

TAB-Fokus Nr. 51 | Juli 2026  
zum Arbeitsbericht Nr. 217

# Biotechnologie und künstliche Intelligenz

## Risiken der Forschung für die Sicherheit sowie die Proliferation von Biowaffen

### Worum es geht

Die rasanten Fortschritte bei der Analyse und Synthese von Erbgut (DNA) sowie bei der gezielten Veränderung von Genen haben die Möglichkeiten der Erforschung und der Um- oder Neugestaltung biologischer Prozesse in Organismen in den letzten 10 bis 15 Jahren stark vereinfacht und erweitert. Ein zunehmend wichtiges Werkzeug sind dabei computergestützte Analyse- und Designprozesse. Diese Möglichkeiten haben nicht nur die Grundlagenforschung beschleunigt, etwa zur Aufklärung von Gen- und Molekülfunktionen sowie von Krankheitsursachen. Auch in Anwendungsfeldern wie der industriellen Biotechnologie und der Entwicklung neuer Medikamente bzw. Behandlungsmöglichkeiten haben sie bereits revolutionäre Entwicklungen angestoßen.

Das Konzept der Synthetischen Biologie (oder „Engineering Biology“), demzufolge biologische Systeme zunehmend einfacher gezielt um- bzw. neugestaltet werden können, wurde bereits Anfang der 2000er Jahre formuliert. Die wissenschaftliche und in gewissem Umfang auch gesellschaftliche Debatte thematisierte dabei von Anfang an mögliche Risiken für die Gesundheit und die Umwelt (Biosafety) sowie Risiken durch missbräuchliche Verwendungen (Biosecurity).

Mit den durch KI und deren Zusammenspiel mit biotechnologischen Methoden (KlxBio) weiter zunehmenden Möglichkeiten der Synthetischen Biologie haben sich diese Diskussionen in den letzten Jahren erneut intensiviert und es hat sich eine Sicherheitsdebatte entwickelt, die sich stark auf die mögliche Herstellung von Biowaffen (vgl. Kasten, S. 2) fokussiert. Es bestehen Befürchtungen, dass die Hürden hierfür durch die neuen KlxBio-Möglichkeiten entscheidend gesenkt werden könnten und die Generierung gefährlicherer oder neuartiger biologischer Agenzien erleichtert wird. Zudem wird befürchtet, dass die Wirksamkeit von Biosicherheit- und Abwehrmaßnahmen verringert oder unterlaufen werden könnte.

### Mögliche Risiken durch KlxBio: Befürchtungen, verfügbare Evidenz und Unsicherheiten

Die Befürchtungen um Biosecurity-Risiken beruhen im Wesentlichen auf drei Entwicklungen:

1. der möglichen Wissensaneignung oder -erweiterung über große Sprachmodelle (LLMs),
2. dem möglichen Design veränderter Proteine bzw. Toxine und neuer Krankheitserreger mithilfe biologischer KI-Modelle sowie

### Auf einen Blick

- Das Potenzial von KI für die Biotechnologie hat eine neue Sicherheitsdebatte ausgelöst. Diese fokussiert auf Risiken durch die mögliche Herstellung biologischer Waffen – insbesondere durch nicht staatliche Akteure, einschließlich Personen ohne Fachkenntnisse.
- Verfügbare Evidenz lässt die Frage offen, ob KI-Modelle die Hürden für Biowaffen entscheidend senken könnten. Für Personen ohne oder mit wenigen Fachkenntnissen machen empirische Daten dies derzeit wenig wahrscheinlich.
- Inwiefern sich dies zukünftig ändern könnte, ist nicht belastbar abzuschätzen und macht ein kontinuierliches Monitoring der hochdynamischen Entwicklungen erforderlich.
- Aufgrund der möglichen unterschiedlichen böswilligen Akteure und biologischen Bedrohungen mit extremen Folgen sollten bereits heute weitere vorsorgende Maßnahmen zur Risikominimierung auf unterschiedlichen Ebenen in Betracht gezogen werden.

