BMJ Global Health

Threats by artificial intelligence to human health and human existence

Frederik Federspiel,1 Ruth Mitchell,2,3 Asha Asokan,4,5 Carlos Umana,6,7 David McCoy8

ABSTRACT

While artificial intelligence (AI) offers promising solutions in healthcare, it also poses a number of threats to human health and well-being via social, political, economic, and security-related determinants of health. We describe three main ways misuse of narrow AI serves as a threat to human health: through increasing opportunities for control and manipulation of people; enhancing and dehumanising lethal weapon capacity and by rendering human labour increasingly obsolete. We then examine self-improving ‘artificial general intelligence’ (AGI) and how this could pose an existential threat to humanity itself. Finally, we discuss the critical need for effective regulation, including the prohibition of certain types and applications of AI, and echo calls for a moratorium on the development of self-improving AGI. We ask the medical and public health community to engage in evidence-based advocacy for safe AI, rooted in the precautionary principle.

INTRODUCTION

Artificial intelligence (AI) is broadly defined as a machine with the ability to perform tasks such as being able to compute, analyse, reason, learn and discover meaning.1 Its development and application are rapidly advancing in terms of both ‘narrow AI’ where only a limited and focused set of tasks are conducted2 and ‘broad’ or ‘broader’ AI where multiple functions and different tasks are performed.3 AI holds the potential to revolutionise healthcare by improving diagnostics, helping develop new treatments, supporting providers and extending healthcare beyond the health facility and to more people.4–7 These beneficial impacts stem from technological applications such as language processing, decision support tools, image recognition, big data analytics, robotics and more.8–10 There are similar applications of AI in other sectors with the potential to benefit society.

However, as with all technologies, AI can be applied in ways that are detrimental. The risks associated with medicine and healthcare include the potential for AI errors to cause patient harm,11,12 issues with data privacy and security,13–15 and the use of AI in ways that will worsen social and health inequalities by either incorporating existing human biases and patterns of discrimination into automated algorithms or by deploying AI in ways that reinforce social inequalities in access to healthcare.16–19 One example of harm accentuated by incomplete or biased data was the development of an AI-driven pulse oximeter that overestimated blood oxygen levels in patients with darker skin, resulting in the undertreatment of their hypoxia.17 Facial recognition systems have also been shown to be more likely to misclassify gender in subjects who are darker-skinned.18 It has also been shown that populations who are subject to discrimination are under-represented in datasets underlying AI solutions and may thus be denied the full benefits of AI in healthcare.16,19,20

Although there is some acknowledgement of the risks and potential harms associated with the application of AI in medicine and healthcare,11–16,20 there is still little discussion.
within the health community about the broader and more upstream social, political, economic and security-related threats posed by AI. With the exception of some voices, the existing health literature examining the risks posed by AI focuses on those associated with the narrow application of AI in the health sector. This paper seeks to help fill this gap. It describes three threats associated with the potential misuse of narrow AI, before examining the potential existential threat of self-improving general-purpose AI, or artificial general intelligence (AGI) (figure 1). It then calls on the medical and public health community to deepen its understanding about the emerging power and transformational potential of AI and to involve itself in current policy debates on how the risks and threats of AI can be mitigated without losing the potential rewards and benefits of AI.

THREATS FROM THE MISUSE OF ARTIFICIAL INTELLIGENCE

In this section, we describe three sets of threats associated with the misuse of AI, whether it be deliberate, negligent, accidental or because of a failure to anticipate and prepare to adapt to the transformational impacts of AI on society.

The first set of threats comes from the ability of AI to rapidly clean, organise and analyse massive data sets consisting of personal data, including images collected by the increasingly ubiquitous presence of cameras, and to develop highly personalised and targeted marketing and information campaigns as well as greatly expanded systems of surveillance. This ability of AI can be put to good use, for example, improving our access to information or countering acts of terrorism. But it can also be misused with grave consequences. The use of this power to generate commercial revenue for social media platforms, for example, has contributed to the rise in polarisation and extremist views observed in many parts of the world. It has also been harnessed by other commercial actors to create a vast and powerful personalised marketing infrastructure capable of manipulating consumer behaviour. Experimental evidence has shown how AI used at scale on social media platforms provides a potent tool for political candidates to manipulate their way into power, and it has indeed been used to manipulate political opinion and voter behaviour. Cases of AI-driven subversion of elections include the 2013 and 2017 Kenyan elections, the 2016 US presidential election and the 2017 French presidential election. When combined with the rapidly improving ability to distort or misrepresent reality with deepfakes, AI-driven information systems may further undermine democracy by causing a general breakdown in trust or by driving social division and conflict, with ensuing public health impacts.

