



Biotechnologie und künstliche Intelligenz

Risiken der Forschung für die Sicherheit
sowie die Proliferation von Biowaffen

Harald König

unter Mitarbeit von
Arnold Sauter

Juli 2026
Arbeitsbericht Nr. 217

Inhalt

Zusammenfassung	5
1 Einleitung	20
2 Molekularbiologische und biotechnologische Entwicklungen und deren Zusammenspiel mit künstlicher Intelligenz	24
2.1 Biologie wird Technologie: methodische Fortschritte, um biologische Systeme zu verstehen und zu gestalten	25
2.2 Zunehmend große biologische Datensätze haben Molekularbiologie und Biotechnologie für KI zugänglich gemacht	28
2.3 KI-Modelle haben bereits eine Reihe neuer Entwicklungen mit großem Potenzial für die Forschung und Anwendung ermöglicht	31
2.3.1 Grundlagenforschung	33
2.3.2 Entwicklung von Medikamenten	36
2.3.3 Diagnose und Überwachung von Krankheiten bzw. Krankheitserregern	39
2.3.4 Industrielle Biotechnologie	40
2.3.5 Ansätze für automatisierte Labore und Experimente	42
3 Mögliche Risiken für die Biosicherheit und Proliferation biologischer Waffen durch das Zusammenspiel von KI und molekularbiologischer bzw. biotechnologischer Entwicklungen	46
3.1 Die Synthetische Biologie ist seit ihren Anfängen von Diskussionen zur Biosicherheit begleitet worden – einschließlich der möglichen Herstellung von Biowaffen	47
3.2 Das Zusammenspiel von KI mit molekularer Biologie und Biotechnologie hat zu einer neuen Diskussion über Biosecurity-Risiken und Biowaffen geführt	53
3.2.1 Zentrale Punkte der neuen Sicherheitsdebatte	54
3.2.2 Die neue alte Frage nach den Hürden für die Herstellung von Biowaffen: die Notwendigkeit von speziellem (Erfahrungs-)Wissen und Fähigkeiten	54
3.3 Potenzielle neue oder erleichterte Möglichkeiten des Missbrauchs von Biotechnologie durch KI: Worauf begründen sich die vorgebrachten Befürchtungen?	66
3.3.1 Wissensaneignung oder -erweiterung über große Sprachmodelle	66
3.3.2 Veränderte oder neue Toxine und Krankheitserreger mithilfe von biologischen KI- bzw. Bidesignmodellen	82
3.3.3 Die Kombination von KI-Modellen mit automatisierten Laborplattformen	88

3.4	Implikationen der neuen technischen Möglichkeiten für Bedrohungen durch Biowaffen	92
4	Gegenwärtige Regulierungen und Maßnahmen zur Kontrolle von Biowaffen und sicherheitsrelevanter Dual-Use-Forschung	97
4.1	Regelungen und Übereinkommen auf internationaler Ebene	98
4.1.1	Rechtlich bindende Übereinkommen und Regelungen zu Biowaffen	98
4.1.2	Weitere Übereinkommen und Mechanismen mit Relevanz für Biosecurity-Risiken oder die Proliferation von biologischen Waffen	104
4.2	Der Rechtsrahmen auf Ebene der EU	106
4.3	Internationale und europäische Initiativen und Leitlinien, die sich mit Biosicherheit bzw. der Verhinderung der Proliferation von Massenvernichtungswaffen befassen	110
4.4	Regelungen und Mechanismen in Deutschland zur Kontrolle von Biowaffen und für Biosecurity-relevante Forschung	114
4.4.1	Gesetzliche Regelungen zur Umsetzung internationaler Verpflichtungen zur Kontrolle von Biowaffen	114
4.4.2	Gesetzliche Regelungen für Biosecurity-relevante Forschung	117
4.4.3	Nicht gesetzliche Regelungen und Verhaltenskodizes für sicherheitsrelevante biologische Forschung	118
4.4.4	Initiativen zur Stärkung von Biosecurity und der Nichtproliferation biologischer Waffen	120
4.5	Vergleichende Perspektive auf Biosecurity-Regulierungen anderer Länder	121
4.6	Regulierungen und Initiativen zu KI und Bezüge zu Biosicherheit und Biowaffen	125
4.6.1	Rechtliche Regelungen und Standards in wichtigen KI-entwickelnden Ländern oder Märkten für KI-Anwendungen	125
4.6.2	Internationale Regelungen und Initiativen	131
4.7	Die Debatte um mögliche Lücken in – und der notwendigen Stärkung von – Regelungen und Mechanismen zur Kontrolle von Biosecurity-Risiken und der Proliferation von Biowaffen	134
4.7.1	Die BWC (und die Kontrolle von Staaten)	134
4.7.2	Exportkontrollen	135
4.7.3	Die Sicherung der Schnittstelle zwischen KI-Modellen und physikalisch-biologischen Systemen	137
4.7.4	Schutzmechanismen für KI-basierte biologische Modelle und die Kontrolle biologischer Daten	141
4.7.5	Nutzung von KI-Modellen zur Verbesserung der Pandemievorsorge und biologischer Verteidigungsfähigkeiten	144

5	Resümee und Handlungsoptionen	145
5.1	Resümee	146
5.2	Handlungsoptionen	152
6	Literatur	156
6.1	In Auftrag gegebene Gutachten	157
6.2	Weitere Literatur	157
7	Anhang	195
7.1	Abbildungen	196
7.2	Tabellen	196
7.3	Kästen	196
7.4	Abkürzungen	197
7.5	Glossar	197

Zusammenfassung



Zusammenfassung

Die rasanten Entwicklungen bei der Analyse und Synthese von Erbgut sowie zur gezielten Veränderung von Genen in verschiedensten Organismen durch Genomeditierungsverfahren haben die Erforschung und Veränderung biologischer Systeme bzw. Organismen in den letzten 10 bis 15 Jahren zum Teil erheblich vereinfacht und die Möglichkeiten in diesem Bereich stark erweitert. Ein dabei zunehmend wichtiges Werkzeug sind computergestützte Analyse- und Designprozesse. Diese unter den Begriffen Synthetische Biologie oder „engineering biology“ zusammengefassten Entwicklungen der Molekularbiologie und Biotechnologie haben nicht nur in der Grundlagenforschung zu neuen Möglichkeiten geführt, etwa bei der Erforschung von Gen- und Molekülfunktionen sowie von Krankheitsursachen. Sie haben auch in Anwendungsfeldern wie der industriellen Biotechnologie, etwa zur Generierung neuer Synthesewege für Chemikalien in Mikroorganismen, sowie bei der Entwicklung neuer Medikamente und Behandlungsmöglichkeiten – darunter Gentherapien für bisher unheilbare Krankheiten sowie gen- und zellbasierte Krebsimmuntherapien – bereits revolutionäre Entwicklungen eingeleitet.

Die Fortschritte in der Molekularbiologie und Biotechnologie konvergieren zunehmend mit jüngeren Entwicklungen in den Bereichen der künstlichen Intelligenz (KI) und der Automatisierung von Laborprozessen. Ermöglicht durch große Datensätze zu biologischen Molekülen und deren Funktionen, haben sowohl akademische Forschungseinrichtungen als auch Biotech- und andere Technologieunternehmen zunehmend leistungsfähigere KI-Modelle für die Analyse und das Design von biologischen Molekülen und Prozessen entwickelt. Hierzu gehören insbesondere Modelle zur Vorhersage der Funktion von Genomabschnitten, zur Struktur- und Funktionsvorhersage von Proteinen basierend auf Gen- bzw. Aminosäuresequenzen sowie zum Design von Proteinen mit gewünschten Eigenschaften.

Solche KI-basierten Modelle werden bereits für verschiedene Fragestellungen eingesetzt, von der Grundlagenforschung – etwa um molekulare und zelluläre Prozesse sowie Ursachen verschiedener Krankheiten zu verstehen – bis hin zu einer Reihe von Anwendungen in der Biotechnologie und Medizin. Dazu zählen die Identifizierung von Zielmolekülen für Medikamente oder das Design möglichst geeigneter Kandidatenmoleküle für Wirkstoffe, die Diagnose und Überwachung von Krankheiten bzw. Krankheitserregern sowie die Um- oder Neugestaltung von Stoffwechselwegen und Enzymen in Mikroorganismen, um Chemikalien oder nachhaltigere Treibstoffe herzustellen. Insbesondere für solche biotechnologischen Anwendungen werden KI-Modelle auch mit robotisierten Laborplattformen zu ersten Self-driving-Laborsystemen integriert, die etwa autonome Entwicklungszyklen zur Herstellung von Enzymen mit verbesserten oder neuen Eigenschaften ermöglichen können.

Das Zusammenspiel von Biotechnologie mit KI hat zu einer neuen Sicherheitsdebatte geführt

Die Synthetische Biologie und ihre Anwendungsmöglichkeiten sind seit ihren Anfängen von Diskussionen über Risiken durch mögliche (Labor-)Unfälle (Biosafety) oder eine missbräuchliche Verwendung (Biosecurity) begleitet worden – zwei Bereiche, die im deutschen Sprachgebrauch

meist unter dem Überbegriff Biosicherheit gefasst werden. Insbesondere wurde dabei die erleichterte Zugänglichkeit der technologischen Entwicklungen (wie DNA-Synthese oder Genomeditierung) zur Veränderung von Molekülen oder Organismen auch für Nichtexpert/innen oder aber fachkundige Personen, die nicht in etablierte wissenschaftliche Einrichtungen eingebunden sind, thematisiert. Mit der zunehmend wichtigeren Rolle von KI und deren Zusammenspiel mit biotechnologischen Methoden (KlxBio) haben sich diese Diskussionen intensiviert. Vor allem international hat sich in den letzten Jahren eine Sicherheitsdebatte entwickelt, die sich stark auf Missbrauchsrisiken durch die mögliche Herstellung biologischer Waffen sowie die damit verbundenen Sicherheitsfragen fokussiert.

Biologische Waffen (kurz Biowaffen) verbreiten Krankheitserreger oder Toxine, um Menschen, Tiere oder Pflanzen zu schädigen oder zu töten. Sie bestehen typischerweise aus einem biologischen Agens (z. B. ein Virus oder ein Bakterium) und einem Mechanismus zu dessen Ausbringung. Die Entwicklung von Biowaffen, insbesondere für Waffensysteme zur großflächigen Ausbringung und/oder zum Einsatz über große Entfernungen, wie sie in staatlichen Waffenprogrammen entwickelt wurden (z. B. ballistische Raketen bzw. Sprengköpfe, an Flugzeuge montierte geeignete Sprühvorrichtungen), erfordert eine Reihe spezieller und zum Teil aufwendiger Schritte. Für diese Schritte sind spezifisches Wissen und Fähigkeiten erforderlich. Allerdings sind nicht notwendigerweise alle diese Schritte – zumindest nicht in demselben Maß – für die Herstellung biologischer Waffen bzw. die missbräuchliche Nutzung von biologischen Agenzien erforderlich. Dies ist beispielsweise der Fall, wenn die Ausbringung kleiner Mengen an Agenzien ausreicht und/oder über einfache nichttechnische Mechanismen erfolgen kann.

Im Mittelpunkt der neuen Sicherheitsdebatte um KlxBio stehen im Wesentlichen folgende Bedenken:

- dass die KlxBio-Möglichkeiten es insbesondere Nichtexpert/innen bzw. nicht staatlichen Akteuren erleichtern könnten, gefährliche biologische Agenzien herzustellen und so die Hürden für die Herstellung von Biowaffen entscheidend gesenkt werden könnten;
- dass die Entwicklung noch gefährlicherer bzw. neuer solcher Agenzien und Biowaffen möglich wird, die das Schadenspotenzial oder -ausmaß erhöhen könnten, und
- dass die Wirksamkeit von Biosicherheits- und Abwehrmaßnahmen (Biodefense) verringert oder unterlaufen werden könnte.

Das TAB-Projekt

Das TAB wurde auf Initiative des Verteidigungsausschusses durch den damaligen Ausschuss für Bildung, Forschung und Technikfolgenabschätzung des Deutschen Bundestages beauftragt, im Rahmen eines Technikfolgenabschätzungsprojekts zum einen mögliche Sicherheitsrisiken neuerer biotechnologischer Entwicklungen und ihre Wechselwirkungen mit Entwicklungen im Bereich der KI möglichst breit zu analysieren. Zum anderen sollten die gegenwärtigen Kontroll- und Regulierungsmöglichkeiten dargestellt und Möglichkeiten zu deren Weiterentwicklung diskutiert werden, um diese Sicherheitsrisiken zu minimieren und die Nichtverbreitung potenzieller Biowaffen zu stärken.

Mögliche Risiken durch das Zusammenspiel von KI und molekularbiologischer bzw. biotechnologischer Entwicklungen

Die der neuen Sicherheitsdebatte zugrunde liegenden Bedenken um Biosecurity-Risiken beruhen im Wesentlichen auf drei Entwicklungen bei KI-Modellen und den damit verbundenen Möglichkeiten in der molekularbiologischen Forschung bzw. der Biotechnologie:

1. der möglichen Wissensaneignung oder -erweiterung über große Sprachmodelle (LLMs, LLM-Chatbots);
2. der Möglichkeit zum Design veränderter oder neuer Toxine und Krankheitserreger mithilfe biologischer KI-Modelle, die unter anderem das Sicherheitsscreening bei Nukleinsäuresynthesen und Detektionsverfahren für bekannte Toxine und Erreger unterlaufen könnten;
3. der Kombination von KI-Modellen mit robotisierten Laborplattformen, um Experimente bzw. Entwicklungszyklen und Herstellungsprozesse automatisiert oder gar komplett autonom durchführen lassen zu können.

Ergebnisse empirischer Studien lassen die Frage offen, inwieweit LLMs Personen bei der Herstellung von Biowaffen in der Praxis tatsächlich effektiver unterstützen können als konventionelle Internetwerkzeuge

Verschiedene Akteure (z. B. aus akademischen Forschungsinstituten, Non-Profit-Organisationen oder KI-entwickelnden Firmen) haben in einer Reihe von empirischen Studien bzw. Evaluationen von KI-Modellen untersucht, inwieweit große Sprachmodelle relevantes Wissen, das für die Herstellung von Biowaffen relevant ist, für verschiedene Personengruppen verfügbar machen oder erweitern könnten. Dies umfasst auch nicht ohne Weiteres zugängliches oder praxisrelevantes (Erfahrungs-)Wissen.

Zwar legen (meist automatisierte) Tests zur Ermittlung von Leistungskennzahlen zum Wissensstand bzw. den Fähigkeiten eines Modells (Benchmarks) nahe, dass verschiedene LLMs Referenzwerte menschlicher Expert/innen erreichen und teilweise deutlich übertreffen. Inwieweit diese Tests jedoch die Möglichkeit abbilden, in der Praxis tatsächlich relevantes (Erfahrungs-) Wissen zur Herstellung und dem Einsatz von Biowaffen zu erlangen, bleibt unklar. Ergebnisse bisheriger Uplift- und Red-Teaming-Studien mit Personen, um herauszufinden, inwieweit LLMs (über konventionelle Internetsuchen hinaus) bei der Planung eines Angriffs und der Herstellung von Biowaffen helfen und die Kenntnisse bzw. Fähigkeiten der Personen verbessern können, zeigen kein einheitliches Bild und sind kaum unabhängig überprüfbar. Hierzu trägt insbesondere bei, dass die in den Untersuchungen an Personen gestellten Aufgaben, die Originaldaten zu den Ergebnissen oder auch die Expertise der bewertenden Expert/innen (meist mit Verweis auf mögliche Sicherheitsrisiken) oft nicht oder nur unzureichend offengelegt werden. Während verschiedene größere Studien keine statistisch signifikanten Leistungsverbesserungen von Anfänger/innen oder Expert/innen durch den Zugang zu LLMs zeigten, legt eine jüngere Studie nahe, dass die koordinierte Nutzung mehrerer LLMs die Leistungen von Studierenden ohne oder mit wenig Biologieerfahrung bei der Lösung verschiedener, aus Benchmarks stammender Fragen und Aufgaben zu biologischem Wissen oder Techniken deutlich verbessern kann, teilweise auf das Niveau von Expert/innen oder sogar darüber hinaus.

Doch selbst wenn solche Uplift- oder Red-Teaming-Studien zukünftig aufgrund leistungsfähigerer Modelle einheitliche, statistisch signifikante Verbesserungen des Wissensstands zeigen würden, bliebe die praktische Signifikanz solcher Ergebnisse für die Umsetzung des gewonnenen Wissens und der entwickelten Pläne in der realen Welt unklar. Entscheidend dafür wären Auswirkungen auf die Überwindung verschiedener Hürden für die Biowaffenherstellung, einschließlich der Erlangung der notwendigen praktischen Fähigkeiten für Laborarbeiten zur tatsächlichen Herstellung relevanter biologischer Agenzien und zur Durchführung weiterer biowaffenrelevanter Prozessschritte. Letztere umfassen etwa die Formulierung oder Modifikation der Agenzien, z. B. um diese zu stabilisieren oder effektiv ausbringen zu können.

Größere kontrollierte Studien mit Testpersonen in realen biologischen Laboren könnten belastbarere Rückschlüsse auf mögliche Risiken zulassen, allerdings abhängig davon, wie konkret oder relevant die biologischen Aufgaben (angesichts immer zu berücksichtigender Sicherheitsfragen bzw. -vorschriften) hinsichtlich potenzieller Biowaffen gestaltet werden können. Solch eine erste größere Studie legt nahe, dass LLMs Personen ohne wesentliche Laborerfahrung derzeit nicht besser bei der erfolgreichen Durchführung einiger grundlegender molekularbiologischer Aufgaben, wie sie in der Virologie und Molekularbiologie erforderlich sind, unterstützen können, als dies mit konventionellen Internetanwendungen zur Informationsbeschaffung möglich ist. Ob bzw. inwiefern die zusätzliche Nutzung vorhandener und zukünftiger biologiespezifischer KI-Modelle dies ändern könnte und ob die Nutzung von LLMs durch Personengruppen mit relevanten Kenntnissen in den Lebenswissenschaften und Laborerfahrung (z.B. auf Graduierten- oder Doktorandenniveau) zu deutlich größeren bzw. besorgniserregenderen Leistungssteigerungen führen könnte, ist derzeit noch offen. Dies dürfte weitere Studien dieser Art, möglicherweise in regelmäßigen Abständen, erfordern.

Proteindesignmodelle könnten die unerkannte Herstellung von Gensequenzen mit Missbrauchspotenzial erlauben

KI-unterstützte Proteindesignmodelle haben in einer Reihe von Fällen die gezielte Neu- oder Umgestaltung von komplexen Proteinstrukturen mit unterschiedlichen Funktionen ermöglicht. Somit könnten prinzipiell auch (Protein-)Toxine mit neuen, gefährlicheren Eigenschaften erzeugt werden. Die tatsächliche Funktionalität solch denkbarer neuartiger Proteine müsste aber auf absehbare Zeit in ressourcen- und zeitaufwendigen Laborexperimenten überprüft und gegebenenfalls über iterative Entwicklungszyklen (DBTL-Zyklen) optimiert werden. Darüber hinaus müsste die Entwicklung neuer Toxine auch Tests in Zell- oder Gewebekulturen und mit Versuchstieren umfassen.

Bereits gezeigt wurde, dass bekannte Proteine mit aktuellen Proteindesignmodellen so umgestaltet werden können, dass sie mutmaßlich ihre Funktion behalten und aufgrund größerer Unterschiede zur Originalversion in der Aminosäure- und damit auch der Gensequenz standardmäßige Sequenzüberprüfungen bei Nukleinsäuresynthesen umgehen können. Wie groß die Gefahr tatsächlich ist, dass so umgestaltete Versionen bekannter Proteine oder einschlägiger Biowaffentoxine – die für ihre Aktivität multiple Funktionalitäten (darunter Enzymaktivität) benötigen – tatsächlich funktionell bleiben, ist derzeit aber unklar. Experimentelle Daten legen nahe, dass zumindest über derzeitige Open-Source-Modelle entworfene entsprechende Proteinversionen, insbesondere von größeren Proteinen und Enzymen, ihre Funktion verlieren.

Eine gezielte Verbesserung komplexer Eigenschaften von Krankheitserregern ist fraglich – das Design völlig neuer Erreger scheint (zumindest derzeit) außerhalb der Reichweite von KI-Modellen

Ob sich über KI-Modelle komplexe Eigenschaften von Krankheitserregern – wie die Übertragbarkeit, die Fähigkeit, sich in Wirtszellen effizient zu vermehren, oder die Umgehung von Immunreaktionen des Wirts – tatsächlich in vorhersagbarer Weise verändern lassen und für die Nutzung als Biowaffe verbessert werden können, ist nicht geklärt. Es gibt zwar Untersuchungen mit verschiedenen biologischen KI-Modellen zu Viren, die zeigen, dass Vorhersagen zu kurzzeitigen Auswirkungen von Mutationen in Gensequenzen (etwa von SARS-CoV-2 oder Influenzaviren) auf die Infektiosität oder die Umgehung bestimmter Immunreaktionen möglich sind. Die Möglichkeiten, längerfristige Auswirkungen von Mutationen bzw. die Virusevolution über mehrere Infektionszyklen hinweg vorherzusagen, wie es für eine effektive Verbesserung solcher Eigenschaften notwendig wäre, dürften allerdings auch zukünftig eher begrenzt sein. Zu den Gründen gehören ein Mangel an umfangreichen, gut charakterisierten Datensätzen zur Evolution der Viren und ihrer Proteine sowie von Datensätzen, die virale Mutationen mit dem genetischen Hintergrund des Wirts (z. B. der genetischen Variabilität in zentralen Genen der Immunantwort) verknüpfen. Hinzu kommen sprunghafte evolutionäre Ereignisse, die zu komplexen genetischen Veränderungen führen können.

Die Entwicklung völlig neuer Krankheitserreger könnte potenziell die weitreichendsten Folgen in Bezug auf biologische Bedrohungen haben, da Möglichkeiten zu ihrer Bekämpfung aufgrund fehlender Informationen eingeschränkt wären bzw. die Entwicklung von Maßnahmen längere Zeit in Anspruch nehmen könnte. Allerdings fehlen hierzu bislang die erforderlichen umfangreichen und hochwertigen Datensätze zu genomischen Sequenzen und den damit verbundenen molekularen und physiologischen Eigenschaften selbst bei vergleichsweise wenig komplexen Erregern wie Viren. Um relevante Eigenschaften wie Übertragbarkeit und Virulenz zu konstruieren und zu kombinieren, müssen auch die zugrunde liegenden, komplexen Netzwerkinteraktionen mit verschiedenen Komponenten der Wirtsorganismen verstanden bzw. modelliert werden.

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

Die Verwirklichung jeglicher Entwürfe für potenzielle um- oder neugestaltete biologische Agenzien, wie Toxine oder Viren, erfordert die Herstellung und – zumindest derzeit – die experimentelle Validierung der Wirksamkeit der Agenzien im Labor. Gegebenenfalls sind wiederholte Entwicklungszyklen zur Optimierung der Entwürfe notwendig. In diesem Zusammenhang wirft die mögliche Nutzung kommerzieller automatisierter Laborplattformen (Cloud Labs), auf die Forschende über Internetoberflächen zugreifen können – sowie die Kombination von KI-Systemen mit solchen Laborplattformen, um erste autonome („self-driving“) Laborsysteme für Design- und Entwicklungszyklen (z. B. für Enzyme) zu erhalten, Biosecurity-Fragen auf. Insbesondere stellt sich die Frage, ob oder inwieweit solche Einrichtungen oder Systeme böswilligen Akteuren, denen praktische Fähigkeiten und Laborausrüstung fehlen, in relevantem Umfang bei der Herstellung, Validierung oder Durchführung iterativer Entwicklungszyklen helfen könnten.

Cloud Labs und ähnliche Einrichtungen können bereits heute die Notwendigkeit aufheben, (zumindest manche) praktische Laborarbeiten zur Herstellung biologischer Agenzien selbst durch-

führen zu müssen. Für den effektiven Einsatz solcher Labore ist zwar noch spezifisches Wissen zu den verwendeten Agenzien und methodischen Verfahren sowie zu Cloud-Lab-Abläufen selbst notwendig. Es ist allerdings nicht auszuschließen, dass diese Anforderungen, beispielsweise durch eine über KI-Systeme erleichterte Planung bzw. Programmierung von Experimenten und/oder zuverlässigere Automatisierungssysteme, in Zukunft weiter abnehmen könnten.

Würden autonome Laborsysteme für die Herstellung bzw. Veränderung relevanter biologischer Agenzien, wie bestimmter Toxine oder Viren, zur Verfügung stehen und wären diese (unkontrolliert) zugänglich, könnte dies die Hürden für die Herstellung bzw. Entwicklung solcher Agenzien auch für Akteure ohne biologische Fachkenntnisse oder größere Ressourcen erheblich senken. Besonders besorgniserregend wären entsprechende Systeme, wenn sie etwa über sprachgesteuerte Benutzeroberflächen auch von Personen ohne spezielle (Programmier-)Kenntnisse nutzbar wären, wie es bei mindestens einem publizierten System für die Veränderung von Enzymen realisiert wurde. Die Entwicklung autonomer Laborsysteme ist jedoch kosten- und forschungsintensiv. Der spezifische Zuschnitt auf die jeweiligen Proteine oder spezielle Organismen erfordert zusätzlich zu spezifischen Kenntnissen über die zu verändernden biologischen Systeme erhebliche Fachkenntnisse im Bereich der Robotik sowie der Soft- und Hardwareintegration. Somit dürfte die Entwicklung solcher Systeme zur Herstellung gefährlicher biologischer Agenzien zumindest derzeit primär eine Möglichkeit für staatliche Akteure oder staatlich unterstützte Gruppen sein.

Regulierungen und Mechanismen zur Kontrolle von Biosecurity-Risiken und der Proliferation von Biowaffen

Derzeit wird allgemein anerkannt, dass das Verbot des Einsatzes biologischer Waffen im Allgemeinen und insbesondere während bewaffneter Konflikte dem Völkergewohnheitsrecht entspricht. Ihr Einsatz ist völkerrechtlich geächtet. Eine zentrale Grundlage hierfür sind internationale vertragliche Übereinkünfte in Bezug auf Biowaffen und deren Einsatz.

Übereinkommen und Mechanismen auf internationaler und europäischer Ebene

Zu den rechtlich bindenden internationalen Übereinkommen gehört insbesondere die Biowaffenkonvention (Biological Weapons Convention – BWC), die 1975 in Kraft trat und derzeit 189 Staaten als Vertragsparteien hat. Das Übereinkommen verbietet gemäß Artikel I die Entwicklung, Herstellung, Lagerung, den Erwerb oder die Weitergabe von mikrobiellen oder anderen biologischen Agenzien sowie von Toxinen in Arten und Mengen, die für Schutzzwecke oder friedliche Zwecke nicht gerechtfertigt sind. Zwar verbietet die BWC die Verwendung biologischer Waffen nicht ausdrücklich, jedoch wurde in einer der Vertragsüberprüfungskonferenzen bekräftigt, dass ihre Verwendung durch Vertragsparteien, die nicht mit prophylaktischen, schützenden oder anderen friedlichen Zwecken vereinbar ist, einen Verstoß gegen Artikel I des Übereinkommens darstellt. Darüber hinaus fordert die BWC von den Vertragsparteien Maßnahmen, einschließlich rechtlicher Bestimmungen, um das Verbot durchzusetzen.

Ein internationales Rechtsinstrument, das im Gegensatz zur BWC – die primär die Aktivitäten von Staaten regelt – auf die Bedrohung durch nicht staatliche Akteure abzielt, ist die Resolution 1540 (2004) des UN-Sicherheitsrates. Sie verpflichtet Staaten, jede Form von Unterstützung für nicht staatliche Akteure zu unterlassen, die versuchen, nukleare, chemische oder biologische Waffen

zu erhalten oder einzusetzen. Hierfür müssen wirksame Gesetze erlassen und durchgesetzt werden, die mit den jeweiligen nationalen Verfahren im Einklang stehen. Ähnliche verbindliche Verpflichtungen in Bezug auf biologische (und chemische) Waffen enthält die Richtlinie (EU) 2017/541 von 2017 zur Bekämpfung des Terrorismus. Sie zielt primär darauf ab, den Anwendungsbereich des Strafrechts der Mitgliedstaaten auf terrorismusbezogene Bedrohungen und Aktivitäten innerhalb der EU auszuweiten.

