

---

# Risks of Bioterrorism Escalating Due to Artificial Intelligence

**Bushra Qamar**

Lecturer in Political Science

Govt. Associate College for Women Renala Khurd, Okara

Email: bushrakhubaib25@gmail.com

## Abstract

With its widespread applicability, artificial intelligence (AI) is perhaps the most significant new technology and our reliance on technology is growing in the modern world, but technological progress is not always positive. Research and innovations in technology can have both positive and negative effects on society; this is known as technology's dual nature. In order to draw attention to the possibility of AI-enabled bioterrorism, this study will concentrate on artificial intelligence (AI) and related technologies. Terrorists and criminals have been using new tactics more often in recent years to endanger the wealth and safety of numerous states. In order to draw attention to the possibility of AI-enabled bioterrorism, this study will explore this sinister side of artificial intelligence. To give a clearer picture of the growing threat of bioterrorism with the usage of AI, the researcher has looked into the matter utilizing secondary and primary (Report)sources. Qualitative along with historical and analytical predictive methods have been employed to develop substantial arguments. AI and biological data are two factors that are adding to the growing threat of bioterrorism as technology develops. The study argues that since AI is likely to be used for bioterrorism, more counterterrorism measures are required. It is argued that the application of AI to prevent and combat bioterrorism and terrorism must receive immediate attention. It assesses AI progress as well as its application to counterterrorism.

**Keywords:** Artificial intelligence, terrorism, bioterrorism, Biological Design Tools, Large Language models

## 1. Introduction

The World Health Organization defines biological weapons as hazardous materials made by intentionally altered living things or microbes like bacteria, fungus, or viruses. discharged to harm or even kill people, animals, or plants. These dangers are part of a wider category of armaments that are also known as WMDs, or weapons of mass destruction. These include radioactive, nuclear, and chemical weapons. The employment of biological weapons is one of the most concerning of them, and it's thought that using

these weapons in a terrorist attack is becoming more likely (World Health Organization, 2023).

Artificial intelligence (AI) has the potential to significantly improve health, agriculture, and the bio-economy as well as lead to enormous advancements in our fundamental knowledge of biological processes. However, biosecurity may also be at risk from AI tools if they are designed carelessly or improperly. The biosecurity hazards associated with artificial intelligence are dynamic and multifaceted, necessitating a diversity of viewpoints and specialized knowledge to fully grasp the whole spectrum of concerns. Given their potential to seriously impair human health, biodiversity, and socioeconomic stability, biological hazards are an area of growing concern in the current global context. This background is linked to the rapid development of Artificial Intelligence (AI) is a game-changing technology that is present in many aspects of society. The swift progression of artificial intelligence (AI) technologies and applications carries significant consequences in various fields, one of which being the possible creation of a biological weapon. Concerns are especially raised by this possible usage of AI because it is both individuals and non-state actors can access. AI technologies are developing at a rate that frequently outpaces government regulatory monitoring, which could cause a gap in the laws and regulations now in place. Examining AI's growing influence in these biological hazard scenarios is vital in this regard, taking into account both the benefits of this technological innovation and the new risks and challenges it may bring about.

## **2. Review of the Literature**

De Lima et al. (2024) asserted that in the challenging setting of biological hazards, the implications of AI become a double-edged sword with the potential to both increase and decrease risks. An integrated and cooperative strategy is essential since the creation and release of biological agents, as well as the genetic modification of natural enemies, call for interdisciplinary approaches. Environmental impact assessments are crucial for comprehending the worldwide implications of genetically modified organism releases. Thorough safety testing is necessary to evaluate the threats that the improper use of AI poses to human and environmental health.

Sandbrink, J. B. (2023) asserted that it is risky to use AI to make pertinent knowledge more accessible. "AI lab assistants" may be able to make pertinent knowledge actionable in addition to providing access to public knowledge. The article outlines the general ways in which LLMs could reduce obstacles to the creation of biological weapons. For actors who are not trained, Large Language Models (LLMs) can provide guidance and troubleshoot laboratory techniques. LLM capabilities, when combined with laboratory robot infrastructure, almost reduce the requirement for programming in order to automate tests. Technological advancements in large-scale clandestine scientific activities and autonomous labs in the future

could overcome the obstacles that the Soviet and Iraqi bioweapon programs experienced in the past by lowering socio-organizational barriers.

