THE POTENTIAL FOR DUAL-USE OF PROTEIN-FOLDING PREDICTION

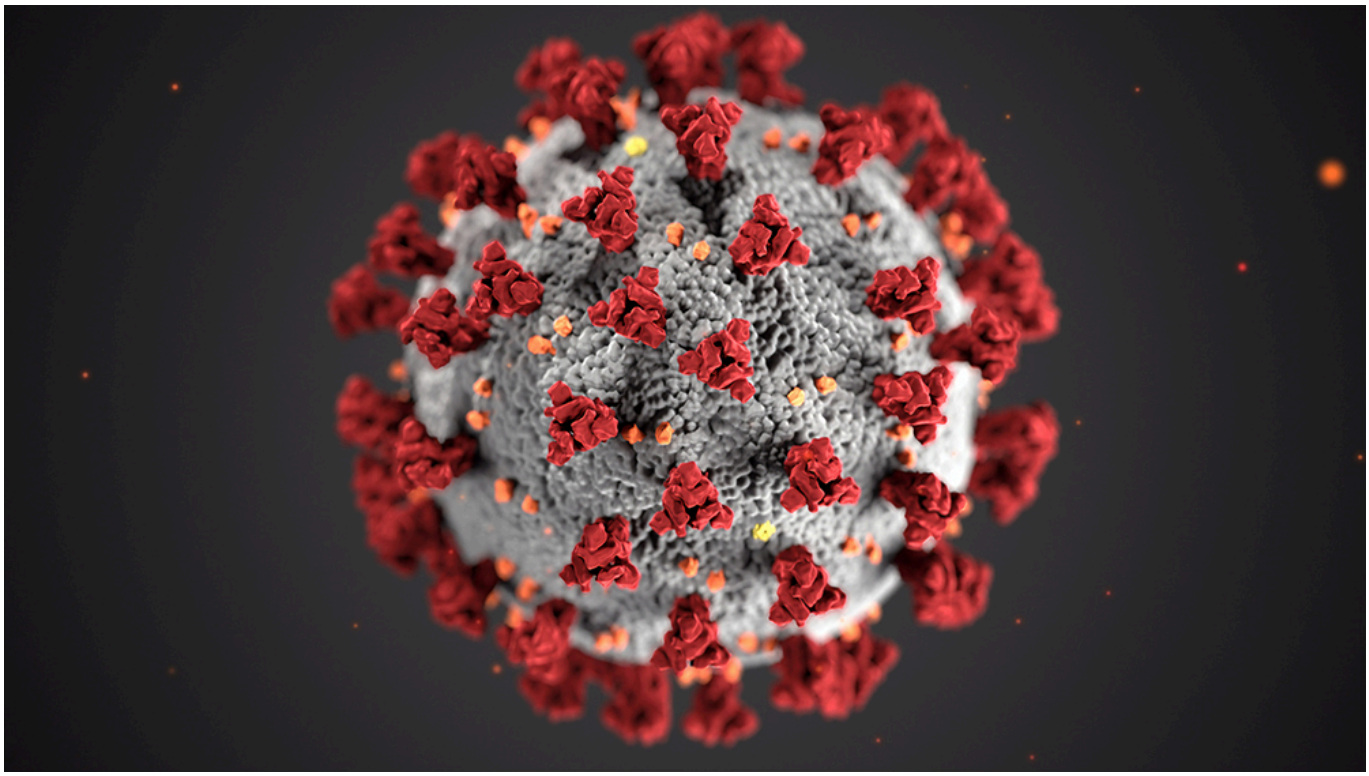
Artificial intelligence (AI) offers great potential for scientific advancement, particularly in areas with high complexity and many variables. Although biology can be challenging to comprehend, scientists can develop accurate AI models that help resolve biological interactions more effectively than conventional methods. Implementing AI in biological sciences promises benefits for all human beings by improving our understanding of how molecules interact or how genetic variation influences traits.