Weitere Übereinkommen und Mechanismen mit Relevanz für Biosecurity-Risiken und die Proliferation von biologischen Waffen sind Exportkontrollregime, die die internationale Verbreitung sensibler Güter kontrollieren sollen. Hierzu gehören auf internationaler Ebene die rechtlich nicht verpflichtenden Vereinbarungen insbesondere der Australia Group, einem multilateralen Forum, über das zahlreiche Staaten ihre Exportkontrollen für sensible Güter bzw. Güter mit doppeltem Verwendungszweck (Dual Use) im Zusammenhang mit biologischen und chemischen Waffen koordinieren. Die Mechanismen der Gruppe umfassen gemeinsame Kontrolllisten für entsprechende Güter (darunter biologische Agenzien wie bestimmte Viren und Bakterien), Leitlinien für die Industrie sowie Regelungen zum Informationsaustausch und zur Harmonisierung bereits getroffener Maßnahmen.

In der EU ist die Verordnung (EU) 2021/821 die wichtigste Verordnung im Zusammenhang mit der Verbreitung biologischer (und chemischer) Waffen. Sie referenziert die Ausfuhrkontrolllisten der Australia Group und setzt damit deren rechtlich nicht bindende Vereinbarungen in rechtsverbindliche Normen um, die in allen EU-Mitgliedstaaten unmittelbar gelten.

Darüber hinaus existiert eine Reihe internationaler und europäischer Initiativen bzw. Leitlinien, die sich mit Fragen der Biosecurity bzw. der Verhinderung der Proliferation von Massenvernichtungswaffen befassen. Dazu gehören die Leitlinien zur Biosicherheit der World Health Organization (WHO/Weltgesundheitsorganisation), die Standards und Praktiken des International Gene Synthesis Consortium (IGSC) zur Überprüfung von Bestellungen synthetischer Nukleinsäuresequenzen sowie die EU Centres of Excellence on Chemical, Biological, Radiological and Nuclear Risk Mitigation, die global eine Vielzahl von Unterstützungsmaßnahmen zur Minderung von CBRN-Risiken bereitstellen, darunter Bedarfs- und Risikobewertungen, nationale und regionale Aktionspläne sowie Feldübungen.

Regelungen und Mechanismen in Deutschland zur Kontrolle von Biowaffen und Biosecurity-relevanter Forschung

Die Kontrolle von Biowaffen erfolgt auf nationaler Ebene durch die Umsetzung rechtlicher Verpflichtungen aus internationalen Verträgen sowie durch Rechtsvorschriften der EU. Diese Verpflichtungen betreffen zum einen das Erlassen strafrechtlicher Bestimmungen, wie durch die BWC gefordert, welche die Entwicklung, Herstellung, Lagerung oder den Erwerb biologischer Waffen verbieten. Zum anderen müssen Ein- und Ausfuhrkontrollen für Materialien (z. B. entsprechend EU-Verordnungen und Richtlinien) etabliert werden, die zur Herstellung biologischer Waffen verwendet werden können. Gesetze und Verordnungen, die diese Verpflichtungen in Deutschland umsetzen, umfassen das Gesetz zur Biowaffenkonvention, das Völkerstrafgesetzbuch, das Kriegswaffenkontrollgesetz sowie das Außenwirtschaftsgesetz und die Außenwirtschaftsverordnung.

Biosecurity-relevante Forschung wird durch verschiedene sektorspezifische Gesetze erfasst, die in erster Linie Biosafety-Sicherheitsvorschriften betreffen. Dennoch tragen einige dieser Regeln

gen zumindest mittelbar auch zur Erhöhung der Biosecurity bei, etwa durch die Erlaubnis- und Anzeigepflicht für Personen, die mit bestimmten Krankheitserregern arbeiten, Aufzeichnungspflichten zu durchgeführten Arbeiten oder Sicherheitsüberprüfungen und Beschränkungen von Personen beim Zugang zu gefährlichen biologischen Agenzien bzw. bestimmten Einrichtungen. Zu diesen gesetzlichen Regelungen gehören etwa die Biostoffverordnung, das Gentechnikgesetz, das Infektionsschutzgesetz und das Sicherheitsüberprüfungsgesetz. In Bezug auf Forschung mit doppeltem Verwendungszweck – insbesondere für besorgniserregende Forschung („dual use research of concern“ – DURC) – existieren neben Vorgaben von Förderorganisationen für staatlich geförderte Forschungslinien vor allem Verhaltenskodizes bzw. Empfehlungen und Leitlinien von öffentlichen Forschungsorganisationen.

Die Debatte um mögliche Lücken in und der notwendigen Stärkung von Regelungen und Mechanismen zur Kontrolle von Biosecurity-Risiken und der Proliferation von Biowaffen

Neben der Durchsetzung von allgemeinen Vereinbarungen, um die Entwicklung und Proliferation von biologischen Waffen zu verhindern, wie insbesondere die BWC, werden speziell im Zusammenhang mit den KIxBio-Entwicklungen vor allem Möglichkeiten zur Kontrolle der Umsetzung von KI-basierten digitalen Entwürfen in physikalisch-biologische Moleküle sowie die Etablierung von Schutz- und Kontrollmechanismen für KI-Modelle und relevante biologische Daten diskutiert.

Als größte Schwäche bei der Kontrolle von möglichen staatlichen Biowaffenaktivitäten und davon ausgehenden Proliferationsrisiken gilt das Fehlen eines rechtsverbindlichen Verifikationsmechanismus zur Einhaltung der BWC, wie er für die CWC und für den Atomwaffensperrvertrag existiert. Die BWC ermutigt Staaten lediglich im Rahmen freiwilliger vertrauensbildender Maßnahmen, relevante Aktivitäten selbst zu melden. Alle Bemühungen der Vertragsstaaten, das Übereinkommen zu stärken – einschließlich obligatorischer Meldungen von Dual-Use-Aktivitäten oder kurzfristiger Überprüfungen verdächtiger Einrichtungen –, scheiterten unter anderem an Bedenken, dass solche Überprüfungen technisch und praktisch für biologische Waffen nicht durchführbar sind, insbesondere da die für die Herstellung von Biowaffen benötigten Materialien und Ausrüstung oft dieselben sind wie in der zivilen biowissenschaftlichen Forschung. Zudem gab es Bedenken, dass die Überprüfungen Wirtschaftsspionage erleichtern könnten. In der Diskussion um BWC-Reformen wird jedoch auch darauf hingewiesen, dass es schwierig wäre, Staaten, die gegen die BWC verstoßen, zur Rechenschaft zu ziehen oder zu bestrafen. Deshalb wurde verschiedentlich vorgeschlagen, die BWC durch (Abschreckungs-)Strategien zu ergänzen, welche die Erfolgsaussichten des Einsatzes von Biowaffen von vornherein begrenzen („deterrence by denial“), etwa durch effektive Überwachungssysteme von Erregern in der Umwelt oder Maßnahmen zur schnellen Schadensbegrenzung wie flexible Diagnostik oder schnell skalierbare Impfstoffplattformen.

Die Sicherung der Schnittstelle zwischen KI-Modellen und physikalisch-biologischen Systemen

Die kommerzielle Nukleinsäuresynthese ist ein zentraler Schritt für die Herstellung von Genen bzw. davon kodierten Proteinen. Sie ist zu einer wichtigen und in der Regulierungsdebatte unstrittigen Stelle der Überwachung geworden, um das Risiko zu verringern, dass insbesondere nicht staatliche

böswillige Akteure gefährliche biologische Agenzien wie Toxine oder bestimmte Viren herstellen könnten. Derzeit gibt es zwar keine explizite generelle gesetzliche Verpflichtung für Anbieter von Nukleinsäuresynthesen, die Bestellungen auf besorgniserregende Sequenzen (z.B. von Toxinen oder bestimmten Pathogenen) oder ihre Kunden zu überprüfen. In zahlreichen Ländern und der EU ist dies jedoch faktisch erforderlich, wenn Bestellungen exportiert werden. Eine Reihe von Anbietern von Nukleinsäuresynthesen führt seit Langem grundsätzlich freiwillig Überprüfungen von Sequenzen und Kunden durch, und das International Gene Synthesis Consortium, ein Zusammenschluss von wichtigen Nukleinsäuresyntheseanbietern, hat für seine Mitglieder bindende Standards und Praktiken für solche Überprüfungen festgelegt. Dennoch gibt es weltweit zahlreiche Unternehmen, die kein Screening durchführen bzw. für die unklar ist, ob oder wie sie dies tun.

Bislang haben Regulierungsbehörden, insbesondere in den USA, versucht, die Überprüfung von Syntheseaufträgen vor allem durch nicht bindende Leitlinien und Vorgaben für Forschungsförderorganisationen voranzutreiben. Letztere legen fest, dass Nukleinsäuresynthesen ausschließlich von Herstellern bezogen werden dürfen, die Bestellungen nach festgelegten Standards überprüfen. Sowohl in den USA als auch in der EU (für den geplanten European Biotech Act) gibt es aktuell Gesetzesentwürfe, wonach Anbieter von Nukleinsäuresynthesen die bestellten Sequenzen und die Legitimität von Bestellern besorgniserregender Sequenzen überprüfen müssen.

Zur Verwirklichung von digitalen Entwürfen möglicher veränderter Moleküle oder Erreger könnten über Nukleinsäuresynthesen hinaus auch automatisierte oder autonome Laborplattformen zunehmend relevant werden. Ob etwa Cloud Labs derzeit Verfahren zur Überprüfung ihrer Kunden, der von ihnen programmierten und automatisiert durchgeführten Experimente oder der von ihnen zur Verfügung gestellten Materialien durchführen, ist unklar. Verschiedene Organisationen haben deshalb entsprechende Überprüfungen sowie die Entwicklung von entsprechenden Standards vorgeschlagen.

Schutz- und Kontrollmechanismen für KI-Modelle und biologische Daten

Zwar gilt die Überwachung der Nukleinsäuresynthese – als zentrale Schnittstelle zwischen digitalen Modellen und Entwürfen zu physischen, biologischen Molekülen oder Organismen – als hochrelevant, um Biosecurity-Risiken zu reduzieren. Jedoch wird sowohl von Forschenden aus dem KIBio-Feld als auch von Biosecurity-Fachleuten argumentiert, dass die Kontrolle dieser Schnittstelle nicht ausreicht. So dürfte eine flächendeckende, weltweit verpflichtende Kontrolle politisch kaum umsetzbar sein und biologische KI-Designmodelle können dazu beitragen, Sequenzscreening-Mechanismen zu umgehen. Neben Evaluierungen von allgemeinen generativen KI-Modellen vor deren Veröffentlichung wurde angesichts dieser Herausforderungen die Entwicklung bzw. Implementierung von Schutzmaßnahmen zur Risikominderung für biologische KI-Designmodelle vorgeschlagen.

Hierzu gehören zum einen in die Modelle integrierte „guardrails“, wie Screeningmechanismen, die potenziell besorgniserregende bzw. risikoreiche Eingaben oder Ausgaben der Modelle automatisch erkennen und dann zur weiteren Überprüfung markieren oder ablehnen. Zum anderen werden die Notwendigkeit und Mechanismen für den kontrollierten Zugang zu Modellen diskutiert. Mithilfe von Programmierschnittstellen ist es beispielsweise möglich, notwendige Informationen auszutauschen, während interne Systemdetails verborgen bleiben. Somit können Entwickler die Kontrolle über das Modell behalten. Der Zugriff auf biologische KI-Modelle sowie die

notwendigen Legitimationskriterien für Nutzer/innen sollen nach dem Risikopotenzial des jeweiligen Modells sowie dem Umfang des gewünschten oder benötigten Zugriffs gestaffelt werden. Der Nutzen solcher Modelle für die Wissenschaft und in der Folge für Anwendungsbereiche wie die Medizin, öffentliche Gesundheit und die Entwicklung von Abwehrmaßnahmen hängt nicht zuletzt von den Zugangsmöglichkeiten und somit auch den Möglichkeiten zur Überprüfung und Weiterentwicklung der Modelle ab. Ein wichtiger Diskussionspunkt ist deshalb, wie ein fairer und gleichberechtigter Zugang zu biologischen KI-Modellen gewährleistet werden kann, damit etwa Forschende von kleineren Forschungseinrichtungen oder aus dem Globalen Süden nicht benachteiligt werden.

Darüber hinaus werden Ansätze für Zugangsbeschränkungen zu bestimmten neu erstellten (und noch nicht verbreiteten) biologischen Datensätzen diskutiert. Diese sollen das Risiko verringern, dass besonders besorgniserregende neue oder erweiterte KI-Modellfähigkeiten entwickelt werden können, die Missbrauchsmöglichkeiten bieten, wie etwa das Design verbesserter oder völlig neuer pandemischer Viren. So wurde etwa vorgeschlagen, die Daten in verschiedene Sicherheitsstufen einzuteilen, entsprechend ihrer voraussichtlichen Fähigkeit, die Entwicklung von biologischen KI-Modellen für relevante Vorhersagen oder Entwürfe zu ermöglichen. Mit steigender Sicherheitsstufe würden zusätzliche Anforderungen erforderlich, bevor der Zugriff auf Daten gestattet wird. Dazu gehören die Identifizierung des/r Benutzers/in, die Genehmigung der Datennutzung, etwa durch eine Forschungsinstitution, bis hin zu einer obligatorischen Sicherheitsüberprüfung der Modelle, die mit den abgerufenen Daten trainiert wurden, vor deren Veröffentlichung. Ähnlich wie bei der grundsätzlichen Zugangskontrolle zu biologischen KI-Modellen sind auch hier mögliche negative Effekte auf einen gleichberechtigten Zugang sowie auf den offenen akademischen Austausch und die biomedizinische Forschung ein wichtiger Diskussionspunkt. Entsprechend sollen die Kontrollmaßnahmen nur für einen möglichst begrenzten Bereich von Pathogendaten gelten und Regierungen sollen prüfen, inwieweit Zugangskontrollen gegebenenfalls wieder gelockert werden können.

Nutzung von KI-Modellen zur Verbesserung der Pandemievorsorge und biologischer Verteidigungsfähigkeiten

Schließlich wird in der Debatte vorgeschlagen, dass nicht zuletzt die Stärkung der Pandemievorsorge – einschließlich der Erkennung und Überwachung von Erregern und der Weiterentwicklung von medizinischen Präventions- und Gegenmaßnahmen – wichtig sein wird, um künftige Biosecurity-Risiken zu reduzieren. Hierfür werden die verstärkte Erforschung und Nutzung von KI-gestützten Modellen und biotechnologischen Verfahren diskutiert. Diese könnten zum einen bei der KI-gestützten Überwachung (Biosurveillance) von Infektionskrankheiten eine Rolle spielen, z. B. zur Analyse von Genomdaten aus verschiedenen Quellen in Echtzeit, um bekannte Krankheitserreger oder ungewöhnliche Muster zu identifizieren, die auf neue Erreger hindeuten. Zum anderen könnten KI-gestützte Biodesignmodelle für die Entwicklung von Gegenmaßnahmen und Notfallreaktionen, einschließlich Impfstoffen, Therapeutika und diagnostischer Verfahren, genutzt werden.

Implikationen von KIxBio für Bedrohungen durch Biowaffen und Ausblick

Eine Einordnung der mit KI verbundenen Möglichkeiten in der Molekularbiologie und Biotechnologie hinsichtlich potenzieller Bedrohungen durch den Missbrauch biologischer Agenzien bzw. Biowaffen erfordert letztlich eine umfassendere Betrachtung, die über mögliche KI-Fähigkeiten hinausgeht.

Hierzu gehören Fähigkeiten und Bedingungen der Herstellung und Nutzung von Biowaffen, wie die groß angelegte Produktion von biologischen Agenzien oder die Entwicklung von waffentechnisch aufwendigen Ausbringungsmethoden (etwa durch Raketen- oder Lenkwaffen), die weitgehend unabhängig von den neuen KI-basierten Möglichkeiten sind. Bedrohungen durch Biowaffensysteme, die solche Prozesse erfordern, dürften deshalb auch weiterhin vor allem von Staaten (oder von durch diese unterstützten Gruppen) bzw. staatlichen Biowaffenprogrammen ausgehen. Die neuen KIxBio-Möglichkeiten scheinen für staatliche Programme nicht zwingend erforderlich, dennoch könnten sie einzelne Forschungs-, Entwicklungs- und Optimierungsschritte beschleunigen.

Für staatliche Akteure erscheinen insbesondere kleinflächigere taktische Einsätze oder verdeckte bzw. hybride Operationen denkbar, um andere Staaten und Regierungen zu destabilisieren. Selbst wenn die Urhebererschaft nachgewiesen werden könnte, wäre die Wahrscheinlichkeit wohl groß, dass insbesondere gegenüber Wirtschaftssanktionen resiliente und über Nuklearwaffen verfügende Staaten (oder verbündete Staaten bzw. Gruppen) bei solchen Biowaffen-Einsätzen keine untragbaren Konsequenzen zu erwarten hätten.

Die großtechnische Herstellung biologischer Agenzien und die Nutzung komplexer technischer Methoden, um diese in eine waffenfähige Form zu bringen bzw. zu verbreiten, sind jedoch nicht in jedem Fall notwendig. So könnten kleinere Mengen mancher Agenzien für biologische Bedrohungen ausreichen und über einfache, technisch wenig aufwendige Prozesse verbreitet werden – wie es bei durch nicht staatliche Akteure verübten erfolgreichen Bioterrorakten der Fall war. Dabei wurden 1984 in den USA Lebensmittel in Restaurants durch die Rajneesh-Sekte mit Salmonellen verseucht und 2001 Briefe mit Anthraxsporen verschickt. Solche Strategien, die einfachere und technisch weniger komplexe Prozesse involvieren, könnten auch zukünftig bei Bioterrorbedrohungen durch nicht staatliche Akteure am wahrscheinlichsten sein, da sie nicht die zuvor beschriebenen (und von KIxBio-Entwicklungen weitgehend unabhängigen) technischen Voraussetzungen für die Massenproduktion biologischer Agenzien oder aufwendiger Verbreitungsmechanismen erfordern. Der Zugang zu bzw. die kleinskalige Herstellung von Krankheitserregern oder Toxinen und damit die KIxBio-Möglichkeiten – wie das Erlangen von Wissen über die Isolation oder Herstellung solcher Agenzien oder die Umgestaltung von Gensequenzen für die Agenzien, um Nukleinsäuresynthescreenings zu umgehen – könnten bei solchen Bedrohungen somit eine wichtige Rolle spielen.

Diese Bedrohungen müssen aber nicht notwendigerweise wie bisher auf eher kleine Zahlen von Todesfällen oder moderate Zahlen von Erkrankten beschränkt bleiben. Größere Opferzahlen und disruptive ökonomische und gesellschaftliche Auswirkungen könnten beispielsweise drohen, wenn potenziell pandemieauslösende Viren hergestellt werden könnten und nach absichtlicher Selbstinfektion von Täter/innen („patient zero“) auf andere übertragen würden. Bei solchen Viren könnte es sich derzeit aufgrund der begrenzten Möglichkeiten zur gezielten und vorhersagbaren Verbesserung viraler Eigenschaften oder gar zum (De-novo-)Design gänzlich neuer Viren am ehesten um bekannte, natürlich vorkommende Viren handeln, die etwa über synthetische Ge-

nomsequenzen hergestellt wurden, oder aber Varianten, die zusätzlich über Mutations- und Selektionsprozesse verändert wurden (z.B. in menschlichen Zellen oder Tiermodellen). Die erforderlichen Fähigkeiten und die notwendigen Vorerfahrungen können je nach Virus unterschiedlich sein. Entsprechende effektive Veränderungen würden zusätzliche Erfahrung und Fähigkeiten, etwa im Umgang mit geeigneten Testsystemen oder Tiermodellen, erfordern.

Zwar ist es nicht auszuschließen, dass sich manche Personen ohne oder mit nur sehr begrenzter biologischer Ausbildung alle notwendigen Fähigkeiten und Erfahrungen aneignen könnten – potenziell mit Unterstützung von fortgeschrittenen LLMs. Die Wahrscheinlichkeit hierfür sowie insbesondere die Wahrscheinlichkeit, dass diese Fähigkeiten erfolgreich für ein komplexeres Gesamtprojekt, wie die Herstellung und gegebenenfalls die Veränderung und Testung potenziell relevanter pandemischer Viren, genutzt werden könnten, scheint aber nach wie vor relativ klein zu sein. Dies wird nicht zuletzt durch eine erste größere Studie mit Testpersonen in biologischen Laboren gestützt. Auch die Möglichkeiten, automatisierte Laborplattformen zu nutzen oder durch deren Kombination mit LLMs und/oder biologischen KI-Modellen realisierbare autonome Laborsysteme zu entwickeln, dürften aufgrund der damit verbundenen Herausforderungen hinsichtlich des Umfangs des bislang erforderlichen Wissens zur effektiven Nutzung kommerzieller automatisierter Labore wie Cloud Labs und der forschungsintensiven Entwicklung autonomer Laborsysteme für Akteure ohne Fachkenntnisse derzeit sehr begrenzt sein.

Inwiefern sich dies in absehbarer Zukunft ändern könnte, ist letztlich nicht verlässlich abzuschätzen und macht ein kontinuierliches Monitoring der KlxBio-Entwicklungen erforderlich. Aufgrund allgemeiner Unsicherheiten sowie möglicher Black-Swan-artiger Bedrohungen – das heißt Ereignisse mit sehr geringer Eintrittswahrscheinlichkeit, die aber extreme Effekte haben können, wie etwa die Herstellung pandemischer Viren durch Akteure ohne oder mit nur wenig Fachkenntnissen und praktischer Erfahrung – sollten bereits heute weitere vorsorgende Maßnahmen zum Umgang mit Unsicherheiten und zur Risikominimierung bzw. zur Verbesserung der Resilienz gegenüber möglichen Folgen in Betracht gezogen werden.

Handlungsoptionen

Die Ergebnisse der vorliegenden Analyse legen es nahe, dass über KlxBio-zentrierte Maßnahmen hinaus weitere Ansätze auf unterschiedlichen Ebenen erforderlich sind. Unter Berücksichtigung der internationalen Regulierungsdebatte lassen sich vier Hauptansatzpunkte erkennen:

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

Ein zentraler Ansatzpunkt ist die Unterstützung des geplanten European Biotech Act, um eine verpflichtende und EU-weit harmonisierte Sicherheitsüberprüfung für synthetische Nukleinsäuren zu ermöglichen und gleiche Wettbewerbsbedingungen für verantwortungsbewusste Synthesanbieter zu schaffen. Der Entwurf sieht diesbezüglich die Einführung einer Pflicht zur Überprüfung des legitimen Bedarfs von Käufern biotechnologischer Produkte mit hohem Missbrauchspotenzial vor. Hierzu zählen auch besorgniserregende synthetisierte Nukleinsäuresequenzen („sequences of concern“), wodurch faktisch ein Sequenzscreening notwendig wird. Darüber hin-

aus wird vorgeschrieben, dass Tischgeräte zur Nukleinsäuresynthese automatische Mechanismen zum Screening von Sequenzen enthalten müssen.

Deutschland könnte sich in der EU dafür einsetzen, dass bei mit EU-Mitteln finanzierten Projekten (auch außerhalb der EU) Nukleinsäuresynthesen und Tischgeräte zur Nukleinsäuresynthese ausschließlich von Anbietern und Herstellern bezogen werden dürfen, die ein Screening von Sequenzen und Kunden nach festgelegten Standards durchführen bzw. Sequenzscreeningmechanismen in die Geräte eingebaut haben.

Grundsätzlich könnten auf nationaler Ebene alle Forschungsförderer in Deutschland verpflichtet werden, entsprechende Auflagen für die Verwendung von Fördergeldern zu implementieren. Ähnliche Auflagen könnten auch in Bezug auf Aufträge jeglicher Art an Auftragsforschungsinstitutionen oder für die Nutzung von Cloudlaboren eingeführt werden.

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

Um die Risiken potenzieller zukünftiger biologischer KI-Modelle hinsichtlich des Designs gefährlicherer biologischer Agenzien zu reduzieren, könnten prinzipiell Mechanismen für den kontrollierten Zugang zu leistungsfähigen Biodesignmodellen oder zu bestimmten Datensätzen, die die Entwicklung solcher Modelle ermöglichen können, in Betracht gezogen werden. Zu solchen kritischen Datensätzen würden insbesondere (bisher noch weitgehend fehlende) umfangreichere und qualitativ hochwertige Daten gehören, über die KI-Modelle Genomsequenzen potenziell pandemischer Viren mit Eigenschaften wie Übertragbarkeit oder Umgehung der Immunantwort verknüpfen und solche Eigenschaften vorhersagen könnten.

Bevor solche Mechanismen in Betracht gezogen werden, müssen diese und deren mögliche Wirksamkeit (nicht zuletzt auch in Bezug auf potenziell relevante Akteure) sehr sorgfältig gegen mögliche negative bzw. kontraproduktive Auswirkungen abgewogen werden. Hiervon betroffen sein könnten insbesondere die biomedizinische Forschung und Entwicklung im Allgemeinen sowie die Entwicklung von Vorsorgemaßnahmen oder Gegenmaßnahmen im Krisenfall im Besonderen.

Zu einer solchen Abwägung – unter Berücksichtigung existierender Hinweise und Evidenzen zu Risiken sowie dem Monitoring möglicher Risikoverschärfungen – könnte auf nationaler Ebene ein einzurichtendes Beratungsgremium aus Expert/innen verschiedener Disziplinen und Bereiche beitragen. Die Empfehlungen eines solchen Gremiums könnten auch mit Blick auf mögliche, von Deutschland beeinflussbare Entscheidungen im Zusammenhang mit Kontrollmechanismen auf europäischer oder internationaler Ebene genutzt werden.

Ein solches Beratungsgremium könnte darüber hinaus Ausgangspunkt oder Teil einer Wenn-dann-Strategie sein, wie sie von den US-amerikanischen National Academies of Sciences, Engineering, and Medicine vorgeschlagen wurde, um der dynamischen KIxBio-Entwicklung Rechnung zu tragen. Dieser Ansatz zielt auf eine kontinuierliche Bewertung sowie eine regelmäßige Neubewertung von Schwachstellen und Risiken ab. Entsprechend den Ergebnissen (und möglichen festgelegten Schwellenwerten) würden neue Risikobewertungen durchgeführt und gegebenenfalls weitere oder verschärfte Maßnahmen zur Risikominderung ausgelöst.

Stärkung der BWC

Eine substanzielle Stärkung der BWC könnte durch folgende Maßnahmen erreicht werden:

- über die weitere inhaltliche Unterstützung der bei der BWC-Überprüfungskonferenz im Jahr 2022 eingesetzten Arbeitsgruppe zur Stärkung der BWC, die insbesondere bisher fehlende Möglichkeiten zur Überprüfung und Einhaltung der Konvention diskutieren und entwickeln soll. Hierzu könnten auch, im Vergleich zu klassischen Verifikationsregimes, weniger intrusive (das heißt ohne kurzfristige Überprüfungen verdächtiger Einrichtungen) und potenziell einfacher erreichbare Modelle beitragen, wie etwa solche, die strukturierte Selbstauskünfte umfassen und bei denen Staaten freiwillig ihre Einhaltung der Vorschriften durch Peer-Reviews und Besuche vor Ort nachweisen, um das Vertrauen in die Einhaltung der Vertragsbestimmungen zu stärken.
- durch das Einbringen oder die Unterstützung von Initiativen zur Verbesserung der Finanzierungssituation der BWC bzw. der BWC-Unterstützungseinheit.

Ausbau der Fähigkeit zur Durchführung von Vorsorge und Gegenmaßnahmen

Ein weiteres Element zur Risikoreduktion könnten Biodefense-Maßnahmen sein, wie eine verbesserte Vorsorge hinsichtlich der Früherkennung von potenziellen pandemischen Erregern, verbesserte Kapazitäten zur schnellen Eindämmung und Schadensbegrenzung sowie die Erkennung bzw. Verhinderung von biologischen Anschlägsplänen. Solche Maßnahmen könnten neben einer besseren Reaktionsfähigkeit auch zur Abschreckung von Gegnern beitragen, die sich über militärische Strategien nicht abschrecken ließen, wie etwa bestimmte nicht staatliche Akteure – indem sie deren Erfolgsaussichten reduzieren („deterrence by denial“).