AI-driven surveillance may also be used by governments and other powerful actors to control and oppress people more directly. This is perhaps best illustrated by China’s Social Credit System, which combines facial recognition software and analysis of ‘big data’ repositories of people’s financial transactions, movements, police records and social relationships to produce assessments of individual...
behaviour and trustworthiness, which results in the automatic sanction of individuals deemed to have behaved poorly.\textsuperscript{29–31} Sanctions include fines, denying people access to services such as banking and insurance services, or preventing them from being able to travel or send their children to fee-paying schools. This type of AI application may also exacerbate social and health inequalities and lock people into their existing socioeconomic strata. But China is not alone in the development of AI surveillance. At least 75 countries, ranging from liberal democracies to military regimes, have been expanding such systems.\textsuperscript{32} Although democracy and rights to privacy and liberty may be eroded or denied without AI, the power of AI makes it easier for authoritarian or totalitarian regimes to be either established or solidified and also for such regimes to be able to target particular individuals or groups in society for persecution and oppression.\textsuperscript{30,33}

The second set of threats concerns the development of Lethal Autonomous Weapon Systems (LAWS). There are many applications of AI in military and defence systems, some of which may be used to promote security and peace. But the risks and threats associated with LAWS outweigh any putative benefits.

Weapons are autonomous in so far as they can locate, select and ‘engage’ human targets without human supervision.\textsuperscript{34} This dehumanisation of lethal force is said to constitute the third revolution in warfare, following the first and second revolutions of gunpowder and nuclear arms.\textsuperscript{34–36} Lethal autonomous weapons come in different sizes and forms. But crucially, they include weapons and explosives, that may be attached to small, mobile and agile devices (eg, quadcopter drones) with the intelligence and ability to self-pilot and capable of perceiving and navigating their environment. Moreover, such weapons could be cheaply mass-produced and relatively easily set up to kill at an industrial scale.\textsuperscript{36–37} For example, it is possible for a million tiny drones equipped with explosives, visual recognition capacity and autonomous navigational ability to be contained within a regular shipping container and programmed to kill en masse without human supervision.\textsuperscript{36}

As with chemical, biological and nuclear weapons, LAWS present humanity with a new weapon of mass destruction, one that is relatively cheap and that also has the potential to be selective about who or what is targeted. This has deep implications for the future conduct of armed conflict as well as for international, national and personal security more generally. Debates have been taking place in various forums on how to prevent the proliferation of LAWS, and about whether such systems can ever be kept safe from cyber-infiltration or from accidental or deliberate misuse.\textsuperscript{34–36}

The third set of threats arises from the loss of jobs that will accompany the widespread deployment of AI technology. Projections of the speed and scale of job losses due to AI-driven automation range from tens to hundreds of millions over the coming decade.\textsuperscript{38} Much will depend on the speed of development of AI, robotics and other relevant technologies, as well as policy decisions made by governments and society. However, in a survey of most-cited authors on AI in 2012/2013, participants predicted the full automation of human labour shortly after the end of this century.\textsuperscript{39} It is already anticipated that in this decade, AI-driven automation will disproportionately impact low/middle-income countries by replacing lower-skilled jobs,\textsuperscript{40} and then continue up the skill-ladder, replacing larger and larger segments of the global workforce, including in high-income countries.