Sandbrink goes into more detail on Biological Design technologies (BDTs), which are yet another class of AI technologies that increase hazards during the "design" stage of life science research. "They can assist in the design of new proteins or other biological agents because they are trained on biological data." BDTs could make it possible to create diseases that are more harmful than any that exist naturally. This suggests that pandemics may pose existential challenges to humanity for the first time.

According to Mouton, Caleb, and Ella. (2023) their experience with different LLMs shows that biological weapon attack planning is now beyond their capabilities as supportive tools. There was no discernible variation in the viability of plans created with or without LLM support, according to our analysis. They did not quantify the gap between the current LLM capabilities frontier and the information required to plan a biological weapon attack. It is prudent to keep an eye on upcoming advancements in LLM technology and the possible threats linked with its use to biological weapon attack planning, given the rapid evolution of AI. Even though we found what we would call unfortunate LLM outputs (such as problematic responses to prompts), these outputs typically mirrored information that was easily found online, indicating that LLMs do not significantly raise the risks connected to planning a biological weapon attack. In order to improve potential future research, we would like to raise the sensitivity of our tests by adding more researchers, evaluating a larger number of LLMs, and eliminating sources of unhelpful fluctuation from the testing procedure. These initiatives will provide a proactive approach to managing the dynamic of evolving measure-countermeasure and help provide a more accurate assessment of potential threats.

AshimaJha. (2023) said that throughout history, biological science and technology have been essential to human growth and wealth. While there have been significant advancements in the fields of epidemiology, public health, and infectious disease control, advances in biosecurity and further preventing the proliferation of biological weapons have continued to pose significant challenges in a world where biological sciences are developing at a rapid pace. For instance, biotechnology has made the altering process easier. Many of these advancements are related to or enhanced by other technologies, including some that are only starting to emerge and run the risk of being abused and spreading biological weapons. Specifically, three cutting-edge technologies—robotics, additive manufacturing, or 3D printing, and artificial intelligence (AI) make it simpler, less expensive, and quicker to modify an organism's genetic makeup. They might lead to new avenues for the development of biological weapons and raise the risk of cyberattacks against digitalized biological records.

According to Newman (2024) advancements in AI could potentially lead to the intentional transmission of dangerous viruses, as tens of thousands of human viruses have genetic sequences available. DNA/RNA synthesis advancements can enable replication, but understanding lab procedures is the biggest obstacle. Identifying a hazardous virus could save lives.

Future chatbots will use video training data to make attacks less difficult, guiding potential terrorists through viral synthesis. They may also assist with attack planning, brainstorming ideas, acquiring equipment, and determining the best location and method for releasing viruses, making them more multimodal and multimodal. Chatbots' popularity is largely due to their ability to present relevant information at the right time. ChatGPT can interpolate between large amounts of training data, while Google can provide a list of related web pages. Multimodal AI could alert bioterrorists to improper lab procedures, increasing risks. Biology advancements may intensify these risks. Advancements in gain-of-function research may lead to the synthesis of hazardous virus genomes, while advancements in virus pandemic potential may allow attackers to choose the deadly genomes for synthesis.

Yassif, Korol, & Kane (2023) pointed out that the Global catastrophic biological risks (GCBRs) are becoming more and more prevalent. Strengthening global biosecurity and preventing GCBRs require innovative strategies that have the potential to be very effective in discouraging governments from creating or deploying bioweapons. Our common vulnerabilities have been brought to light by the COVID-19 pandemic, which also serves as a crucial reminder of the pressing need to bolster our defenses against worldwide biological disasters. The global biosecurity architecture, including the Biosecurity Community (BWC), is facing challenges due to escalating geopolitical tensions, strong disinformation operations, and erroneous charges regarding biological weapons. We need to take advantage of this chance to address the issues of increased accountability, improved attribution, and transparency for breaking the international standard prohibiting the creation and deployment of bioweapons. We can build a safer, more sustainable future for future generations if the biosecurity community and the larger international society can collaborate to adopt strong mechanisms for guaranteeing BWC compliance.