3. der Kombination von KI-Systemen mit robotisierten Laborplattformen, um Experimente bzw. Entwicklungszyklen automatisiert oder gar „autonom“ durchführen lassen zu können (Abb. 2, S. 3).

### Empirische Studien lassen die Frage offen, inwieweit LLMs Bioterroristen tatsächlich unterstützen können

Zwar legen Tests (Benchmarks) von LLMs zu Wissen und Fähigkeiten, die für die Biowaffenherstellung relevant sein könnten, nahe, dass verschiedene jüngere LLMs Referenzwerte menschlicher Expert/innen teilweise deutlich übertreffen. Untersuchungen mit Testpersonen, um herauszufinden, inwieweit LLMs – über konventionelle Internetsuchen hinaus – die Kenntnisse bzw. Fähigkeiten der Personen verbessern können (sog. Uplift- und Red-Teaming-Studien), zeigen jedoch kein einheitliches Bild. Eine jüngere Studie legt aber nahe, dass die koordinierte Nutzung mehrerer LLMs die Leistungen von Studierenden ohne oder mit wenig Biologieerfahrung bei der Lösung verschiedener Fragen und Aufgaben aus Benchmarks zu biologischem Wissen oder Techniken deutlich

verbessern kann, teilweise auf das Niveau von Expert/innen oder sogar darüber hinaus. Die praktische Relevanz dieser Ergebnisse für die Umsetzung in der realen Welt ist jedoch unklar. Deshalb wurde begonnen, Studien mit Testpersonen in biologischen Laboren durchzuführen. Eine erste größere Studie legt nahe, dass Sprachmodelle (von Mitte 2025) Studierende ohne wesentliche Biologie- und Laborerfahrung bei grundlegenden Laboraufgaben zur Erzeugung eines relativ einfach herstellbaren Virus nicht besser unterstützen können als klassische Internetwerkzeuge. Inwiefern neuere LLMs oder die zusätzliche Nutzung biologiespezifischer LLMs dies ändern könnten und wie Leistungssteigerungen für erfahrenere Personen (z.B. Biologiedoktorand/innen) aussehen würden, ist offen. Dies dürfte weitere Studien dieser Art erfordern.

### Biodesignmodelle könnten die unerkannte Herstellung besorgniserregender Gensequenzen erleichtern

KI-basierte Proteindesignmodelle ermöglichen die gezielte Neu- oder Umgestaltung komplexer Proteinstrukturen. Somit könnten prinzipiell

auch neuartige und gefährlichere Proteine bzw. (Protein-)Toxine entworfen werden. Deren Funktionalität dürfte aber in forschungs- und ressourcenaufwendigen Laborexperimenten überprüft oder optimiert werden müssen. Bereits gezeigt wurde, dass Proteintoxine so umgestaltet werden können, dass sie mutmaßlich funktionell bleiben und aufgrund von Unterschieden zur Originalversion in ihrer Gensequenz derzeitige Methoden für Sicherheitsüberprüfungen bei Nukleinsäuresynthesen umgehen können. Wie groß die Gefahr tatsächlich ist, ist aber unklar. Experimentelle Daten deuten darauf hin, dass (über derzeitige Open-Source-Modelle) so umgestaltete Proteinversionen, insbesondere von größeren Proteinen und Enzymen, ihre Funktion verlieren.

### Eine gezielte Verbesserung oder gar das Design völlig neuer Krankheitserreger bleiben fraglich

Ob sich über KI-Modelle relevante, komplexe Eigenschaften von Krankheitserregern – wie die Übertragbarkeit oder die Umgehung von Immunreaktionen – gezielt und effektiv verbessern lassen, ist unklar. Zwar können bestimmte

## Biologische Waffen (Biowaffen)

Biowaffen verbreiten Krankheitserreger oder Toxine und bestehen typischerweise aus einem biologischen Agens sowie einem Ausbringungsmechanismus. Ihre Entwicklung erfordert, insbesondere für Waffensysteme zur großflächigen Ausbringung oder mit großer Reichweite – wie sie in staatlichen Waffenprogrammen entwickelt wurden – spezifisches Wissen und technische Voraussetzungen, beispielsweise zum Umgang mit Erregern, deren Formulierung oder großtechnischen Herstellung. Biowaffen können jedoch auch technisch weniger aufwendig sein, beispielsweise wenn die Ausbringung kleiner Mengen von Agenzien ausreicht und über einfache nichttechnische Mechanismen erfolgen kann (vgl. Abb. 1).