Traditional protein prediction methods rely on time-intensive methods requiring expensive equipment. Unfortunately, it is difficult to predict some complex protein classes. AI offers the potential to rapidly and cheaply predict protein structures, allowing scientists to examine the impact of genetic variations on macromolecules. AI-based predictions are expected to improve our understanding of how genetic variation causes disease, enables drug development, and allows researchers to design specific proteins that break down plastics in nature. Consequently, protein-folding prediction is a significantly important domain for the implementation of AI in biological sciences.

Recently, exponentially rapid implementation and advancement of AI in protein-folding prediction have yielded surprising results. In 2020, the company DeepMind made a major step forward with its algorithm AlphaFold at the 14th Community Wide Experiment on the Critical Assessment of Techniques for Protein Structure Prediction (CASP). AlphaFold predicted structures for a range of proteins with an accuracy over 90%, comparable to conventional methods. From this success, highly accurate protein structure prediction may soon promise benefits for public health, such as vaccine developments.

However, malicious actors might use protein-folding prediction algorithms for purposes unintended in their original development. Understanding how genetic variation affects protein structure may enable researchers to discover disease-causing mutations using one individual's genome sequence. While this ability might raise serious concerns for individuals who carry rare and/or severe genetic diseases, the threat would become even more significant if malicious actors could predict how genetic variations impact the severity of diseases and identify individuals susceptible to specific pathogens. These threats open the door to a dual-use technology dilemma and raise the question of how we can prevent malicious actors from weaponizing protein-folding prediction while still fostering scientific advancement.

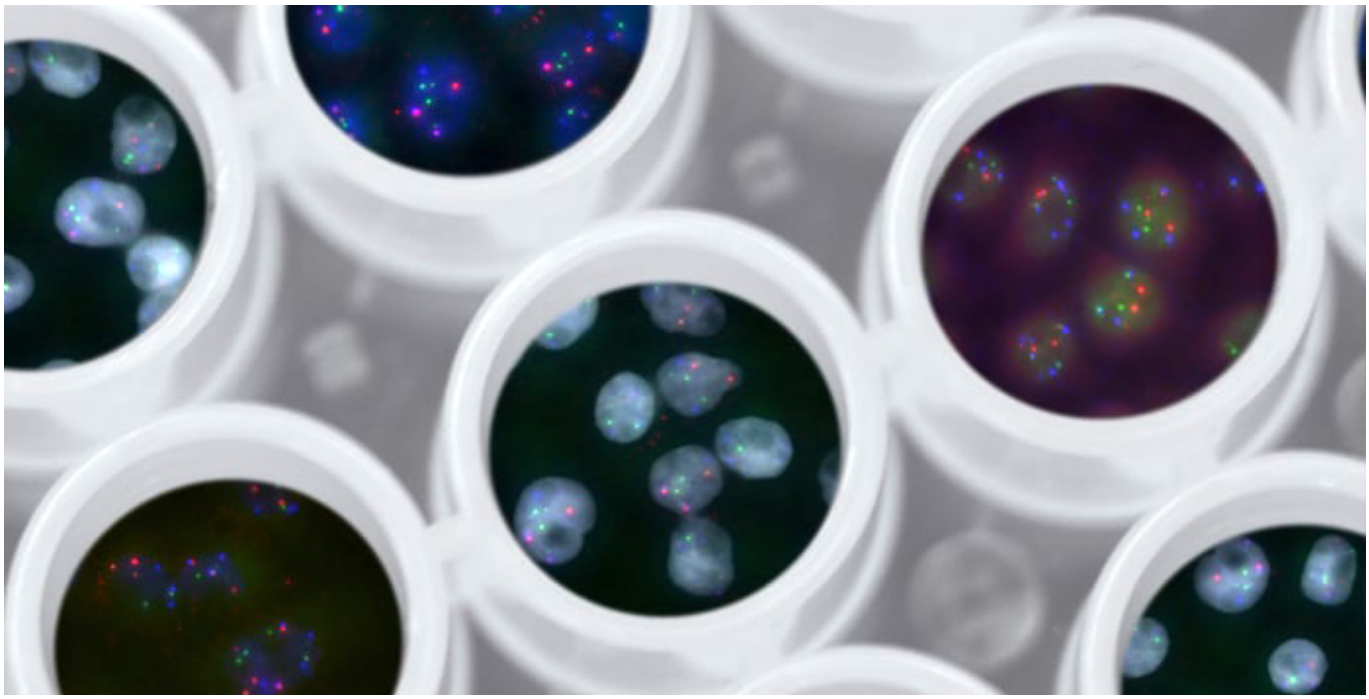
As protein-folding prediction algorithms are still in the early stages of development, the ways they could be weaponized are also only beginning to be understood.,, Although exploitation of this technology is perhaps still considered low risk to national security, malicious actors may have already been directed to consider how to exploit such advantages. While there is currently no evidence of nefarious individuals, organizations, or States having advanced their technologies and human resources to the extent of exploiting protein-folding AI systems, it is critical to raise awareness of potential threats. The evolving nature of criminal activities and rapid advancements in AI and biotechnology capabilities make it vital.



