Combating AI Bias Through Responsible Leadership

Artificial intelligence — once just the fascination of science fiction writers — is now poised to transform the global economy and permeate lives in ways never thought possible. Chatbots help schedule appointments. Smart thermostats automatically adjust and warm or cool to one's liking. Refrigerators remind us when we're running low on milk.

Analysts suggest that AI will grow the global economy by $15.7 trillion by 2030, and the international big-data analytics industry alone is expected to grow from $130.1 billion in 2016 to more than $203 billion by 2020.

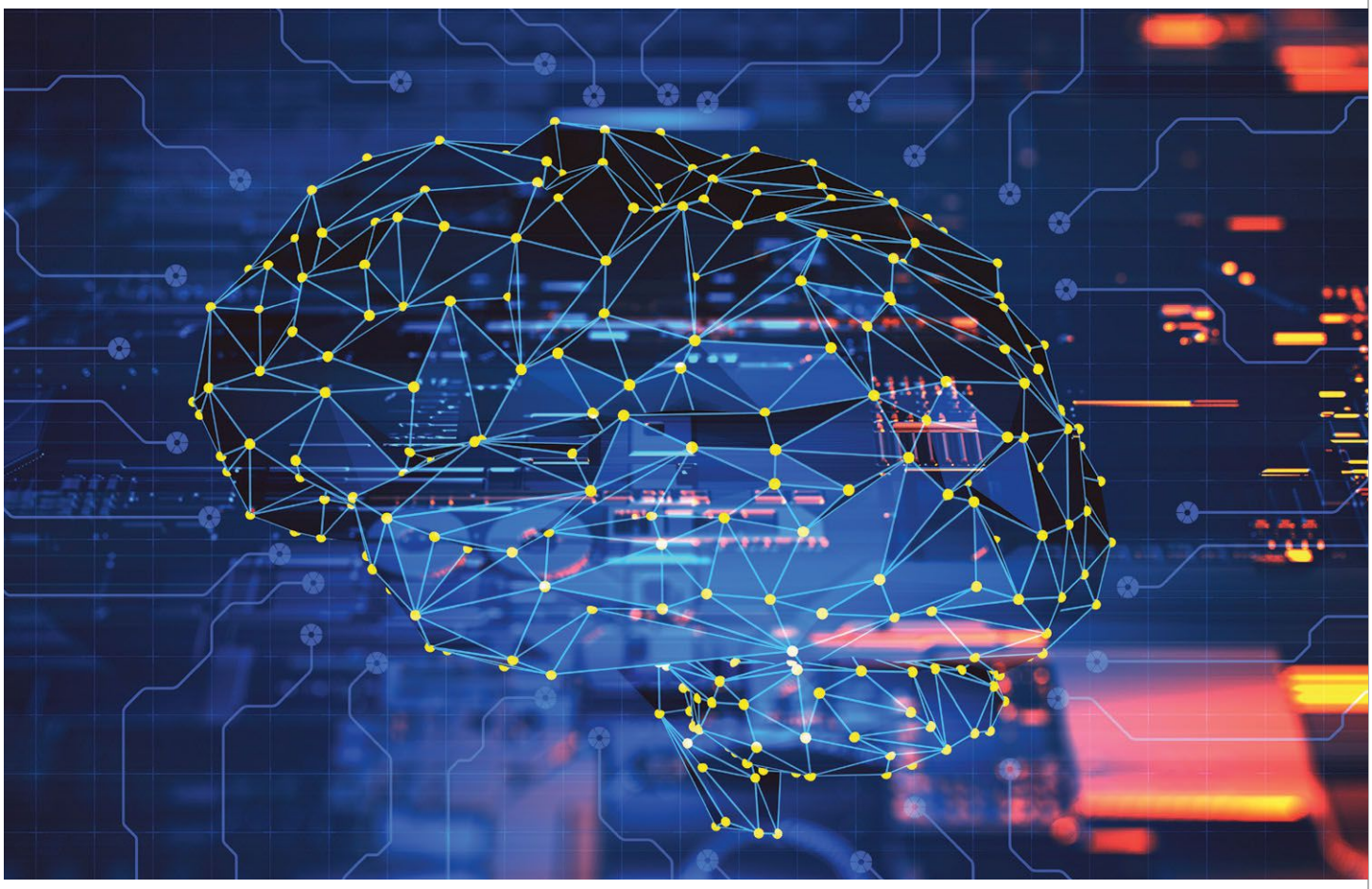
Living and working in this age of technological possibilities is intriguing and exciting — and made even more so because the U.S. government actively supports and promotes AI's advancement. However, the speed with which we're advancing and embracing innovations in artificial intelligence are outpacing efforts to fully understand and mitigate its challenges, notably the inherent biases hidden in the AI algorithms used to inform decisions.

As long as that remains the case, and in spite of its projected positive global economic impact, AI's proliferation will continue to give rise to concerns about its ethical and responsible use, its role in decision-making and its impact on leaders' executive function, the cognitive processes that make it possible to plan, focus attention, remember, juggle multiple tasks and think flexibly.

U.S. government agencies already are making significant investments in the field. The National Science Foundation invests over $100 million each year in its research. The Defense Advanced Research Projects Agency is investing $2 billion in its AI Next campaign, a project that aims to build more trusting, collaborative partnerships between humans and machines.

The Defense Department created the Joint Artificial Intelligence Center to coalesce the military services and defense agencies' AI initiatives. Additionally, last year the Department of Energy's Oak Ridge National Laboratory unveiled Summit, the world's most powerful and smartest scientific supercomputer, surpassing China's 93-petaflop TaihuLight, which had been the world's fastest supercomputer since 2016.