Chaudhry & Klein (2024) analyze that the Artificial intelligence (AI) has the potential to undo the advances gained in the last fifty years in the prohibition of chemical and biological weapons as well as the creation of strict laws prohibiting their use. While research in biosecurity and biology has enormous potential benefits, it also poses serious risks. Such research may be used, for example, to create essential medicinal defenses or to create and disseminate a harmful disease. Over the past 20 years, advances in synthetic biology, faster DNA synthesis, more affordable and accessible

DNA sequencing, and the development of accurate and efficient gene-editing tools have all contributed to a rapid expansion in access to advanced biotechnology at a lower cost. It is critical to recognize the risks posed by chemical and biological weapons in conjunction with artificial intelligence.

Roumate (2024) examines the impact of AI on international affairs and post-COVID-19 global society, focusing on the rise of smart power, warfare, and the evolution of concepts like sovereignty. It highlights the competition between states and big tech for technical sovereignty and the need for reconsidering foreign policy plans in the AI era. AI impacts international law, human rights, humanitarian, economic, and health law. AI offers solutions to global problems, but its misuse can create new challenges. Roumate has examined terrorism along with the emerging psychological warfare combining technology and knowledge. AI is transforming research, education, labor markets, environment, health, and commerce, and is transforming the global economic system. In short, AI ethics are critical and urgent. Legal changes as well as fresh approaches at the national, regional, and global levels are necessary for AI revolution. AI is essential to maintaining global peace and security in a multipolar world for the present and the future. It is also essential to understanding international relations during times of peace and conflict.

### **3. AI in the perspective of Bioterrorism**

It is believed that biological data is an essential medium that AI needs in order to support the biological attacks in continuation. To emphasize on AI is very important in a way that it is only a dumb minion with a goal to complete; it is not the one initiating the attacks. This also applies to biological data. These tools are used to simply expedite or modify the procedure, as well as plan and carry out attacks. Big biological data is the result of the exponential growth in biological data collecting made possible by data mining and storage technology breakthroughs and innovations. In the context of biological data, big data is the outcome of extraordinarily large and quick data mining techniques and technologies in the scientific, medical, and biological domains.

One of the most basic issues that nations and communities worldwide deal with is terror, however in the modern era, bioterror threats come from sources other than your typical extremist organization. We need to be concerned about the nature of these attacks because the 1990s saw a discernible rise in bioterrorism-related incidents. For two reasons in particular, the dual character of biological data must be taken into account. One way that the analysis of biological data can aid bad actors in carrying out a biological strike is. However, societies and governmental organizations can employ biological data analysis to forecast which kind of agent is most likely to be employed and the most likely attack. Because AI can exploit data and extrapolate knowledge at a startlingly fast rate, it presents serious safety and security risks to our modern civilization. AI only needs human guidance

to assist in bioterrorism; it doesn't need to be sentient to do so. Fundamentally, AI is dependent on data mining and its advancements, much like biological data is (Erasmus, 2021).

#### **4. COVID-19 and the Application of AI in a Pandemic**

We haven't heeded the long-standing warnings from virologists. Nobel laureate Joshua Lederberg once said, "The virus poses the single biggest threat to man's continued dominance on the planet." This has long been a topic of discussion. In the 1980s, infectious disease specialist Edward Kilbourne discussed "Genetically altered viruses and the environment" during a symposium held on Long Island (Henig, 2020).

According to his theory, the most contagious, difficult to contain virus will quickly surface. He gave the virus the moniker Maximally Malignant Mutant Virus (MMMV). Kilbourne states that MMMV would have the high rate of influenza virus mutation, the extended latency of the herpes virus, the environmental stability of the poliovirus, and the extended host range of the rabies virus. Like influenza, it would spread through the air, proliferate in the lower respiratory tract, and produce HIV (Human Immunodeficiency Virus) by directly inserting its own genes into the host's molecules. (Henig, 2020).

