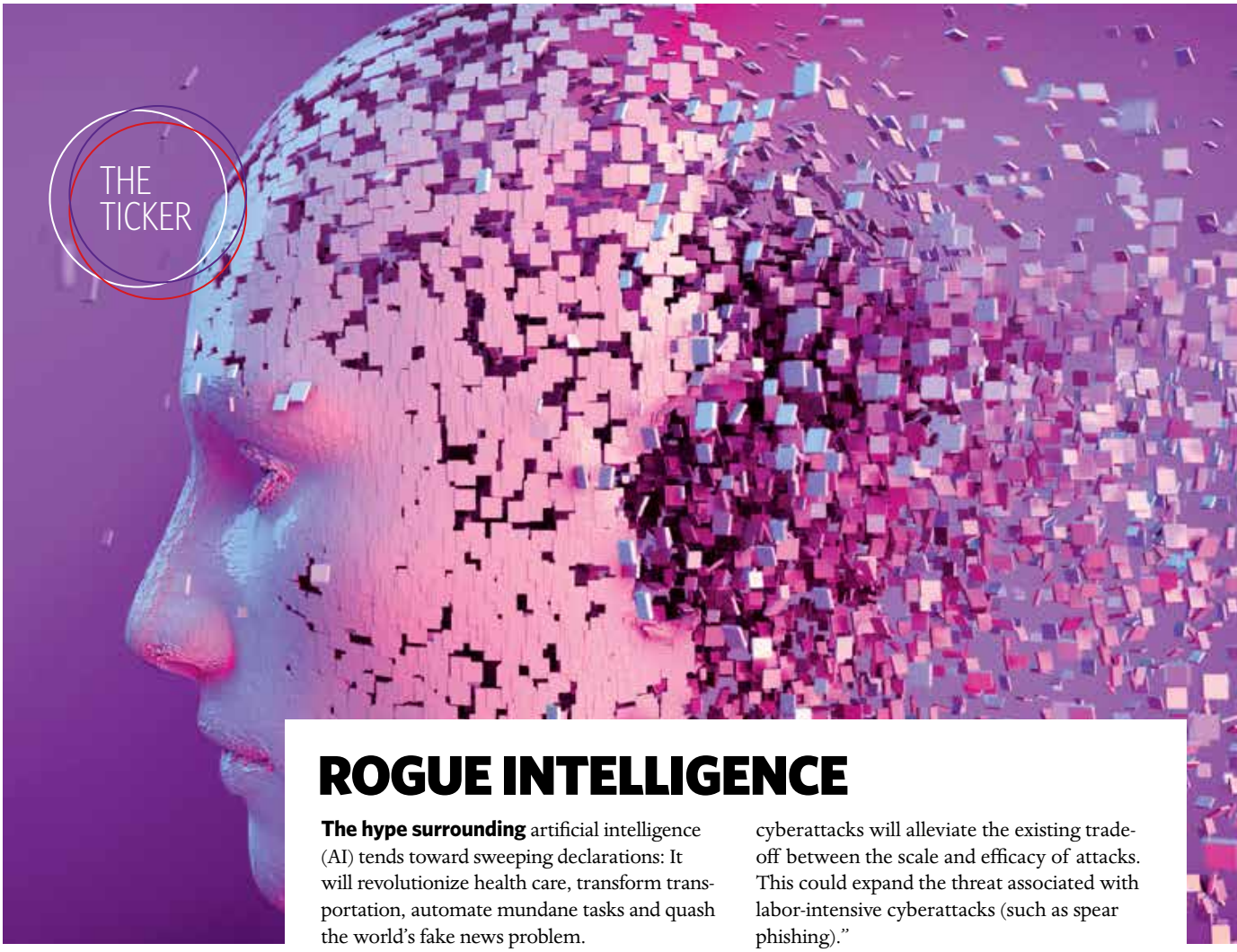

ISTOCKPHOTO

ROGUE INTELLIGENCE

The hype surrounding artificial intelligence (AI) tends toward sweeping declarations: It will revolutionize health care, transform transportation, automate mundane tasks and quash the world's fake news problem.

But all this world-saving potential might come with a dark side that goes well beyond eliminating jobs. AI as it exists today—not some far off "superintelligence" akin to general human intelligence, but the kind of tech companies like Google are now deploying or that is plausible in the next five years—could be exploited by rogue states, terrorists and criminals. That is according to *The Malicious Use of Artificial Intelligence*, a report published earlier this year by AI experts at a number of institutions, including the University of Cambridge, and research firm OpenAI.