AI's strength in predictive analytics provides the intelligence community a significant strategic advantage by enhancing early warning cyber attack indicators, boosting intrusion detection and monitoring, heightening analysis and integration, enhancing software analysis, and reinforcing strategic and tactical planning of cyber operations. AI algorithms across all phases of a cyber attack, such as social engineering, vulnerability discov-



ISTOCK

ery and exploit development targeting, can be used to target and exploit vulnerable enemy AI-enabled assets.

AI's power is its unmatched ability of pattern recognition, anomaly detection and predictive analytics. However, its weakness is its inability to discover and destroy the biases programmed in its algorithms. This flaw has a direct and potentially detrimental influence on the decision-making of leaders in the private and public sectors.

The reuse of code from various programs by developers has seeded the progression of barely distinctive webs of algorithms that rewrite their own code, generate rules and create their own truth. This observable fact is rapidly disengaging AI algorithms from human control and oversight. In the wake of unfettered and unchallenged AI algorithms, decision-makers are unavoidably inundated by big data, and precipitously surrender to AI bias without question.

Biased algorithms have been known to levy cruel and uneven consequences. They drive decisions on job selections, prison sentencing guidelines, the stock market, housing loans, credit scores, college admittance, and a multitude of other decisions every day that profoundly affect people's lives. Consider, for instance, the dire consequences of AI bias regarding decisions on prison sentencing, which are based, in part, on recidivism scores generated by criminal risk assessment algorithms.

Populations that are historically and disproportionately targeted by law enforcement face the daunting reality of being given higher recidivism scores. Consequently, because of the entrenched biases in the data and algorithms, a vicious sentencing cycle is perpetuated. Because most criminal risk assessment tools are proprietary, it's not possible to interrogate decisions that are made or to hold decision-makers accountable.

Mathematically powered algorithms are based on the choices of imperfect humans, even if those choices are made with the best of intentions. Countless software system models, which increasingly manage cybersecurity environments, are encoded with human prejudice, dislikes, elucidations and bias. Without proper interrogation, as in the prison-sentencing example, these obscure biased algorithms, which lack transparency, could be the decision between life and death.

Artificial intelligence also has the potential to turn the workforce upside down. As it transforms the global business and decision-making landscape, leaders must prepare for a new paradigm. Managers will need to adapt by leaving repetitive tasks such as accounting, human resources and administrative management to AI so that they can concentrate on harnessing the power of AI and emerging technologies to calibrate and construct swifter and more economical methods to deliver products and services to customers, while harnessing the creativity of employees in a diverse and integrated fashion.

This shift in leadership roles will have a direct effect as well on executive function, the part of the brain that regulates analytics, verbal reasoning, inhibition, discretion, mental flexibility and complex decision-making among other traits. What impact will AI have on the executive function of decision-makers?

Arguably, humans are erecting systems beyond their intellectual means to control them. Leaders are likely to reject or suppress their own cognitive instincts by surrendering authority and executive function to AI, regardless of its biases.

The ethical ramifications for the immeasurable separation between algorithms and real people are great. Ultimately, leaders will have to decide who will make the decisions and who will assume liability and responsibility for the decisions made. If AI is to take an essential position in business, leaders must strengthen their executive functions and detect and remove bias to ensure fairness, transparency and, ultimately, trust.

"Responsible AI," a term of art used to address the growing concern of AI bias, integrates risk mitigation and ethical concerns into algorithms and data sets from the start. Responsible AI is a holistic approach to governance that includes rules as well as evidence-based management practices, which take execution and oversight into account throughout the entire AI lifecycle.

The technical and societal challenges and risks associated with AI, which impact nearly every facet of one's life, must be addressed through robust technical standards and governance. On the governance side, the National Institute of Standards and Technology is a sensible starting point. Current NIST research already focuses on how to measure and enhance the security and trustworthiness of AI systems.

Human interrogation and oversight of AI's underlying algorithms must also be employed to eradicate bias and reduce the risks of using it in business decisions. Proper governance and security measures, such as rapid-detection mechanisms to correct and terminate rogue AI elements and the continuous monitoring and updating of algorithms, will ensure that authentic experiences and user feedback are integrated at all times. AI is considered by many to be better at decision-making than human intelligence. However, this doesn't necessarily mean that AI makes better decisions. The technology exploits the critical thinking skills that humans possess and coalesces them with enormous computational power. Thus, the need to acknowledge the complementary power of human intelligence in relation to AI is essential.

> "If AI is to take an essential position in business, leaders must strengthen their executive functions and detect and remove bias to ensure fairness..."

As example of this partnership's positive effect, a team of pathologists from Harvard created an AI tool that detects cancer cells with 92 percent accuracy. When using conventional tools, the pathologists detected cancer cells with 96 percent accuracy. But, most notably, when the two combined forces the results were significantly more accurate at 99.5 percent.

AI's impending disruptions are not likely to arrive all at once. However, the thrust of development is rapid and the ramifications more extensive than most executives and decision-makers recognize. Leaders who are prudent can investigate the future posture of the workforce and prepare for the advent and dominance of artificial intelligence.

To plot a course in this uncertain future, leaders must redefine their roles and enact responsible AI by setting forth laws and regulations to identify the boundaries for its use in decision-making and its consequences and impact on leadership and their authority, all without stifling innovation. ND

Tamie Santiago is a collegiate associate professor of cybersecurity management and policy at the University of Maryland University College, Global Campus.