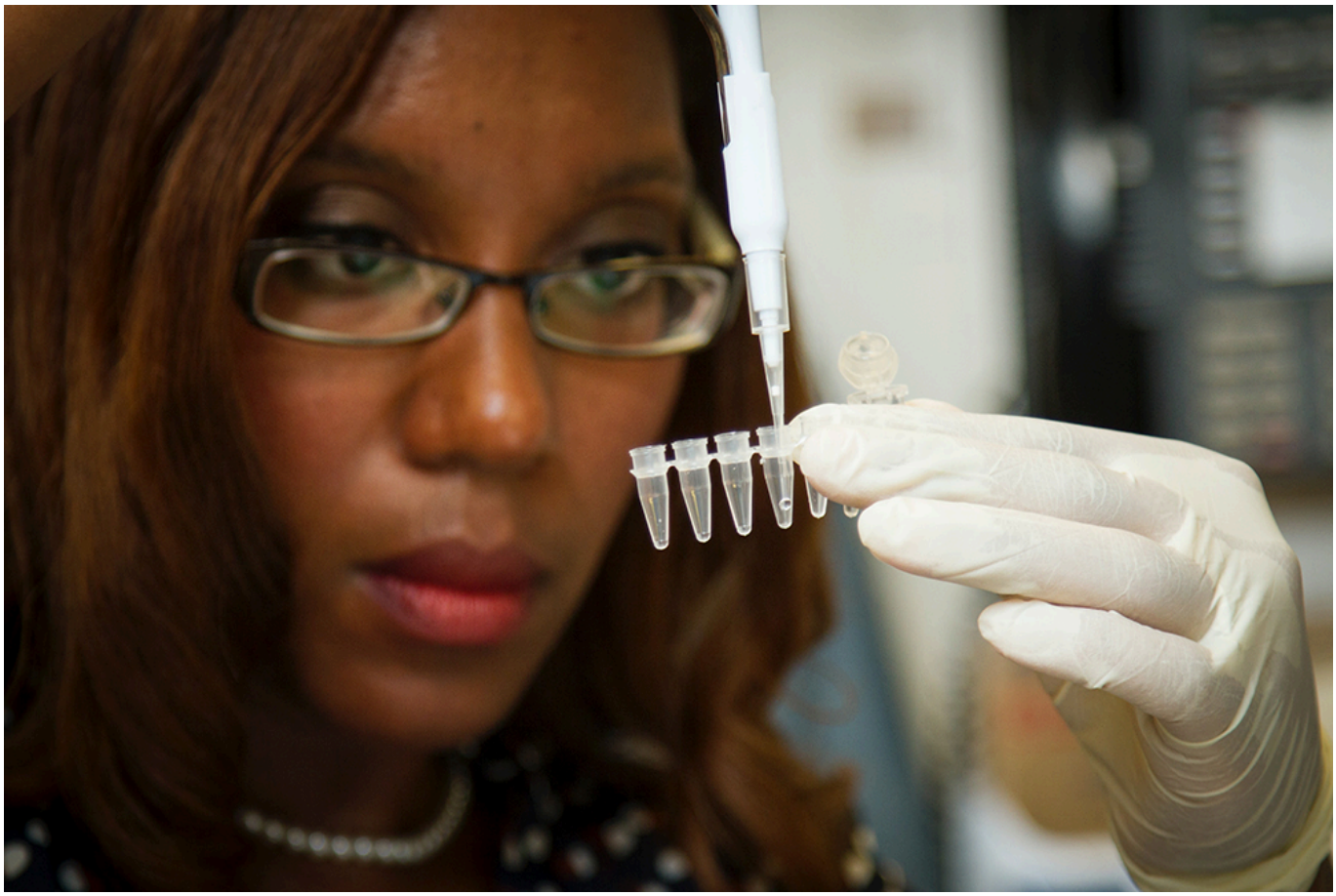
One important aspect regarding the security of emerging technologies is the accessibility of source code. Although open science fosters scientific development, it should also be acknowledged that malicious actors can exploit transparency for illicit purposes. Once a source code is released for an advanced AI, malicious actors could use or modify it to cause harm. Depending on the advancement of such technology, even the description of methodology or pseudo-code may be sufficient for malicious actors to recreate the technology partially or in full capacity. Thus, security challenges can arise when advances are made in AI, especially when the original developments are considered safe.

