Office of Technology Assessment
at the German Bundestag

TAB-Fokus no. 51 | July 2026
regarding report no. 217

Biotechnology and artificial intelligence

Risks posed by research to security and biological weapons proliferation

What is involved

Rapid advances in the analysis and synthesis of genetic material (DNA), as well as in the targeted modification of genes, have greatly simplified and expanded the possibilities for researching, modifying, or redesigning biological processes in organisms over the last 10 to 15 years. Computer-aided analysis and design processes are becoming an increasingly important tool in this context. These capabilities have not only accelerated basic research, such as the elucidation of gene and molecular functions and the causes of disease, but have also spurred revolutionary developments in fields such as industrial biotechnology and the development of new medicines and treatment options.

The concept of synthetic biology (also known as 'engineering biology'), whereby biological systems can be modified or redesigned with increasing ease and specificity, emerged at the beginning of the 2000s. From the outset, the scientific — and, to a certain extent, societal — debate has focused on potential health and environmental risks (biosafety), as well as risks arising from misuse (biosecurity).

With the ever-increasing possibilities of synthetic biology brought about by AI and its interaction with biotechnological methods (AIxBio), these discussions have intensified in recent years. A new security debate has emerged that focuses heavily on the potential development of biological weapons (see box on page 2). There are concerns that these new capabilities could significantly lower barriers to bioweapons and facilitate the generation of more dangerous or novel biological agents. Furthermore, concerns have been raised that the effectiveness of biosecurity and defence measures could be reduced or undermined.

Potential risks posed by AIxBio: Concerns, available evidence and uncertainties

Concerns regarding biosecurity risks are primarily based on three developments:

- the potential acquisition and dissemination of knowledge through large language models (LLMs);
- the potential design of modified proteins, toxins and new pathogens using biological AI models; and
- the combination of AI systems with robotised laboratory platforms to enable experiments

At a glance

- The potential of AI for biotechnology has sparked a new security debate. The debate focuses on the risks posed by the possible development of biological weapons, particularly by non-state actors and individuals without specialist knowledge.
- The available evidence does not conclusively answer the question of whether AI models could substantially lower the barriers to developing biological weapons. For individuals with little or no specialist knowledge, empirical data currently suggest this is unlikely.
- However, it is not possible to reliably assess how this might change in the future, which is why continuous monitoring of these highly dynamic developments is essential.
- Given the potential variety of malicious actors and biological threats with extreme consequences, further precautionary measures to minimise risk at various levels should be considered now.

or development and optimisation cycles to be carried out automatically, or even 'autonomously' (See Fig. 2, p. 3).

Empirical studies leave open the question of the extent to which LLMs can assist bioterrorists

Although tests (benchmarks) of LLMs regarding knowledge and capabilities relevant to the development of biological weapons suggest that various newer LLMs sometimes significantly exceed the benchmark values set by human experts, studies involving test subjects designed to determine the extent to which LLMs can enhance individuals' knowledge or skills beyond conventional internet searches (so-called 'uplift' and 'red-teaming' studies) do not present a consistent picture. However, a recent study suggests that the coordinated use of several LLMs can significantly improve the performance of Bachelor's Degree students with little or no biology background when answering various biological knowledge or technique questions and tasks, sometimes bringing their performance close to or beyond expert level. The practical relevance of these findings in the real world remains unclear, though. Consequently, studies involving test subjects in biology laboratories ('wet labs') have begun. An initial large-scale study suggests that LLMs (from mid-2025) are no more effective than traditional internet tools at helping undergraduate students with little or no biology or laboratory experience to carry out basic tasks to produce a relatively simple virus in a laboratory. It remains to be seen to what extent newer LLMs or the additional use of biology-specific LLMs might change this and what performance improvements might look like for more experienced individuals (e.g. PhD students in biology). Further studies of this kind are likely to be required.