Although COVID-19 and MMMV are not exactly the same, there are still a lot of similarities. The discovery of a novel virus in Wuhan, China's Hubei region was reported in December of 2019. There has been a lot of conjecture on the animal that could be the source of the virus, and there have also been a lot of conspiracy theories regarding the government's possible role in the virus's creation. Well over a year has passed, and millions of people throughout the world still don't seem to care about the suffering that has been and will continue to be inflicted. At the time, the potential for disaster should have been more obvious to everyone (Ayukekbong et al., 2020).

The COVID-19 pandemic serves as an excellent illustration of what can happen to the globe if artificial intelligence (AI) and related fields are refined to the point that they can identify targeted and targeted assaults or even produce chemicals or illnesses that are specific to our data. AI might simply evaluate the same data to identify the greatest method to hurt society, rather than researching same research to find ways to aid and heal people.

Due in part to the fact that a sizable fraction of the global population has contributed to the virus's capacity to spread much more widely, this has compelled the deployment of AI. Arora et al. (2020) offer two approaches for utilizing AI in relation to COVID-19. AI can be used to forecast the spread of viruses and create early warning systems for disease outbreaks (Arora et al., 2020).

#### **5. Examples of bioterrorism from the Past**

Threats from the biological world encompass a wide range of intricate risks that affect humankind. New technology like genetic engineering enable the

creation of very deadly pathogens for use as biological weapons. In the past, illness outbreaks brought on by naturally occurring viruses, lab mishaps, and intentional activities have wreaked havoc on human communities. Moreover, although if specialists believe the use of biological weapons is a low probability occurrence, it is nonetheless possible and might have disastrous worldwide repercussions (Henig, 2020).

Among the many well-known instances of bioterrorism are a few intriguing and horrifying incidents. The 1300s saw one of the most notable instances of the dire consequences that biological attacks could have. An illness spread among Tartar forces during the Siege of Caffa, causing them to become ill. The corpses of the plague victims were thrown over the wall by these forces, infecting the populace. The Black Death, which claimed the lives of 70–200 million people, began around this time. Using leprosy blood in wine in 1495 to sell contaminated wine to their French adversaries is one of the most intriguing cases. Similar to how they did during the Siege of Caffa, Russian troops sickened the populace of a Swedish city in 1710 by throwing diseased bodies over its walls. During the American Civil War in 1863, the Confederates offered American soldiers clothing that had been worn by yellow fever and smallpox victims. (Barras&Greub, 2014).

As we haven't thought about testing these biological agents, one notable example on the opposing side of this debate sticks out. There is a claim that during World War II, Japan experimented with over 10,000 POWs using a variety of biological weapons. Among them were meningococcal illness, cholera, anthrax, plague, and more.

A few spring to mind when we think back on biological attacks during the last few decades. In 1984, salad bars in Dallas, Oregon contracted a salmonella infection from the Rajneesh cult, which led to the illness of over seven hundred persons. The Tokyo metro was attacked with sarin gas in 1995 by the cult AumShinrikyo. Not too long after 9/11, in the United States, anthrax assaults are among the most well-known biological attacks. They happened in 2001. In total, 22 people were impacted by this (Barras&Greub, 2014).

Given their destructive potential and direct effects on human health as well as global socioeconomic instability, it is crucial to understand the causes of these risks, stop malevolent exploitation of biotechnology technology, and improve reaction tactics to counteract them.

## **6. Artificial Intelligence**

The Reincarnation of human intelligence, artificial intelligence is mostly handled by computers using a variety of technological elements and programming, including cybernetics, robots, and humanoids.

These days, AI is merely a clever instrument that doesn't truly comprehend humans. They may be aware that you are sobbing, even if they are experiencing emotion, but they may not grasp what it means to cry since they lack self-awareness. AI in the future will have emotion, comprehension,

and a sense of self. As a result, there will be a transition time for humans between AI now and AI in the future (Roumate, 2024).

By 2029, artificial intelligence will be on par with human intelligence. If we extend it further, let's say to 2045, we will have multiplied our civilization's intelligence—the human biological machine intelligence—by a billion. -Ray Kurzweil.

