The Intersection Between Artificial Intelligence and Biological Nonproliferation Objectives

*By **Linus B. Höller**, MA Candidate in **Nonproliferation and Terrorism Studies at the Middlebury Institute of International Studies** at Monterey and the Moscow State Institute of International Relations.*

Introduction

The explosion into the mainstream of artificial intelligence in the past two years has presented a remarkable departure from the typical humdrum of international organizations tasked with overseeing the aging treaties seeking to control entire classes of weapons of mass destruction. Speaking at a side event to the United Nations General Assembly's First Committee, leaders of the four main international nonproliferation watchdogs – the (two) organizations overseeing the nuclear, chemical and biological worlds – spoke of the grave risks that artificial intelligence could pose if it were to be leveraged for the wrong ends. But, to the surprise of some of the audience, they also touted it as one of the most significant developments for good in recent years.[1]

This paper seeks to evaluate the role that artificial intelligence may play in the coming years based on trends and behaviors we are already witnessing.

[1] Höller, Linus. "Leaders Wrestle with a Potent Mix: AI and Weapons of Mass Destruction." *Defense News*, October 30, 2024. https://www.defensenews.com/global/europe/2024/10/30/leaders-wrestle-with-a-potent-mix-ai-and-weapons-of-mass-destruction/.

Specifically, this brief survey work will focus on the impact of AI on the world of bioweapons nonproliferation and touch on its implications for biosecurity more broadly.

The Basics

Where exactly the boundaries lie for what is and isn't artificial intelligence is a blurry matter, and the term has been caught up in the hype and popular excitement of the arrival of mainstream tools that have revolutionized the way people interact with computers. These tools, such as ChatGPT or image generators like Dall-E, generally fall into the category of Generative AI: They create something seemingly out of thin air. However, artificial intelligence likewise encompasses a whole range of other applications, many of which are much less consumer-facing or glamorous than the apparent oracle that is OpenAI's large language model. Machine learning and neural networks, for instance, are revolutionizing research and software development. Natural language processing, computer vision (a particularly challenging field) and robotics applications are just a handful of other domains.

This paper will use the term AI relatively loosely, as it isn't an in-depth discussion of the technologies behind these tools but rather of the effect of these new abilities.

Somewhat similarly, the bounding lines between biological and chemical warfare/terrorism can be somewhat blurred, especially when it comes to toxins. For the sake of this paper and for the sake of simplicity, we will also operate with a relatively loose description of biological warfare/terrorism and biosecurity as relating to living beings, particularly microorganisms, as well as organic particles such as prions and viruses.

Finally, there will be references in this paper to the existing global nonproliferation infrastructure. In the case of biological weapons, this primarily refers to the Biological Weapons Convention of 1972, the first treaty to outlaw an entire class of WMD. Unlike treaties that followed, such as the Chemical Weapons Convention, the BWC did not provide for the creation of an organization tasked with its implementation or verification. A so-called Implementation Support Unit within the UN's Office for Disarmament Affairs has taken on this unenviable role; the size of the team has relatively recently been increased from three to four. For comparison, the OPCW – the Organization for the Prohibition of Chemical Weapons – is staffed with around 400 people.

The Upsides

The good news first: AI is not just revolutionizing chatbots and image editing, but also science and technology and their intersection with nonproliferation. Speaking at the aforementioned side event in October 2024, the representative of the BWC's ISU, Courtney Crissa, pointed out that "advances

in biotechnology and AI can … present opportunities for strengthening the convention." With an eye to the lack of a verification mechanism, she expressed hope that artificial intelligence and machine learning might be able to close that gap.

For instance, artificial intelligence could be used to better analyze the submissions through the treaty's confidence-building measures mechanism. Relying on a computer to pick up on patterns and inconsistencies would not only be quicker than humans (and free the precious few staff up to focus on tasks that require their expertise and cannot as simply be automated) but conceivably also more accurate, flagging areas of concern that a human reader might miss, especially when pressed for time.[2] Combining this relatively basic application with a large language model, particularly one purpose-built with reliable scientific literature relevant to bioweapons and their development, could produce even better results. The program would then be able not just to scan for inconsistencies or pre-determined red flags, but to use the web of knowledge available to it to make judgments on the risk level represented in each report.