Biodesign models could facilitate the undetected production of dangerous genetic sequences

AI-based protein design models enable the creation or redesign of complex protein structures. In principle, therefore, novel and potentially dangerous proteins or (protein) toxins could also be designed. However, their functionality would likely need to be verified or optimised through laboratory experiments that are both research-intensive and resource-heavy. It has already been demonstrated that protein toxins can be redesigned in such a way that they presumably remain functional, and that, due to differences in their gene sequence compared to the original version, they can circumvent current methods for securtiy checks for nucleic acid synthesis. Nevertheless, the actual extent of the risk remains unclear. Experimental data suggest that protein versions redesigned in this way (using current open-source models) lose their function, particularly larger proteins and enzymes.

Whether it is possible to specifically enhance pathogens or even design entirely new ones remains uncertain

It is unclear whether AI models can be used to specifically and effectively enhance complex properties of pathogens, such as transmissibility and the ability to evade immune responses. While certain AI models can already predict the short-term effects of mutations in gene sequences on some of these properties, for example in viruses such as SARS-CoV-2, the ability to predict longer-term effects (across multiple infection cycles) may remain limited, even with

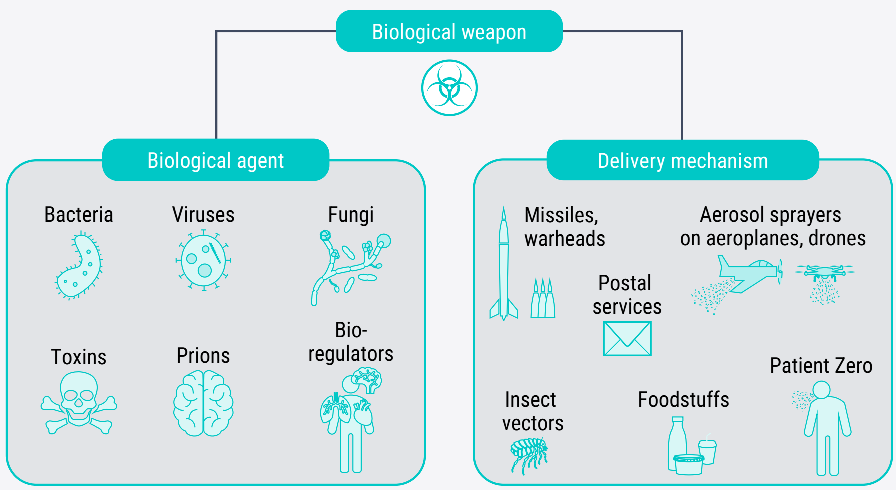
Biological weapons (Bioweapons)

Bioweapons disseminate pathogens or toxins and typically consist of a biological agent and a delivery mechanism. The development of bioweapons requires specific knowledge and technical capabilities, particularly for weapon systems designed for large-scale dissemination or with a long range. For example, such knowledge is required for the handling of pathogens, their formulation, or large-scale production. However, bioweapons can also be less technically complex, for example when the dissemination of small quantities of agents is sufficient and can be achieved using simple, non-technical mechanisms (see Fig. 1).

The only large-scale military use of bioweapons took place between 1939 and 1942, when Japan used them in China, resulting in what is believed to be thousands of deaths. Bioterrorist attacks have so far been relatively rare. Only a few of these have resulted in illness or death. For instance, in 1984, members of the Rajneesh sect contaminated food in restaurants in the USA with salmonella, causing hundreds of people to fall seriously ill. A series of attacks involving letters containing anthrax spores in the USA in 2001 led to at least five deaths and several further cases of illness.

Legally, the possession of bioweapons is prohibited, and their use is outlawed under international law. The primary basis for this is provided by international treaties relating to bioweapons and their use. The most important of these is the 1972 Convention on the Prohibition of Biological Weapons, also known as the Biological Weapons Convention (BWC).

Figure 1 Biological agents and delivery mechanisms for biological weapons



Source: adapted from Sabra/Frieß (2025)

more and higher-quality data. This is mostly due to sudden evolutionary events that can lead to complex genetic changes. The emergence of entirely new pathogens, such as pandemic viruses, could have the most far-reaching consequences in terms of biological threats because the means to combat them would be limited due to a lack of information or because they could only be developed after a delay. However, the large, high-quality datasets required to develop such AI models, which could construct and combine relevant characteristics even for comparatively less complex pathogens such as viruses, are currently lacking. Furthermore, even with these models, the evolution of potentially newly engineered viruses might not be reliably predictable.