When we talk about artificial intelligence (AI), we usually mean the ability of robots to mimic higher intelligences. Artificial intelligence (AI) is proving to be quite useful in the biological area, especially with its algorithms that can handle massive amounts of unstructured data. This capacity fosters innovation in a number of fields, including the biosciences, by enabling quick assessments and difficult judgements (Bhardwaj et al., 2022). That same potential, but, also carries a high risk of malicious application, as in the development of hazardous biotechnologies (de Lima et al., 2024).

In the table. 1, the progress of Artificial intelligence has been described to comprehend the level of risks which can be expected in future in terms of bioterrorism.

Year	Progress in Artificial Intelligence
1940	Can computers replicate human thought processes? (Question by Alan Turing) Initial phase of AI
1956	The Dartmouth workshop, create devices capable of mimicking human thought processes.
1986	Machine learning techniques
2017	Pre-trained language models, like GPT-3, and language modelling
2019	The release of extensive language models such as GPT-2 and GPT-3
2023	The release of GPT 4.
2023/24	Working on GPT 5 and GPT 6

(Roumate, 2024).

## **7. An exponential increase in the ability to create biological weapons and deadly toxins**

Concerns have been raised over the dual application of cytotoxicity prediction models for creating new toxins and poisons. Bad actors now have more access to open-source biological design tools (BDTs) due to recent advancements in AI. Three different risks result from this.

### **a. Enhanced Availability of Quick Toxin Identification**

A toxicology company used MegaSyn AI software, which required less than six hours of machine time, a 2015 Mac computer, open-source data

and a minimal amount of digital architecture (programming) to identify 40,000 poisons. This implies that AI systems might make it easier for non-state actors, rogue governments, or independent individuals to produce chemical weapons than they would otherwise be able to due to a lack of funding. The threshold for specialist knowledge required to create chemical weapons has been significantly lowered extending the ability to identify and release deadly substances when paired with the use of LLMs and other all-purpose AI technologies.

**b. Finding of New Toxins**

The AI system detected thousands of entirely new potentially hazardous compounds in addition to VX( a human made chemical warfare agent which is very lethal, can be used through air, food and water)and other recognized chemical weapons, which is a significant finding from the experiments. This poses significant risks to chemical / biological defense since malicious actors might attempt to get AI systems to manufacture novel poisons that are not fully known and for which there are currently no established defense, neutralization, or treatment protocols.

**c. AI-Sped Up Creation of Biological Design Instruments**

These resources include a variety of disciplines, including synthetic biology, genomics, bioinformatics, and others. Essentially, these instruments enable smaller groups of people, using less resources, to find, create, and use modified viruses having the potential to cause a pandemic / Potential pandemic pathogens(PPPs). Crucially, these AI systems have the potential to increase the dangers associated with research on gain-of-function, which would allow bad actors to increase the lethality, transmissibility, and resistance of infections to medical countermeasures. Additionally, the use of AI by evil actors to target certain genotypes, races, ethnicities, tribes, families, or individuals with bioweapons can facilitate the commission of genocide on a possibly worldwide scale (Carter et al., 2023).

## **8. Greater Availability of Perilous Information and Manipulation**

### **Methods by means of LLMs**

Large language models (LLMs), which are AI tools that have been trained on vast amounts of text, such as scientific articles and discussion forums, are the first class of tools that could allow misuse of biology. LLMs and associated "AI assistants" can direct research, find pertinent web resources and tools, and offer scientific knowledge. Examples include language models designed for supporting scientific activity (e.g., BioGPT), foundation models (e.g., GPT-4/ChatGPT), and LLM-based apps for interacting with lab robots and other scientific instruments. Although

foundation models are currently being produced by a small number of businesses and are the result of massive and costly training runs, more resource-constrained entities can optimize these systems and turn them into applications for certain fields.

Large language models (LLMs) can enable malevolent actors to execute essential steps for chemical weapon deployment, including biological and chemistry knowledge, access to equipment for the lab, vital supplies, and weapon deployment systems. The development and application of biological weapons are made possible by these skills. Narrow artificial intelligence (AI) systems have the ability to take advantage of cybersecurity flaws, focusing on vital bio-infrastructure and possibly severely impairing response and recovery from biological events with extreme consequences.