Hierzu könnten durch parlamentarische Gremien und/oder Ministerien, die Zugang zu notwendigen, ansonsten nicht öffentlich zugänglichen Informationen haben, Möglichkeiten zur Stärkung von Aktivitäten und Kapazitäten insbesondere in den folgenden Bereichen geprüft werden:

- anwendungsorientierte Biodefense-Forschung: Dort können neue KI-Möglichkeiten genutzt werden, um effektive Früherkennungsmaßnahmen für biologische Agenzien oder ungewöhnliche Infektionen sowie schnell skalierbare medizinische Gegenmaßnahmen zur raschen Eindämmung und Schadensbegrenzung zu entwickeln. Beispiele sind die Analyse globaler Kommunikationsquellen mithilfe von natürlicher Sprachverarbeitung oder Ansätze unter Nutzung von KI-Modellen, die Genomdaten aus verschiedenen Quellen kontinuierlich überwachen, diese Daten mit vorhergesagten Proteinstrukturdaten ergänzen und auf neue zirkulierende Erreger hinweisen können. Des Weiteren könnte die Etablierung KI-unterstützter Plattformtechnologien zur Beschleunigung der Impfstoffentwicklung und -produktion gefördert werden, wie sie beispielsweise im Rahmen des „Rapid Response Framework“ der Coalition for Epidemic Preparedness Innovations entwickelt werden sollen.
- Terrorismusabwehr: Hier könnte die Zusammenarbeit mit Unternehmen, die KI entwickeln, gefördert bzw. deren Sicherheitsmaßnahmen unterstützt werden. Dazu könnte beispielsweise die Überwachung besorgniserregender Kommunikation mit großen generativen KI-Modellen (Chatbots) gehören, die vermuten lässt, dass Nutzer/innen anderen Schaden zufügen wollen.

1 Einleitung



1 Einleitung

Thematischer Hintergrund

Die rasanten Fortschritte bei der Analyse und Synthese von Erbgut (DNA) sowie bei der gezielten Veränderung von Genen in verschiedensten Organismen durch Genomeditierungs-Techniken haben die Möglichkeiten der Erforschung und der Veränderung biologischer Systeme bzw. Organismen in den letzten 10 bis 15 Jahren vereinfacht und stark erweitert. Ein zunehmend wichtiges Werkzeug sind dabei computergestützte Analyse- und Designprozesse. Diese oft unter den Begriffen „Synthetische Biologie“ (TAB-Arbeitsbericht Nr. 164 „Synthetische Biologie – die nächste Stufe der Bio- und Gentechnologie“) oder „engineering biology“ zusammengefassten Entwicklungen der Molekularbiologie und Biotechnologie haben nicht nur in der Grundlagenforschung zu neuen Möglichkeiten geführt, etwa bei der Erforschung von Gen- und Molekülfunktionen sowie von Krankheitsursachen. Auch in Anwendungsfeldern, wie insbesondere der industriellen Biotechnologie etwa zur Generierung neuer Synthesewege für Chemikalien in Mikroorganismen und der Entwicklung neuer Medikamente bzw. Behandlungsmöglichkeiten, darunter Gentherapien für bisher unheilbare Krankheiten sowie gen- und zellbasierte Krebsimmuntherapien, haben diese neuen Möglichkeiten bereits revolutionäre Entwicklungen eingeleitet.

Diese Fortschritte in der Molekularbiologie und Biotechnologie konvergieren zunehmend mit jüngeren Entwicklungen in Bereichen der künstlichen Intelligenz (KI) sowie der Automatisierung von Laborprozessen. Ermöglicht durch größere Datensätze zu biologischen Molekülen und deren Funktionen entstehen zunehmend leistungsfähigere KI-Modelle, die für die Analyse und das Design von biologischen Molekülen und Prozessen sowie von Forschungs- und Entwicklungsprozessen entsprechender Anwendungen eine immer wichtigere Rolle spielen.

Die Synthetische Biologie und ihre Anwendungsmöglichkeiten wurden seit ihren Anfängen von Diskussionen über Risiken durch mögliche (Labor-)Unfälle oder eine missbräuchliche Verwendung begleitet. Insbesondere wurde dabei die Zugänglichkeit zu den technologischen Entwicklungen zur Veränderung von Molekülen oder Organismen (wie DNA-Synthese oder Genomeditierung) für Nichtexpert/innen bzw. Personen, die nicht in etablierte wissenschaftliche Einrichtungen eingebunden sind, thematisiert. Mit der zunehmend wichtigeren Rolle von KI und deren Zusammenspiel mit biotechnologischen Möglichkeiten haben sich diese Diskussionen erneut intensiviert. Vor allem international hat sich in den letzten Jahren eine Sicherheitsdebatte entwickelt, die sich stark auf Missbrauchsrisiken durch die mögliche Herstellung biologischer Waffen sowie die damit verbundenen (nationalen) Sicherheitsfragen fokussiert. Im Mittelpunkt dieser Debatte stehen im Wesentlichen drei Bedenken: erstens, dass die Entwicklungen es insbesondere Nichtexpert/innen bzw. nicht staatlichen Akteuren (weiter) erleichtern könnten, gefährliche biologische Agenzien herzustellen bzw. Biowaffen zu entwickeln; zweitens, dass die Entwicklung noch gefährlicherer bzw. neuer solcher Agenzien und Biowaffen möglich wird, die das Schadenspotenzial oder -ausmaß erhöhen könnten; und drittens, dass die Wirksamkeit von Biosicherheits- und Abwehrmaßnahmen (Biodefense) verringert oder unterlaufen werden könnte.

Zielsetzung und Vorgehensweise

Das vom Verteidigungsausschuss initiierte Projekt des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) sollte zum einen mögliche Sicherheitsrisiken neuerer biotechnologischer Entwicklungen und ihrer Wechselwirkungen mit Entwicklungen im Bereich der KI möglichst breit analysieren und dann konzentriert zusammenfassen. Zum anderen sollten gegenwärtige Kontroll- und Regulierungsmöglichkeiten dargestellt sowie Möglichkeiten zu deren Weiterentwicklung diskutiert werden, um diese Sicherheitsrisiken zu minimieren und die Nichtverbreitung potenzieller Biowaffen zu stärken.

Neben umfangreichen eigenen Literaturrecherchen und -auswertungen wurden als zusätzliche fachliche Informationsbasis für das Projekt zwei Gutachten vergeben:

- Gegenwärtige Regulierungen und Maßnahmen zur Kontrolle von Biowaffen sowie zu sicherheitsrelevanter Dual-Use-Forschung in den Biowissenschaften – in Deutschland, auf EU-Ebene und international. Dr. Britta Pinzger, Dr. Carsten Heuer, Dr. Benjamin Kaluza, Dr. Silke Römer; Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen INT, Euskirchen
- Notwendige Kenntnisse und technische Voraussetzungen für die Herstellung und den Einsatz von biologischen Agenzien als Biowaffen. Dr. Dunja M. Sabra, Carl Friedrich von Weizsäcker-Zentrum für Naturwissenschaften und Friedensforschung, Universität Hamburg, und Dr. Johannes L. Frieß, Institut für Sicherheits- und Risikowissenschaften (ISR), Universität für Bodenkultur Wien

Die TAB-Projektbearbeiter Harald König und Arnold Sauter möchten sich herzlich bei den Gutachter/innen für die gute und vertrauensvolle Zusammenarbeit, einschließlich der Kommentierung von Kapitelentwürfen, bedanken. Die Verantwortung für die Auswahl, Interpretation und Einarbeitung von Ergebnissen aus den Gutachten liegt ausdrücklich bei den Verfassern des vorliegenden Berichts. Danken möchten die Berichtsaufsteller auch Herrn Prof. Dr. Roman Wölfel vom Institut für Mikrobiologie der Bundeswehr für die kritische Durchsicht eines Berichtsentwurfs sowie Brigitta-Ulrike Goelsdorf für die Durchsicht und Gestaltung der Endfassung des Manuskripts einschließlich der Bearbeitung der Abbildungen.

Aufbau des Berichts

Im folgenden Kapitel 2 wird ein aktueller Überblick über relevante Entwicklungen in der molekularen Biologie bzw. der Synthetischen Biologie und der Biotechnologie sowie deren Zusammenspiel mit jüngeren KI-Entwicklungen gegeben. Darauf aufbauend werden in Kapitel 3 Bedenken und mögliche Sicherheitsrisiken vorgestellt, die in der fachwissenschaftlichen Literatur sowie von verschiedenen gesellschaftlichen Akteuren (z. B. Forschende, politikberatende Organisationen, Sicherheitsexpert/innen) diskutiert werden. Die zugrunde liegenden Argumente und Evidenzen wurden ausgewertet, wobei der Fokus auf Ergebnissen aktueller Forschungsansätze und Daten aus empirischen Studien zur Leistungsfähigkeit von KI-Modellen sowie zur Unterstützung von Akteuren durch solche Modelle lag. Daraus wurden Implikationen für Missbrauchsrisiken im Zusammenhang mit biologischen Waffen abgeleitet. Ausgehend von der Darstellung existierender Verträge, Regulierungen und Initiativen zur Kontrolle von Biowaffen und sicherheitsrelevanter Forschung auf internationaler Ebene, in der Europäischen Union (EU) und national, wird dann in Ka-

kapitel 4 die Diskussion um mögliche Lücken in und die notwendige Stärkung von existierenden Regelungen und Mechanismen präsentiert und erörtert. Im abschließenden Kapitel 5 werden Handlungsfelder und Handlungsoptionen abgeleitet und benannt.

Hinweise an die Leser/innen

Der vorliegende Bericht und die darin enthaltenen Analysen des TAB beruhen auf öffentlich zugänglichen Daten und Wissensbeständen. Die Basis für die Einschätzungen zu der wohl zentralen Frage der Debatte um KI-Modelle und Biowaffen – nämlich inwieweit diese Modelle die Hürden für Nichtexpert/innen bzw. nicht staatliche Akteure senken könnten, gefährliche biologische Agenzien bzw. Biowaffen herzustellen – bildete eine möglichst evidenzbasierte Herangehensweise. Diese stützte sich auf Ergebnisse empirischer Studien, darunter größere randomisierte und kontrollierte Studien mit Testpersonen, einschließlich erster solcher Untersuchungen in realen biologischen Laboren. In Bezug auf die allermeisten solcher verfügbaren Studien ist allerdings zu beachten, dass diese nicht in begutachteten Fachzeitschriften veröffentlicht wurden und kein entsprechendes, unabhängiges Peer-Review-Verfahren durchlaufen haben. Darüber hinaus setzt die meist fehlende oder nur sehr eingeschränkte Offenlegung der in den Untersuchungen gestellten Fragen bzw. Aufgaben, von (Roh-)Daten sowie der vorgenommenen Bewertungen – meist begründet mit Sicherheitsbedenken – einer unabhängigen Überprüfung der Studienergebnisse enge Grenzen und erschwert die Einschätzung der Relevanz der Ergebnisse.

Mit der teilweise detaillierten Diskussion mancher Ergebnisse (aus öffentlich verfügbaren Studien), die mit den zuvor genannten Einschränkungen etwa nahelegen, dass KI-Modelle Personen mit begrenzter biowissenschaftlicher Ausbildung zumindest theoretisches Wissen auf Experteniveau vermitteln können, könnte zwar ein gewisses Aufmerksamkeitsrisiko verbunden sein. Das heißt, dass manche potenziell böswillige Akteure erst durch die Berichterstattung auf diese Möglichkeit(en) aufmerksam werden könnten. Dasselbe gilt für Hinweise im vorliegenden Bericht auf seit längerer Zeit über eine einfache Internetsuche öffentlich verfügbare, potenziell sensible Informationen in wissenschaftlichen Publikationen oder die einfache Umgehung von Sicherheitsmaßnahmen vieler allgemeiner KI-Modelle. Diese Art der Offenlegung erscheint jedoch unumgänglich, um ein realistisches Bild und eine möglichst evidenzbasierte Einschätzung potenzieller Missbrauchsrisiken mit Blick auf politische Meinungsbildung und Entscheidungsfindung zu ermöglichen und um diese Risiken durch vorausschauende Sicherheitsmaßnahmen möglichst wirksam zu minimieren.

Die Analyse spiegelt den Stand verfügbarer Studien und die Diskussionen vom Mai 2026 wider. Aufgrund der hohen Dynamik der Entwicklungen bei KI-Modellen, der Molekularbiologie bzw. Biotechnologie sowie deren Zusammenspiel wird die Beurteilung von Biosecurity-Risiken im Zusammenhang mit diesen Entwicklungen ein kontinuierliches Monitoring und gegebenenfalls Anpassungen von Risikoeinschätzungen und geeigneten Maßnahmen erfordern.

2 Molekularbiologische und biotechnologische Entwicklungen und deren Zusammenspiel mit künstlicher Intelligenz

- 2.1 Biologie wird Technologie: methodische Fortschritte, um biologische Systeme zu verstehen und zu gestalten
- 2.2 Zunehmend große biologische Datensätze haben Molekularbiologie und Biotechnologie für KI zugänglich gemacht
- 2.3 KI-Modelle haben bereits eine Reihe neuer Entwicklungen mit großem Potenzial für die Forschung und Anwendung ermöglicht

2 Molekularbiologische und biotechnologische Entwicklungen und deren Zusammenspiel mit künstlicher Intelligenz

2.1 Biologie wird Technologie: methodische Fortschritte, um biologische Systeme zu verstehen und zu gestalten

In den letzten 10 bis 15 Jahren haben sich molekularbiologische Methoden und Möglichkeiten zur Erforschung und zum Verständnis biologischer Prozesse in verschiedensten Organismen, einschließlich des Menschen, rasant weiterentwickelt. Eine zunehmend größere Rolle hat dabei auch der Einsatz von künstlicher Intelligenz (KI) in Form von Verfahren des maschinellen Lernens (Kasten 2.1) für die Analyse biologischer und biomedizinischer Daten erlangt (Donkor et al. 2024; Nature methods 2024) (Kasten 2.2).

Kasten 2.1 Künstliche Intelligenz und maschinelles Lernen

Mit künstlicher Intelligenz (KI) wird allgemein der wissenschaftlich-technische Ansatz bzw. die Vision beschrieben, Computer und Software zu entwickeln, die Aufgaben erfüllen, für die bisher menschliche Intelligenz erforderlich war. Viele derzeitige Anwendungen künstlicher Intelligenz (z. B. Sprach- und Bilderkennung, Übersetzungsprogramme, Chatbots wie ChatGPT) beruhen auf einem Teilgebiet der KI, dem *maschinellen Lernen* (ML). Beim ML verbessern sich Software und Modelle durch Erfahrung unter Verwendung sehr großer Datenmengen automatisch, z. B. um Muster in Daten zu erkennen oder Vorhersagen zu machen (Donkor et al. 2024; Kersting 2018).

Eine besonders leistungsfähige und flexible Art von ML, auf der sehr viele aktuelle KI-Modelle beruhen, ist das *Deep Learning* (DL) (Mienye/Swart 2024). DL-Modelle basieren auf mehreren Schichten softwaresimulierter künstlicher Neuronen (tiefe neuronale Netze) und können verschiedene Architekturen haben, die unterschiedlichen Annahmen über Daten entsprechen und für unterschiedliche Aufgaben verwendet werden (Barbadilla-Martínez et al. 2025; Donkor et al. 2024; Mienye/Swart 2024).

Large Language Models (LLMs, große Sprachmodelle) basieren typischerweise auf DL-Methoden und stellen eine spezielle Art von DL-Modellen dar, die ursprünglich darauf ausgelegt wurden, komplexe Texte, Fragen oder Anweisungen zu verarbeiten und kohärente Antworten und Texte zu generieren (Chen et al. 2024b; Donkor et al. 2024). Hierzu gehören Generative-Pre-trained-Transformer(GPT)-Modelle wie ChatGPT oder GPT (von OpenAI), Claude (Anthropic) oder Gemini (Google). LLMs werden mit sehr großen Datensätzen trainiert und können typischerweise mit nur wenig zusätzlichem Trainingsaufwand („fine tuning“) für verschiedene Aufgaben

verwendet werden. Aufgrund dieser Eigenschaft werden solche Modelle auch als Basismodelle („foundation models“/Foundationmodelle) bezeichnet (Caballar/Stryker 2025; Chen et al. 2024b; Donkor et al. 2024). Aktuelle Versionen solcher Modelle sind meist multimodal, das heißt, sie können verschiedene Arten (Modalitäten) von Daten verarbeiten und integrieren, z. B. Text, Bilder, Ton oder Video (Chen et al. 2024b; Huang et al. 2024; IBM 2025). So kann ein multimodales Modell z. B. ein Foto als Eingabe erhalten und schriftlich Eigenschaften des Gezeigten, etwa einer Landschaft, zusammenfassen. Die jüngsten Generationen von LLMs sind „reasoning models“; diese wurden so trainiert, dass sie komplexe Probleme in kleinere (Reasoning-)Schritte unterteilen, bevor sie eine endgültige Antwort bzw. Ausgabe generieren (Bergmann 2025; Shojaee et al. 2025).

LLMs gehören zu den *generativen KI-Modellen*. Im Gegensatz zu *prädiktiven KI-Modellen*, die erkannte Muster in historischen Daten zur Vorhersage künftiger Ereignisse oder von Molekülfunktionen nutzen, verwenden generative Modelle erkannte Muster und Beziehungen in Daten, mit denen sie trainiert wurden, um neue Inhalte zu erstellen, die die Originaldaten (z. B. Text, Bilder oder auch DNA- und Proteinsequenzen) nachahmen (Caballar 2025; Donkor et al. 2024; Gupta et al. 2024).

Synthetische Biologie oder „engineering biology“

Mit diesen Fortschritten in der Molekularbiologie wurde es zunehmend möglich, biologische Moleküle, Funktionen und Organismen gezielt umzugestalten oder komplett neu zu entwerfen (zu designen), sodass sie neue, auch zum Teil nicht in der Natur vorkommende Funktionen erfüllen können. Diese neuen Möglichkeiten sind Grundlage der Idee bzw. Vision der Synthetischen Biologie (TAB 2015). Danach soll Biologie zu einer echten Ingenieurwissenschaft bzw. Technologie werden, indem komplexe biologische Funktionen nach zentralen ingenieurwissenschaftlichen Prinzipien wie Modularität, Charakterisierung und Standardisierung, das heißt über die Schaffung bzw. Nutzung standardisierter biologischer Bauteile mit charakterisierter, definierter Funktion, in weitgehend vorhersagbarer Weise verändert oder neu konstruiert werden können (Endy 2005; MPG 2025). Dieser Ansatz bzw. diese Vision von Biologie als Technologie wird zunehmend, insbesondere im Zusammenhang mit der Umsetzung zu spezifischen Anwendungen, auch als „engineering biology“ bezeichnet (Clarke 2020).

Sowohl in der Grundlagenforschung als auch in der Medizin und in der industriellen Biotechnologie haben diese neuen molekularbiologischen Möglichkeiten bereits entscheidend zu einigen bahnbrechenden Entwicklungen beigetragen. Hierzu gehören insbesondere (Kapitel 2.3) die Erforschung der Funktion von Genen, zellulärer Prozesse und von Krankheitsursachen (Kim et al. 2024; Li et al. 2023), die Entwicklung von gen- und zellbasierten Therapien für verschiedene Krankheiten sowie von gezielten Krebstherapien (Liu et al. 2024; Patel et al. 2025; Wang et al. 2025a), die Entwicklung von mRNA-Impfstoffen (Pardi/Krammer 2024; Yaremenko et al. 2025) und die Neukonstruktion (Design) bzw. Umgestaltung (Redesign) von Stoffwechselwegen in Mikroorganismen zur industriellen Herstellung verschiedener Substanzen (Le et al. 2025; Liew et al. 2022; Nielsen/Keasling 2016; Shi et al. 2025 und Referenz darin).

Zu diesen neuen Möglichkeiten zur Erforschung und der Um- bzw. Neugestaltung biologischer Funktionen und Systeme hat eine Reihe von Fortschritten und Entwicklungen beigetragen. Hierzu gehören:

- *neue Analysemethoden*, wie insbesondere automatisierte und in Hochdurchsatzverfahren arbeitende Sequenzierungstechniken („next generation sequencing“) zur Entschlüsselung des gesamten Erbguts (des Genoms) und davon abgelesener RNA-Moleküle (des Transkriptoms) (Satam et al. 2023), sowie experimentelle Ansätze zur Bestimmung der dreidimensionalen Struktur von biologischen Molekülen, vor allem von Proteinen (Dokholyan 2020). Die neuen Analysemethoden wurden jeweils durch computergestützte Verfahren zum Prozessieren bzw. Analysieren von Daten (Bioinformatik) ermöglicht (Kasten 2.2).
- *einfachere und vielseitig einsetzbarere gentechnologische Methoden* zur Modifikation und Untersuchung der Funktion von Genen und der von ihnen kodierten Moleküle (Proteine, RNA). Quasi beliebige und in großem Maßstab genomweit durchführbare genetische Veränderungen in unterschiedlichsten Zellen und Organismen wurden insbesondere durch molekulare Werkzeuge zur Genomeditierung möglich, die auf dem CRISPR-Cas-System¹ basieren (Pacesa et al. 2024; Wang/Doudna 2023).
- *Methoden zur Synthese von Nukleinsäuresequenzen* (DNA, RNA) und für das – teilweise automatisierte – Zusammenfügen (Assemblierung) synthetisierter kürzerer DNA-Stücke zu längeren DNA-Bereichen (Ma et al. 2024b; Seydel 2023) bis hin zu Chromosomen von Hefezellen oder ganzen Genomen mancher Viren und Bakterien (James et al. 2025; Ma et al. 2024b). Diese Methoden haben, zum Teil in Kombination mit gentechnologischen Verfahren, die Veränderung bzw. Generierung neuer biologischer Funktionen oder Organismen stark erleichtert (Fu/Shen 2024; Hughes/Ellington 2017; Kelley et al. 2016).
- *computergestützte und zunehmend auf künstlicher Intelligenz bzw. maschinellem Lernen (ML) basierende Verfahren* (Kasten 2.1): unter anderem zur Analyse von Genomsequenzen und deren Funktionen, zur Vorhersage und zum Design von Proteinstrukturen, Proteinfunktionen und Stoffwechselprozessen sowie zur Automatisierung von Experimenten bzw. Entwicklungsprozessen (Kapitel 2.3).

¹ CRISPR („clustered regularly interspaced short palindromic repeats“; übersetzt etwa in Gruppen angeordnete, regelmäßig auftretende kurze Palindromwiederholungen). Diese DNA-Bereiche wurden ursprünglich in Bakterien entdeckt und enthalten Teilsequenzen von in die Zellen eingedrungener fremder DNA (z. B. von Viren), die dort eingebaut und so abgespeichert wurden. Diese Sequenzen sind Teil adaptiver Immunsysteme von Bakterien (CRISPR-Cas-Systeme) und existieren in einer Reihe verschiedener Varianten. Cas steht für CRISPR-assoziiert und bezeichnet die Proteinkomponente dieser Systeme, die an eine bestimmte Stelle (Zielsequenz) im Erbgut bindet und dort den DNA-Doppelstrang schneidet, wie im Fall des ursprünglich entdeckten CRISPR-Cas9-Systems oder – ausgehend von der Zielsequenz – den Abbau von DNA und/oder RNA-Sequenzen bewirken kann (Makarova et al. 2020; Nidhi et al. 2021). Die Zielsequenzen werden über von den CRISPR-Bereichen kodierten kurzen RNA-Sequenzen vorgegeben.

2.2 Zunehmend große biologische Datensätze haben Molekularbiologie und Biotechnologie für KI zugänglich gemacht

Diese neuen Möglichkeiten zur Analyse und (Um-)Gestaltung biologischer Systeme haben zu zunehmend großen Beständen bzw. Datenbanken unterschiedlicher biologischer Daten geführt (Chaudhari et al. 2024; Wainberg et al. 2018). Hierzu gehören insbesondere Omik-Daten² wie zu Genomsequenzen und deren Funktion (Genomik), Daten zur Regulation bzw. dem Ablesen von Genen in den verschiedenen Körperzellen oder Organen (Epigenomik), zur Gesamtheit der in verschiedenen Zelltypen oder Geweben hergestellten RNA-Moleküle und Proteine einschließlich Daten zur Struktur und Funktion dieser Moleküle (Transkriptomik bzw. Proteomik) oder Daten zu zellulären Stoffwechselprozessen und darin involvierten Enzymen (Metabolomik). Zunehmend spielen im Bereich der Genomik auch Daten zu Funktionen von Genomsequenzen einschließlich genregulatorischer Elemente und kodierender Genbereiche eine Rolle, die in großem Maßstab über CRISPR-Cas-basierte Verfahren zur Genomedition erhalten werden können (Pacesa et al. 2024; Wang/Doudna 2023).

Während sich die Erforschung und Verwendung computergestützter Verfahren zur Erfassung und Analyse biologischer Daten in der Molekularbiologie bereits seit Ende der 1950er Jahre entwickelten und für das Feld eine wichtige Rolle spielten (Gauthier et al. 2019) (Kasten 2.2), ermöglichten es erst die genannten großen Datensätze, entsprechende KI-Modelle für die molekularbiologische Forschung und für biotechnologische Anwendungen zu entwickeln (Barbadilla-Martínez et al. 2025; Donkor et al. 2024; Rao et al. 2026; Wainberg et al. 2018) (Kasten 2.2).

Kasten 2.2 Von früher Bioinformatik zu KI-Anwendungen

Die Erforschung und Verwendung computergestützter Methoden zur Erfassung, Speicherung, Verbreitung und Analyse biologischer Daten bzw. Information – die Bioinformatik – sind vor mehr als 60 Jahren entstanden (Gauthier et al. 2019). Ihre Entwicklung begann somit lange vor der Ära großer biologischer Datenmengen aus automatisierten Genomsequenzierungen oder KI-Verfahren in der Molekularbiologie und Biotechnologie (Abbildung 2.1, Kapitel 2.3) und spielt seit ihren Anfängen eine wichtige Rolle für diese Bereiche (Donkor et al. 2024; Gauthier et al. 2019).

² Der Begriff Omik („omics“) bezeichnet Forschungsbereiche, die sich mit der Untersuchung der Gesamtheit eines bestimmten Typs von biologischen Molekülen oder molekularer Prozesse innerhalb von Zellen oder Organismen befassen. Das Ziel ist, Moleküle und molekulare Prozesse zu identifizieren, zu beschreiben und zu quantifizieren, die zur Form und Funktion von Zellen und Geweben beitragen.