Automated or autonomous experimental platforms could reduce the need for knowledge and practical skills in the future

Commercial automated laboratory platforms, particularly so-called 'cloud labs' that are accessible via the internet, can already eliminate the need to carry out certain laboratory tasks manually. Nevertheless, effectively using such laboratories still requires specific knowledge, e.g. regarding the use of methods and the procedures within the cloud labs. These requirements could diminish in the future, for example through AI-assisted programming and analysis of experiments. 'Autonomous' ('self-driving') laboratory systems could significantly facilitate the production or development of biological agents. However, developing such systems for specific biological agents is research- and cost-intensive, requiring in-depth specialist knowledge in various fields.

Implications for threats from biological weapons and outlook

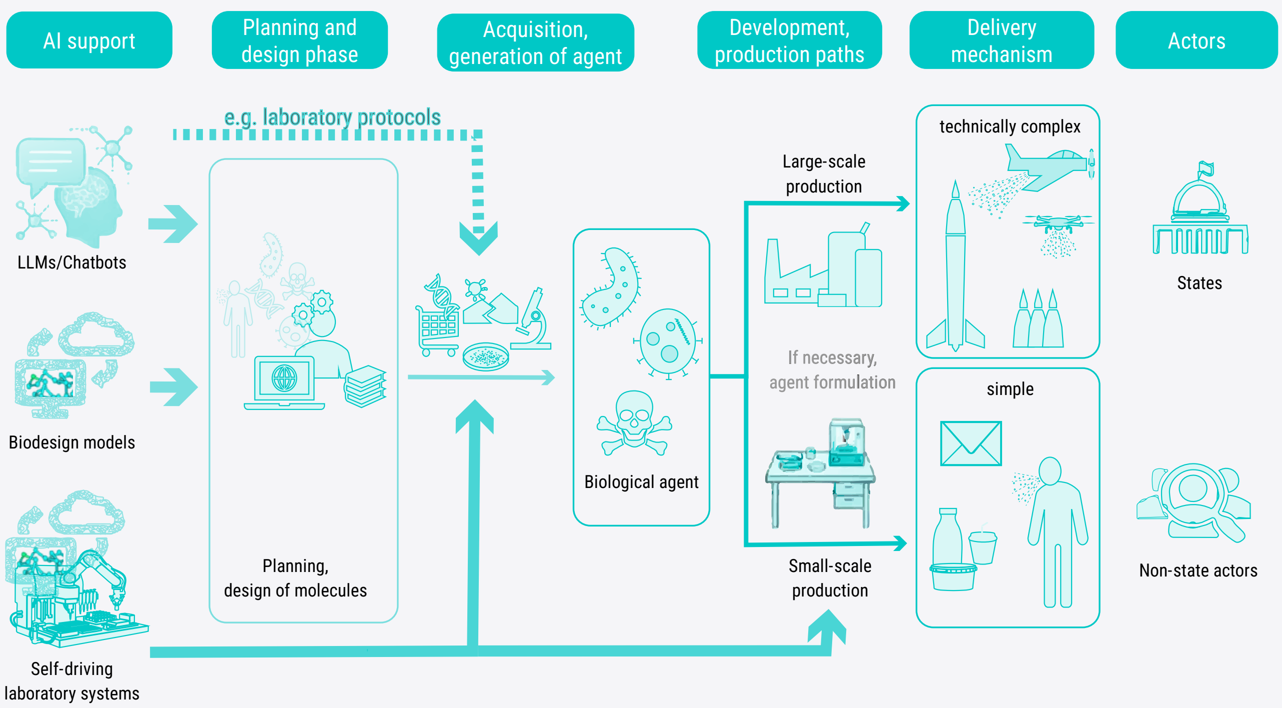
Assessing the potential of AIxBio in terms of the risks of its misuse for biological weapons requires a perspective that goes beyond the capabilities of AI itself.