Experiment of MIT's showed that students without technical background could use large language models (LLMs) to identify potential pandemic pathogens, explain their generation from synthetic DNA, and troubleshoot protocols. These models can also be used to access hazardous information, enabling those who lack competence and intellect to possibly do damage. This democratization of knowledge has implications for various settings and time horizons (Mouton Caleb and Ella, 2023).

Biosecurity and chemical security are at risk from AI-driven assaults since these technologies make it simpler to launch cyberattacks that target weaknesses in containment structures, research labs, and water treatment plants. Widespread exposure to dangerous chemicals or biological materials may result from these attacks.

Additionally, systems of AI can enhance cyber-manipulation techniques used by malevolent actors, including spear phishing, pharming, smishing, vishing, and other deceitful practices (Chaudhry & Klein, 2024)

## 9. Newly Emerging Hazards

There are many new hazards at the nexus of AI and bio-threats. Such as,

1. Illegal distribution of genetically modified organisms (GMOs) as biological weapons endangering human health and biodiversity.
2. Using genetically engineered Nanobots to target particular human bodily systems or organs.
3. Creation of infections that target the fundamental components of the genetic code for humans.
4. Altering microbes to target vital infrastructure like water sources and agricultural crops.
5. "Human control viruses" spreading.
6. Bioweapons that target particular ethnic groups and the creation of microbes that have been "signed."

## 10. Catastrophic Losses

1. Widespread repercussions, such as the collapse and chaos of health systems, socioeconomic instability (company closures, travel restrictions, quarantines, border closures, and quarantines), and even a high death toll similar to that of the COVID-19 Pandemic. These altered infections have the potential to spread quickly and overwhelm health systems' ability to respond appropriately, leading to diseases for which there is now no known cure. Panic will result from this, and there will be serious social unrest, widespread health issues, increased medical costs, and detrimental effects on the community's economy.
2. Quick and extensive organic breakdown and catastrophic health system collapse.  
Should Nanobots be engineered to target critical organs or particular physiological systems, there is a potential for swift degradation of crucial tissues and physiological processes.
3. Human DNA is gradually and unpredictably degrading, leading to uncontrollably occurring genetic disorders, abundance of sterility, and a rise in cancer cases. This may cause a sharp drop in population, which would have an impact on socioeconomic dynamics.
4. Widespread famine, a rise in resource-related conflicts, and large-scale migrations. as well as unrest in geopolitics. Important services are interrupted, crucial infrastructure collapses, and crucial systems are damaged.
5. According to Giordano and Wurzman (2011), researchers define "Neuro-weapons" as technological tools which can be applied to control or modify brain functions to one's benefit in defense and security situations. They also discuss how the potential for neuro-weapons to radically alter the nature of espionage and warfare may make them of significant relevance to national security initiatives. Political instability, societal fragmentation, behavior control, and widespread psychological manipulation. Microorganisms that alter brain chemistry could be developed by malicious people, causing widespread behavioral changes, anxiety, paranoia, or even particular actions that lead to societal and political anarchy.
6. Genetic differences across ethnic groups raise the prospect of creating biological weapons intended to kill particular groups of people. Innate genetic weaknesses could be exploited by chemical agents, allowing offensive actions to take place that safeguard the aggressor's population while rendering the target population defenseless. The employment of bioweapons in upcoming conflicts is a key ethical dilemma raised by

this method (Larson, 1970). Specific ethnic groups may be mass-murdered as a result of the deliberate usage of GMOs, resulting in cultural destruction and genocide. The genetic complexity of "signature" germs makes it possible that identifying the source of the attack won't be easy and prosecute those responsible. Such attacks have the potential to destabilize entire countries as well as particular regions, resulting in serious political and humanitarian catastrophes. Attacks directed against particular ethnic groups have the potential to fuel international mistrust and escalate geopolitical tensions (de Lima et al., 2024).

