities, Australian Strategic Policy Institute (October 2018), https://www.aspi.org.au/report/picking-flowers-making-honey.
[94] Del Quentin Wilber, "The saga of the Chinese spies and the stolen corn seeds: Will it discourage economic espionage?" Los Angeles Times, October 31, 2016, https://www.latimes.com/nation/la-na-seeds-economic-espionage-20161031-story.html.
[95] The Office of Public Affairs, U.S. Department of Justice, "Chinese Scientist Sentenced to Prison in Theft in Engineered Rice," Press release, April 4, 2018, https://www.justice.gov/opa/pr/chinese-scientist-sentenced-prison-theft-engineered-rice.
[96] United States District Court, Eastern District of Missouri, United States, Plaintiff v. Haitao Xiang, Defendant, 4:19CR980 Hearing, Opinion, Memorandum, and Order by Henry Edward Autrey United States Court Judge (October 15, 2021), https://casetext.com/case/united-states-v-haitao-xiang.
[97] U.S. House Agriculture Committee and U.S. House of Representatives Permanent Select Committee on Intelligence, Agriculture Intelligence Measures Act or the AIIM Act, 117th Cong., H.R.1625 (March 8, 2021), https://www.congress.gov/bill/117th-congress/house-bill/1625.

CONCLUSION

As espionage efforts are likely to continue with a focus on AI technologies utilized in the agriculture sector, U.S. advancements in TEVV will continue to highlight the differences in AI approaches between the U.S. and China. Through the United States' repeated prioritization of building trust in AI systems through testing, the U.S. subsequently enables farmers to better understand their technologies through comprehensive model evaluation and validation features. Thus, through agriculture, AI becomes increasingly user-friendly and accessible to the general public.

Additionally, while China continues to engage in espionage to accelerate their agricultural technologies, the U.S. has a unique opportunity to further ethical, transparent, and secure technology. Analyzing the agricultural sector application of AI reveals the promise TEVV yields for U.S. technological advancements. Not only will it enable the U.S. to accelerate AI adoption through furthering R&D efforts in a high-reward environment, but also will help set a precedent for responsible AI use. As such, for the U.S. to maintain its strategic advantage, TEVV for AI in agriculture is critical.

POLICY RECOMMENDATIONS: AI IN AGRICULTURE

- ***The DoD's Sustainability Report and Implementation Plan*** should include T&E policies to quantify the effectiveness of AI technologies deployed to support the Department's climate mitigation strategies.
- ***Leverage AI for carbon pledge verification*** to ensure regenerative agriculture practices are validated and verifiable.
- ***Leverage AI to better track Hydrofluorocarbons (HFC) production*** and require synthetic greenhouse gas producers utilize independent TEVV to ensure the validity of the models and quantify progress.
- ***Increase investment into AI TEVV for computer vision models***, with the goal of automating practices such that TEVV will accelerate the agricultural sector's ability to deploy models safely into the field and improve food security challenges.

LOOKING AHEAD: 2021 - 2022

In addition to technical progress, AI advancements in 2021 brought moral questions to the forefront. From rising tensions driven by the relationship between state and citizen, to the increasing prevalence of ethical documents, the globe has wrestled with questions of how AI should be used. These questions may not be easily answered and will surely continue into 2022. However, whether they are explicitly answered or not, the increasing pace of AI development across business and society means AI use will inevitably be defined by how it is adopted. As a result, it is imperative for the U.S. and its allies to think about managing risk within models before they are deployed; otherwise, models that are not sufficiently tested and validated may perform in ways that do not align with Western values.

In 2022, the U.S. has an opportunity to make major strides while it still maintains the lead in AI. With China's ethics position articulated, the U.S. now can work with like-minded allies and partners to promote a global standard for AI use and draw a clear contrast to the CCP's authoritarian use against its citizenry. As 2021 confirmed, China focuses on protecting the state by controlling information flow. In contrast, the U.S. focuses on protecting the individual through promoting data privacy and responsible use, as well as by distinguishing between private and public entities. The differentiation between AI use for state and citizenry is a defining question because it reflects the worldviews both countries espouse. In this way, it sits at the core of the U.S.-China competition.

In 2021, we witnessed one area where the U.S. can make a difference in defining responsible use standards with TEVV: AI-enabled agricultural activities. While this work is still in early stages, there are trends that will gain increasing attention in 2022, such as the use of AI and blockchain to track the lifecycle of food down to how it is shipped and stored. Since this use case concurrently addresses the issue of China's agricultural espionage, it may have major implications for who succeeds in the U.S.-China competition. As a result, the U.S. must ensure it has strong TEVV practices in place to protect the AI it is increasingly using to reduce carbon emissions, find agricultural efficiencies, improve labor shortages, and enhance supply chain resiliency.

While the U.S. maintained the lead in AI in 2021, leading is not a guarantee. Consequently, the U.S. will need to take active measures to retain its qualitative advantage. This involves encouraging more researchers to stay in academia, where they can sustain the quantity and quality of research output. Additionally, they can ensure the next generation receives a top-notch AI education, which will continue to grow its domestic workforce in both public and private sectors. In 2022, creating more educational programs across the workforce will become increasingly important for AI development and safe adoption. These skills must include properly testing, evaluating, verifying, and validating AI systems and ensuring that these methods are constantly updated. As businesses and society increasingly adopt AI, coupled with the rapid advancement of technology, the U.S. workforce must keep up with threats to AI systems. If they do not, they risk eroding their AI advantage by making their systems prone to vulnerabilities, or may deploy AI that behaves contrary to the ethical considerations that gained more attention in 2021.

In 2021, the world woke up to what it means to use AI. Now, in 2022, they can use TEVV to uphold this meaning and accelerate our advancement.