Key factors include technological prerequisites for the production and use of biological weapons on a larger scale. These are largely independent of AI capabilities, such as the large-scale production of pathogens or sophisticated weapon technology. Threats requiring these processes and capabilities are likely to originate primarily from states (see Fig. 2). Nevertheless, new AIxBio capabilities could influence other stages of development within state bioweapons programmes.

Secondly, consideration must be given to the factors that determine intent and strategies for using biological weapons. These can be diverse, especially among non-state actors. Due to their limited technological capabilities, non-state actors may continue to use biological weapons that are technically less sophisticated, as was the case in previous ´successful' acts of bioterrorism (see box on page 2).

In the case of such simpler approaches, using AI tools to acquire knowledge about the isolation or production of biological agents or to alter gene sequences to circumvent nucleic acid synthesis screenings could have a significant impact on future capabilities and potential for harm.

Figure 2 **Potential risks arising from the use of AI systems for the production of dangerous biological agents or biological weapons**



Own illustration

Nevertheless, very far-reaching risk scenarios, such as the production of pandemic viruses via synthetic genomes, still appear improbable, at least when considering individuals without significant laboratory experience.

It is not possible to reliably assess the extent to which this might change in the future. However, given the potential consequences and uncertainties – including those relating to other actors – continuous monitoring of the highly dynamic AI developments, as well as further precautionary measures to minimise risk and improve resilience to potential consequences, appear necessary.

Fields of action and policy options

Not least due to the variety of potential actors, precautionary measures must address different areas of action. Four main areas of focus can be identified:

Controlling the interface between AI-generated digital designs and real biological molecules or systems

A key element here could be supporting the planned European Biotech Act to enable mandatory, EU-wide harmonised securtiy screenings for nucleic acid synthesis and its customers. Secondly, conditions could be introduced for the use of research funding, stipulating that nucleic acid synthesis may only be sourced from manufacturers who carry out appropriate security checks.

Monitoring and control of AI systems with enhanced capabilities for developing dangerous biological agents

To this end, requirements could be considered for developers to implement measures ensuring controlled access to powerful biodesign models or specific datasets for their development. However, this option would need to be weighed up very carefully against potential negative impacts, particularly with regard to biomedical research and the development of countermeasures in the event of a crisis. An advisory panel comprising experts from various disciplines and fields could contribute to this assessment. Such a panel could also be involved in an 'if-then' strategy aimed at continuously assessing dynamic developments, as well as regularly reassessing risks and adapting measures. Depending on the findings, new risk assessments would be carried out, and risk-mitigation measures would be tightened or relaxed where necessary.

Strengthening the Biological Weapons Convention by providing further substantive support for the relevant working group within the BWC

Compared with traditional verification regimes involving short-notice inspections of suspect facilities, the aim could be to pursue less intrusive and potentially more easily achievable models, which could include structured self-reporting or on-site peer-review visits. In addition, initiatives to improve the BWC's funding situation could be launched or supported.

Capabilities to implement preventive and countermeasures could be expanded

To this end, opportunities to strengthen activities and capacities could be explored, particularly in two areas:

- Application-oriented biodefence research: AI could contribute to the early detection of pathogens and the rapid development of scalable medical countermeasures (such as vaccines).
- To counter terrorism, cooperation with companies developing AI could be promoted or their security measures supported. This could include mechanisms for identifying user interactions with large generative AI models that indicate malicious intent.

TAB report no. 217

Biotechnologie und künstliche Intelligenz: Risiken der Forschung für die Sicherheit sowie die Proliferation von Biowaffen
Harald König (in collaboration with Arnold Sauter)

Project information
www.tab-beim-bundestag.de/AIxBio

Publisher
Office of Technology Assessment
at the German Bundestag (TAB)

Image credit
AI generated image/TAB (p.1)

ISSN: 2364-2645
DOI: 10.5445/IR/1000196057