Additionally, AI-powered tools are promising to revolutionize the way that open-source intelligence is conducted. In the context of life sciences, one possible application would be to consistently crawl the internet for scientific publications and academic research data and simultaneously evaluate it. This

[2] Cropper, Nicholas R, Shrestha Rath, Ryan J C Teo, Kelsey Lane Warmbrod, and Mary J Lancaster. "A Modular-Incremental Approach to Improving Compliance Verification With the Biological Weapons Convention." *Health Security* 21, no. 5 (2023): 421–27. https://doi.org/10.1089/hs.2023.0078.

would allow a program to flag research that may be related to covert weapons development by a state or even, potentially, nonstate actors.[3] It would have the added benefit that the agency could use the knowledge network of the field built up by such an AI for its own capacity-building efforts. Simultaneously, notable *omissions* in the research output from any particular state or institution could also present a red flag.

In addition to increasing treaty effectiveness, AI could also prove instrumental in increasing resilience against biological attacks or accidents. For instance, AI could help detect outbreaks earlier by connecting disparate data points and could also contribute to coordinating more effective responses once such an outbreak has been identified.[4] These data points should, of course, include clinical data and disease/symptom reports, but could also harness social media[5], cell phone location trends, and other datasets that might not currently be actively evaluated in this context but could contribute to an early detection.

If the outbreak – whether natural or not – cannot be nipped in the bud even despite these early-warning systems, AI could be used to rapidly evaluate the incoming data, for instance, to determine potential vaccine targets, forecast the efficacy of different vaccine candidates and, in aggregate, significantly

[3] Ibid.
[4] Revill, James, Clarissa Rios, and Louison Mazeaud. "What Will Be the Impact of AI on the Bioweapons Treaty? ." Bulletin of the Atomic Scientists, November 16, 2024. https://thebulletin.org/2024/11/what-will-be-the-impact-of-ai-on-the-bioweapons-treaty/.
[5] Cambeiro, Juan. "How AI Can Help Prevent Biosecurity Disasters." Institute for Progress, July 10, 2023. https://ifp.org/how-ai-can-help-prevent-biosecurity-disasters/.

speed up vaccine development.[6] Similarly, the technology could be used to determine the best courses of treatment and expected antibiotic response. AI has also already been used in protein design and drug discovery, including for drugs that are undergoing clinical trials.[7]

Before an attack can take place, the perpetrator needs to produce the biological agent they want to use. In the following section, we will discuss some of the risks associated with AI in lowering the barrier, especially for actors who might previously have been unable to access these techniques. One risk that has been highlighted is that of cloud labs: A user uploads a genetic sequence and receives the developed product by mail. While many services already screen any orders, a significant number do not.[8] Additionally, existing screening methods – especially list-based methods that compare orders against a predetermined set of matches – can be insufficient even under the best of circumstances and especially when faced with the power of generative AI to either alter existing sequences in a way that makes them perform the same but not be flagged, or to determine entirely new harmful products (for instance, new toxins). Real-world experiments underscore the

[6] Revill, James, Clarissa Rios, and Louison Mazeaud. "What Will Be the Impact of AI on the Bioweapons Treaty? ." Bulletin of the Atomic Scientists, November 16, 2024. https://thebulletin.org/2024/11/what-will-be-the-impact-of-ai-on-the-bioweapons-treaty/.
[7] Cambeiro, Juan. "How AI Can Help Prevent Biosecurity Disasters." Institute for Progress, July 10, 2023. https://ifp.org/how-ai-can-help-prevent-biosecurity-disasters/.
[8] Sandbrink, Jonas. "ChatGPT Could Make Bioterrorism Horrifyingly Easy." *Vox*, August 7, 2023. https://www.vox.com/future-perfect/23820331/chatgpt-bioterrorism-bioweapons-artificial-inteligence-openai-terrorism.

fact that this is not a far-fetched concern. Stanford, for example, grew opioids in genetically modified yeast as early as nine years ago.[9]

The Downsides

Perhaps the most significant concern about the intersection between the life sciences and AI is that the new tools that are becoming broadly available significantly lower the barriers that previously existed to developing and acquiring functioning bioweapons. Biological warfare is, compared to other weapons of mass destruction, a tedious and thankless job to prepare: It relies on living beings, so the producer needs to maintain conditions that these organisms can survive and thrive in and can develop in the way that the malicious actor intends, and ultimately the agent needs to be dispersed in a way that doesn't neutralize it before it even has the chance to reach its target.