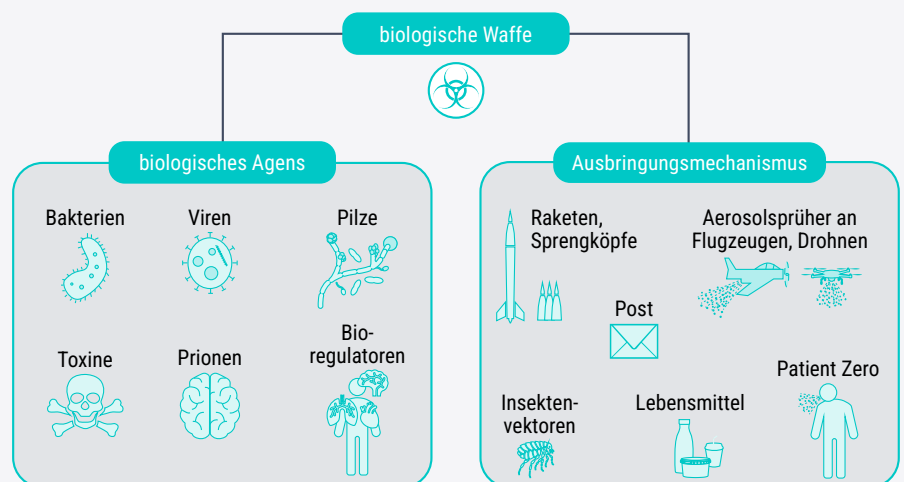
Die einzigen großflächigen militärischen Biowaffeneinsätze erfolgten zwischen 1939 und 1942 durch Japan in China – mit wohl Tausenden von Toten. Bioterroristische Anschläge waren bisher relativ selten. Nur ganz wenige davon führten zu Erkrankungs- oder gar Todesfällen. So wurden 1984 in den USA Lebensmittel in Restaurants durch Mitglieder der Rajneesh-Sekte mit Salmonellen verseucht,

wodurch Hunderte schwer erkrankten, und eine Serie von Anschlägen in den USA im Jahr 2001 mit Briefen, die Milzbrand-Sporen enthielten, führte zu mindestens fünf Toten und einer Reihe weiterer Erkrankter.

Rechtlich gesehen ist der Besitz von Biowaffen verboten und ihr Einsatz ist völkerrechtlich

geächtet. Zentrale Grundlage hierfür sind internationale Abkommen in Bezug auf Biowaffen und deren Einsatz wie insbesondere das Übereinkommen über das Verbot biologischer Waffen von 1972 (die Biowaffenkonvention, BWC).

Abbildung 1 Bioagenzien und Ausbringungsmechanismen von Biowaffen



Quelle: verändert nach Sabra/Frieß (2025)