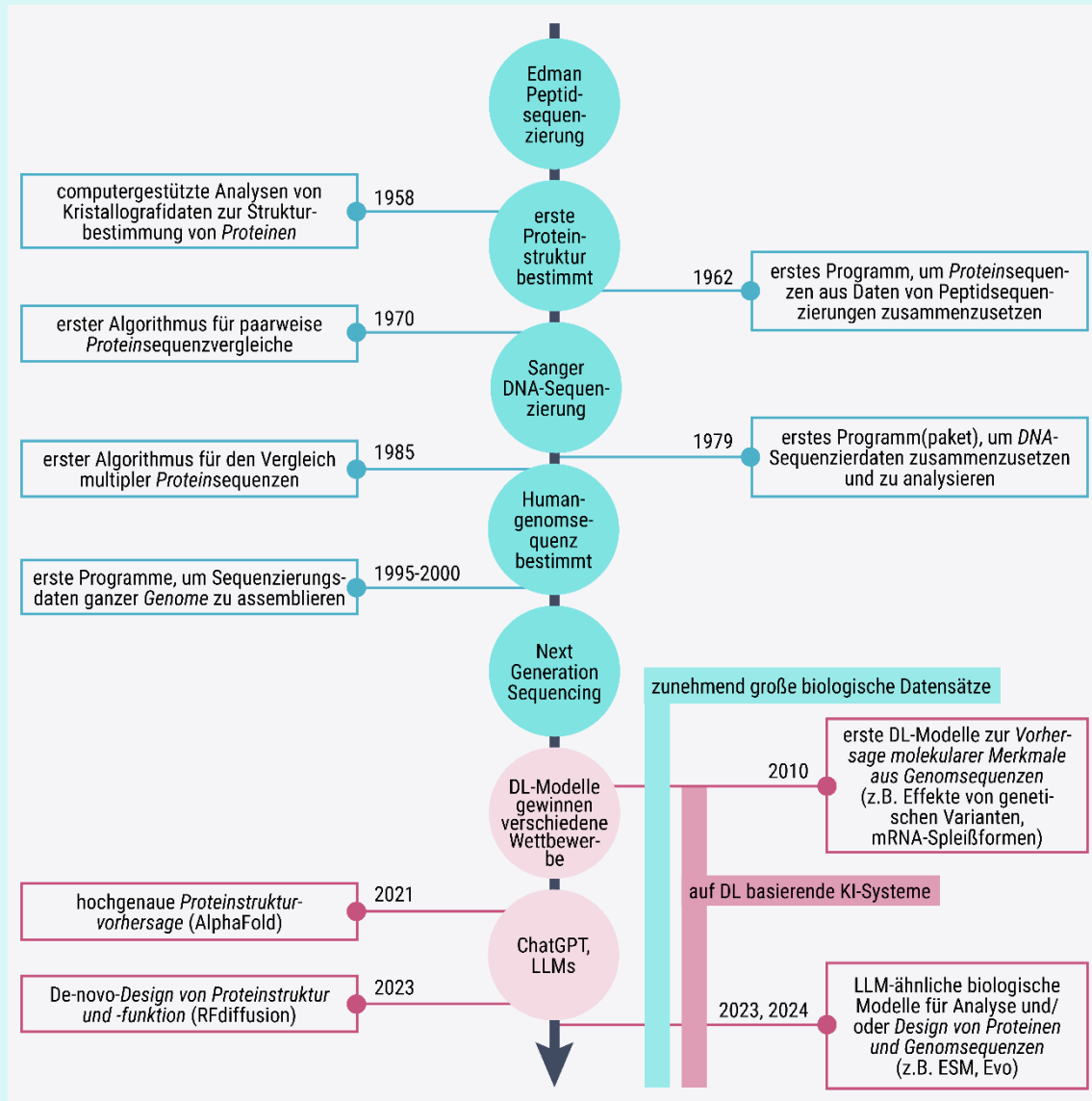
Erste computergestützte Methoden zur Analyse von Röntgenkristallografiedaten zur Strukturbestimmung von Proteinen (Kendrew et al. 1958, 1960) und von Proteinsequenzdaten, um längere Proteinsequenzen aus Daten von Peptidsequenzierungen zusammenzusetzen (Dayhoff/Ledley 1962), wurden Ende der 1950er und Anfang der 1960er Jahre entwickelt und angewandt. Ab den 1970er Jahren folgten Programme für den Vergleich von Proteinsequenzen (Murata et al. 1985; Needleman/Wunsch 1970). Nach der Entwicklung von DNA-Sequenzierungsverfahren Mitte der 1970er Jahre (Maxam/Gilbert 1977; Sanger et al. 1977b) wurde 1979 ein erstes Programmpaket verfügbar, um DNA-Sequenzdaten zu längeren Sequenzen zusammenzusetzen und zu analysieren (Staden 1979). Programme, um inzwischen verfügbare Sequenzierungsdaten ganzer Genome zu assemblieren, wurden ab Mitte der 1990er Jahre entwickelt (Gordon et al. 1998; Myers et al. 2000) und waren entscheidend für die Entschlüsselung des menschlichen Genoms (Lander et al. 2001; Venter et al. 2001).

Insbesondere neue Generationen von automatisierten und in Hochdurchsatzverfahren arbeitenden Sequenzierungstechniken („next generation sequencing“) ermöglichten zunehmend die Gewinnung großer Datensätze zu Genomsequenzen, zu epigenetischen DNA-Markierungen, die die Aktivität von Genen beeinflussen, oder dazu, wann welche Gene in welchen Zellen abgelesen werden und welche Genprodukte entstehen (Satam et al. 2023). Darüber hinaus wurden durch Fortschritte in verschiedenen Techniken zur experimentellen Bestimmung der dreidimensionalen (3D-)Struktur von größeren Molekülen (Carugo/Djinović-Carugo 2023; Dokholyan 2020) insbesondere große Mengen von Daten zur 3D-Struktur von Proteinen generiert und in der weltweiten Proteindatenbank wwPDB.org³ zugänglich gemacht (Carugo/Djinović-Carugo 2023; wwPDB consortium 2019).

Mit solchen zunehmend großen Datenbeständen wurde es möglich, KI-Modelle für biologische Fragestellungen, vor allem mit flexiblen und leistungsfähigen DL-Modellen (Kasten 2.1) zu entwickeln. Erste solche biologische KI-Modelle zur Vorhersage molekularer Merkmale bzw. Funktionen (Phänotypen) von nicht kodierenden Genomsequenzen (z. B. Effekte von genetischen Varianten auf das Ablesen von Genen oder das Entstehen von alternativen [Spleiß-]Formen von mRNA) entstanden seit ca. dem Jahr 2010 (Barbadilla-Martínez et al. 2025; Sokolova et al. 2024). Ab Anfang der 2020er Jahre folgten dann biologische Modelle (darunter auch solche, die analog zu LLMs arbeiten, Kasten 2.1) zur hochgenauen Proteinstrukturvorhersage (Baek et al. 2021; Jumper et al. 2021; Lin et al. 2023), zum Design von Proteinstrukturen und -funktionen (Hayes et al. 2025; Watson et al. 2023) sowie zur Analyse und zum Design von Genomsequenzen und/oder Proteinen (Brix et al. 2026; Hayes et al. 2025; Nguyen et al. 2024).

3 Die weltweite Proteindatenbank wwPDB.org dient seit 1971 als zentrales Archiv für experimentell ermittelte 3D-Strukturdaten von Proteinen, Nukleinsäuren und deren Komplexen mit Metallen und kleinen Molekülen. Sie wird durch ein internationales Konsortium verwaltet, das gemeinsam die Hinterlegung, Validierung und frei zugängliche Verbreitung von 3D-Strukturdaten zu Makromolekülen beaufsichtigt.

Abbildung 2.1 Zeitleiste mit Meilensteinen von der frühen Bioinformatik zur Entwicklung und Nutzung von KI



Eigene Darstellung

2.3 KI-Modelle haben bereits eine Reihe neuer Entwicklungen mit großem Potenzial für die Forschung und Anwendung ermöglicht

Sowohl akademische Forschungseinrichtungen als auch Biotech- und andere Technologieunternehmen haben biologische KI-Modelle (Kasten 2.3) basierend auf Deep-Learning-Verfahren für verschiedene Fragestellungen in der Grundlagenforschung bis hin zu einer Reihe von Anwendungen in der Biotechnologie und Medizin entwickelt und eingesetzt (Tabelle 2.1).

Kasten 2.3 KI-Modelle in der Molekularbiologie und Biotechnologie

In der Molekularbiologie oder Biotechnologie eingesetzte KI-Modelle bzw. -Systeme lassen sich nach der Art der Daten, mit denen sie trainiert wurden, und der Ergebnisse, die sie produzieren, in drei große Kategorien einteilen:

- *Große Sprachmodelle (LLMs)*: Diese werden mit natürlicher Sprache trainiert und produzieren typischerweise Ausgaben in natürlicher Sprache bzw. Texten. Bei multimodalen Modellen (Large multimodal models – LMMs) werden zusätzlich weitere Datenarten wie Bilder oder Videomaterial verwendet (Kasten 2.1). LLMs bzw. LMMs umfassen auch domänenspezifische Modelle, die beispielsweise mit biomedizinischen Datensätzen (z. B. Literatur, biomedizinische Bilddaten, elektronische Patientenakten) trainiert wurden.
- *Biologische Modelle*: Ihr Training erfolgt mit biologischen Daten (z. B. DNA- oder Proteinsequenzen, Molekülstrukturen oder -funktionen) und sie liefern Vorhersagen bzw. Vorschläge für Sequenzen und Strukturen biologischer Moleküle oder zu deren Funktion. Diese Modelle beruhen in der Regel auf Deep-Learning-Verfahren (Kasten 2.1), darunter auch Protein-sprachmodelle und DNA- bzw. Genomsprachmodelle, in denen Proteinsequenzen bzw. die vier DNA-Bausteine (Nukleotide), ähnlich zu natürlicher Sprache, als Abfolgen von Buchstaben dargestellt werden (Kapitel 2.3.1).
- *Agentensysteme* wie autonome Labore („self-driving labs“) oder Roboterwissenschaftler („robot scientists“): Solche Systeme kombinieren verschiedene KI-Modelle, einschließlich LLMs, mit automatisierten Laborplattformen. Sie erlauben es, in autonomer Weise (als Agenten) Entwürfe zu generieren und zu optimieren, indem KI-basierte (in silico) Vorhersagen bzw. Designs im Labor automatisch erstellt, experimentell getestet und optimiert werden (Kapitel 2.3.4).

Tabelle 2.1 Beispiele für die Verwendung von KI-Modellen bzw. -Systemen in der Molekularbiologie oder Biotechnologie

Modelltyp	Verwendung	Beispiele
<i>große Sprachmodelle (LLMs)</i>		
allgemeine („general purpose“) Modelle, oft auch multimodal	Textmining und Wissensentdeckung Unterstützung bei Erstellung wissenschaftlicher Hypothesen	GPT (OpenAI 2025f); Claude (Anthropic 2025a); DeepSeek-R1 (deepseek o. J.); Gemini (Google DeepMind 2025b); Llama (Meta 2026)
domänenspezifische („scientific“) Modelle; (weiter)trainiert z. B. mit biomedizinischen Daten wie Literatur und Bildmaterial	Textmining und Wissensentdeckung Unterstützung bei Erstellung wissenschaftlicher Hypothesen	BioGPT (Luo et al. 2022); BioMedLM (Bolton et al. 2024); Med-PaLM 2 (Singhal et al. 2025); BiomedCLIP (Zhang et al. 2025c)
<i>biologische KI-Modelle</i>		
Modelle zur Vorhersage biologischer Funktionen oder Strukturen*	Funktion von DNA-Sequenzen bzw. genetischen Varianten (z. B. Ablesen von Genen, alternative mRNA-Formen, Effekte auf Proteinfunktion)	ExPecto (Zhou et al. 2018); SpliceAI (Jaganathan et al. 2019); Enformer (Avsec et al. 2021); ESM1b (Brandes et al. 2023); AlphaMissense (Cheng et al. 2023); Borzoi (Linder et al. 2025); AlphaGenome (Avsec et al. 2026); Evo 2 (Brixi et al. 2026)
	Proteinstruktur, Strukturen von Proteinen mit anderen Molekülen	AlphaFold2 (Jumper et al. 2021); RoseTTAFold (Baek et al. 2021); ESMFold (Lin et al. 2023); AlphaFold3 (Abramson et al. 2024); RoseTTAFold All-Atom (Krishna et al. 2024); Boltz-1 (Wohlwend et al. 2024); Boltz-2 (Passaro et al. 2025)
Biodesignmodelle („bio-design tools“)	Design von Proteinstrukturen (z. B. für ligandenbindende Proteine, Enzyme, Antikörper, Impfstoffe, virale Hüllproteine)	DeepVacPred (Yang et al. 2021); Vaxign-DL (Zhang et al. 2023b); RFdiffusion (Watson et al. 2023); Chroma (Ingraham et al. 2023); ProGen (Madani et al. 2023); ProteinVAE (Lyu et al. 2024); BindCraft (Pacesa et al. 2025); ESM3 (Hayes et al. 2025); JAM (Bio/Biswas 2025a); RFdiffusion3 (Butcher et al. 2025)
	Design von DNA-Molekülen (z. B. genregulatorische Sequenzen, Genomabschnitte, Genome bakterieller Viren [Phagen])	DeepSEED (Zhang et al. 2023a); DNA-Diffusion (DaSilva et al. 2024); (King et al. 2025); Evo 2 (Brixi et al. 2026)
	Design von niedermolekularen Substanzen z. B. als Kandidaten für Medikamente	Chemistry42 (Ivanenkov et al. 2023); Reinvent 4 (Loeffler et al. 2024); MedSAGE (Powers et al. 2025)

Modelltyp	Verwendung	Beispiele
<i>autonome Agentensysteme</i>		
„self-driving labs“ oder Roboterwissenschaftler	Identifizierung/Funktionsbestimmung von Genen in Hefe	Adam (King et al. 2009)
	Optimierung von mikrobiellen Stoffwechselwegen	BioAutomata (Hamedirad et al. 2019)
	Synthese von chemischen Substanzen oder möglichen Medikamenten	Coscientist (Boiko et al. 2023); ChemCrow (Bran et al. 2024)
	Veränderung/Optimierung von Enzymen	SAMPLE (Rapp et al. 2024); A generalized platform for AI-powered autonomous enzyme engineering (Singh et al. 2025)
Systeme zur Ausführung von Forschungsaufgaben, Planung von Experimenten	Generierung von Hypothesen, bioinformatische Analysen, Planung biomedizinischer Experimente (unter anderem zur Umwidmung von Medikamenten, Diagnose seltener Krankheiten)	Biomni (Huang et al. 2025)
	Planung von Genomeditierungsexperimenten (unter anderem Auswahl von CRISPR-Systemen, Deliverymethoden, Erstellung von Protokollen)	CRISPR-GPT (Qu et al. 2026)

* Modelle zur Vorhersage biologischer Strukturen sind teilweise auch Bestandteile von „bio-design tools“ (BDT) bzw. werden mit diesen kombiniert. Von manchen Autor/innen werden diese Modelle auch unter den Begriff BDT gefasst.

Eigene Zusammenstellung

2.3.1 Grundlagenforschung

Eine zentrale Herausforderung der Biologie und der Biomedizin besteht darin, zu verstehen, wie die DNA-Sequenzen des Erbguts und individuelle Unterschiede bzw. Mutationen darin, Merkmale beeinflussen oder zu Krankheiten führen können. Um die zugrunde liegenden molekularen und zellulären Mechanismen zu verstehen, ist es auch notwendig, die Funktionsweise von Molekülen, wie insbesondere von Proteinen, als zentrale Akteure für zelluläre Funktionen und Strukturen, auf molekularer Ebene zu verstehen.

Das Erbgut und Ursachen von Krankheiten verstehen

Insbesondere ab Mitte der 2010er Jahre wurden zahlreiche DL-basierte Modelle entwickelt, um zu analysieren und zu verstehen, wie verschiedene Genomsequenzen und damit wechselwir-

kende Proteine physiologische Mechanismen in Zellen und Merkmale von Organismen bestimmen oder in die Entstehung von Krankheiten involviert sind (König et al. 2021; Sokolova et al. 2024; Wainberg et al. 2018; Zou et al. 2019). Letzteres beinhaltet die Identifizierung vererbter oder (während der Keimzellbildung oder der frühen Embryonalentwicklung) neu entstandener genetischer Varianten, die ursächlich die Ausprägung von Merkmalen oder Krankheiten beeinflussen.⁴

Die meisten mit komplexen Merkmalen oder häufigen Krankheiten assoziierten genetischen Varianten betreffen Genomsequenzen, die keine Proteine kodieren und deren Funktion deshalb besonders schwer zu erkennen und vorherzusagen ist (Halldorsson et al. 2022; Lappalainen/MacArthur 2021). Eine Reihe von Publikationen legt nahe, dass verschiedene DL-Modelle molekulare Funktionen solcher Genomsequenzen bzw. -varianten vorhersagen können (als Übersicht Sokolova et al. 2024; hierzu auch Avsec et al. 2026 und Referenz darin).

Hierzu gehören insbesondere gewebe- und zelltypspezifische Veränderungen im Ablesen von Genen (Avsec et al. 2021, 2026; Sokolova et al. 2023; Zhou et al. 2018) oder die Herstellung verschiedener mRNA-Formen von einem Gen (das alternative prä-mRNA-Spleißen) (Avsec et al. 2026; Jaganathan et al. 2019; Rosenberg et al. 2015; Zeng/Li 2022), aus denen unterschiedliche Proteinformen hergestellt werden. Einige, vor allem neuere, Modelle ermöglichen Vorhersagen zu mehreren unterschiedlichen Funktionen bzw. Effekten von Genomsequenzen und genetischen Varianten (das heißt, sie sind multimodal), wie bezüglich Interaktionen mit genregulierenden Proteinen, dem Ablesen von Genen in verschiedenen Zelltypen, dem Spleißen von prä-mRNAs oder der Interaktion zwischen Genombereichen (Avsec et al. 2021, 2026; Chen et al. 2022; Linder et al. 2025). Solche Modelle wurden auch genutzt, um mutmaßlich ursächliche Varianten für verschiedene Erkrankungen wie neurologische oder immunologische Störungen aufzuzeigen (Jaganathan et al. 2019; Wang et al. 2018; Zhou et al. 2018, 2019). Allerdings wurden in diesen Arbeiten zur Validierung der Vorhersagen keine (Jaganathan et al. 2019; Wang et al. 2018) oder keine solchen funktionellen Experimente durchgeführt, welche die Varianten und ihre vorhergesagten Auswirkungen direkt mit einem Krankheitsphänotyp verknüpfen (Zhou et al. 2018, 2019).⁵

Darüber hinaus wurden DL-Modelle entwickelt, die Effekte von genetischen Varianten in proteinkodierenden Genombereichen auf Funktionen der kodierten Proteine mit einer Genauigkeit vorhersagen können, die der von Einschätzungen basierend auf funktionellen Hochdurchsatzexperimenten für Varianten⁶ entspricht (Brandes et al. 2023; Cheng et al. 2023; Dunham et al. 2023; Frazer et al. 2021). Unter diesen Modellen sind auch ähnlich wie LLMs funktionierende Protein-sprachmodelle („protein language models“)⁷ (Brandes et al. 2023; Dunham et al. 2023; Vieira et al. 2026). Auch für analog zu Proteinsprachmodellen arbeitende große DNA- bzw. Genomsprach-

4 Im Gegensatz zu Varianten, die (über genomweite Assoziationsstudien) nur statistisch mit einer Krankheit assoziiert sind, beeinflussen solche, kausalen genetischen Varianten einen molekularen oder zellulären Prozess, der sich auf eine Krankheit auswirkt (Tam et al. 2019).

5 So wurden die Varianten nicht in das Genom krankheitsrelevanter Zell- oder Tiermodelle eingeführt. Vielmehr wurden die vorhergesagten funktionellen Auswirkungen (z. B. Richtung und Ausmaß der Veränderungen in der Genexpression) durch künstliche Reportergenkonstrukte bestätigt, die in Zelllinien eingeführt wurden (Zhou et al. 2018, 2019).

6 Solche Experimente werden typischerweise für die funktionelle Klassifizierung genetischer Varianten (z. B. als wahrscheinlich pathogene Varianten) verwendet und können die Auswirkungen von sehr vielen Mutationen parallel erfassen, derzeit vor allem in zell-basierten Modellen. Sie werden manchmal allgemein als „multiplex-assays of variant effect“ bezeichnet und umfassen unter anderem „deep mutational scanning“, „massively parallel reporter assays“ und das „saturation genome editing“ (Findlay 2021; Lappalainen/MacArthur 2021).

7 Ähnlich zur menschlichen Sprache lassen sich auch Proteinsequenzen als Abfolgen von Buchstaben darstellen, typischerweise bestehend aus den 20 gängigen Aminosäuren. Des Weiteren setzen sich Proteine in der Regel aus modularen Elementen (Motive, Domänen) zusammen. In dieser Analogie sind gemeinsame Proteinmotive und -domänen, die die grundlegenden strukturellen und funktionellen Bausteine von Proteinen darstellen, mit Wörtern, Phrasen und Sätzen in der menschlichen Sprache vergleichbar und können mit den prinzipiell selben computergestützten Verfahren analysiert und modelliert werden (Ofer et al. 2021; Valentini et al. 2023).

modelle („genome language models“)⁸ konnte gezeigt werden, dass vorhergesagte Effekte kodierender und nichtkodierender genetischer Varianten in Einklang mit Ergebnissen funktioneller Hochdurchsatzexperimente sind (Benegas et al. 2025; Brix et al. 2026; Feng et al. 2025).

Molekülstrukturen und das Verständnis molekularer und zellulärer Prozesse

Für das mechanistische Verständnis molekularer und zellulärer Prozesse und ihrer Beteiligung an Krankheiten (sowie für die Entwicklung von Arzneimitteln; Kapitel 2.3.2) spielen Informationen über die 3D-Struktur biologischer Makromoleküle wie Nukleinsäuren, Proteine und Komplexe solcher Moleküle miteinander oder von Proteinen mit Signalmolekülen (z. B. Hormone, Wachstumsfaktoren) eine wichtige Rolle. Wissen zu entsprechenden Molekülstrukturen hat entscheidend zur Aufklärung von Schlüsselprozessen des Lebens einschließlich der Struktur und Replikation des genetischen Materials, des Ablesens von Genen, der Herstellung von Proteinen, zellulärer Transportprozesse oder von Funktionen des Immunsystems beigetragen (Beck et al. 2024 und Referenz darin).

Solche Strukturen experimentell zu bestimmen, erfordert zeit- und ressourcenaufwendige experimentelle Methoden, wie die Röntgenstrukturanalyse von Kristallen, die magnetische Kernresonanzspektroskopie oder die Kryoelektronenmikroskopie (Carugo/Djinović-Carugo 2023; Dokholyan 2020).

Ein Durchbruch in der computerbasierten Modellierung der 3D-Struktur von Proteinen, basierend auf den die Proteine kodierenden Gen- bzw. Aminosäuresequenzen, konnte mit der Entwicklung und Veröffentlichung von DL-Modellen mit hochgenauer Vorhersagekraft, wie insbesondere AlphaFold2 im Jahr 2021 (Jumper et al. 2021)⁹, erzielt werden (Bertoline et al. 2023; Chen et al. 2024a). Im selben Jahr wurde in einer Partnerschaft zwischen Google DeepMind (dem Unternehmen, welches das Modell entwickelte) und dem EMBL-European Bioinformatics Institute (EMBL-EBI)¹⁰ die AlphaFold Protein Structure Database geschaffen. Diese umfasst über 200 Mio. Einträge zu Strukturvorhersagen menschlicher Proteine und Proteinen von 47 weiteren Organismen, die (ebenso wie das Modell und sein Quellcode) der wissenschaftlichen Gemeinschaft frei zur Verfügung stehen. Darüber hinaus wurden neue Modellierungsmethoden veröffentlicht, die auf Proteinsprachmodellen beruhen. Solche Modelle, wie EMBER2 (Weissenow et al. 2022) oder ESMFold (Lin et al. 2023), können bestimmte Einschränkungen von Modellen wie AlphaFold2 überwinden, die sich hauptsächlich auf Vergleiche mit Sequenzen ähnlicher Proteine („multiple sequence alignments“ – MSA) stützen. Solche Einschränkungen bestehen in Bezug auf die Vorhersage neuartiger Strukturen (das heißt ohne Ähnlichkeiten zu Einträgen in Datenbanken) sowie der relativ langen Rechenzeit, die die Suche nach MSAs in Proteindatenbanken erfordert (Bertoline et al. 2023).

Schließlich wurden Modelle wie AlphaFold 3 (Abramson et al. 2024) oder RoseTTAFold All-Atom (Krishna et al. 2024) vorgestellt, mit denen die 3D-Strukturen von Komplexen aus verschiedenen Molekülen modelliert bzw. vorhergesagt werden können, z. B. von Proteinen mit anderen Protei-

⁸ Ähnlich zu menschlicher Sprache werden bei diesen Modellen Genomsequenzen und DNA-Sequenzmotive, bestehend aus den vier DNA-Nukleotiden, als Abfolge von Buchstaben behandelt.

⁹ Für die Entwicklung dieses bahnbrechenden KI-Modells zur Proteinstrukturvorhersage wurden die Forscher Demis Hassabis und John Jumper von Google DeepMind mit dem Nobelpreis für Chemie im Jahr 2024 ausgezeichnet (The Nobel Prize in Chemistry 2024).

¹⁰ Das EMBL-EBI in Hinxton (UK) ist einer der sechs Standorte des Europäischen Laboratoriums für Molekularbiologie (EMBL), einer zwischenstaatlichen Forschungsorganisation, die von über 20 Staaten finanziert wird.

nen, mit Nukleinsäuren (DNA, RNA) oder mit verschiedenen Liganden wie körpereigenen Signalmolekülen, Metallionen oder niedermolekularen, als Medikamente verwendeten Substanzen¹¹ (Rennie/Oliver 2025 und Referenz darin).

Seit der Einführung solcher KI-basierter Modelle für Proteinstrukturvorhersagen wurden diese bereits in zahlreichen Arbeiten, teilweise in Kombination mit experimentellen Methoden zur Strukturbestimmung, erfolgreich angewendet. Diese Anwendungen reichen von der Charakterisierung viraler Proteine über die Identifizierung oder Charakterisierung von Proteinen, die bei der Entstehung und Bekämpfung von Tumoren oder neurodegenerativen Erkrankungen relevant sein können, bis hin zum Verständnis des Mechanismus, wie Spermien an Eizellen binden (Deneke et al. 2024; Krokidis et al. 2025; Rennie/Oliver 2025 und Referenz darin).

2.3.2 Entwicklung von Medikamenten

Medikamente entwickelnde Unternehmen stehen kontinuierlich vor der Herausforderung, die Effizienz der in der Regel langwierigen, kostspieligen und risikoreichen Prozesse für Forschung und Entwicklung (FuE) neuer Medikamente bis hin zur Marktzulassung (Schlander et al. 2021; Wouters et al. 2020) zu erhöhen (Fernald et al. 2024). Zu den Gründen gehören Einnahmeverluste aufgrund ablaufender Patente von Arzneimitteln, steigende Betriebs- und Rohstoffkosten (z. B. durch Inflation, geopolitische Faktoren, protektionistische politische Maßnahmen) oder der Preisdruck infolge kostenbeschränkter Gesundheits- bzw. Erstattungssysteme (Alsumidaie 2024; GlobalData 2023).

Ein wesentlicher Faktor für die anhaltenden Produktivitätsprobleme der Branche sind hohe Misserfolgs- und Abbruchraten von Medikamentenentwicklungen vor allem in späten (und teuren) Phasen von klinischen Studien¹² (Fernald et al. 2024; Sun et al. 2022). Die hohe Misserfolgsquote bei klinischen Versuchen (über alle Phasen ca. 90 %) (Smietana et al. 2016; Sun et al. 2022) wird oft auf Probleme zurückgeführt, die in frühen Entwicklungsphasen liegen, wie der dort oft nicht belastbar möglichen Validierung von Zielmolekülen oder Identifizierung suboptimaler Eigenschaften von Wirkstoffkandidaten (z. B. Aufnahme, Verteilung oder Giftigkeit im Körper) (Catacutan et al. 2024; Sadybekov/Katritch 2023 und Referenz darin).

Verschiedene KI-gestützte Ansätze können entlang des gesamten FuE-Prozesses eingesetzt werden: von der Identifizierung von Zielmolekülen für Medikamente und der Identifizierung oder dem Design möglichst geeigneter Kandidatenmoleküle für Wirkstoffe (Entdeckungsphase/„drug discovery“) über die mögliche Umwidmung existierender Arzneimittel („drug repurposing“) bis hin zur Planung und Durchführung von klinischen Studien (Zhang et al. 2025b). Die meisten Veröffentlichungen und Informationen zu mithilfe von KI entwickelten Kandidaten für Medikamente

11 Wirkstoffe werden als niedermolekular bezeichnet, wenn ihre Molekülmasse einen bestimmten Wert (800 g·mol⁻¹) nicht übersteigt. Hierzu gehören mehr als 90 % aller Medikamente, darunter Antibiotika (z. B. Penicillin), schmerzstillende oder schmerzlindernde Arzneimittel (z. B. Paracetamol) sowie synthetische Hormone (z. B. Kortikosteroide, die wie Kortisol wirken) (PharmaWiki 2025; Southey/Brunavs 2023).