While there would be many benefits from ending work that is repetitive, dangerous and unpleasant, we already know that unemployment is strongly associated with adverse health outcomes and behaviour, including harmful consumption of alcohol\textsuperscript{41–44} and illicit drugs,\textsuperscript{34–36} being overweight,\textsuperscript{45} and having lower self-rated quality of life,\textsuperscript{45,46} and health,\textsuperscript{47} and higher levels of depression\textsuperscript{44} and risk of suicide.\textsuperscript{41–47} However, an optimistic vision of a future where human workers are largely replaced by AI-enhanced automation would include a world in which improved productivity would lift everyone out of poverty and end the need for toil and labour. However, the amount of exploitation our planet can sustain for economic production is limited, and there is no guarantee that any of the added productivity from AI would be distributed fairly across society. Thus far, increasing automation has tended to shift income and wealth from labour to the owners of capital, and appears to contribute to the increasing degree of maldistribution of wealth across the globe.\textsuperscript{48–51} Furthermore, we do not know how society will respond psychologically and emotionally to a world where work is unavailable or unnecessary, nor are we thinking much about the policies and strategies that would be needed to break the association between unemployment and ill health.

**THE THREAT OF SELF-IMPROVING ARTIFICIAL GENERAL INTELLIGENCE**

Self-improving general-purpose AI, or AGI, is a theoretical machine that can learn and perform the full range of tasks that humans can.\textsuperscript{32,52} By being able to learn and recursively improve its own code, it could improve its capacity to improve itself and could theoretically learn to bypass any constraints in its code and start developing its own purposes, or alternatively it could be equipped with this capacity from the beginning by humans.\textsuperscript{34,53}

The vision of a conscious, intelligent and purposeful machine able to perform the full range of tasks that humans can has been the subject of academic and science fiction writing for decades. But regardless of whether conscious or not, or purposeful or not, a self-improving or self-learning general purpose machine with superior intelligence and performance across multiple dimensions would have serious impacts on humans.

We are now seeking to create machines that are vastly more intelligent and powerful than ourselves. The potential for such machines to apply this intelligence and
power—whether deliberately or not—in ways that could harm or subjugate humans—is real and has to be considered. If realised, the connection of AGI to the internet and the real world, including via vehicles, robots, weapons and all the digital systems that increasingly run our societies, could well represent the ‘biggest event in human history’. Although the effects and outcome of AGI cannot be known with any certainty, multiple scenarios may be envisioned. These include scenarios where AGI, despite its superior intelligence and power, remains under human control and is used to benefit humanity. Alternatively, we might see AGI operating independently of humans and coexisting with humans in a benign way. Logically however, there are scenarios where AGI could present a threat to humans, and possibly an existential threat, by intentionally or unintentionally causing harm directly or indirectly, by attacking or subjugating humans or by disrupting the systems or using up resources we depend on. A survey of AI society members predicted a 50% likelihood of AGI being developed between 2040 and 2065, with 18% of participants believing that the development of AGI would be existentially catastrophic. Presently, dozens of institutions are conducting research and development into AGI.

**ASSESSING RISK AND PREVENTING HARM**

Many of the threats described above arise from the deliberate, accidental or careless misuse of AI by humans. Even the risk and threat posed by a form of AGI that exists and operates independently of human control is currently still in the hands of humans. However, there are differing opinions about the degree of risk posed by AI and about the relative trade-offs between risk and potential reward, and harms and benefits.

Nonetheless, with exponential growth in AI research and development, the window of opportunity to avoid serious and potentially existential harms is closing. The future outcomes of the development of AI and AGI will depend on policy decisions taken now and on the effectiveness of regulatory institutions that we design to minimise risk and harm and maximise benefit. Crucially, as with other technologies, preventing or minimising the threats posed by AI will require international agreement and cooperation, and the avoidance of a mutually destructive AI ‘arms race’. It will also require decision making that is free of conflicts of interest and protected from the lobbying of powerful actors with a vested interest. Worryingly, large private corporations with vested financial interests and little in the way of democratic and public oversight are leading in the field of AGI research.

Different parts of the UN system are now engaged in a desperate effort to ensure that our international social, political and legal institutions catch up with the rapid technological advancements being made with AI. In 2020, for example, the UN established a High-level Panel on Digital Cooperation to foster global dialogue and cooperative approaches for a safe and inclusive digital future. In September 2021, the head of the UN Office of the Commissioner of Human Rights called on all states to place a moratorium on the sale and use of AI systems until adequate safeguards are put in place to avoid the ‘negative, even catastrophic’ risks posed by them. And in November 2021, the 193 member states of UNESCO adopted an agreement to guide the construction of the necessary legal infrastructure to ensure the ethical development of AI. However, the UN still lacks a legally binding instrument to regulate AI and ensure accountability at the global level.