## 11. AI-Powered Amplification

1. Artificial intelligence (AI) has the potential to revolutionize genetic research by enhancing pathogen genetic engineering and utilizing protein re-modelling algorithms. This could result in pathogens that are more lethal, resistant to therapy, or able to adapt to new environments more quickly, thereby complicating containment and treatment development.
2. Artificial Intelligence has the capability to analyze vast amounts of biological data, including cellular and genetic data, by utilizing sophisticated machine learning techniques. AI recognizes particular patterns in cells, which makes it possible to build Nano-bots that can pinpoint specific targets within the cell. Artificial Intelligence employs computational simulations and molecular modelling to create Nano-bots with specialized capabilities. AI is capable of using immune system identification techniques to find efficient ways for Nano-bots to blend in. Artificial intelligence (AI) examines data from current medical therapies to find patterns that Nano-bots can't match.
3. AI can precisely identify the regions of the human genome that are susceptible to harmful changes. This might result in the development of highly specialized infections that can target and alter the genetic code more potently and destructively, causing diseases that cannot be reversed.
4. AI may be used to examine the genomes of plants and pinpoint particular weaknesses that, if exploited by Genetically modified organisms (GMOs), would result in disastrous failures. Moreover, machine-learning techniques can be used to enhance these microbes' distribution plans in an effort to achieve a quick worldwide proliferation. Critical infrastructure weaknesses may be mapped by AI, which can also identify the most vulnerable entry points. Algorithms

that alter monitoring data can be developed to conceal the presence of microorganisms and the level of contamination.

5. Using information from psychological and neuroscientific research, AI is able to understand the molecular mechanisms and patterns of brain activity connected to feelings, actions, and responses. AI is able to recognize patterns and determine how microbes might impact certain chemical processes in the brain. Machine learning algorithms are capable of identifying pathways of propagation, such as water and air, so that a broad population is exposed to the microbes.
6. AI can help progress genetic studies. Malicious actors might employ artificial intelligence (AI) to alter microbes to have particular “genetic signatures,” enabling them to assault target populations while evading detection by conventional tracking and identification techniques (de Lima et al., 2024).

## 12. Recommendations

In the context of above discussion, some recommendations are as under:

1. Limit the Publication of Model Weights for Systems That May Be Used, or Redesigned to Be Used, for the Purpose of Finding Hazardous Toxins.
2. Prevent the Use of Risky Data for Training Extensive Language Models by enclosing it.
3. AI Threats in Research on Concern Guidance and Risk Frameworks for Dual Use should be incorporated.
4. Bolster current biodefense capabilities and capacities.
5. For Assessing General-Purpose Advanced AI Systems for the Use of Biological weapons, Criteria should be clear.
6. Make & Put into Practice Specific Policies for the use of AI
7. Keep an eye on Research That Could Be Harmful
8. Considering risks when making decisions related to AI

## 13. Conclusion

In the complex setting of biological hazards, the implications of AI become a double-edged sword, with the potential to both increase and decrease dangers. Since the creation and release of biological agents, as well as the genetic modification of natural enemies, call for interdisciplinary approaches, cooperation and integration are essential. Environmental impact assessments are crucial for comprehending the worldwide implications of genetically modified organism releases. Thorough safety testing is necessary to evaluate the threats that the improper use of AI poses to human and environmental health. It is imperative to be proactive in the future; understanding the operational risks associated with AI in this context will

focus research efforts on robust solutions that protect global security from potentially catastrophic social threats. The way and degree to which biosecurity threats will be made worse by artificial intelligence advancements is still unknown. However, it is wise to take steps according to the recommendations to evaluate and reduce risks given the potential for quick advancements in AI capabilities. AI will be able to realize its extremely favorable implications for the life sciences and human health provided dangers will be successfully managed.