AI tools, such as large language models, can be used to provide guidance on the manufacture of biological weapons and, in so doing, significantly reduce the need for specialized knowledge. While previously, a terrorist organization may have needed to recruit a PhD student in biochemistry if they sought to develop biological weapons, now they can ask Perplexity and, in many cases,

[9] Abate, Tom. "Stanford Researchers Genetically Engineer Yeast to Produce Opioids." Stanford University, August 15, 2015. https://news.stanford.edu/stories/2015/08/opioids-yeast-smolke-081315.

get similarly high-quality instructions (and in most cases, they will be easier to understand).[10]

While this applies to known agents, advanced AI tools could also be used to assist in the development of new or modified toxins and pathogens. This particularly applies to the field of genetic editing, which could also be used to increase the lethality or other desired effects of existing pathogens. AI may also be (and has already been[11]) used to determine molecular structures of previously unknown toxins and make determinations about how to best produce or harvest them.

The ability to use AI to alter the effects of already existing bioweapons might have larger knock-on effects beyond simply creating a more potent or capable agent. Using the help of artificial intelligence tools, pathogens could conceivably be modified in such a way as to target specific populations, perhaps determined by genotype or geography. The optimization of agents to have more precise – and perhaps more limited – effects might also alter the threshold for their use by states.[12] The fundamental calculus underlying the international agreements not to produce, stockpile or use biological weapons could be called into question if the ability to make more controllable agents

[10] James Martin Center for Nonproliferation Studies. "AI and Nonproliferation: CNS Experts Lead the Way." James Martin Center for Nonproliferation Studies, November 21, 2023. https://nonproliferation.org/ai-and-nonproliferation-cns-experts-lead-the-way/.
[11] Calmers University of Technology. "Toxic Chemicals Can Be Detected with New AI Method." ScienceDaily, May 2, 2024. https://www.sciencedaily.com/releases/2024/05/240502113755.htm.
[12] Drexel, Bill, and Caleb Withers. "AI and the Evolution of Biological National Security Risks." CNAS, August 13, 2024. https://www.cnas.org/publications/reports/ai-and-the-evolution-of-biological-national-security-risks.

becomes widespread or, perhaps more importantly, the idea of such a concept becomes commonplace in certain policy circles.

There are other strategic considerations, too, that could affect the effectiveness of existing nonproliferation and disarmament measures. For instance, AI could accelerate the "design-build-test-learn" feedback loop, making it easier for states to renege on their commitments not to develop or stockpile biological weapons and make up for any know-how that may have been lost since the BWC came into force.[13] In short, the efficiency gains by AI in this domain could lead to a higher chance of a quick break-out.

Conclusions

Naturally, there is a lot more to be said about this topic, and this paper has barely scratched the surface. The key takeaways, however, are the following: Artificial intelligence in all of its forms is already fundamentally reshaping the life sciences field and, by extension, the biological aspect of nonproliferation. There certainly is cause for concern as a result of these new technologies, particularly for their making the production of biological weapons more attainable and their ability to turbocharge longstanding non-peaceful research objectives. However, at the same time, these tools have proven invaluable additions to the toolkit of science for good. Whether in vaccine

[13] Drexel, Bill, and Caleb Withers. "AI and the Evolution of Biological National Security Risks." CNAS, August 13, 2024. https://www.cnas.org/publications/reports/ai-and-the-evolution-of-biological-national-security-risks.

development, epidemiology or education, these incredible pieces of software are set to be transformative in a positive way, too.

At the risk of editorializing: The solution here does not seem to try to restrict access to these tools or the information they provide. The genie is out of the bottle, and these tools and their abilities are here to stay. Instead, careful examination of their capabilities and pitfalls will be necessary and researchers, policy practitioners and all other stakeholders must make a conscious effort to keep up with the times and stay actively involved in improving the implementation of artificial intelligence in their own workflows for good.