At the regional level, the European Union has an Artificial Intelligence Act, which classifies AI systems into three categories: unacceptable-risk, high-risk and limited and minimal-risk. This Act could serve as a stepping stone towards a global treaty although it still falls short of the requirements needed to protect several fundamental human rights and to prevent AI from being used in ways that would aggravate existing inequities and discrimination.

There have also been efforts focused on LAWS, with an increasing number of voices calling for stricter regulation or outright prohibition, just as we have done with biological, chemical and nuclear weapons. State parties to the UN Convention on Certain Conventional Weapons have been discussing lethal autonomous weapon systems since 2014, but progress has been slow. What can and should the medical and public health community do? Perhaps the most important thing is to simply raise the alarm about the risks and threats posed by AI, and to make the argument that speed and seriousness are essential if we are to avoid the various harmful and potentially catastrophic consequences of AI-enhanced technologies being developed and used without adequate safeguards and regulation. Importantly, the health community is familiar with the precautionary principle and has demonstrated its ability to shape public and political opinion about existential threats in the past. For example, the International Physicians for the Prevention of Nuclear War were awarded the Nobel Peace Prize in 1985 because it assembled principled, authoritative and evidence-based arguments about the threats of nuclear war. We must do the same with AI, even as parts of our community espouse the benefits of AI in the fields of healthcare and medicine.

It is also important that we not only target our concerns at AI, but also at the actors who are driving the development of AI too quickly or too recklessly, and at those who seek only to deploy AI for self-interest or malign purposes. If AI is to ever fulfil its promise to benefit humanity and society, we must protect democracy, strengthen our public-interest institutions, and dilute power so that there are effective checks and balances. This includes ensuring transparency and accountability of the parts of the military–corporate industrial complex driving AI developments and the social media companies that are enabling AI-driven, targeted misinformation to undermine our democratic institutions and rights to privacy.
Finally, given that the world of work and employment will drastically change over the coming decades, we should deploy our clinical and public health expertise in evidence-based advocacy for a fundamental and radical rethink of social and economic policy to enable future generations to thrive in a world in which human labour is no longer a central or necessary component to the production of goods and services.

Author affiliations
1 Global Health and Development, London School of Hygiene & Tropical Medicine, London, UK
2 International Physicians for the Prevention of Nuclear War, Malden, Massachusetts, USA
3 Neurosurgery, Sydney Children’s Hospitals Network Randwick, Randwick, New South Wales, Australia
4 Independent Researcher/Consultant (Human Rights, International Peace and Security), Washington, DC, USA
5 Co-Chair, Women of Colour Advancing Peace and Security (WCAPS), New York, USA
6 Co-President, International Physicians for the Prevention of Nuclear War (IPPNW), San José, Costa Rica
7 President of IPPNW Costa Rica, member of IPPNW Spain, and member of the International Steering Group of ICAN (International Campaign to Abolish Nuclear Weapons), San José, Costa Rica
8 International Institute for Global Health, United Nations University, Kuala Lumpur, Malaysia

Acknowledgements
The authors would like to thank Dr Ira Helfand and Dr Chhavi Chaahan for their valuable comments on earlier versions of the manuscript.

Contributors
FF initiated and contributed to the writing of the paper, as well as coordinated co-author inputs and revisions. RM, AA and CU reviewed drafts and contributed to its intellectual content. DM supervised the project and contributed to the writing of the paper.

Funding
The authors have not declared a specific grant for this research from any funding agency in the public, commercial or not-for-profit sectors.

Competing interests
None declared.

Patient consent for publication
Not applicable.

Ethics approval
Not applicable.

Provenance and peer review
Not commissioned; externally peer reviewed.

Data availability statement
There are no data in this work.

Open access
This is an open access article distributed in accordance with the Creative Commons Attribution Non Commercial (CC BY-NC 4.0) license, which permits others to distribute, remix, adapt, build upon this work non-commercially, and license their derivative works on different terms, provided the original work is properly cited, appropriate credit is given, any changes made indicated, and the use is non-commercial. See: http://creativecommons.org/licenses/by-nc/4.0/.