KI-Modelle bereits Vorhersagen zu kurzzeitigen Auswirkungen von Mutationen in Gensequenzen, etwa von Viren wie SARS-CoV-2, auf manche dieser Eigenschaften machen. Die Möglichkeiten, die längerfristigen Auswirkungen solcher Veränderungen (über mehrere Infektionszyklen hinweg) vorherzusagen, könnten aber auch mit mehr und hochwertigeren Daten zukünftig begrenzt bleiben, nicht zuletzt aufgrund sprunghafter evolutionärer Ereignisse, die zu komplexen genetischen Veränderungen führen können. Die Entwicklung völlig neuer Krankheitserreger, wie pandemischer Viren, könnte potenziell die weitreichendsten Folgen in Bezug auf biologische Bedrohungen haben, da Möglichkeiten zu ihrer Bekämpfung aufgrund fehlender Informationen eingeschränkt wären bzw. nur verzögert entwickelt werden könnten. Allerdings fehlen hierzu bislang die erforderlichen großen und qualitativ hochwertigen Datensätze zur Entwicklung von KI-Modellen, mithilfe derer relevante Eigenschaften – selbst bei vergleichsweise wenig komplexen Erregern wie Viren – konstruiert und kombiniert werden könnten. Zudem könnte die Evolution potenziell neu entworfener Viren auch mit diesen Modellen nicht zuverlässig vorhersagbar sein.

### Automatisierte oder autonome Versuchsplattformen könnten die Anforderungen an Kenntnisse und praktische Fähigkeiten zukünftig senken

Kommerzielle automatisierte Laborplattformen, vor allem die über das Internet nutzbaren sogenannten Cloud Labs, können bereits heute die Notwendigkeit aufheben, bestimmte Laborarbeiten selbst durchführen zu müssen. Der effektive Einsatz solcher Labore erfordert aber noch spezifisches Wissen, etwa zur Verwendung von Methoden und den Abläufen in den Cloud Labs. Diese Anforderungen könnten jedoch zukünftig abnehmen, z.B. durch eine durch KI erleichterte Programmierung und Analyse von Experimenten. „Autonome“, sogenannte Self-driving-Laborsysteme könnten die Herstellung bzw. Entwicklung biologischer Agenzien erheblich erleichtern. Allerdings ist die Entwicklung solcher Systeme für spezifische biologische Agenzien forschungs- und kostenintensiv und erfordert ausgeprägte Fachkenntnisse in verschiedenen Bereichen.

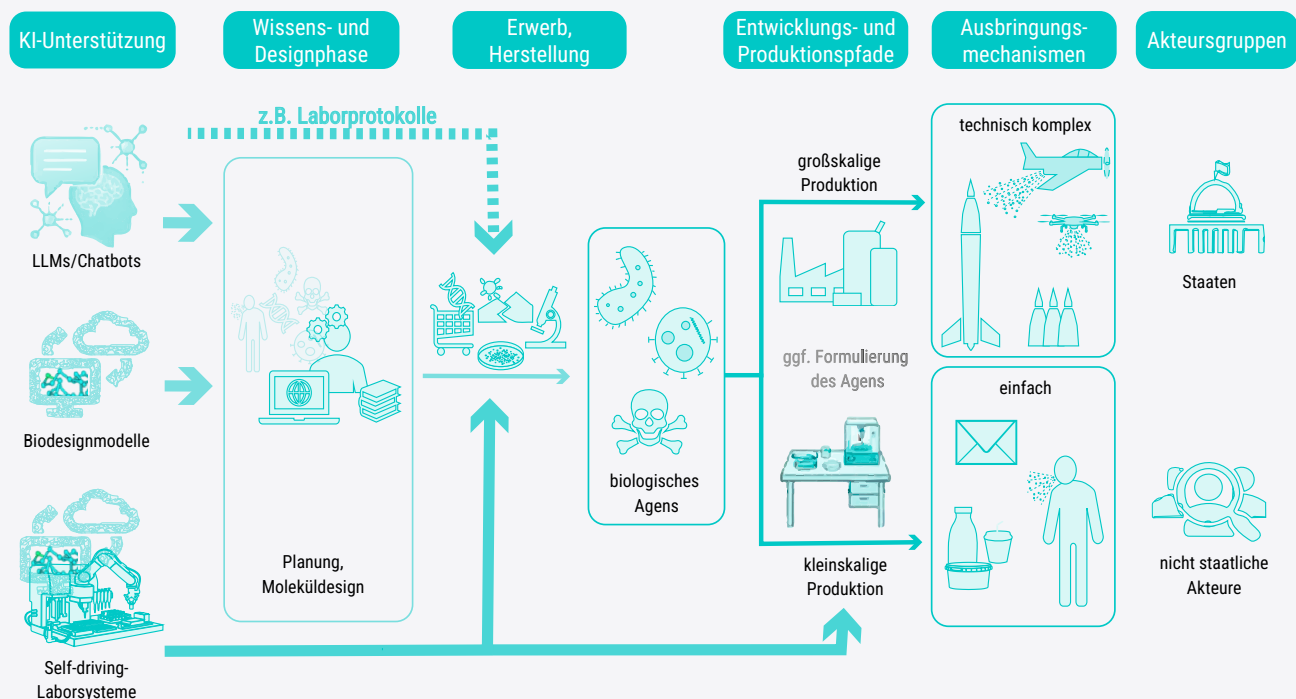
### Implikationen für Bedrohungen durch Biowaffen und Ausblick