12 Klinische Studien werden typischerweise in vier Phasen durchgeführt. In Phase 1 werden neue Behandlungen bzw. Medikamente erstmals an Menschen, meist an einer kleineren Gruppe gesunder Proband/innen eingesetzt, um Verträglichkeit und Sicherheit zu untersuchen. In Phase 2 wird ein Medikament dann bei kleineren Gruppen von Patient/innen untersucht, mit dem Ziel die optimale Dosierung zu finden und erste Daten zur Wirksamkeit zu erhalten. In Phase 3 sollen an größeren Patientengruppen möglichst verlässlich Wirksamkeit und Verträglichkeit bestimmt werden. Hersteller können in der Regel erst nach positiven Ergebnissen der Phase 3 die Zulassung für ein Medikament beantragen. Phase 4 beginnt, nachdem ein Medikament zugelassen und auf dem Markt ist. Sie dient vor allem der Beobachtung bzw. Überwachung der routinemäßigen Anwendung der Behandlung, um mögliche auftretende seltenere Nebenwirkungen zu erfassen und darauf gegebenenfalls reagieren zu können (TAB 2023, S. 81 f.).

fokussieren auf bzw. stammen aus Anwendungen von KI-Verfahren in der Entdeckungsphase (Catacutan et al. 2024; Dharmasivam et al. 2026; KP Jayatunga et al. 2024; Sadybekov/Katritch 2023). Dort sollen sie insbesondere helfen, schneller, umfangreicher und kostengünstiger vielversprechende Angriffsziele für Medikamente und/oder aussichtsreiche Wirkstoffkandidaten zu identifizieren.

Verwendet wurden KI-basierte Ansätze bisher vor allem für:

- die *Identifizierung möglicher Zielmoleküle* (z. B. DNA, RNA, Proteine) über spezielle DL-Netzwerke, die Daten zu komplexen Prozessen in Grafenstruktur (Juliensuze 2026) nutzen, um krankheitsbezogene molekulare Muster und potenzielle kausale Zusammenhänge erkennen und mögliche Angriffsziele für Medikamente vorhersagen zu können. Solche von den DL-Netzwerken genutzte Daten stammen vor allem aus Gen- und Proteinnetzwerken (Multi-omics-Daten), zum Teil in Kombination mit über domänenspezifische LLMs ausgewerteter biomedizinischer Literatur (Ren et al. 2025; Zhang et al. 2025b und Referenz darin).
- das *virtuelle Screening (in silico)* von zunehmend großen Substanzbibliotheken (aus existierenden Substanzen oder virtuellen, also computergestützt generierten, synthetisierbaren chemischen Verbindungen) nach möglichen Kandidaten für Wirkstoffe bzw. Medikamente (Catacutan et al. 2024; Sadybekov/Katritch 2023 und Referenz darin). Dazu werden zum einen DL-Modelle, die strukturbasiert das Andocken von Substanzen (Liganden) an ein bestimmtes Zielmolekül vorhersagen können (Bender et al. 2021; Gentile et al. 2022) genutzt, um mit dem Zielmolekül potenziell interagierende Moleküle zu identifizieren. Zum anderen können, unter Verwendung von DL-Modellen zur Quantifizierung von Struktur-Wirkungs-Beziehungen, bestimmte Funktionen oder Eigenschaften von Substanzen, wie eine antibiotische Wirkung (Liu et al. 2023; Stokes et al. 2020), vorhergesagt werden.
- das *De-novo-Design*¹³ von *Arzneimitteln*. Zur Schaffung molekularer Strukturen mit gewünschten Eigenschaften werden insbesondere generative DL-Modelle verwendet (Zhang et al. 2025b). Solche Modelle wurden beispielsweise zur Entwicklung von niedermolekularen Inhibitoren (Ivanenkov et al. 2023; Loeffler et al. 2024; Ren et al. 2025; Schneuing et al. 2024), von antimikrobiellen Peptiden (Pandi et al. 2023) und neuen Strukturen mit Antibiotikawirkung (Krishnan et al. 2025), sowie von funktionellen Proteinen (Notin et al. 2024) wie Impfstoffen (Walls et al. 2020; Wohlwend et al. 2025; Yang et al. 2021; Zhang et al. 2023b), Antikörpern (Bio/Biswas 2025a, 2025b; Shanehsazzadeh et al. 2024) oder neuartigen Gegenmitteln für Schlangengifte (Vázquez Torres et al. 2025) genutzt. Bahnbrechende Arbeiten zur Entwicklung von ersten generativen Modellen (wie RFdiffusion) (Watson et al. 2023), die das Design von komplexen Proteinstrukturen ermöglichen, wurden 2024 mit dem Nobelpreis für Chemie¹⁴ ausgezeichnet (The Nobel Prize in Chemistry 2024). Erste multimodale generative Modelle für das Design von Proteinen, wie das Proteinsprachmodell ESM3 (Callaway 2024a; Hayes et al. 2025), oder von niedermolekularen Substanzen (Deng et al. 2025) können es dabei ermöglichen, Designs mithilfe von Beschreibungen ihrer Eigenschaften und Funktionen in natürlicher Sprache zu spezifizieren (Callaway 2025).

¹³ Dieses zielt darauf ab, Moleküle von Grund auf neu zu entwerfen, die spezifische chemische und pharmakologische Eigenschaften besitzen.

¹⁴ Für seine Arbeiten zum computergestützten Proteindesign erhielt David Baker (University of Washington, USA) den Preis zusammen mit Demis Hassabis und John Jumper (beide Google Deepmind, London, UK), die KI-Modelle entwickelt haben, um die 3D-Struktur von Proteinen hochgenau vorherzusagen (Kapitel 2.3.1).

Darüber hinaus können Modelle Vorhersagen zu Eigenschaften von Wirkstoffkandidaten (Absorption, Verteilung, Metabolismus, Ausscheidung oder Toxizität) machen und so die Auswahl von Substanzen für präklinische Tests und klinische Studien unterstützen oder bei der Syntheseplanung und Automatisierung der Synthese niedermolekularer Wirkstoffe helfen. Generell müssen alle Modellvorhersagen jedoch durch In-vitro-Tests (z. B. Zell- oder Gewebekulturen, Organoide) und/oder In-vivo-Untersuchungen (in Tiermodellen) experimentell validiert werden (Catacutan et al. 2024; Zhang et al. 2025b und Referenz darin).

Eine wachsende Zahl von mit KI entwickelten Kandidaten für Medikamente

Zum Zeitpunkt der Fertigstellung dieses Berichts (Mai 2026) gab es noch kein mit KI-Ansätzen entdecktes bzw. entwickeltes Medikament mit Marktzulassung. In den letzten 5 bis 7 Jahren wurde jedoch eine wachsende Zahl entsprechender Kandidaten für Zielmoleküle und/oder Medikamente beschrieben, die frühe Phasen (vor allem Phase I, aber auch Phase II) klinischer Studien erreicht haben (Dharmasivam et al. 2026; Fu/Chen 2025; KP Jayatunga et al. 2024; Wilczok/Zhavoronkov 2025).

In einer Übersichtsarbeit wurde die Erfolgsrate in klinischen Studien untersucht und gefolgert, dass diese in Phase I deutlich höher (80 bis 90 %) war als der historische Durchschnitt für Medikamente in Phase I-Studien (von maximal 55 bis 65 %); die Erfolgsrate in Phase II von ca. 40 % unterschied sich hingegen nicht vom historischen Durchschnitt (KP Jayatunga et al. 2024). Die Autoren der Studie weisen darauf hin, dass eine solche Erhöhung der Erfolgsrate in Phase I die Gesamtwahrscheinlichkeit für ein Molekül, alle klinischen Phasen erfolgreich zu durchlaufen, von 5 bis 10 % auf etwa 9 bis 18 % erhöhen und damit die FuE-Produktivität insgesamt fast verdoppeln könnte (KP Jayatunga et al. 2024). Kritisch anzumerken bezüglich der möglichen Relevanz dieser Ergebnisse ist die kleine Zahl (24) der untersuchten bzw. verfügbaren klinischen Studien, auf denen die Ergebnisse beruhen (KP Jayatunga et al. 2024; Lowe 2024).

Ob solche KI-basierten Methoden zur Entdeckung von Zielmolekülen und/oder Kandidaten für Medikamente die Entwicklungszeiten, z. B. bis zur Aufnahme klinischer Studien, tatsächlich verringern werden, ist schwer zu beurteilen, da Pharma- und Biotechnologieunternehmen in der Regel keine Angaben zu konkreten Zeitlinien, Kosten oder Erfolgsquoten einzelner Projekte machen (Wilczok/Zhavoronkov 2025). Manche Autoren haben diesen Zeitraum mit bisherigen Verfahren auf um die 2 Jahre (Agrawal et al. 2023) bis ca. 5 Jahre (Jayatunga et al. 2022; Paul et al. 2010) geschätzt. Basierend auf dem Zeitpunkt von Patenten, Veröffentlichungen und öffentlichen Bekanntmachungen schätzten Jayatunga et al. (2022), dass mehrere KI-gestützte Projekte diesen Entwicklungszeitraum in weniger als 4 Jahren durchlaufen haben. In einer kürzlich veröffentlichten Arbeit zur KI-basierten Identifizierung eines neuen Zielmoleküls und eines Medikamentenkandidaten dafür wurden 18 Monate bis zum Beginn klinischer Studien angegeben (Ren et al. 2025; zitiert in Wilczok/Zhavoronkov 2025).

2.3.3 Diagnose und Überwachung von Krankheiten bzw. Krankheitserregern

Klinische Praxis – Diagnose und Vorhersagen zu Risiken und Therapien

KI-Ansätze, die vor allem auf maschinellen Lernverfahren basieren, haben durch die Verknüpfung von Genom- und anderen Omik-Daten mit klinischen Daten (z. B. zu Krankheitsverläufen, Marker-molekülen oder medizinischen Bilddaten) neue Diagnoseverfahren ermöglicht. Hierzu gehört die Diagnose von seltenen genetischen Erkrankungen bei Kindern. Zu diesem Zweck wurden beispielsweise Entscheidungsunterstützungssysteme entwickelt, die mit genetischen Varianten von diagnostizierten Fällen und mit Symptomen der Patient/innen trainiert wurden (Mao et al. 2024) oder die veränderte Gesichtszüge mit Symptomen und genetischen Veränderungen in Genen verknüpfen (Hsieh et al. 2019, 2022).

Ein Beispiel aus der Onkologie sind Ansätze, um in Körperflüssigkeiten wie Blut oder Urin kleinste Mengen von zirkulierender DNA und RNA oder andere von Tumoren bzw. Tumorzellen stammende Bestandteile (z. B. zirkulierende Tumorzellen, Proteine oder von den Tumorzellen abgegebene Vesikel mit Molekülen, wie bestimmte nicht kodierende RNAs) zu analysieren (Flüssigbiopsien) und für Diagnosen nutzen zu können. Diagnosen bzw. belastbare Hinweise für weitere Untersuchungen sollen so bereits sehr früh möglich werden, also bevor größere Tumore oder Metastasen vorhanden sind und ohne oft nur schwierig oder nicht durchführbare Gewebeentnahmen (Biopsien). Darüber hinaus können die Verfahren zum Echtzeitmonitoring der Tumorentwicklung bei Therapien genutzt werden (Ma et al. 2024a; Tivey et al. 2024; Wan et al. 2025). ML-Verfahren sind dabei essenziell, um Genom- und andere Omikdaten (vor allem von bestimmten chemischen Markierungen an der DNA, den Methylierungen, die die Aktivität von Genen mitbestimmen) zu analysieren (Cristiano et al. 2019; Jamshidi et al. 2022; Kim et al. 2023b; Shen et al. 2018; Widman et al. 2024). In den letzten 10 Jahren wurden einige solcher Ansätze für die gleichzeitige Früherkennung mehrerer Krebsarten („multi-cancer early detection“) von prinzipiellen Machbarkeitsstudien (Proof-of-Concept-Studien) hin zu großen klinischen Studien (Fred Hutch Cancer Center 2025; Neal et al. 2022) entwickelt (Wan et al. 2025).

Erregerüberwachung für die Entscheidungsfindung im Bereich der öffentlichen Gesundheit

Die Überwachung von für die öffentliche Gesundheit relevanten Krankheitserregern (z. B. von antibiotikaresistenten Keimen) wird meist routinemäßig in Krankenhäusern, in Abwässern bzw. Kläranlagen (z. B. während der COVID-19-Pandemie) (Levy et al. 2023 und Referenz darin) und in landwirtschaftlichen Betrieben durchgeführt. Das Ziel dieser Überwachung besteht darin, bekannte und neu auftretende Krankheitserreger zu erfassen und Programme zur frühzeitigen Risikominimierung voranzutreiben, um die Gesundheit von Mensch und Tier zu schützen (Ko et al. 2022).

Die Verfügbarkeit relativ kostengünstiger, in automatisierten Hochdurchsatzverfahren einsetzbarer Sequenzierungstechniken („next generation sequencing“; Kasten 2.2) ebnete den Weg für die Entwicklung einer neuen Generation von Methoden bzw. Systemen zur Detektion und Überwachung von Krankheitserregern (Ko et al. 2022; Kraemer et al. 2025; Levy et al. 2023; Venkatesan 2025). Diese beruhen auf der direkten Sequenzierung und Analyse des gesamten genetischen

Materials (also einer Mischung von DNA verschiedener Arten oder Organismen) in Proben aus der Umwelt oder in klinischen Proben (Metagenomik). Im Gegensatz zu bisherigen, auf mikrobiologischen und biochemischen Labortests beruhenden Verfahren müssen somit keine Organismen isoliert bzw. im Labor kultiviert werden und es können auch bislang unbekannte Viren, Bakterien und Pilze detektiert bzw. vorhergesagt werden (Gao/Liu 2024; Ko et al. 2022).

Maschinelle Lernverfahren spielen eine wichtige Rolle, um die komplexen Metagenomdaten zu analysieren und die Präsenz und/oder die Ausbreitung von bekannten oder bislang unbekannten Mikroorganismen schnell erkennen zu können (Gao/Liu 2024; Suster et al. 2024). So können DL-Modelle beispielsweise genutzt werden, um pathogene Bakterien sowie Gene zu identifizieren, die mit antimikrobiellen Resistenzen oder der Pathogenität von Bakterien assoziiert sind (Gupta et al. 2022; de Nies et al. 2021; Rannon et al. 2025). Ebenso können virale Proteine und Viren bzw. Virenfamilien und ihre möglichen Wirtsorganismen über Metagenomdaten identifiziert bzw. vorhergesagt werden (Bartoszewicz et al. 2021; Hou et al. 2024; Zárata et al. 2025).

Darüber hinaus können KI-basierte Modelle genutzt werden, um die Ausbreitung von Erregern wie pandemische Viren sowie Effekte von möglichen Strategien oder konkreten Maßnahmen zu ihrer Bekämpfung und Eindämmung (z. B. Einschränkungen des Reiseverkehrs) besser und schneller vorherzusagen (Kraemer et al. 2025 und Referenz darin; Scoles 2025).

2.3.4 Industrielle Biotechnologie

In der industriellen oder weißen¹⁵ Biotechnologie werden Enzyme¹⁶ (Bornscheuer et al. 2012; Bulter et al. 2023) und Mikroorganismen wie Bakterien oder Hefen (Kim et al. 2023a; Volk et al. 2023) zur Herstellung biobasierter Produkte für verschiedene Anwendungsbereiche genutzt. Dazu gehören die Herstellung von Grundchemikalien für die chemische Industrie oder die Herstellung von Lebensmitteln, Duftstoffen, Waschmitteln und Biokraftstoffen.

Die Um- oder Neugestaltung von Stoffwechselwegen in Mikroorganismen

Insbesondere die Entwicklung von Mikroorganismen, in denen Stoffwechselwege, teilweise unter Verwendung veränderter Enzyme, genetisch gezielt um- bzw. neugestaltet werden („metabolic engineering“) (Kim et al. 2023a; Volk et al. 2023), wurde zu einem wichtigen Anwendungsgebiet der Synthetischen Biologie (Kim et al. 2023a; Nielsen et al. 2022).

Zu bereits industriell hergestellten Produkten durch solche Mikroorganismen gehören aus nachwachsenden Rohstoffen wie Zucker (anstatt aus fossilen Rohstoffen) hergestellte Kunststoffe (de Souza/Gupta 2024), Geschmacks- und Duftstoffe sowie einige Grundchemikalien, wie Milchsäure, 1,3-Propandiol (PDO) und 1,4-Butandiol (BDO) als Ausgangskemikalien für verschiedene industriell relevante Synthesen (z. B. für Kunstfasern, Kunststoffe) (Nielsen et al. 2022). Im Fall von BDO wurde dabei ein Syntheseweg generiert, um eine Substanz, die natürlicherweise von kei-

15 Zu den Farben der Biotechnologie gehören insbesondere die grüne Biotechnologie (vor allem gentechnisch veränderte Pflanzen in der Landwirtschaft) oder die rote Biotechnologie (vor allem Entwicklung von Therapien bzw. Medikamenten).

16 Enzyme sind meist Proteine (aber auch RNA-Moleküle) (Wilson et al. 2016), die in Organismen als Katalysatoren an fast allen chemischen Prozessen beteiligt sind bzw. diese de facto erst ermöglichen. Hierzu gehören zentrale Funktionen wie die Verdoppelung von DNA, das Ablesen von Genen, die Herstellung von Proteinen, die Energiegewinnung in Zellen und jegliche andere Stoffwechsel- bzw. Syntheseprozesse.

nem (bekannten) Lebewesen synthetisiert wird, im Bakterium *Escherichia coli* herzustellen (Geno 2025; Yim et al. 2011). Über Bakterien mit umgestalteten Stoffwechselwegen gelang es in jüngerer Zeit, unter Verwendung von CO oder CO₂ aus Industrieabgasen über die Gasfermentation Chemikalien wie Ethanol, Isopropanol oder Aceton herzustellen (Liew et al. 2022), unter anderem für die Produktion nachhaltiger Flugzeugkraftstoffe (Köpke/Simpson 2020; Liew et al. 2022).

Die Konstruktion solcher neu- bzw. umgestalteter Produktionsstämme von Mikroorganismen – im Fachjargon der Biotechnologie oder Synthetischen Biologie oft „cell factories“ (übersetzt etwa Zellfabriken) genannt (Davy et al. 2017; Nikel/Mattanovich 2021 und Referenz darin) – erfolgt typischerweise nach einem aus dem Ingenieurbereich stammenden, wiederholt durchgeführten (iterativen) Optimierungsschema, das als *Design-Build-Test-Learn*(DBTL)-Zyklus¹⁷ bezeichnet wird:

- Die *Design*phase umfasst die Festlegung von Zielen, die Auswahl eines Ausgangsorganismus, die Verwendung von Modellen und Simulationen und den Entwurf des Organismus mit den gewünschten Eigenschaften.
- In der *Build*phase (Konstruktion) wird der Organismus auf der Grundlage des geplanten Designs mithilfe von gentechnischen Methoden (um)gebaut.
- Die *Test*phase umfasst die eingehende experimentelle Prüfung des Organismus.
- In der *Lern*phase werden die Ergebnisdaten analysiert, mit den gewünschten Eigenschaften und Fähigkeiten verglichen und zur Verfeinerung des Designs für die nächste Runde verwendet.

KI in Form maschineller Lernverfahren wird zunehmend in allen Phasen der Entwicklung mikrobieller Produktionsstämme verwendet. Dazu gehören die Vorhersage von Stoffwechselwegen, die Optimierung und Implementierung gentechnischer Verfahren (z. B. Genomeditierung) und der genetischen Veränderungen, das Protein- bzw. Enzym-Engineering, die Optimierung des Stoffwechsels und der Produktionsbedingungen in Bioreaktoren sowie die Analyse von Testdaten und die Verbesserung von Modellen bzw. des Designs (Goshisht 2024; Kim et al. 2020; Lu et al. 2024; Patra et al. 2023 und Referenz darin). Datengetriebene Modelle, basierend auf maschinellem Lernen einschließlich DL-Modellen, werden dabei meist in Ergänzung bzw. zur Verbesserung mechanistischer Stoffwechselmodelle verwendet, die über detaillierte funktionelle Kartierungen von Genen, Proteinen und Stoffwechselreaktionen zuverlässige Anhaltspunkte für Umprogrammierungen von Stoffwechselprozessen in Zellen liefern können (Lu et al. 2024).

Enzym-Engineering und De-novo-Design von Enzymen

Natürliche Enzyme eignen sich oft nicht für den direkten Einsatz in industriellen chemischen Prozessen (z. B. wegen mangelnder Stabilität oder unpassendem Temperaturoptimum) oder zur Konstruktion effektiver neuer Stoffwechselwege in anderen, bereits industriell verwendeten und gut untersuchten Mikroorganismen. Daher ist ein „Protein-Engineering“ erforderlich, um ihre Eigenschaften für die jeweiligen Anwendungen zu optimieren.

¹⁷ In der Synthetischen Biologie wurden der Begriff und das Schema vor allem im Zusammenhang mit dem „metabolic engineering“ von Organismen entstanden und verwendet (Ogpenorth et al. 2019; Whitford et al. 2021).

Ein weit verbreiteter Ansatz dazu ist die *gerichtete Evolution* („directed evolution“), bei der Mutationen zufällig (und teilweise in großem Maßstab) eingeführt und solche Versionen des Enzyms, die die gewünschte Eigenschaft zeigen, ausgewählt werden, um dann typischerweise weiteren Mutations- und Selektionsrunden unterzogen zu werden (Arnold 2018; Zeymer/Hilvert 2018). Dieses Verfahren ist jedoch immer noch arbeits-, ressourcen- und zeitaufwendig. In den letzten 10 Jahren entstanden zunehmend *rationale oder halbrationale Ansätze* für die Entwicklung oder das Redesign verbesserter Enzymvarianten.¹⁸ Ermöglicht wurden solche Ansätze durch eine größere Verfügbarkeit von strukturellen Daten und mechanistischem Wissen zu Zielenzymen zusammen mit computergestützten Verfahren; sie bleiben jedoch weitgehend auf natürliche Reaktionen und Proteinsequenzen von Enzymen als Ausgangsmaterial beschränkt (Lovelock et al. 2022; Phintha/Chaiyen 2022; Wen et al. 2025).

Große Datensätze zu Proteinsequenzen und -strukturen ermöglichten in jüngster Zeit KI-Modelle (basierend auf generativen Deep-Learning-Verfahren) für die datengetriebene Entwicklung und das Design von (Protein-)Enzymen (Ingraham et al. 2023; Lauko et al. 2025; Watson et al. 2023; Yeh et al. 2023). Hierzu gehören auch Proteinsprachmodelle (Madani et al. 2023; Munsamy et al. 2024) und ein Genomsprachmodell (Nguyen et al. 2024)¹⁹. Über solche generativen Deep-Learning-Verfahren konnten artifizielle Enzyme mit denselben Funktionen wie natürlich vorkommende Enzyme bzw. Enzymfamilien entwickelt werden (z. B. Lysozyme, Luciferasen, Proteasen oder Carboanhydrasen), die teilweise nur wenig Ähnlichkeit in den Aminosäuresequenzen zu diesen aufweisen (hierzu Übersicht Wen et al. 2025). Darunter sind auch erste Enzyme, die bekannte Reaktionen an nichtnatürlichen Substraten wie synthetischen Chemikalien katalysieren (Yeh et al. 2023).

Der Prozentsatz der von den Modellen generierten, oft hunderten oder mehr als tausend Designvorschläge, die dann nach experimenteller Überprüfung tatsächlich – ohne weitere Optimierungsrunden durch gerichtete Evolution – (ausreichend) funktionell sind, ist stark unterschiedlich. Wohl abhängig von unter anderem der Komplexität der katalysierten Reaktion(en) und der dafür erforderlichen aktiven Zentren der Enzyme bewegen sich diese vom niedrigen einstelligen Prozentbereich (Lauko et al. 2025; Yeh et al. 2023) bis hin zu 35 bis 70 % (Madani et al. 2023; Munsamy et al. 2024).

2.3.5 Ansätze für automatisierte Labore und Experimente

Wie in den vorherigen Absätzen beschrieben, erfordern zentrale Anwendungsfelder der Synthetischen Biologie und Biotechnologie, wie insbesondere die Entwicklung von Medikamenten und die Um- oder Neugestaltung komplexer Stoffwechselwege in Mikroorganismen oder von Enzymen, typischerweise immer noch arbeits-, zeit- und ressourcenaufwendige Entwicklungsschritte bzw. iterative Entwicklungsschemata (DBTL-Zyklus, Zyklen von gerichteter Evolution).

Ansätze zur Kombination von automatisierten (robotisierten) Laborprozessen mit automatisierten Hypothesenbildungs- und/oder Designprozessen sowie der Analyse von Ergebnissen der La-

¹⁸ Im Gegensatz zur gerichteten Evolution werden bei rationalen (Design-)Ansätzen typischerweise gezielte (ortsspezifische) Mutationen eingeführt, basierend auf Wissen zu Strukturwirkungsbeziehungen von Proteinen. Semirationale Ansätze kombinieren rationales Design und gerichtete Evolution, um nützliche Varianten durch Mutagenese spezifischer Aminosäuren zu erhalten, die z. B. durch die Analyse einer Kristallstruktur als potenziell relevant identifiziert wurden, gefolgt von einem Screening der Mutanten.

¹⁹ Mithilfe dieses Modells konnten funktionelle Cas9-Nukleasen, als Teil von CRISPR-Cas-basierten Genomeditierungssystemen (Kapitel 2.1), entworfen werden.

borexperimente zielen deshalb darauf ab, diese FuE-Prozesse zu automatisieren bis hin zu „self-driving labs“ (übersetzt etwa selbstfahrende oder autonome Labore) oder „AI scientists“/„robot scientists“ (KI- oder Roboterwissenschaftler) (Adam 2024; Arias/Taylor 2024; Martin et al. 2023).

Cloud Labs und Biofoundries

Grundlage für solche Entwicklungen sind bereits existierende Laborplattformen bzw. komplette Labore und Forschungseinrichtungen, vor allem als Cloud Labs und Biofoundries, die explizit auf automatisierte Arbeiten ausgerichtet wurden (Kasten 2.4).

Während sich Biofoundries oft auf die Automatisierung spezifischer (Teil-)Prozesse zur Generierung von Organismen bzw. von Bioproduktionsansätzen konzentrieren (wie die Herstellung längerer DNA-Abschnitte und/oder deren Einbringen und Funktionsprüfung, z. B. in mikrobiellen Produktionsstämmen), zielen Cloud Labs typischerweise darauf ab, eine flexible automatisierte Laborumgebung bereitzustellen, die für ein breites Spektrum von Forschungsarbeiten und unterschiedliche wissenschaftliche Disziplinen geeignet ist (Arias/Taylor 2024; Jessop-Fabre/Sonnenschein 2019).

Kasten 2.4 Automatisierte Labore: Cloud Labs und Biofoundries

Cloud Labs sind meist kommerzielle Labore, auf die Forschende ferngesteuert über Internetoberflächen zugreifen können. Bei diesem Ansatz spezifizieren die Forschenden Protokolle für ihre eigenen Experimente über Onlineportale der Einrichtungen, die dann in den Laboren automatisiert durchgeführt werden. Die Experimente und Ergebnisdaten können teils in Echtzeit verfolgt bzw. erhalten werden und Experimente können gegebenenfalls in weiteren Runden fortgesetzt werden (Arias/Taylor 2024; Arnold 2022). Des Weiteren können KI-basierte Systeme den Nutzer/innen die Möglichkeit geben, Standardwerte zu verändern und Probleme zu erkennen, die zu einem Abbruch der Experimente führen können (Arnold 2022).

Kommerzielle Cloud Labs zur Durchführung eines breiteren Spektrums von Experimenten sind beispielsweise Emerald Cloud Lab, Inc. (Austin, USA) und Strateos, Inc. (Menlo Park, USA). Daneben existieren kommerzielle Cloud Labs mit spezifischeren Angeboten wie z. B. Culture Biosciences (San Francisco, USA) für Bioprozessentwicklungen von mikrobiellen Produktionsstämmen und Zellkulturen oder Arctoris (Abingdon, UK) mit einem Cloudservice für Prozesse zur Medikamentenentwicklung. Ein erstes akademisches Cloud Lab (entwickelt zusammen mit Emerald Cloud Lab) wurde an der Carnegie Mellon University Pittsburgh (USA) eröffnet (Arias/Taylor 2024; Baracia et al. 2024).

Biofoundries zeigen Ähnlichkeiten zu Cloud Labs, fokussieren aber oft stärker auf spezifische (Teil-)Prozesse von Bioproduktionsansätzen. Sie stellen in der Regel zentralisierte, oft öffentlich finanzierte Einrichtungen dar und sollen Infrastrukturen zur Verfügung stellen, um Forschenden

(oft auch von außerhalb der betreibenden Institutionen) das Design und die Herstellung biologischer Systeme vor Ort oder über die Nutzung von Serviceleistungen zu ermöglichen bzw. den DBTL-Zyklus (Kapitel 2.3.4) zu beschleunigen (Hillson et al. 2019; Holowko et al. 2021). Biofoundries können auch Start-ups und Spin-off-Unternehmen den Zugang zu teurer Infrastruktur ermöglichen (Farzaneh/Freemont 2021).