These AI-backed attacks will be both digital and physical. The latter could come in many forms, the report's authors write. They include drones and other physical systems, such as the deployment of autonomous weapons systems and autonomous vehicles that have been overtaken and forced to crash. These are new kinds of threats.

Digital attacks aided by AI, on the other hand, will be more familiar—but made easier and more devastating thanks to AI's rise. According to the report, "The use of AI to automate tasks involved in carrying out cyberattacks will alleviate the existing trade-off between the scale and efficacy of attacks. This could expand the threat associated with labor-intensive cyberattacks (such as spear phishing)."

This scenario is not down the road a bit—it is arriving now. Sixty-two percent of security experts believe that AI will be weaponized and used for cyberattacks this year, according to a survey by U.S. software firm Cylance. Similarly, a group of AI scientists and experts wrote open letters to political leaders in Canada and Australia in November 2017 urging them to ban weaponized robots capable of autonomously deciding whether people live or die.

"Lethal, autonomous weapons systems that remove meaningful human control from determining the legitimacy of targets and deploying lethal force sit on the wrong side of a clear moral line," an open letter to Canadian Prime Minister Justin Trudeau stated.

The group calls for an international agreement on banning such systems, *Newsweek* reported. Its letter ends ominously: "If developed, they will permit armed conflict to be fought at a scale greater than ever, and at timescales faster than humans can comprehend. The deadly consequence of this is that machines—not people—will determine who lives and dies."

STARTING A TWEETSTORM

The backlash is going strong. After the 2016 U.S. presidential election, Twitter came under fire for providing Russia-backed automated accounts with a platform to stoke political divisions. But long before that, the tech company was facing criticism for enabling a culture of bullying and misogynistic abuse to grow and fester.

CEO Jack Dorsey acknowledged the problems in a series of tweets sent in March. "We have witnessed abuse, harassment, troll armies, manipulation through bots and human-coordination, misinformation campaigns, and increasingly divisive echo chambers," he wrote. "We aren't proud of how people have taken advantage of our service or our inability to address it fast enough."

With the #MeToo movement going strong, in March Amnesty International published *#ToxicTwitter: Violence and Abuse Against Women Online*, ratcheting up pressure on Twitter to do more to protect women.

The report highlights Twitter's failure "to respect the human rights of women because of its inadequate and ineffective response to violence and abuse." It includes both quantitative and qualitative research conducted from December 2016 through March of this year. The human rights organization interviewed women and individuals who identify as neither male nor female across the United States and United Kingdom, conducted a qualitative survey and combed the site for abusive tweets toward female members of Parliament in the United Kingdom. The report details death threats, rape threats and racist, transphobic and homophobic abuse sent to women.

Amnesty made several recommendations for how Twitter can take action, including:

- Sharing specific examples of violence and abuse that will not be tolerated
- Sharing data on response times to reports of abuse
- Ensuring that decisions to restrict content are consistent with international human rights law and standards.

Vijaya Gadde, Twitter's legal, policy, and trust and safety lead, said in a March statement that the company agrees with many of the report's recommendations and is already working on implementing some of them. But the company also has told Amnesty that it "cannot delete hatred and prejudice from society."

Azmina Dhrodia, technology and human rights researcher at Amnesty International, said in a statement that the organization's investigation shows that "Twitter is failing to provide adequate remedies for those who experience violence and abuse on their platform. As a company, it needs to do much more to respect the human rights of women."

JACK DORSEY: DPA PICTURE ALLIANCE / ALAMY STOCK PHOTO

"We aren't proud of how people have taken advantage of our service or our inability to address it fast enough."

—Jack Dorsey, CEO, Twitter

THE BREXIT BACK OUT

The looming threat of Brexit received a little relief in March after the United Kingdom and the European Union (EU) agreed Britain would effectively remain a nonvoting EU member for 21 months, until the end of 2020.

Despite this delay, not all businesses are keen to keep their U.K. presence wholly intact. One in 7 EU companies with a foothold in Britain have moved parts of that business out of the country because of the potential disruptions to come, according to a survey by the Chartered Institute of Procurement and Supply (CIPS).

And that is not the only move organizations are making. Sixty-three percent of EU businesses that work with U.K. suppliers said they intend to move some of their supply chain out of the United Kingdom. And 14 percent of EU firms with assets in the United Kingdom, including offices, warehouses or factories, have scaled back their operations, while 11 percent have moved some of their workforce out of the U.K. since the Brexit vote in 2016.

"There comes a moment when companies need to put contingency plans into place," John Glen, an economist with CIPS, told Reuters. "We need to start getting real about what will actually happen."