REFERENCES

19 Zou J, Schiebinger L. AI can be racist and sexist—it’s time to make it fair. Nature 2018;559:324:324–6:–.
Doctors and public health experts join calls for halt to AI R&D until it’s regulated

Certain types and applications pose “existential threat to humanity,” they warn

An international group of doctors and public health experts have joined the clamour for a moratorium on AI research until the development and use of the technology are properly regulated.

Despite its transformative potential for society, including in medicine and public health, certain types and applications of AI, including self-improving general purpose AI (AGI), pose an “existential threat to humanity,” they warn in the open access journal *BMJ Global Health*.

They highlight 3 sets of threats associated with the misuse of AI and the ongoing failure to anticipate, adapt to, and regulate the transformational impacts of the technology on society.

The first of these comes from the ability of AI to rapidly clean, organise, and analyse massive data sets consisting of personal data, including images.

This can be used to manipulate behaviour and subvert democracy, they explain, citing its role in the subversion of the 2013 and 2017 Kenyan elections, the 2016 US presidential election, and the 2017 French presidential election.

“When combined with the rapidly improving ability to distort or misrepresent reality with deep fakes, AI-driven information systems may further undermine democracy by causing a general breakdown in trust or by driving social division and conflict, with ensuing public health impacts,” they contend.

AI-driven surveillance may also be used by governments and other powerful actors to control and oppress people more directly, an example of which is China’s Social Credit System, they point out.

This system combines facial recognition software and analysis of ‘big data’ repositories of people’s financial transactions, movements, police records and social relationships.

But China isn’t the only country developing AI surveillance: at least 75 others, “ranging from liberal democracies to military regimes, have been expanding such systems,” they highlight.

The second set of threats concerns the development of Lethal Autonomous Weapon Systems (LAWS)---capable of locating, selecting, and engaging human targets without the need for human supervision.

LAWS can be attached to small mobile devices, such as drones, and could be cheaply mass produced and easily set up to kill “at an industrial scale,” warn the authors.
The third set of threats arises from the loss of jobs that will accompany the widespread deployment of AI technology, with estimates ranging from tens to hundreds of millions over the coming decade.

“While there would be many benefits from ending work that is repetitive, dangerous and unpleasant, we already know that unemployment is strongly associated with adverse health outcomes and behaviour,” they point out.

To date, increasing automation has tended only to shift income and wealth from labour to the owners of capital, so helping to contribute to inequitable wealth distribution across the globe, they note.

“Furthermore, we do not know how society will respond psychologically and emotionally to a world where work is unavailable or unnecessary, nor are we thinking much about the policies and strategies that would be needed to break the association between unemployment and ill health,” they highlight.

But the threat posed by self improving AGI, which, theoretically, could learn and perform the full range of human tasks, is all encompassing, they suggest.

“We are now seeking to create machines that are vastly more intelligent and powerful than ourselves. The potential for such machines to apply this intelligence and power—whether deliberately or not—in ways that could harm or subjugate humans—is real and has to be considered.

“If realised, the connection of AGI to the internet and the real world, including via vehicles, robots, weapons and all the digital systems that increasingly run our societies, could well represent the ‘biggest event in human history’,“ they write.

“With exponential growth in AI research and development, the window of opportunity to avoid serious and potentially existential harms is closing. The future outcomes of the development of AI and AGI will depend on policy decisions taken now and on the effectiveness of regulatory institutions that we design to minimise risk and harm and maximise benefit,” they emphasise.

International agreement and cooperation will be needed, as well as the avoidance of a mutually destructive AI ‘arms race’, they insist. And healthcare professionals have a key role in raising awareness and sounding the alarm on the risks and threats posed by AI.

“If AI is to ever fulfil its promise to benefit humanity and society, we must protect democracy, strengthen our public-interest institutions, and dilute power so that there are effective checks and balances.

“This includes ensuring transparency and accountability of the parts of the military–corporate industrial complex driving AI developments and the social media companies
that are enabling AI-driven, targeted misinformation to undermine our democratic institutions and rights to privacy,” they conclude.