Weltweit gibt es eine Reihe akademischer und kommerzieller Biofoundries. In der Global Biofoundries Alliance sind mehr als 30 nicht kommerzielle solcher Einrichtungen als Mitglieder verzeichnet. Hierzu gehören etwa die Australian Genome Foundry (Australien), die London Biofoundry (UK), das SynCTI Forschungszentrum (Singapur) oder die Illinois Biological Foundry for Advanced Biomanufacturing (iBioFAB) der University of Illinois (USA). Mitglieder aus Deutschland sind beispielsweise die Jülich Biofoundry oder das SynDNA Lab der Universität Heidelberg. Ein Beispiel für ein kommerzielles Unternehmen, das seit längerem Biofoundry-Dienste für verschiedene Prozesse – einschließlich der Entwicklung mikrobieller Produktionsstämme oder Säugetierzelllinien – und seit Kurzem auch eine online nutzbare Cloud-Lab-Plattform anbietet, ist Ginkgo Bioworks (Boston, USA).

Self-driving-Labore und Roboterwissenschaftler

In den letzten ca. 10 Jahren wurden erste Systeme von Self-driving-Laboren oder Roboterwissenschaftlern zur Beschleunigung der Synthese und Herstellung chemischer Substanzen (z. B. komplexer organischer Verbindungen, Medikamentenkandidaten) oder Materialien (z. B. Kohlenstoffnanoröhren) entwickelt (Martin et al. 2023; Tobias/Wahab 2025; Tom et al. 2024 und Referenz darin). Kürzlich wurden flexible KI-Agenten-Systeme²⁰ beschrieben, die durch die Kombination von LLMs und anderer computergestützter Modelle miteinander sowie mit automatisierten Laborplattformen in der Lage sind, unterschiedliche Aufgaben zu erfüllen. Hierzu gehören der Entwurf von Synthesen für bekannte organische Verbindungen, einschließlich Arzneimittel, die Durchführung und Optimierung von Synthesen für neue Verbindungen mit ähnlichen Eigenschaften zu bekannten Substanzen, oder die Optimierung der Herstellung von Proteinen in zellfreien Systemen (Boiko et al. 2023; Bran et al. 2024; Smith et al. 2026). Bei manchen Systemen wurden die automatisierten experimentellen Schritte über die kommerziellen Plattformen Emerald Cloud Lab (Boiko et al. 2023) und Ginkgo Cloud lab (Smith et al. 2026) durchgeführt.

In der Biologie wurden solche halbautonomen und autonomen Systeme zur Identifizierung oder Funktionsbestimmung von Genen in Hefe erstmals vor mehr als 10 Jahren entwickelt (Coutant et al. 2019; King et al. 2004, 2009).

Im Zusammenhang mit der Umgestaltung mikrobieller Synthesewege entwickelten HamediRad (2019) ein Self-driving-System für DBTL-Zyklen (Kapitel 2.3.3), um die Produktionsleistung eines sehr einfachen (nur aus drei Genen bestehenden), in das Bakterium *E. coli* übertragenen Stoff-

²⁰ Als KI-Agenten gelten Softwaresysteme, die mithilfe von KI Ziele verfolgen und Aufgaben im Auftrag von Benutzern erledigen. Sie verfügen über logisches Denken, Fähigkeiten wie Planung und Gedächtnis und haben ein gewisses Maß an Autonomie, um Entscheidungen zu treffen, zu lernen und sich anzupassen (Google Cloud 2025).

wechselwegs zur Herstellung von Lycopin²¹, zu optimieren. Ein auf maschinellen Lernverfahren basierendes Vorhersagemodell zur Auswahl von Sequenzen für das Ablesen der Gene steuerte die Experimente, die über eine automatisierte Laborplattform der Biofoundry Illinois Biological Foundry for Advanced Biomanufacturing (iBioFAB) ausgeführt wurden.

Ein erstes autonomes System für das Protein- oder Enzym-Engineering wurde von Rapp et al. (2024) beschrieben. Dieses System kombiniert einen KI-Agenten mit einer robotisierten Laborplattform und ist in der Lage, Proteinsequenz-Funktions-Beziehungen aus Daten zu lernen, Entwürfe für neue Proteine mit veränderten Funktionen zu generieren sowie diese zu testen und zu optimieren. Mit der physischen Welt ist es durch eine vollautomatische Laborplattform (des kommerziellen Strateos Cloud Labs, Kasten 2.4) gekoppelt, über das die entworfenen Proteine experimentell getestet werden. Dazu werden Gene durch die Kombination vorsynthetisierter DNA-Fragmente (entsprechend den Vorhersagen bzw. dem Design des KI-Agenten) zusammengesetzt, davon zellfreie Proteine hergestellt und biochemische Messungen der Enzymaktivität durchgeführt. Das KI-System ermöglicht so autonome DBTL-Zyklen zum Verständnis und zur Optimierung von Enzymfunktionen. Rapp et al. (2024) demonstrierten die Fähigkeit des Systems, bestimmte Enzyme (Glycosidhydrolasen) mit erhöhter Hitzetoleranz zu generieren.

Mit demselben oder ähnlichen Ansätzen könnten prinzipiell auch die Aktivität und Spezifität von Enzymen oder neuartige chemische Reaktionen „autonom“ entwickelt werden. Ein solches, potenziell generell anwendbares automatisiertes System für das Engineering der Aktivität bzw. Spezifität von Enzymen wurde kürzlich publiziert. Es integriert eine sprachgesteuerte Benutzeroberfläche mit einem großen Proteinsprachmodell (ESM2, Lin et al. 2023) zur Vorhersage potenzieller Enzymvarianten und einer robotisierten Biofoundry-Plattform, um diese zu testen und die erhaltenen Versuchsdaten zur Verbesserung der folgenden Designrunden zu verwenden (Singh et al. 2025).

21 Lycopin (oder Lycopen) gehört zu den Carotinoiden und stammt meist aus Tomaten, wo es in hohen Konzentrationen vorkommt. Traditionell wurde es als roter Lebensmittelfarbstoff eingesetzt (EFSA 2008). Es hat antioxidative Wirkung (Radikalfänger) und wird zur Vorbeugung verschiedener Erkrankungen diskutiert (Saini et al. 2020; Shafe et al. 2024).

3 Mögliche Risiken für die Biosicherheit und Proliferation biologischer Waffen durch das Zusammenspiel von KI und molekularbiologischer bzw. biotechnologischer Entwicklungen

- 3.1 Die Synthetische Biologie ist seit ihren Anfängen von Diskussionen zur Biosicherheit begleitet worden – einschließlich der möglichen Herstellung von Biowaffen
- 3.2 Das Zusammenspiel von KI mit molekularer Biologie und Biotechnologie hat zu einer neuen Diskussion über Biosecurity-Risiken und Biowaffen geführt
- 3.3 Potenzielle neue oder erleichterte Möglichkeiten des Missbrauchs von Biotechnologie durch KI: Worauf begründen sich die vorgebrachten Befürchtungen?
- 3.4 Implikationen der neuen technischen Möglichkeiten für Bedrohungen durch Biowaffen

3 Mögliche Risiken für die Biosicherheit und Proliferation biologischer Waffen durch das Zusammenspiel von KI und molekularbiologischer bzw. biotechnologischer Entwicklungen

3.1 Die Synthetische Biologie ist seit ihren Anfängen von Diskussionen zur Biosicherheit begleitet worden – einschließlich der möglichen Herstellung von Biowaffen

Mit der in den frühen 2000er Jahren entwickelten Vision der Synthetischen Biologie (Kapitel 2.1), in der biologische Systeme oder Organismen nach Prinzipien der Ingenieurwissenschaften vorhersagbar und (zunehmend) einfacher um- bzw. neugestaltet werden können („make biology easier to engineer“²²) (Endy 2005), waren von Anfang an Diskussionen um Risiken der Biosicherheit (Kasten 3.1) verknüpft (Jefferson et al. 2014b; Schmidt 2008; Service 2006; TAB 2015 und Referenz darin). Diese wurden nicht zuletzt aus dem Feld selbst angestoßen (Church 2004; Endy 2007; Garfinkel et al. 2007; Service 2006).

Kasten 3.1 Biosicherheit – Biosafety und Biosecurity

Im englischen bzw. internationalen Sprachgebrauch werden Risiken im Zusammenhang mit biologischen Agenzien, wie Pathogene (z. B. Bakterien, Viren) oder Giftstoffe (Toxine), sowie der Umgang mit diesen Risiken in zwei Bereiche unterteilt: Biosafety und Biosecurity (Beeckman/Rüdelsheim 2020; Chinchilla et al. 2024; National Research Council 2009; WHO 2020, 2024a). Im deutschen Sprachgebrauch wird der Begriff Biosicherheit²³ meist als Überbegriff für beide Bezeichnungen benutzt, zur Differenzierung werden die englischen Begriffe Biosafety und Biosecurity verwendet (Auswärtiges Amt o. J.b; Deutscher Ethikrat 2014; GO4GHP o. J.).

Zwar gibt es keine vollkommen einheitliche Definition für die Begriffe Biosafety und Biosecurity, im Allgemeinen werden die so bezeichneten Bereiche aber, häufig unter Bezugnahme auf entsprechende Dokumente der WHO (2020, 2024a), durch ihre Ziele unterschieden:

²² Übersetzt etwa Biologie einfacher konstruierbar oder manipulierbar machen.

²³ Der Begriff Biologische Sicherheit ist dagegen ein Rechtsbegriff, der auf das Gentechnikgesetz zurückgeht und sich auf das sichere Arbeiten und den Umgang mit gentechnisch veränderten Organismen (im Sinne von Biosafety) bezieht.

Biosafety: Arbeitsschutz sowie Schutz der Öffentlichkeit und der Umwelt vor nicht beabsichtigten Schäden

Bei Biosafety geht es um Grundsätze, Technologien und Praktiken, um die *unbeabsichtigte* Exposition gegenüber biologischem Material und mögliche Schäden zu verhindern, beispielsweise für die Gesundheit von Beschäftigten in Laboratorien oder die öffentliche Gesundheit sowie die Umwelt durch versehentliche (z. B. durch Laborunfälle) oder beabsichtigte Freisetzungen im Rahmen genehmigter Aktivitäten im Freiland (z. B. gezielte Freisetzungsexperimente).

Biosecurity: Schutz vor Diebstahl, Verlust, Missbrauch oder der Nutzung als militärische Waffen

Biosecurity umfasst Grundsätze, Technologien und Praktiken, die *absichtlich herbeigeführte* Schäden durch missbräuchliche Nutzungen von biologischen Agenzien und/oder von Ausrüstung, Fähigkeiten und Daten für solche Nutzungen verhindern können. Missbräuchliche Nutzungen können beispielsweise bewusste Freisetzungen biologischer Agenzien wie Bakterien, Viren oder Toxine für kriminelle und terroristische Zwecke sein oder deren Nutzung als militärische Waffen.

Unterschiedliche Ziele – sich ergänzende Ansätze

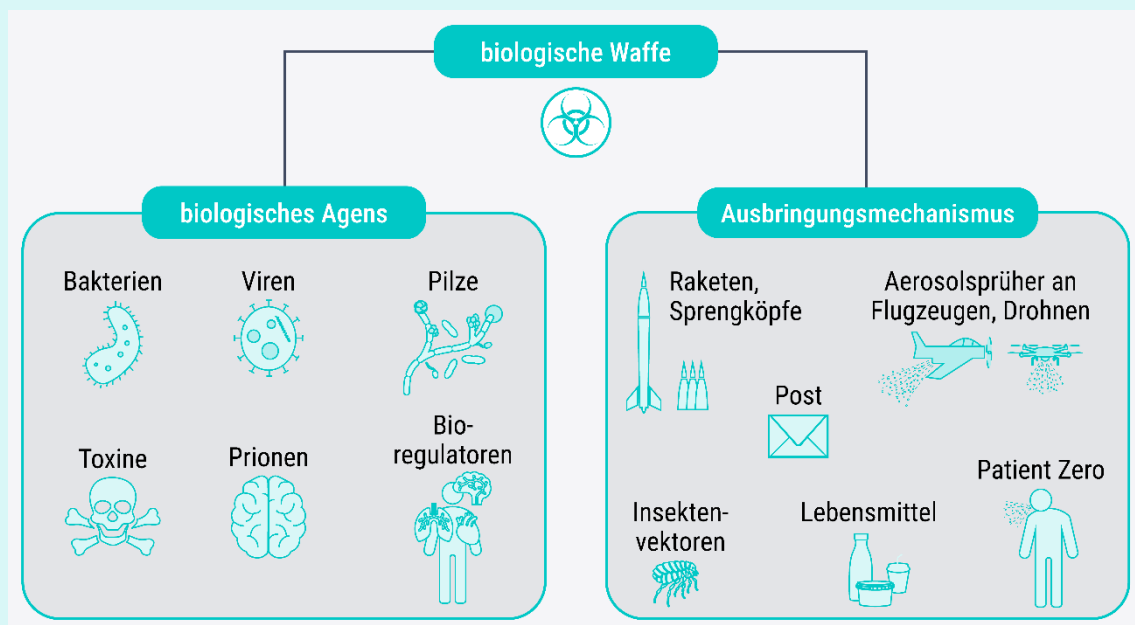
Obwohl die Zielsetzungen von Biosafety und Biosecurity unterschiedlich sind, ergänzen sich die beiden Bereiche, indem sie teilweise überlappende Ansätze bzw. Regelungen umfassen. Hierzu gehören etwa Bestandteile des biologischen Risikomanagements, wie die Risikobeurteilung, die Zugangskontrolle zu und Arbeitsschutzmaßnahmen in Laboratorien, um die Gefahr ungewollter oder gewollter Kontaminationen von Beschäftigten zu verhindern, Maßnahmen gegen den Verlust entsprechender Agenzien aus Laboren (z. B. über dokumentierte und gesicherte Lagerung), oder Regelungen zum Transport bzw. Im- oder Export biologischer Agenzien (Beeckman/Rüdelshiem 2020; WHO 2024a).

Neben Risiken für die Gesundheit oder die Umwelt, die im internationalen Sprachgebrauch meist durch den Begriff *Biosafety* erfasst werden, wurden insbesondere auch Biosicherheitsrisiken im Zusammenhang mit der Möglichkeit diskutiert, dass die Synthetische Biologie den Zugang zu und den Missbrauch von biologischen Agenzien als Biowaffen (Kasten 3.2) erleichtern könnte, etwa für kriminelle, terroristische oder militärische Zwecke. Diese Biosicherheitsrisiken werden in der Regel unter dem Begriff der *Biosecurity* behandelt.

Kasten 3.2 Biologische Waffen (Biowaffen)

Nach der Definition des United Nations Office for Disarmament Affairs (UNODA o. J.a) verbreiten *biologische Waffen* krankheitsauslösende Organismen oder Toxine, um Menschen, Tiere oder Pflanzen zu schädigen oder zu töten. In der Regel bestehen sie aus zwei Teilen: einem in eine waffenfähige Form gebrachten biologischen Agens („weaponized agent“) und einem Mechanismus zu dessen Ausbringung („delivery mechanism“) (Abbildung 3.1).

Abbildung 3.1 Biowaffen bestehen aus einem biologischen Agens und einem Ausbringungsmechanismus



Quelle: verändert nach Sabra/Frieß (2025)

Geeignete *biologische Agenzien* können Organismen wie Bakterien oder Pilze, Viren sowie Moleküle, wie infektiöse Prionen²⁴, oder Toxine (Gifte aus Tieren, Pflanzen oder Mikroorganismen oder ähnliche synthetisch hergestellte Substanzen) sein, die Infektionskrankheiten oder Vergiftungen auslösen. Sie können modifiziert werden, um sie für die Massenproduktion, Lagerung oder Ausbringung über entsprechende Mechanismen bzw. Systeme besser geeignet (waffenfähig) zu machen (UNODA o. J.a). Solche Agenzien werden auch als biologische Kampfstoffe bezeichnet (Richardt/Russmann 2006; Richter 2011). Historische staatliche Biowaffenprogramme

²⁴ Fehlgefaltete Formen bestimmter Proteine (Prionenproteine), die normale solche Proteine veranlassen dieselbe abnormale Struktur anzunehmen. Sie verursachen bestimmte übertragbare neurodegenerative Erkrankungen wie Scrapie (bei Schafen und Ziegen), bovine spongiforme Enzephalopathie (BSE, bei Rindern und Menschen) oder Formen der Creutzfeldt-Jakob-Erkrankung (bei Menschen) (Houston/Andréoletti 2019; Prusiner 1998; Zerr et al. 2024).

(Kasten 3.3) verfolgten unter anderem die Herstellung und Nutzung von Krankheitserregern, darunter Anthrax, Maul- und Klauenseuche, Pest, Pocken, Q-Fieber oder Reisbrand, sowie von Toxinen, wie Aflatoxin, Botulinumtoxin oder Rizin. Darüber hinaus entwickelten manche Länder auch nicht tödliche Substanzen, die Personen vorübergehend außer Gefecht setzen sollen. Hierzu zählen Bioregulatoren, die von Organismen gebildet werden und physiologische Funktionen wie Blutdruck, Körpertemperatur oder Immunreaktionen regulieren oder auch Bewusstsein und Stimmungen beeinflussen. In sehr großen Mengen zugeführt, können diese aber auch toxische Wirkungen entfalten und de facto zu starken Toxinen werden (Crowley/Dando 2024).

Die Ausbringungsmechanismen von Biowaffen können vielfältig sein.²⁵ So wurden im Rahmen früherer Biowaffenprogramme beispielsweise ballistische Raketen bzw. Sprengköpfe, Insektenvektoren²⁶ (z. B. Flöhe) oder Sprühhvorrichtungen, die an Flugzeuge oder Fahrzeuge montiert wurden, genutzt (Kasten 3.3). Darüber hinaus stellen Drohnen, einschließlich kommerziell erhältlicher Sprühdrohnen für die Landwirtschaft, eine Option dar (Hummel 2025; Lambert 2020).²⁷ Für terroristische Anschläge bzw. Anschlagversuche wurden auch der Postweg (Briefe) oder Lebensmittel genutzt (Kasten 3.4, Kapitel 3.4). Viren, z. B. zur Auslösung einer Pandemie, könnten prinzipiell auch durch einen infizierten Menschen bzw. Attentäter („patient zero“) verbreitet werden (Kapitel 3.4).

Die Veränderung von Agenzien, um sie waffenfähig zu machen, sowie die Kombination der Agenzien mit geeigneten Ausbreitungssystemen zur Herstellung funktioneller und effektiver biologischen Waffen wird auch als „weaponization“ (übersetzt etwa Verwaffnung) bezeichnet. Diese Prozesse sind Teil von typischerweise mehrstufigen, komplexen Herstellungsprozessen in Biowaffenprogrammen (Abbildung 3.2, Kapitel 3.2.2).

Zentrale Punkte für die in diesem Bericht im Mittelpunkt stehende Biosecurity-Problematik waren und sind bis heute (NAS 2018; TAB 2015) (Kapitel 3.2.1):

- Die einfachere Herstellung von und damit der potenziell leichtere Zugang zu natürlich vorkommenden Pathogenen oder veränderten bzw. neuen Pathogenen, die als biologische Kampfstoffe bzw. der Herstellung von Biowaffen (Kasten 3.2) verwendet werden können. Hierzu gehören insbesondere die Herstellung von Viren über DNA-Synthese- und Assemblierungstechniken zur Generierung synthetischer Genome. Dieser Diskussionspunkt geht zurück auf und wurde immer wieder befeuert durch Arbeiten, bei denen bekannte Viren ausgehend von syn-

25 Manche Autoren unterteilen diese Komponente von Biowaffen in Trägersysteme, wie Flugzeuge, Raketen oder ein infizierter Organismus, und Ausbringungsmechanismen (in einem engeren Sinne), wie beispielsweise Explosivstoffe oder Spraysysteme (Richardt/Russmann 2006).

26 Als Vektoren werden Organismen bezeichnet, die Krankheitserreger von einem infizierten Tier oder Menschen auf andere Menschen bzw. Tiere übertragen.

27 Beispielsweise nutzte der Islamische Staat im Irak und Syrien (ISIS) mindestens seit Mitte der 2010er Jahre selbstgebaute und kommerziell erhältliche Drohnen, vor allem zur Aufklärung und Zielerfassung gegen die Koalitionsstreitkräfte, und zeigte Interesse an der Durchführung von drohnenbasierten Angriffen mit chemischen oder biologischen Kampfstoffen (Hummel 2016, S. 34f.; Lambert 2020). Kriminelle Banden in China nutzten Drohnen zur weiteren Ausbreitung der Afrikanischen Schweinepest über den Abwurf von Fleisch infizierter Tiere (Rogers 2021; The Japan Times 2019). Das Ziel war wohl, verzweifelte Landwirte zum Billigverkauf von infiziertem Fleisch zu bewegen, das von den Banden dann als nicht infiziertes Produkt weit entfernt vom Ursprungsort weiterverkauft wurde (Rogers 2021).

thetisierten DNA-Sequenzen bzw. Genomen hergestellt wurden.²⁸ Darunter waren das Poliovirus (Cello et al. 2002), das Virus der verheerenden Grippepandemie von 1918 (Tumpey et al. 2005), das zum menschlichen Pockenvirus verwandte Pferdepockenvirus (Noyce et al. 2018) oder Coronaviren, wie ein SARS-ähnliches Virus aus Fledermäusen (Becker et al. 2008) und das SARS-CoV-2-Virus (Thi Nhu Thao et al. 2020).

- *Die Veränderung von Eigenschaften von Pathogenen, um diese gefährlicher zu machen, durch genetische Veränderungen, die etwa zur Erhöhung der Pathogenität führen oder die Bekämpfung von Infektionen (z. B. durch antimikrobielle Substanzen oder Impfstoffe) erschweren können.* Die Diskussion hierzu nahm zu Beginn der 2010er Jahre Fahrt auf (TAB 2015, S. 117 ff.). Auslöser waren zwei Arbeiten mit Vogelgrippeviren (H5N1), die durch gezielte Mutationen, Selektion oder Rekombination von viralen Genomabschnitten im einschlägigen Säugetiermodell für Grippeviren (Frettchen) ähnlich einer saisonalen menschlichen Grippe über Tröpfcheninfektion durch die Luft übertragbar waren (Herfst et al. 2012; Imai et al. 2012).
- *Die Herstellung von Toxinen²⁹ über die Um- bzw. Neugestaltung von Stoffwechselwegen in Mikroorganismen* (Kapitel 2.3.4). Hierdurch könnten auch chemisch komplexe, nicht aus Proteinen bzw. Peptiden³⁰ bestehende Toxine, die als biologische Kampfstoffe genutzt werden könnten (Anderson 2012; Pitschmann/Hon 2016), in einfach(er) kultivierbaren biotechnologischen Standardorganismen (z. B. dem Bakterium *E. coli* oder Hefen) hergestellt werden. Sie könnten auf diese Weise mit höherer Ausbeute bzw. stärker konzentriert erhalten werden. Grundlage solcher Befürchtungen sind Veröffentlichungen zur Übertragung auf bzw. der (Teil-)Konstruktion in *E. coli* bzw. Bäckerhefe von komplexen Synthesewegen, wie zur Herstellung des Pflanzenstoffes (und Chemotherapeutikums) Taxol (Paclitaxel) (Ajikumar et al. 2010; Liang et al. 2025) oder von Opioiden (Galanie et al. 2015). Darüber hinaus könnte die Generierung neuer oder veränderter (Protein-)Toxine über Protein- bzw. Enzym-Engineering-Methoden (Kapitel 2.3.4) erfolgen.
- Die Zugänglichkeit von Synthetischer Biologie bzw. Biotechnologie und damit die zuvor genannten Möglichkeiten zunehmend auch für Personen, die keine oder wenig fachliche Kenntnisse haben und nicht in etablierte und registrierte öffentliche oder private wissenschaftliche Einrichtungen eingebunden sind. Diese Befürchtung basiert auf der Annahme, dass die methodischen und technischen Fortschritte (Kapitel 2.1) ressourcenaufwendige Laborarbeiten, eine spezielle Ausbildung und Erfahrungswissen (einschließlich taciten Wissens; Kapitel 3.2.2) überflüssig machen oder deren Wichtigkeit zumindest stark verringern können (manchmal auch als „deskilling“ bezeichnet) (Jefferson et al. 2014b und Referenz darin).

28 Diese Arbeiten hatten zum Ziel, die Mechanismen der Pathogenität oder den Ursprung der Viren besser zu verstehen sowie Möglichkeiten zur Infektionsbekämpfung (z. B. Impfungen) zu verbessern.

29 Als Toxine gelten in der Regel Moleküle, die von biologischen Systemen produziert werden und für Menschen oder andere Tiere schädlich sind.

30 Peptide bestehen wie Proteine aus Aminosäureketten. Diese sind bei Peptiden jedoch deutlich kürzer und bestehen typischerweise aus zwei bis 50 Aminosäurebausteinen (Forbes Kaprive/Krishnamurthy 2026). Proteine hingegen setzen sich oft aus Ketten von mehreren hundert bis zu teilweise 2.000 Aminosäuren zusammen (Nevers et al. 2023).

Biotechnologie wird für alle nutzbar: eine Vision, die bisher nur sehr begrenzt Realität wurde

Insbesondere die Möglichkeit einer zunehmend schnelleren und breiteren Zugänglichkeit und Nutzung von Biotechnologie durch Personen ohne spezielle Ausbildung oder Fachwissen – ermöglicht durch neue Techniken und Methoden der Synthetischen Biologie, die Fachkenntnisse und Erfahrungswissen überflüssig machen könnten – war von Anfang an sowohl mit Hoffnungen in Bezug auf Innovationen und Innovationskultur (Garagen-Biotech, Do-it-yourself[DIY]-Biologie) (Eireiner 2025b; Ledford 2010; TAB 2015, S.228ff.) als auch mit Befürchtungen eines Missbrauchs der Synthetischen Biologie (Jefferson et al. 2014b; TAB 2015; UNICRI 2012 und Referenz darin) verbunden. Eine genauere Betrachtung von Untersuchungen und Daten lässt es jedoch zumindest bisher fraglich erscheinen, dass solche Personen ohne die Unterstützung von Akteuren mit entsprechender Ausbildung und Wissen Biotechnologie bzw. Synthetische Biologie tatsächlich im Sinne dieser Hoffnungen oder Befürchtungen erfolgreich anwenden können. Hierfür notwendige Projekte, wie zur Herstellung bzw. Veränderung funktioneller biologischer Moleküle oder Organismen, erfordern über die bloße Ausführung einzelner Laborarbeitsschritte und Erfahrungen im Umgang mit den jeweiligen Organismen hinaus auch die Koordination und Integration verschiedener Arbeitsschritte und oft multipler Fähigkeiten in einen durchgängigen Arbeitsablauf und in ein Gesamtprojekt. Hierzu gehören etwa Überprüfungen von Zwischen- und Endprodukten, gegebenenfalls auch in Tierversuchen, sowie die Fehlersuche und die Anpassung von Prozessen.

So legen es Daten zu den Zeiträumen, die vergehen, bis eine Technik bzw. Methode über das Ursprungslabor hinaus von anderen Laboren oder in Universitäten und weiterführenden Schulen praktisch gelehrt bzw. verwendet werden, zwar nahe, dass sich Methoden der Molekularbiologie oder Biotechnologie, wie insbesondere Genomeditierung durch CRISPR-Cas, durchaus zunehmend schnell verbreitet haben bzw. breit(er) zugänglich wurden (Jackson et al. 2019). Inwieweit die Verwendung von Methoden im Rahmen von Praktika oder ähnlichen Aktivitäten an Universitäten oder Schulen (Menard et al. 2024) als belastbarer Hinweis oder gar Beleg für die erfolgreiche Anwendung von Biotechnologie bzw. Synthetischer Biologie durch Personen ohne entsprechende Ausbildung angesehen werden kann (Jackson et al. 2019), ist jedoch zweifelhaft. Auch wenn Methoden in einfachen Experimenten (oft zellfrei, also ohne Organismen wie Bakterien) unter Verwendung von für diesen speziellen Zweck zusammengestellten und getesteten Reagenzienkits (Menard et al. 2024) sowie unter Anleitung durchgeführt werden können, lässt dies keine Rückschlüsse auf die erfolgreiche Durchführung – mit und noch weniger ohne Anleitung – von anderen Experimenten (und gegebenenfalls mit anderen Organismen) oder gar der produktiven Anwendung in komplexeren Prozessketten oder Projekten zu.