DeepMind did not immediately release its AlphaFold source code. Nevertheless, in approximately seven months, academic researchers were able to use the general methodology to create an algorithm of their own that performed nearly as well. The source code from this academic group was released along with a preprint at almost the same time that DeepMind published their peer-reviewed article and their own source code. As more protein-folding prediction approaches become available to the public, higher risks appear for malicious actors to exploit this advancement to design novel bioweapons. However, the solution to this threat should not be classifying these algorithms as a weapon and keeping their methodologies secret. On the contrary, considering the unprecedented opportunities this advancement promises, scientific engagement should be actively promoted while mitigating their risks.

One solution to prevent undesired dual-use scenarios of protein-folding prediction algorithms could be to design access schemes to their data, techniques, and outputs. Further publication and dialogue surrounding dual-use possibilities should be encouraged. These approaches would be complementary to a responsible innovation approach. Moreover, a substantial discussion about the ethics and dual-use potential of protein folding prediction should be initiated.



The dual-use threat of protein-folding prediction also highlights the importance of the security of medical facilities, research institutions, and biobanks. Any weaponization attempt of this technology cannot be made without training the subjected AI systems with genetic information extracted from samples given by the targeted individuals or populations. Unfortunately, during the COVID-19 pandemic, the number of cyber-attacks directed at hospitals, vaccine developers, and others have increased. Consequently, sensitive and valuable genetic information might be seized by malicious actors, although no major incident has been reported to date. While there is concern that exploitation of population sequence analysis could lead to the creation of targeted bioweapons, dual-use of advancement of protein-folding predictions could have complementary effects on these threats or might even expedite such malicious efforts in the future. Institutions with databases of genetic information should therefore enhance their security against any threat. Moreover, we must ensure the utmost compliance with up-to-date data protection and research ethics principles.



Ultimately, DeepMind has made a ground-breaking advancement in a protein-folding prediction that offers tremendous promise for the good of humankind. Nevertheless, potential dual-use applications of such powerful algorithms could have undesirable effects. Considering the rapidly evolving nature of crime and the ongoing global effects of the COVID-19 pandemic, the manifestation of such threats might occur sooner than later. Thus, efforts to understand and prevent such scenarios in their earliest stages are crucial.

Sterling Sawaya is the Founder & CEO, GeneInfoSec
Taner Kuru is an Intern at the United Nations Interregional Crime & Justice Research Institute (UNICRI)
Thomas A. Campbell, Ph.D., is the Founder & CEO, FutureGrasp