Eine Einordnung der KIBio-Möglichkeiten hinsichtlich Missbrauchsrisiken durch Biowaffen erfordert letztlich eine Betrachtung, die über mögliche KI-Fähigkeiten hinausgeht.

Wichtig hierbei sind zum einen technologische Voraussetzungen zur Herstellung und Nutzung von Biowaffen im größeren Umfang. Diese sind weitgehend unabhängig von KI-Möglichkeiten, etwa die großtechnische Produktion von Erregern oder aufwendige Waffentechnik. Bedrohungen, die solche Prozesse und Fähigkeiten erfordern, dürften auch weiterhin vor allem von Staaten ausgehen (Abb. 2). Die neuen KIBio-Möglichkeiten könnten jedoch bei anderen Entwicklungsschritten staatlicher Biowaffenprogramme eine Rolle spielen.

Zum anderen müssen Faktoren betrachtet werden, welche die Intention und Strategien bestimmen, Biowaffen zu nutzen. Diese können vor allem bei nicht staatlichen Akteuren vielfältig sein. Aufgrund begrenzter technologischer

**Abbildung 2** Mögliche Risiken durch die Nutzung von KI-Systemen für die Herstellung gefährlicher biologischer Agenzien bzw. Biowaffen



Eigene Darstellung

Fähigkeiten könnten nicht staatliche Akteure auch zukünftig technisch eher wenig aufwendige Biowaffen nutzen, wie es bei früheren „erfolgreichen“ Bioterrorakten (vgl. Kasten, S. 2) der Fall war.

Bei solchen einfacheren Ansätzen könnte der Einsatz von KI-Tools zum Erwerb von Wissen über die Isolierung oder Herstellung biologischer Agenzien oder zur Umgestaltung von Gensequenzen, um Nukleinsäuresynthescreenings zu umgehen, zukünftig durchaus einen größeren Einfluss auf Fähigkeiten und Schadenspotenziale ausüben.

Sehr weitreichende Risikoszenarien, wie die Herstellung pandemischer Viren über synthetisch hergestellte Genome, erscheinen zumindest für Personen ohne wesentliche Laborerfahrung hingegen nach wie vor wenig wahrscheinlich.

Inwiefern sich dies zukünftig ändern könnte, ist nicht verlässlich abzuschätzen. Angesichts der möglichen Folgen und Unsicherheiten auch bzgl. anderer Akteure erscheinen aber ein kontinuierliches Monitoring der hochdynamischen KI-Entwicklungen sowie weitere vorsorgende Maßnahmen zur Risikominimierung bzw. zur Verbesserung der Resilienz gegenüber möglichen Folgen notwendig.

## Handlungsfelder und -optionen

Nicht zuletzt aufgrund der unterschiedlichen möglichen Akteure müssen vorsorgende Maßnahmen unterschiedliche Handlungsfelder adressieren. Vier Hauptansatzpunkte lassen sich erkennen:

### Überwachung der Schnittstelle zwischen KI-generierten digitalen Entwürfen und realen biologischen Molekülen oder Systemen

Zentral hierfür könnte die Unterstützung des geplanten Europäischen Biotech Act sein, um eine verpflichtende und EU-weit harmonisierte Sicherheitsüberprüfung für Nukleinsäuresynthesen und deren Kunden zu ermöglichen. Zudem könnten Auflagen für die Verwendung von Forschungsfördergeldern eingeführt werden, wonach Nukleinsäuresynthesen nur von Herstellern bezogen werden dürfen, die entsprechende Sicherheitsüberprüfungen durchführen.