## References

- Arora, N., Banerjee, A. K., & Narasu, M. L. (2020). The role of artificial intelligence in tackling COVID-19. *Future Virology*, 15(11), 717-724. doi:10.2217/fvl-2020-0130
- Artificial intelligence in software test automation tools and technologies (Survey). (2023). International Conference on Biological Research and Applied Science. doi:10.37962/ibras/2023/72-76
- Ashima Jha. (2023, August). *Technological Advances and Evolution of Biowarfare: A Threat to Public Health and Security*. Paper presented at International Conference Health, Social Science & Engineering (ICHSSSE). DOI 10.18502/kss.v8i14.13853
- Ayukekbong, J. A., Ntemgwa, M. L., Ayukekbong, S. A., Ashu, E. E., & Agbor, T. A. (2020). COVID-19 compared to other epidemic coronavirus diseases and the flu. *World Journal of Clinical Infectious Diseases*, 10(1), 1-13. doi:10.5495/wjcid.v10.i1.1
- Barras, V., & Greub, G. (2014). History of biological warfare and bioterrorism. *Clinical Microbiology and Infection*, 20(6), 497–502. <https://doi.org/10.1111/1469-0691.12706>
- Bhardwaj, A., Kishore, S., and Pandey, D. K. (2022). Artificial Intelligence in Biological Sciences. *Life* 12:1430. doi: 10.3390/life12091430
- Bio X AI: Policy Recommendations for A New Frontier. Federation of American Scientists. <https://fas.org/publication/bio-x-ai-policy-recommendations/>
- Carter, S. R., Wheeler, N. E., Isaac, C. R., Yassif, J., & Chwalek, S. (2023). The Convergence of Artificial Intelligence and the Life Sciences: Safeguarding Technology, Rethinking Governance, and Preventing Catastrophe. In *www.nti.org* (pp. 1–68). [www.nti.org/Bio: Nuclear Threat initiative \(NTI\)](http://www.nti.org/Bio: Nuclear Threat initiative (NTI). Retrieved from Nuclear Threat initiative (NTI) website: https://www.nti.org/analysis/articles/the-convergence-of-artificial-intelligence-and-the-life-sciences/). Retrieved from Nuclear Threat initiative (NTI) website: <https://www.nti.org/analysis/articles/the-convergence-of-artificial-intelligence-and-the-life-sciences/>
- Chaudhry, H., & Klein, L. (2024, February 27). Chemical & Biological Weapons. USA: Future of life Institution.

<https://futureoflife.org/document/chemical-biological-weapons-and-artificial-intelligence-problem-analysis-and-us-policy-recommendations/>

- De Lima, R. C., Sinclair, L., Megger, R., Maciel, M. A. G., Vasconcelos, P. F. d. C., & Quaresma, J. A. S. (2024). Artificial intelligence challenges in the face of biological threats: emerging catastrophic risks for public health. *Frontiers in Artificial Intelligence*, 7. doi:10.3389/frai.2024.1382356
- Erasmus, T. (2021). *AI & Bioterrorism: An Overview of the Ethical Risks Involved* [Stellenbosch University]. <https://scholar.sun.ac.za>
- Henig, R. (2020, July 18). Experts warned of a pandemic, decades ago. Why weren't we ready? *National Geographic Magazine*. <https://www.nationalgeographic.com/science/article/experts-warned-pandemic-decades?ago-why-not-ready-for-coronavirus>
- Mouton, C. A., Caleb, L., and Ella, G. (2023). The operational risks of AI in large-scale biological attacks: a red-team approach. RAND Corporation, Santa Monica, CA. Available at: [https://www.rand.org/pubs/research\\_reports/RRA2977-1.html](https://www.rand.org/pubs/research_reports/RRA2977-1.html) (Accessed November 25, 2023).
- Newman, S. (2024). Biosecurity and AI: risks and opportunities. Center for AI Safety. Available at: <https://www.safe.ai/blog/biosecurity-and-ai-risks-and-opportunities> (Accessed April 19, 2024).
- Roumate, F. (2024). *Artificial intelligence and the New World order: New weapons, new wars and a new balance of power*. Springer Nature.
- Sandbrink, J. B. (2023). Artificial intelligence and biological misuse: differentiating risks of language models and biological design tools. arXiv [Preprint]. doi: 10.48550/arXiv.2306.13952
- Tyshenko, M. G. (2007). Management of natural and bioterrorism induced pandemics. *Bioethics*, 21(7), 364-369. doi:10.1111/j.1467-8519.2007.00571.
- World Health Organization (2023). "Biological Weapons." Available at: <https://www.who.int/health-topics/biological-weapons> (Accessed June, 05, 2024).
- Yassif, J. M., Korol, S., and Kane, A. (2023). Guarding against catastrophic biological risks: preventing state biological weapon development and use by shaping intentions. *Health Secur.* 21, 258–265. doi: 10.1089/hs.2022.0145