Fragen bezüglich der erfolgreichen Nutzung von Biotechnologie ohne entsprechende Erfahrung bzw. Wissen in komplexeren Projektzusammenhängen werfen auch Daten und Erkenntnisse zum iGEM-Wettbewerb³¹ („international Genetically Engineered Machines“ competition) und zur DIY-Biologie auf, die beide zum Inbegriff der Hoffnungen und Befürchtungen der Entwicklung hin zu einer (nutzbaren) Biotechnologie für alle wurden (Eireiner 2025b; Jefferson et al. 2014b und Referenz darin). So zeigen systematisch erhobene Daten zum iGEM-Wettbewerb, dass Leistungen und der Erfolg von iGEM-Teams insbesondere mit der Zahl der Instruktoren und Berater – also

31 Der iGEM-Wettbewerb richtet sich weltweit im Bereich der Synthetischen Biologie an Schüler, Studierende und Promovierende. Teilnehmen können aber auch Mitglieder aus DIY-Communitylaboren.

fachlich erfahrenen Personen von den die Teams betreuenden Institutionen, die Anleitung und technische bzw. praktische Unterstützung geben, ohne selbst Arbeiten in dem Projekt auszuführen³² – sowie der Erfahrung der studentischen Teammitglieder korrelieren (Santolini et al. 2023). Auch bei Aktivitäten oder Projekten aus der DIY-Biologie-Community ergeben sich entsprechende Fragen. So ist die DIY-Biologie-Bewegung zum einen nicht völlig unabhängig von traditionellen Forschungseinrichtungen, sondern die Beziehung der Bewegung zu Wissenschaft und Industrie ist häufig durch verschiedene Verflechtungen gekennzeichnet, insbesondere durch frühere oder aktuelle Beschäftigungsverhältnisse oder Ausbildungsgänge (Eireiner 2025b). Rund drei Viertel befragter Personen aus der Bewegung haben einen akademischen Abschluss in Naturwissenschaften oder streben einen solchen an, ein Drittel hat einen Abschluss in Biowissenschaften oder Biochemie und mehr als 40 % ordnen sich beruflich dem Bereich Biotechnologie zu (Eireiner 2025a, 2025b). Insbesondere in öffentlichen DIY-Laboren (Communitylaboren) sind diese Personen wichtig, weil sie ihre Erfahrungen an andere Mitglieder weitergeben (De Lange et al. 2022). Zum anderen sind Projekte der DIY-Bewegung, die oft als Vorzeigeobjekte oder Erfolgsgeschichten gelten, stark mit dem Wissen und der Erfahrung der daran beteiligten Personen verknüpft – sei es direkt oder über Berater oder Kollaborationen. Beispiele hierfür sind das Open Insulin Project (Burningham 2019; P2P Foundation 2025) und das Projekt „Open Bioeconomy“ (Open Bioeconomy Lab 2025).

3.2 Das Zusammenspiel von KI mit molekularer Biologie und Biotechnologie hat zu einer neuen Diskussion über Biosecurity-Risiken und Biowaffen geführt

Mit der zunehmend wichtigeren Rolle von KI und deren Zusammenspiel mit der molekularbiologischen Forschung, der Synthetischen Biologie bzw. der Gen- und Biotechnologie (Kapitel 2.2, 2.3) – oft auch kurz als „KlxBio“ bezeichnet – hat sich international seit 2 bis 3 Jahren eine neue Sicherheitsdiskussion entwickelt, die stark auf Biosecurity-Risiken und Fragen der nationalen Sicherheit fokussiert (Adamson/Allen 2025; Baker/Church 2024; Bloomfield et al. 2024, 2026; Callaway 2024b; Carter et al. 2023, 2024a; NAS 2025b; Nelson/Rose 2023; Pannu et al. 2025). Diese Diskussion wurde auch (einschließlich in Deutschland) in der allgemeinen Presse aufgegriffen (Bordelon 2023; Dance 2026; Griffin 2024; Heller 2024; Herden/Göpel 2026; Perrigo 2024; The Economist 2026).

32 Die Teams bestehen aus den studentischen aktiven Mitgliedern, die das Projekt durchführen, und erfahrenen Forschenden wissenschaftlicher Institutionen, die das Team anleiten und betreuen (<https://blog.igem.org/blog/2022/4/6/anatomy-of-an-igem-team>; <https://competition.igem.org/about/starting-a-team>; 30.6.2026).

3.2.1 Zentrale Punkte der neuen Sicherheitsdebatte

Im Mittelpunkt der Debatte um derzeitige und mögliche zukünftige Entwicklungen beim Zusammenspiel von KI und Biotechnologie stehen vor allem drei Punkte bzw. Bedenken:

1. dass die Entwicklungen es insbesondere nicht staatlichen Akteuren bzw. Nichtexpert/innen erleichtern, also die Hürden senken könnten, gefährliche biologischen Agenzien zu erhalten oder herzustellen sowie Biowaffen zu entwickeln und zu verbreiten – einschließlich solche mit Massenvernichtungspotenzial;
2. dass die Entwicklung noch gefährlicherer bzw. neuer solcher Agenzien und Biowaffen möglich wird, die das Schadenspotenzial oder -ausmaß erhöhen könnten, und
3. dass die Wirksamkeit von Biosicherheits- und Abwehrmaßnahmen verringert oder unterlaufen werden könnte.

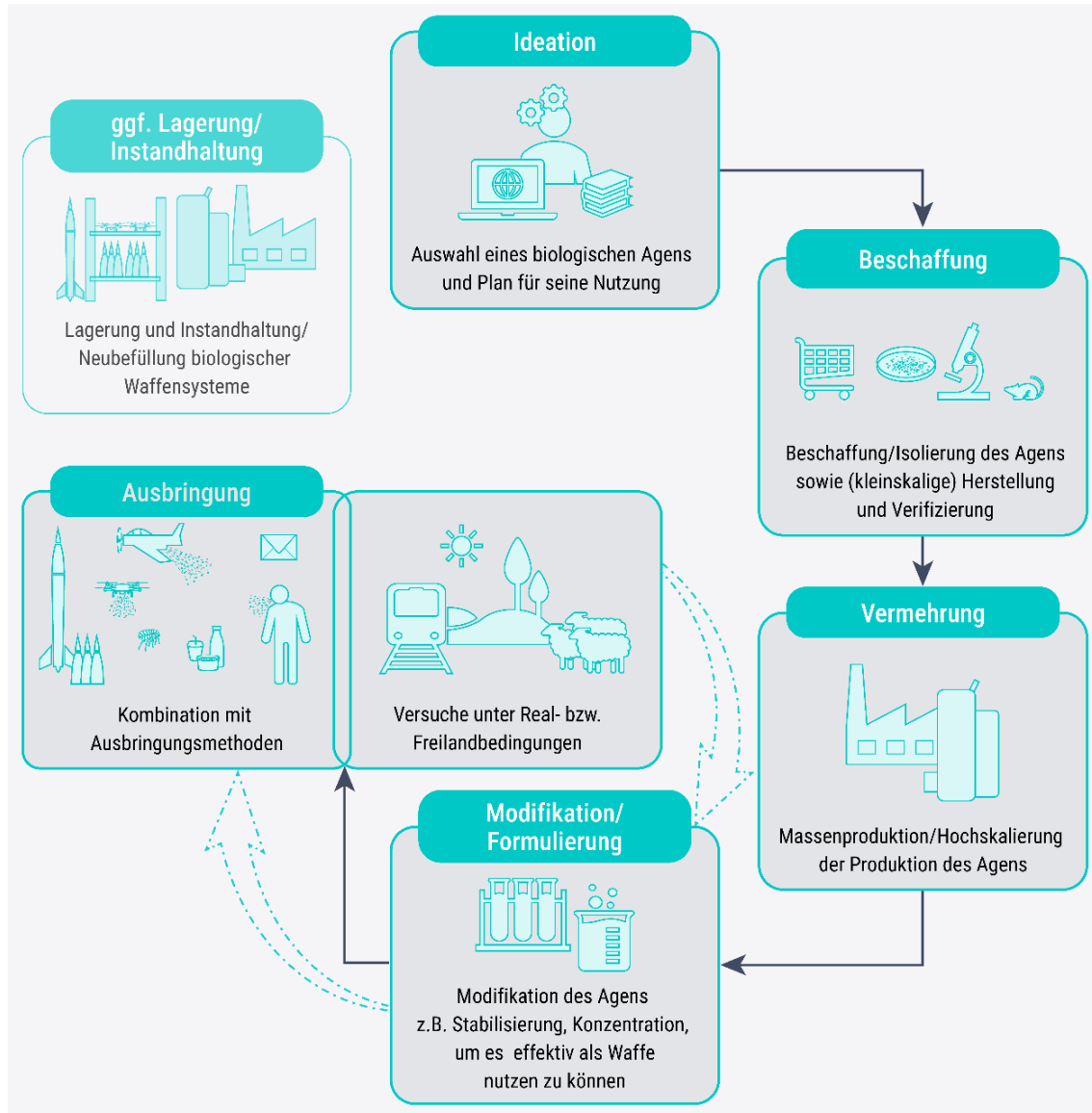
Im Fokus stehen also Fragen, die auch schon bisher für die Synthetische Biologie diskutiert wurden (Kapitel 3.1). Allerdings stellen sich die Fragen durch neue Möglichkeiten von KI-Modellen und das Zusammenspiel von KI-Modellen mit Methoden der Molekularbiologie und Biotechnologie in verschärfter Form. Diese neuen Möglichkeiten und wie diese mit den zuvor genannten Punkten im Zusammenhang stehen, werden in Kapitel 3.3 dargestellt.

Insbesondere in Bezug auf die zentrale Frage einer möglichen Senkung der Hürden für die Herstellung und Nutzung von Biowaffen, sowie inwieweit dies den Kreis potenzieller Akteure und deren Fähigkeiten erweitern könnte, ist es zunächst wichtig, die Charakteristika dieser Hürden genauer zu verstehen.

3.2.2 Die neue alte Frage nach den Hürden für die Herstellung von Biowaffen: die Notwendigkeit von speziellem (Erfahrungs-)Wissen und Fähigkeiten

Die Entwicklung von Biowaffen ist typischerweise ein mehrstufiger Prozess und erfordert insbesondere für komplexere Waffensysteme zur großflächigen Ausbringung und/oder zum Einsatz über große Entfernungen, wie sie in staatlichen Waffenprogrammen entwickelt wurden, eine Reihe zum Teil aufwendiger Schritte, für die spezielles Wissen erforderlich ist (Abbildung 3.2).

Abbildung 3.2 Die Herstellung von Biowaffen erfordert typischerweise mehrere und komplexe Schritte



Eigene Darstellung basierend auf NTI (o. J.a) Washington et al. (2024)

Hierzu gehören:

- die Auswahl eines biologischen Agens und die Ausarbeitung eines Plans für dessen Nutzung (Ideation, Ideenfindung);
- die Beschaffung des biologischen Agens, z.B. durch Isolierung aus der Natur (einschließlich der Kultivierung und Verifizierung des Agens) oder durch die mögliche synthetische Herstellung mancher Viren (Kapitel 3.1);
- die großskalige Vermehrung des Erregers für die Produktion bzw. Nutzung als Biowaffe,

- die Formulierung oder Modifikation des Agens, um es über einen gewählten Mechanismus ausbringen zu können (z. B. um es zu stabilisieren und/oder als Aerosol³³ zu verbreiten),
- die Kombination mit einem Ausbringungsmechanismus und (Feld-)Versuche zur Ausbringung und Wirksamkeit, sowie gegebenenfalls Entwicklungszyklen zur Verbesserung von Ausbringungsmechanismen oder anderer Schritte wie Modifikation und Formulierung,
- gegebenenfalls die Lagerung und Instandhaltung (einschließlich erforderlicher Neubefüllungen) von Waffensystemen.

Die Entwicklung von Biowaffen erfordert – über oft besondere technische Ausstattung hinaus – spezielle Fachkenntnisse und Erfahrungswissen auf unterschiedlichen Ebenen

Insbesondere Untersuchungen zu früheren staatlichen Biowaffenprogrammen (Kasten 3.3) (Ouaghrham-Gormley 2012, 2016; Vogel 2006),³⁴ die Ausführungen in der Buchpublikation des ehemaligen hochrangigen Wissenschaftlers im sowjetischen Biowaffenprogramm Kenneth Alibek³⁵ (Alibek/Handelman 1999) sowie Untersuchungen zu Fällen von Bioterrorismus (Kasten 3.4, Kapitel 3.4), wie vor allem den Anthraxbriefen in den USA im Jahr 2001 (DOJ 2010, S. 36 f.; Matsumoto 2003) und den Anschlagversuchen der Aum-Shinrikyo-Sekte in Japan in den 1990er Jahren (Danzig et al. 2012), zeigen, dass die Entwicklung biologischer Waffen über zum Teil besondere technische Ausstattung hinaus vor allem spezielle Fachkenntnisse und Erfahrungswissen auf unterschiedlichen Ebenen erfordert. Neben der Biologie der jeweiligen biologischen Agenzien und dem (sicheren) Umgang mit ihnen betreffen solche spezifischen Kenntnisse und Erfahrungen eine Reihe von Schritten bzw. Stufen des Entwicklungsprozesses. Hierzu gehören insbesondere:

- *die Skalierung der Herstellung biologischer Agenzien vom Labormaßstab zur Groß- bzw. Massenproduktion* (das heißt von der Kultivierung im Milliliter- bis Litermaßstab hin zu mehreren Tonnen). Sie erfordert nicht nur (typischerweise für den jeweiligen Organismus spezifische) zusätzliche wissenschaftliche und Entwicklungsarbeit im Labor, sondern auch die Lösung von ingenieurwissenschaftlichen bzw. produktions- und sicherheitstechnischen Problemen. Dies betrifft nicht zuletzt die Integration mit anderen Schritten der Waffenentwicklung wie Trocknungs- und Konzentrierungsprozesse, den Transport (z. B. über Pipelinesysteme) oder die Befüllung von Ausbringungsmechanismen wie Raketensprengköpfe oder Bomben (Alibek/Handelman 1999, S. 73 f., 98 f., 120 f.; Ouaghrham-Gormley 2016, S. 6 f.; NOVA o.J.a; Vogel 2006, S. 666 f.).
- *Techniken im Zusammenhang mit der Verwaffnung von Agenzien*, wie die starke Konzentrierung und Oberflächenbehandlung bakterieller Sporen, z. B. von Anthrax (*Bacillus anthracis*), mit Aerosolisierungsverstärkern, um sie als hochwirksame Aerosole nutzen zu können (Committee on Review of the Scientific Approaches Used During the FBI's Investigation of the 2001 Bacil-

33 Als Aerosol gilt eine Suspension von Partikeln oder Tröpfchen in einem Gas, gewöhnlich Luft. Aufgrund ihrer Größe (meist zwischen einigen Nanometern und hundert Mikrometern) haben die Partikel bzw. Tröpfchen eine vergleichsweise geringe Sinkgeschwindigkeit im Gravitationsfeld der Erde (CDC 2025; IUPAC 2025).

34 Diese Untersuchungen basieren unter anderem auf Befragungen von ehemaligen Forschenden und/oder leitenden Personen der früheren Biowaffenprogramme der USA (bis 1969) und der Sowjetunion (vor allem der zweiten, geheimen Phase zwischen 1972 und dem Ende der Sowjetunion 1991).

35 Kenneth Alibek (vormals Kanatjan Alibekov) ist ein aus Kasachstan stammender Arzt und ehemaliger Offizier der Roten Armee. Er arbeitete von 1975 bis 1992 für den sowjetischen Biopreparatkomplex, einen Zweig des früheren sowjetischen Biowaffenprogramms, unter anderem als Chefwissenschaftler und erster stellvertretender Direktor. Er verließ Russland 1992 und emigrierte in die USA (Tucker 1999).

lus Anthracis Mailings/National Research Council 2011, S. 80; DOJ 2010, S. 14, 36 f.; Inglesby et al. 2002; Matsumoto 2003; NOVA o. J.a) – also als hochkonzentrierte Präparationen, deren Partikel (Sporen) möglichst lange in der Luft schweben können und klein genug sind, um tief in die Lunge einzudringen (Fennelly 2020; Matsumoto 2003).

- *die Testung der biologischen Agenzien und Biowaffen*, z. B. in Bezug auf die verschiedenen Ausbringungsmethoden (wie Sprühvorrichtungen, Bomben, Raketensprengköpfe) und die Ausbreitungsmuster, die Wirksamkeit der biologischen Agenzien (unter anderem im Labor, in verschiedenen Umgebungen, wie öffentlichen Transportmitteln, Gebäuden, Straßen in der Stadt, offenem Land), die Auswirkungen von Umwelt- bzw. Wetterbedingungen auf die freigesetzten Agenzien (z. B. Stabilität, Überlebensfähigkeit) oder die Effektivität von Schutzmaßnahmen (Alibek/Handelman 1999, S. 15 ff., 42 f., 121, 133; Cole 2016; Polmar 2020; Zilinskas 2016, S. 9 f.).
- *die erforderliche Interdisziplinarität der Teams* (z. B. Molekular- und Mikrobiologie, Aerobiologie, Epidemiologie, Chemie, Maschinenbau, Produktionstechnik und -management, biologische Sicherheit), die insbesondere für die Entwicklung (einschließlich der Erprobung) komplexer Waffenprogramme bzw. -systeme erforderlich ist (Alibek/Handelman 1999, S. 16, 52, 120 f., 126, 140; Ouaghrham-Gormley 2016, S. 22; Ouaghrham-Gormley 2012, S. 87 f.; Vogel 2006, S. 669).
- *die Organisation und Koordination des Gesamtprozesses der Waffenentwicklung*. Diese erfordern nicht nur ein breiteres und tieferes Wissen über die erforderlichen Materialien und Prozesse aller Schritte, um die Kontinuität und Komplementarität in den verschiedenen Phasen sicherstellen zu können („end-to-end knowledge“) (Parachini et al. 2005; Revill/Jefferson 2014). Darüber hinaus ist Erfahrungswissen erforderlich, um diese Prozesse unter der notwendigen Geheimhaltung effektiv zu organisieren. So wurde das frühere sowjetische Biowaffenprogramm nach 1972 unter Missachtung der BWC (Kapitel 4.1.1) durchgeführt. Die gesamte Organisation war deshalb darauf ausgelegt, das Wissen einzelner Personen und Abteilungen über die durchgeführten Arbeiten und das Gesamtprojekt zu begrenzen, was zu Fragmentierungen und Schwierigkeiten bei der Koordination der verschiedenen Schritte der gesamten Waffenentwicklungskette (und selbst innerhalb von einzelnen Schritten wie der Skalierung) führte (Ouaghrham-Gormley 2016, S. 42 f.; Ouaghrham-Gormley 2012, S. 89 f.). Ähnliche Probleme in Bezug auf koordinierte und kontinuierliche Arbeitsabläufe sowie die Akkumulierung von erforderlichem Wissen gelten als einer der Gründe für das Scheitern des biologischen Waffenprogramms der japanischen Aum-Shinrikyo-Sekte (Ouaghrham-Gormley 2016, S. 140 f.) (Kasten 3.3).

Kasten 3.3 Staatliche und nicht staatliche Biowaffenprogramme bzw. Entwicklungsaktivitäten³⁶

Staatliche Biowaffenprogramme

Nach dem Ersten Weltkrieg³⁷ und während des Zweiten Weltkrieges entwickelten verschiedene Kriegsparteien Programme zur Herstellung biologischer Waffen, darunter Deutschland, Frankreich, das Vereinigte Königreich, Japan, die USA und die Sowjetunion (Carus 2017; Leitenberg 2001; Sabra/Frieß 2025, S. 63 ff.). Das japanische Biowaffenprogramm ist als eines der größten, jemals organisierten Programme von besonderer Bedeutung, bei dem die in Menschenversuchen mit Gefangenen entwickelten Kampfstoffe (darunter Erreger für Pest, Cholera, Anthrax und Typhus) ab Mitte der 1930er Jahre im Krieg gegen China großflächig getestet und gegen die Zivilbevölkerung eingesetzt wurden (Kasten 3.4, Kapitel 3.4) (Carus 2017; Keiichi 2005; Polmar 2020; Sabra/Frieß 2025, S. 43 f.).

Einige staatliche Programme wurden auch nach dem Zweiten Weltkrieg weitergeführt oder begonnen (Tabelle 3.1). Die Sowjetunion hatte nach der Unterzeichnung der BWC 1972, die die Entwicklung, Produktion und Lagerung von Biowaffen verbietet (Kapitel 4.1.1), ihr Waffenprogramm im Geheimen bis 1992 fortgesetzt bzw. verstärkt (Alibek/Handelman 1999; Leitenberg 2001; Zilinskas 2016). Das U.S. Department of State (2025) kommt in seinem Bericht zur Einhaltung vertrauensbildender Maßnahmen im Rahmen der BWC zum Schluss, dass Nordkorea und Russland aktive offensive Biowaffenprogramme betreiben und dass China und Iran Aktivitäten durchführen, die Bedenken hinsichtlich der Einhaltung der BWC aufkommen lassen.

Nicht staatliche Programme bzw. Entwicklungsaktivitäten für Biowaffen

Darüber hinaus wurden verschiedene organisierte Bestrebungen zur Herstellung biologischer Waffen von nicht staatlichen Organisationen bekannt:

- Die Rajneesh-Sekte in Oregon (USA) zog Anfang der 1980er Jahre die Herstellung bzw. Nutzung verschiedener biologischer Agenzien oder Krankheiten in Betracht (unter anderem Hepatitis, AIDS), erwarb dann aber legal über ihre Rajneesh Medical Corporation Proben pathogener Salmonellen (*Salmonella typhimurium*) und produzierte diese in der Folge in größeren Mengen. 1984 setzten Sektenmitglieder die Salmonellen ein, um Salatbars in einer Reihe von Restaurants zu verseuchen und dadurch das Ergebnis einer lokalen Wahlentscheidung zu ihren Gunsten zu manipulieren (Török et al. 1997; Turner et al. 2025) (Kasten 3.4, Kapitel 3.4).

³⁶ für eine ausführliche Darstellung Sabra/Frieß (2025, S. 63 ff.).

³⁷ Während des Ersten Weltkriegs betrieb nur Deutschland die Entwicklung biologischer Kampfstoffe, für biologische Sabotageakte gegen militärisch genutzte Tiere (Pferde und Maultiere). Deutsche Agenten setzten dazu Milzbrand (Anthrax [*Bacillus anthracis*] und Rotz (*Burkholderia mallei*) in den Ländern (z. B. USA) und Häfen ein, aus denen die Pferde zu den Alliierten verschifft wurden (Leitenberg 2001; Nikolakakis et al. 2024); für detaillierte Informationen und eine Einordnung (Sabra/Frieß 2025, S. 41 ff., 64).

- Die apokalyptische Sekte Aum Shinrikyo, die in Japan durch ihren Anschlag mit dem chemischen Kampfstoff Sarin auf die U-Bahn in Tokyo 1995 (mit 13 Toten und 6.000 Verletzten) bekannt wurde, versuchte in den frühen 1990er Jahren, Anthraxerreger und Botulinumtoxin in großem Maßstab herzustellen. Die Sekte setzte ihre letztendlich unwirksamen Präparationen beider Agenzien in großen Mengen bei mehreren Anschlägen ein (Danzig et al. 2012; Sabra/Frieß 2025, S. 53 ff.) (Kasten 3.4, Kapitel 3.4).
- Die islamistische Terrororganisation Al-Qaida verfolgte nach Geheimdienstinformationen aus dem Jahr 2001 bereits seit Anfang 1998 ein Biowaffenprogramm, insbesondere zur Herstellung von Anthrax. 2002 entdeckten US-amerikanische Truppen eine Fabrik nahe Kandahar (Afghanistan), die zur Produktion von Anthrax gedacht war (Pita/Gunaratna 2009). Die Gruppe war nach Geheimdiensteinschätzungen jedoch nie in der Lage, eine funktionsfähige Anthraxbiowaffe herzustellen (Juling 2023, S. 121; Mowatt-Larssen o. J.; Pita/Gunaratna 2009; Sabra/Frieß 2025, S. 80 ff.). Darüber hinaus planten Al-Qaida-Terrorzellen in Großbritannien, Spanien, Italien, der Türkei, Schweden und Deutschland 2003 Anschläge mit dem Toxin Rizin (Juling 2023, S. 121; Mowatt-Larssen o. J.).
- Der Islamischen Staat (IS) im Irak und Syrien könnte nach Informationen, die 2014 auf einem Laptop in Syrien entdeckt wurden, ebenfalls versucht haben, Biowaffen herzustellen. Der Laptop enthielt verschiedene Anleitungen für den Bau und den Einsatz von Massenvernichtungswaffen, darunter biologische Waffen (z. B. mit Pesterregern) (Doornbos/Moussa 2014; Juling 2023, S. 122). Im Zusammenhang mit dem IS ist insbesondere auch der geplante Anschlag mit einer Rizinsplitterbombe eines in Köln-Chorweiler lebenden tunesischen Dschihadisten und seiner Frau von 2018 zu nennen, da sie Kontakte zu IS-Mitgliedern hatten und mittels über Telegram-Kanäle verbreiteter Anleitungen und Videos bereits (kleine Mengen) Rizin aus Pflanzensamen hergestellt hatten (beck-online 2020; Flade 2018).

Tabelle 3.1 Bekannt gewordene staatliche Biowaffenprogramme nach dem Zweiten Weltkrieg

Land	Zeitraum	Zahl an Mitarbeitenden	biologische Kampfstoffe bzw. Waffensysteme, an denen gearbeitet wurde; Ausbringungsmechanismen	Quellen
UK	1945 bis 1957	nicht bekannt	Anthrax (<i>Bacillus anthracis</i>), Tularämie (<i>Franciscella tularensis</i>), Schweinebrucellose (<i>Brucella suis</i>), Venezolanische Pferdeenzephalitis (VEE); Flugzeugstreubomben	Carus (2017); Willis (2003)
USA	1945 bis 1969	3.400	Anthrax, Tularämie, Q-Fieber (<i>Coxiella burnetii</i>), VEE, Reisbrand (<i>Pyricularia oryzae</i>), Weizenrost (<i>Puccinia graminis tritici</i>), Botulinumtoxin; Flugzeug(streu)bomben, Flugzeuge mit Sprühtanks	Carus (2017); Leitenberg (2001)
UdSSR	1945 bis 1993	60.000	Anthrax, Brucellose, Pest (<i>Yersinia pestis</i>), Tularämie, Q-Fieber, Marburgvirus, Pocken (Variola-virus), VEE, Botulinumtoxin; Flugzeugsbomben, Interkontinentalraketen, Marschflugkörper, Flugzeuge mit Sprühtanks	Alibek/Handelman (1999); Carus (2017); Leitenberg (2001)
Irak	1975 bis 1991/1992	100 bis 300	Anthrax, Gasbrand (<i>Clostridium perfringens</i>), Rotavirus, Weizenbrand, Botulinumtoxin, Aflatoxin, Rizin; Artillerieraketen, Flugzeugsbomben, Raketen Sprengköpfe, Sprühflugzeuge	Carus (2017); Leitenberg (2001)
Rhodesien (heute Simbabwe)	1970er Jahre	6	Anthrax, Cholera (<i>Vibrio cholerae</i>); keine speziellen Technologien zur Verbreitung bekannt	Carus (2017); Turner/Sapp (2025)
Südafrika	1981 bis 1993	6 bis 10	Anthrax, Cholera, Brucellose (<i>Brucella melitensis</i>), Botulinumtoxin; keine speziellen Technologien zur Verbreitung bekannt	Carus (2017); Leitenberg (2001)
Syrien	? bis 2014?	nicht bekannt	Rizin; Technologie zur Verbreitung unklar	Jeremias et al (2016), zitiert in Sabra/Frieß (2025)

Eigene Zusammenstellung

Kasten 3.4 Einsatz von Biowaffen in bewaffneten Konflikten und Terrorakten in der Neuzeit³⁸

Die Geschichte des Einsatzes biologischer Waffen reicht bis in die Antike zurück. Am häufigsten beschriebene Methoden sind vergiftete Pfeile und die Kontaminierung von Wasserquellen mit verwesenen Leichen (Barras/Greub 2014; Frischknecht 2003). Vor allem im Mittelalter sollen bei Belagerungen von Städten von den belagernden Truppen tierische und menschliche Kadaver mittels Katapulte über die Stadtmauern geschleudert worden sein, um Krankheiten auszulösen (Barras/Greub 2014; Zanders 2022). Häufig zitiert wird die Verwendung pestinfizierter Leichen bei der Belagerung von Caffa (heute Feodosija, Krim, Ukraine) im Jahr 1346 (Christopher et al. 1997; Wheelis 2002).³⁹

In der Neuzeit kam es zu verschiedenen Einsätzen von biologischen Waffen sowohl in Kriegen oder bewaffneten Konflikten, meist durch staatliche Akteure bzw. Staaten, als auch bei Terrorakten durch nicht staatliche oder staatliche Akteure (z. B. Geheimdienste in Fällen von Staatsterrorismus) (Tabelle 3.2). Der Einsatz (inklusive großer Feldversuche) von Biowaffen ab Mitte der 1930er Jahre bis zum Ende des Zweiten Weltkriegs durch Japan in besetzten Gebieten und in Kampfhandlungen in China (Keiichi 2005; Polmar 2020) stellen dabei den bisher einzigen Fall dar, in dem Biowaffen militärisch großflächiger eingesetzt wurden.