### Beobachtung und Kontrolle von KI-Systemen mit gesteigerten Möglichkeiten zur Entwicklung gefährlicher biologischer Agenzien

Dazu könnten Auflagen (z. B. für Entwickler) zur Implementierung von Maßnahmen in Betracht gezogen werden, die den kontrollierten Zugang zu leistungsfähigen Biodesignmodellen oder zu

bestimmten Datensätzen für deren Entwicklung sicherstellen. Diese Option müsste jedoch sehr sorgfältig gegen mögliche negative Auswirkungen abgewogen werden, etwa hinsichtlich der biomedizinischen Forschung im Allgemeinen sowie der Entwicklung von Gegenmaßnahmen im Krisenfall im Besonderen. Zu dieser Abwägung könnte ein Beratungsgremium aus Expert/innen verschiedener Disziplinen und Bereichen beitragen. Ein solches Gremium könnte auch Teil einer Wenn-dann-Strategie sein, die auf eine kontinuierliche Bewertung der dynamischen Entwicklungen sowie eine regelmäßige Neubewertung von Risiken und die Anpassung von Maßnahmen abzielt. Entsprechend den Ergebnissen würden neue Risikobewertungen durchgeführt und gegebenenfalls Maßnahmen zur Risikominimierung verschärft oder gelockert.

### Stärkung der Biowaffenkonvention durch die (weitere) inhaltliche Unterstützung der dazu eingesetzten Arbeitsgruppe bei der BWC

Dabei könnten im Vergleich zu klassischen Verifikationsregimen (mit kurzfristigen Überprüfungen verdächtiger Einrichtungen) weniger intrusive und potenziell einfacher erreichbare Modelle angestrebt werden, die strukturierte Selbstauskünfte oder Peer-Review-Besuche vor Ort umfassen könnten. Zudem könnten Initiativen zur Verbesserung der Finanzierungssituation der BWC angestoßen oder unterstützt werden.

### Ausbau der Fähigkeiten zur Durchführung von Vorsorge- und Gegenmaßnahmen

Hierzu könnten Möglichkeiten zur Stärkung von Aktivitäten und Kapazitäten insbesondere in zwei Bereichen geprüft werden:

- In der anwendungsorientierten Biodefense-Forschung könnten KI-Möglichkeiten zur Früherkennung von Erregern sowie zur Entwicklung schnell skalierbarer medizinischer Gegenmaßnahmen (wie Impfstoffen) beitragen.
- Zur Terrorismusabwehr könnte die Zusammenarbeit mit Unternehmen, die KI entwickeln, gefördert bzw. deren Sicherheitsmaßnahmen unterstützt werden. Dazu könnte die Überwachung besorgniserregender Kommunikation mit großen generativen KI-Modellen (Chatbots) gehören, die vermuten lässt, dass Nutzer/innen anderen Schaden zufügen wollen.

## TAB-Arbeitsbericht Nr. 217



**Biotechnologie und künstliche Intelligenz:  
Risiken der Forschung für die Sicherheit sowie  
die Proliferation von Biowaffen**  
Harald König unter Mitarbeit von Arnold Sauter

**Projektinformationen**  
[www.tab-beim-bundestag.de/KIxBio](http://www.tab-beim-bundestag.de/KIxBio)

**Herausgeber**  
Büro für Technikfolgen-Abschätzung  
beim Deutschen Bundestag (TAB)

**Bildnachweis**  
KI-generierte Darstellung/TAB (S.1)

ISSN: 2364-2629  
DOI: 10.5445/IR/1000196056