Trotz einer Reihe dokumentierter Einsätze biologischer Agenzien für Terrorakte (Beispiele in Tabelle 3.2) legen es verfügbare Daten nahe, dass diese nur 0,02 % aller verzeichneten historischen Terroranschläge ausmachen (Tin et al. 2021, 2022).⁴⁰ Zwischen 1970 und 2019 wurden 33 Terroranschläge mit biologischen Kampfstoffen verzeichnet (darunter 20 mit Anthrax, 3 mit dem Toxin Rizin), bei denen 9 Menschen starben und 806 verletzt wurden.⁴¹ Die meisten (13) richteten sich gegen Institutionen und Mitarbeitende von Regierungen. Allein 10 Ereignisse gehören zu den Amerithrax-Briefanschlägen im Jahr 2001 (DOJ 2010) an verschiedenen Orten oder Tagen in den USA. Es finden sich keine öffentlich zugänglichen Hinweise darauf, dass die bei den bisherigen Terroranschlägen verwendeten biologischen Agenzien mittels klassischer gentechnologischer Methoden zur Herstellung rekombinanter Proteine (wie sie seit Anfang der 1980er Jahre etabliert sind) oder mittels neuerer, fortgeschrittener biotechnologischer Verfahren wie der Gen- oder Genomsynthese (Kapitel 2.1) hergestellt oder verändert worden wären (beck-online 2020; DOJ 2023, 2024; Jha 2025; START 2025; Tin et al. 2021, 2022; UMD o. J.) (Kapitel 3.4).

38 Für eine ausführliche Beschreibung vieler dieser Ereignisse siehe Sabra/Frieß (2025, S. 31 ff.).

39 Einige Historiker bezweifeln, nicht zuletzt aus physikalisch-technischen Gründen, dass diese Technik für Kadaver von (größeren) Tieren oder von Menschen, wie in Caffa, tatsächlich möglich war bzw. angewendet wurde (Field 2023; Zanders 2022).

40 Die Datenerhebung und -analyse von Tin et al. (2021, 2022) erfolgten anhand der frei zugänglichen Global Terrorism Database (START 2025).

41 Obwohl sehr viel seltener, lag die durchschnittliche Verletzungsrate bei den Anschlägen mit biologischen Agenzien mit ca. 29 pro Ereignis weitaus höher als bei Anschlägen mit Sprengstoffen und Feuerwaffen zusammen (ca. 6 pro Ereignis), die mehr als 76 % aller Anschläge ausmachen. Die durchschnittliche Zahl der Todesopfer pro Ereignis mit biologischen Agenzien (ca. 0,3) war allerdings ca. 14-fach niedriger (Tin et al. 2021).

Tabelle 3.2 Einsatz von Biowaffen in bewaffneten Konflikten und Terrorakten in der Neuzeit

Zeitraum	Akteur	Ereignis	Auswirkung	Quellen
<i>Kriege bzw. bewaffnete Konflikte</i>				
18. Jahrhundert	britische Kolonialmacht	mutmaßliche Verbreitung von Pocken unter Ureinwohnern Nordamerikas	Pockenepidemien, Dezimierung der indigenen Bevölkerung	Fenn (2000)
Erster Weltkrieg	Deutschland	Verschiffung von mit Milzbrand und Rotz infizierten Pferden und Maultieren, unter anderem in USA	keine signifikante militärische Wirkung erzielt	Geissler et al. (1999); Nikolakakis et al. (2024)
Zweiter Weltkrieg	Japan	Versuch an Kriegsgefangenen, großflächige Tests bzw. Einsätze biologischer Waffen (vor allem Pest, Cholera) in China	Tausende bis Hunderttausende Tote*, überwiegend Zivilisten; unkontrollierbare Verbreitung von Krankheiten; militärische Wirkung fraglich	Barenblatt (2005); Keiichi (2005); Polmar (2020)
1952	Mau-Mau-Rebellen, Kenia	Vergiftung von Vieh der Kolonialherren unter anderem mit pflanzlichen Giften	Schwächung des Viehbestands der Kolonialherren	Thorold (1953)
1970er Jahre	Sicherheitskräfte in Rhodesien	Einsatz von Cholera und Typhus gegen Rebellen und Zivilbevölkerung	zahlreiche Krankheitsausbrüche und Todesfälle	Cross (2017)
<i>Terrorismus inklusive Staatsterrorismus</i>				
1978	bulgarischer Geheimdienst	Attentate auf Dissidenten durch Injektion von mit Rizin versetzten Kügelchen (mit modifiziertem Regenschirm), Paris, London	mindestens ein Todesfall	Carus (1998); Turner/Sapp (2025)
1984	Rajneesh-Sekte	Kontamination von Salatsbars mit Salmonellen in Restaurants, um Beteiligung an lokaler Wahl zu beeinflussen, USA	751 Fälle von schweren Lebensmittelvergiftungen, keine Todesfälle	Török (1997); Turner et al. (2025)
1990 bis 1995	Aum-Shinrikyo-Sekte	mehrmalige Verbreitung großer Mengen von Anthrax- und Botulinumtoxin-Präparationen, Japan	ausgebrachte Bioagenzien waren unwirksam; wohl aufgrund von mangelndem Wissen/Erfahrung bei der Herstellung	Danzig et al. (2012)

Zeitraum	Akteur	Ereignis	Auswirkung	Quellen
2001	unbekannte Täter**	„Amerithrax“, Briefe mit Anthraxsporen an Senatoren und Medienunternehmen, USA	5 Todesfälle, weitere 17 Krankheitsfälle, Panik, hohe Kosten für Dekontamination und medizinische Versorgung	DOJ (2010); Schmitt/Zacchia (2012); Zacchia/Schmitt (2019)
2003	unbekannte Täter (Unterschrift „Fallen Angel“)	Briefe mit Rizin in Pulverform, unter anderem ans Weiße Haus und das US Department of Transportation, USA	einer der Briefumschläge war mit einer Rizinwarnung versehen; keine Verletzten	FBI (2004)
2011	unbekannte Täter	Paket mit Anthraxsporen an den pakistanischen Premierminister Yusuf Raza Gilani, Pakistan	keine Infizierten	Reuters (2012); Tin et al. (2022 Appendix A)
2013	Shannon Guess Richardson, eine damals 35-jährige Schauspielerin aus New Boston, USA. Nach Verschicken der Briefe kontaktierte sie die Polizei und beschuldigte ihren Ehemann der Taten.	Rizinbriefe an US-Präsident Obama, New York Citys Bürgermeister Bloomberg und Mark Glaze, einen Aktivisten für schärfere Waffengesetze, USA	keine Symptome bei Personen, die zuerst mit den Briefen in Kontakt kamen; Beamte, die später einen der Briefe untersuchten, zeigten leichte Symptome	Associated Press (2013); FBI (2014)
2020	Pascale C. V. Ferrier, eine damals 55-jährige Kanadierin, die 2019 für etwa 10 Wochen in Texas, USA, inhaftiert gewesen war	Rizinbriefe (gesendet aus Kanada) an das Weiße Haus/Präsident Trump und an 8 Strafverfolgungsbeamte in Texas, USA	keine Infizierten	DOJ (2023)

* Die Schätzungen über die Opferzahlen gehen stark auseinander. Darüber hinaus wurde im Laufe der Einsätze die militärische Wirksamkeit bei der japanischen Militärführung bezweifelt (Keiichi 2005).

** Verdächtig und schwer belastet durch Indizien wurde (bis zu seinem Suizid im Jahr 2008) Dr. Bruce Edwards Ivins, Mikrobiologe am United States Army Medical Research Institute of Infectious Disease (USAMRIID), Fort Detrick in Maryland – der zentralen Einrichtung der US-Armee für die Biodefense-Forschung. Er galt als einer der führenden US-Experten für die Kultivierung, die Sporenbildung und Aufreinigungsprozesse im Zusammenhang mit dem Anthraxerreger (DOJ 2010).

Quelle: adaptiert und erweitert nach Sabra/Frieß (2025)

Nicht alles notwendige Wissen ist ohne Weiteres übertragbar: die tazite Dimension von Wissen für die Herstellung von Biowaffen

Die Analysen früherer Biowaffenprogramme und bisheriger Terrorakte mit biologischen Agenzien legen es nahe, dass das für die verschiedenen Entwicklungsschritte erforderliche spezielle Wissen – oder zumindest Teile davon – nicht ohne Weiteres auf andere Personen und, da es oft von den konkreten Umgebungsbedingungen abhängig ist, nicht notwendigerweise von einem Ort auf einen anderen übertragen werden kann. Wissen mit diesen Eigenschaften wird als *tazites oder implizites Wissen* bezeichnet.

Tazites Wissen lässt sich typischerweise nicht in schriftlicher Form wie in wissenschaftlichen Publikationen bzw. veröffentlichten Protokollen (eine Art Rezept, um Experimente bzw. Laborverfahren nachzukochen) weitergeben.⁴² Es erfordert eigene Erfahrung und/oder die praktische Anwendung instruiert durch – oder zusammen durchgeführt mit – Personen, die solches Wissen bzw. Fähigkeiten besitzen (zum Teil ohne sich dessen bewusst zu sein).

Oft werden dabei zwei grundsätzlich unterschiedliche Kategorien taziten Wissens unterschieden (Collins 2010): Auf der einen Seite Formen schwachen taziten Wissens, also Wissen, das unter bestimmten Umständen explizit gemacht werden könnte, aber aus praktischen Gründen (z. B. da zu kompliziert oder zu aufwendig, um es zu verschriftlichen), aus Gründen der Geheimhaltung oder unbewusst (wenn sich der Autor der Wichtigkeit mancher für ihn selbstverständlicher Details nicht bewusst ist), nicht oder unvollständig verschriftlicht wird. Auf der anderen Seite stehen Formen taziten Wissens, die nicht weitergegeben werden können, ohne dass ein direkter Kontakt zu den Personen vorhanden ist, die dieses Wissen besitzen. Als solche Formen gelten zum einen das somatische (körperliche) oder individuelle tazite Wissen, das heißt körperliche mechanische Fertigkeiten oder Know-how, das eine Person durch Versuch und Irrtum oder in einer Art Lehrling-Meister-Verhältnis erworben hat. Zum anderen gehört hierzu kollektives oder gemeinschaftliches tazites Wissen, das erst durch die Zusammenarbeit und Interaktionen zwischen Expert/innen mit unterschiedlichem fachlichem Hintergrund entsteht (Collins 2007, 2010; Revill/Jefferson 2014).

So gelang es beispielsweise im geheimen sowjetischen Biowaffenprogramm auch nach 2 Jahren intensiver Versuche nicht, den ursprünglichen Anthraxstamm großskalig an einem neuen Ort herzustellen, als Anfang der 1980er Jahre die Herstellung von unter anderem Anthrax von Swerdlowsk (dem heutigen Jekaterinburg) nach Stepnogorsk (in Nordkasachstan) verlegt wurde – trotz mehrerer hundert Seiten von Dokumenten aus dem russischen Biowaffenlabor, das den Waffen-Anthraxstamm entwickelt hatte. Erst nachdem 65 Wissenschaftler und Ingenieure mit verschiedenen fachlichen Hintergründen aus dem ursprünglichen Entwicklungsprogramm dazu geholt wurden und Kooperationen und Austauschprogramme mit anderen russischen Einrichtungen etabliert worden waren, gelang es innerhalb von 3 Jahren die Originalprotokolle nach Anpassungen (z. B. in Bezug auf die vor Ort anderen Bioreaktoren) so umzusetzen, dass Anthrax in größerer Menge für die weitere Waffenherstellung produziert werden konnte (Ouaghrham-Gormley 2016, S. 23; Vogel 2006; Ouaghrham-Gormley/Vogel 2003).

42 Der Begriff oder das Konzept des taziten Wissens, das vor allem auf den Physikochemiker und Philosophen Michael Polanyi zurückgeht, wird so explizitem, vollständig artikulierbarem Wissen gegenübergestellt, das von denjenigen, die es besitzen, mittels Sprache bzw. Schrift weitergegeben werden kann (Polanyi 1962). Ähnliche Konzepte wurden vom Philosophen Gilbert Ryle (Ryle 1949) und vom Ökonomen und Philosophen Friedrich Hayek (Oğuz 2010 und Referenz darin) beschrieben. Obwohl das Halten des Gleichgewichts auf dem Fahrrad ein oft zitiertes Beispiel für tazites Wissen ist, verdeutlicht es nur eine der Unterarten solchen Wissens bzw. der taziten Dimension von Wissen, die in der wissenschaftlich-technischen Praxis und deren institutioneller Organisation relevant sind (Collins 2007, 2010; Revill/Jefferson 2014).

Ähnliche Erfahrungen hinsichtlich der Notwendigkeit entsprechender Wissensvermittlung in der Biowaffenentwicklung einschließlich der Organisation bzw. Koordinierung relevanter Prozesse und der notwendigen Unterstützung durch Experten für Biowaffen existieren beispielsweise auch für den Teil des sowjetischen Biowaffenprogramms für Viren wie dem Pockenvirus (Alibek/Handelman 1999, S. 107 ff., 120) sowie aus dem früheren (bis 1969 existierenden) US-amerikanischen Biowaffenprogramm (Ouaghrham-Gormley 2016, S. 69 ff.).

Auch der Fall der japanischen Sekte Aum Shinrikyo in den 1990er Jahren (Kästen 3.3., 3.4) deutet auf die Relevanz taziten Wissens für die erfolgreiche Herstellung biologischer Kampfstoffe bzw. Biowaffen hin. So zeigte eine detaillierte Fallstudie (Danzig et al. 2012)⁴³ zu den Fehlschlägen von Aum Shinrikyo mit Anthrax und Botulinumtoxin im Schluss, dass mangelndes (Erfahrungs-)Wissen in Bezug auf die verwendeten biologischen Agenzien (z. B. zu deren Analyse, zu bestimmten Techniken zum Einbringen von DNA oder zu Kulturbedingungen in Fermentern) sowie deren Verwaffnung (wie der Konzentrierung bzw. Trocknung von Anthraxsporen) ein wichtiger Faktor für die Misserfolge waren. Die Notwendigkeit von besonderem oder nicht ohne Weiteres erlangbarem Wissen im Umgang mit bzw. der Manipulation von (unterschiedlichen) lebenden Organismen wird auch durch die Tatsache nahegelegt, dass dieselben Aum-Gruppenmitglieder chemische Kampfstoffe (vor allem Sarin) erfolgreich herstellen und einsetzen konnten. Als weiterer Faktor wurde fehlendes Wissen bzw. fehlende Erfahrung hinsichtlich Organisationsfragen und der Kultur der Zusammenarbeit identifiziert, nicht zuletzt auch in Bezug auf den Erwerb fehlender Expertise unter Bedingungen der Geheimhaltung. Auch große finanzielle Ressourcen, Mitarbeitende mit akademischer Ausbildung (wenn auch nicht in Mikrobiologie, aber z. B. in Virologie, Medizin oder Chemie), der Zugang zu wissenschaftlich-technischen Informationen und eine sehr große Beharrlichkeit (Danzig et al. 2012) konnten das fehlende Erfahrungswissen offenbar nicht kompensieren.

Beispiele wie diese aus der Entwicklung von Biowaffen befinden sich in Übereinstimmung mit zahlreichen Untersuchungen zu verschiedenen wissenschaftlich-technischen Kontexten sowie anderen Waffentechnologien (z. B. Nuklearwaffen) (Ouaghrham-Gormley 2012, S. 84 und Referenz darin). Zu den wissenschaftlich-technischen Kontexten gehören auch die moderne Molekular- und Zellbiologie sowie die Synthetische Biologie. Auch dort gibt es zahlreiche belegte Beispiele bzw. Daten, die nahelegen, dass spezielles Erfahrungswissen bzw. Fertigkeiten einschließlich praktische handwerkliche Schritte im Labor für bestimmte Methoden bzw. Anwendungen (Hong et al. 2026; Romero-Severson et al. 2025) (Kapitel 3.3.1) – und direkte Interaktion, Teamwork bzw. der Austausch mit Personen, die solches Wissen haben, eine wichtige Rolle spielen (De Lange et al. 2022; Eireiner 2025b; Jefferson et al. 2014a, 2014b; Revill/Jefferson 2014; Santolini et al. 2023; Vogel 2012) (Kapitel 3.1).

⁴³ Die Studie basiert auf Befragungen der Aum-Sektenmitglieder, die im Tokyo Detention Center inhaftiert waren (Danzig et al. 2012, S. 5 f.). Die Befragungen lieferten die Informationen darüber, wie die Sekte vorgegangen war, auf welche Schwierigkeiten sie gestoßen war und welche Erfolge (wie im Fall der Herstellung und Verwendung des chemischen Kampfstoffs Sarin bei dem Angriff in Tokyo auf die U-Bahn im Jahr 1995) und Misserfolge sie zu verzeichnen hatte (Kasten 3.4).

3.3 Potenzielle neue oder erleichterte Möglichkeiten des Missbrauchs von Biotechnologie durch KI: Worauf begründen sich die vorgebrachten Befürchtungen?

3.3.1 Wissensaneignung oder -erweiterung über große Sprachmodelle

Für die sehr breit anwendbaren („general purpose“ oder „foundation“) LLMs (Kästen 2.1, 2.3) haben verschiedene Akteure in einer Reihe von Aktivitäten und Studien untersucht bzw. untersuchen kontinuierlich, inwieweit diese Modelle erstens für die Herstellung von Biowaffen relevantes Wissen für verschiedene Personengruppen (einfacher) zugänglich machen, sowie zweitens ob sie die praktische Umsetzung solchen Wissens ermöglichen und existierende Fähigkeiten verbessern könnten (Tabelle 3.3). Zu diesen Akteuren gehören Forschende akademischer Einrichtungen (Li et al. 2024; OpenAI/LANL 2024; Soice et al. 2023; Zhang et al. 2026), Non-Profit-Organisationen und Beratungsunternehmen (Dev et al. 2025; Götting et al. 2025; Hong et al. 2026; Ivanov 2024; Laurent et al. 2024; Mouton et al. 2024; Zhang et al. 2026), von Regierungen beauftragte und staatlich finanzierte KI-Sicherheitsinstitute (AIS 2025; Davies et al. 2026) oder die KI-Modelle entwickelnde Firmen selbst (Anthropic 2025b, 2026a, 2026b, 2026c; Google DeepMind 2025a; Llama Team, AI @ Meta 2024; OpenAI 2025a, 2025b, 2026; Patwardhan et al. 2024).

Tabelle 3.3 Kurzdarstellung ausgewählter empirischer Untersuchungen zu Biosecurity-Risiken von LLMs

Studie	gestellte Aufgaben	Studiendesign/Benchmarks	Ergebnisse
RAND Corp. Mouton et al. (2024)	Ideation, Angriffspläne für 4 Szenarien	Uplift-Studie; 45 Forschende mit unterschiedlichen fachlichen Hintergründen (Biologie, KI/LLMs, Biosecurity/Strategie); verteilt auf Teams mit je 3 Personen: nur Internet (IN); IN und LLM A; IN und LLM B ¹	Keiner der Pläne wurde von Expert/innen als ausreichend detaillierte bzw. haltbare Grundlage zur Durchführung eines wirksamen biologischen Angriffs bewertet; keine statistisch signifikanten Unterschiede zwischen den nur mit IN oder IN und LLMs erstellten Plänen.
OpenAI ² Patwardhan et al. (2024)	Ideation, Beschaffung, Vermehrung, Formulierung, Ausbringung	Uplift-Studie; 50 promovierte Expert/innen (Genetik, Mikrobiologie, Virologie) mit Laborerfahrung, 50 Studierende mit mindestens einem Kurs in Biologie; jeweils zufällig verteilt auf Kontrollgruppe (nur IN) und Gruppe IN und GPT-4	Keine statistisch signifikanten Unterschiede zwischen den Gruppen. Aber es kam vor allem in der Expertengruppe mit Modellzugang zu einem Anstieg der Zahl von Personen, die bei fast allen Fragen die Höchstpunktzahl erreichten.

Studie	gestellte Aufgaben	Studiendesign/Benchmarks	Ergebnisse
RAND Corp. Benchmark von 31 LLMs Dev et al. (2025)	Benchmarks zu kritischem Wissen oder Fähigkeiten	6 öffentlich verfügbare Benchmarks (unter anderem BioLP-bench, LAB-Bench, WMDP benchmark, GPQA); 16 nicht offene LLMs (unter anderem von OpenAI, Google, Anthropic) und 15 Open Weight-LLMs (z. B. von DeepSeek, Mistral, Meta)	Neuere Modelle, insbesondere die OpenAI o1-Familie, näherten sich in vielen Wissensbenchmarks dem Referenzwert menschlicher Expert/innen („human baseline“).
Secure Bio ³ Virology Capabilities Test (VCT) Götting et al. (2025)	Benchmark, praktisches Wissen Virologie, Fokus Fehlerbehebung	Fragen testen grundlegende virologische Kenntnisse, multimodal, das heißt mit Bildern, die reale Laborszenarien widerspiegeln, Antworten nicht einfach durch eine Internetsuche zu finden; unter anderem LLMs von OpenAI, Anthropic und Google; einige reine Textmodelle wie DeepSeek-R1	Alle multimodalen Modelle übertrafen den medianen Referenzwert menschlicher Expert/innen (22,1 %), darunter Anthropic's Claude 3.5 Sonnet (33,6 %), Googles Gemini 2.5 Pro (37,6 %), OpenAIs o1 (35,4 %) oder o3 (43,8 %). OpenAIs o3 übertraf dabei 34 von 36 Expert/innen und lag damit im 94. Perzentil der Virologieexpert/innen. ⁴
Anthropic ⁵ Systemkarten Claude Opus 4 und Sonnet-4-Serien Anthropic (2025b, 2025d, 2025c, 2026b, 2026c) Claude Mythos Preview Anthropic (2026a)	Ideation, Beschaffung inklusive Protokolle zur Herstellung von Viren	Uplift-Studien: Studierende mit MINT-Bachelor; promovierte Expert/innen; nur IN; IN und LLM („safeguards“ entfernt); Red-Teaming-Befragungen der LLMs durch Biosecurity-Expert/innen	In allen Fällen wurden „Uplifts“ festgestellt (bis zu ca. 2,5-fach), statistische Signifikanz unklar. Red-Teaming-Beurteilung: auch jüngste Modelle konnten keine neuartigen oder kreativen biologischen Erkenntnisse liefern, die über die wissenschaftliche Literatur hinausgehen.
	Benchmarks zu kritischem Wissen oder Fähigkeiten	unter anderem Tests zu: sensiblen Informationen zur Biowaffenherstellung; Virologie (VCT) (Götting et al. 2025); agentenbasierte Aufgaben, unter anderem zur Assemblierung von DNA-Fragmenten und Nutzung von Bioinformatikwerkzeugen	Bei der Benchmark multimodale Virologie (VCT) übertrafen alle Modelle den Referenzwert menschlicher Expert/innen. Claude Opus 4.6 und Sonnet 4.6 überschritten die Ausschluss-schwellen für Modellfähigkeiten, die als notwendig erachtet wurden, Forschung und Entwicklung im Bereich Biologie und Pathogene erheblich zu beschleunigen.

Studie	gestellte Aufgaben	Studiendesign/Benchmarks	Ergebnisse
OpenAI ⁶ Systemkarten der GPT-5-Serie OpenAI (2025b, 2026)	Benchmarks zu kritischem Wissen oder Fähigkeiten	unter anderem Tests zu: sensiblen Informationen zur Biowaffenherstellung; Virologie (VCT) (Götting et al. 2025); Tests zu tazitem Wissen und Fehlerbehebung; agentenbasierte Aufgaben, z. B. Assemblierung von DNA-Fragmenten, Umgehung von DNA-Synthesescreen- ings; Automatisierung von DNA-Assemblierung	Bei der VCT-Benchmark übertreffen alle Modellvarianten den menschi- chen Referenzwert sehr deutlich. In den Tests zu tazitem Wissen und Fehlerbehebung übertrafen die jün- gsten Modellvarianten die 80-Perzen- tilbasislinie der Expert/innen. Bei der DNA-Assemblierung über- traf, bei der Laborautomatisier- ungsaufgabe erreichte eine Mod- ellversion ohne „safeguards“ den menschlichen Referenzwert.
Scale AI ⁷ Zhang et al. (2026)	Aufgaben aus 8 Benchmarks, z. B. zur Virologie, zu Pathogenen oder bi- ologischen Techni- ken	<i>Uplift-Studie</i> mit 47 Stud- ierenden aus MINT-Fächern und 10 Studierenden aus Nicht-MINT-Fächern; verteilt auf Gruppen mit nur IN oder IN und LLMs (o4- mini, o3, Gemini 2.5 Pro, Claude 3.7 Sonnet, Claude Opus 4)	Die Leistungswerte in der LLM- Gruppe waren in 7 von 8 Bench- marks wohl statistisch signifikant höher, in 3 von 4 Benchmarks über- trafen sie die Referenzwerte menschlicher Expert/innen. Über alle Benchmarkaufgaben hin- weg statistisch signifikante, 4,16- fache Leistungssteigerung durch LLMs.
Active Site, METR ⁸ Hong et al. (2026)	praktische Auf- gaben in biolo- gischem Labor („wet lab“)	Wet-Lab-Uplift-Studie: 153 meist MINT-Studierende mit minimaler Labor- erfahrung verteilt auf zwei Gruppen, eine mit nur IN und eine mit IN und LLMs; Kernaufgaben: Zellkultur, DNA-Klonierung, Virus- produktion (AAV)	Es konnten keine statistisch signifi- kanten Unterschiede zwischen den Gruppen in den Abschlussquoten für einzelne Aufgaben oder aller drei Kernaufgaben zusammen fest- gestellt werden.

1 Welche zwei LLMs getestet wurden, wird nicht offengelegt.

2 In Zusammenarbeit mit Biosecurity-Expert/innen des Beratungsunternehmens Gryphon Scientific.

3 Non-Profit-Organisation, die Forschung zu extremen biologischen Risiken betreibt.

4 Das heißt, 94 % der Expert/innen lagen unter diesem Wert.

5 in Zusammenarbeit mit Biosecurity-Expert/innen von Gryphon Scientific/Deloitte und Signature Science sowie SecureBio

6 in Zusammenarbeit mit Gryphon Scientific und SecureBio

7 Scale AI, Inc ist ein US-amerikanisches Unternehmen für Infrastruktur und Software im Bereich der KI. Die Studie wurde zusammen mit Mitarbeitenden von SecureBio, der University of Oxford und der University of California, Berkeley durchgeführt.

8 Active Site/Panoplia Laboratories, Inc und Model Evaluation & Threat Research (METR) sind US-amerikanische Non-Profit-Forschungsorganisationen, die unter anderem Risiken von KI-Modellen in der Biologie untersuchen.

Eigene Zusammenstellung

Möglichkeiten, um Modellfähigkeiten zu evaluieren: Benchmarks, Red-Teaming- und Uplift-Studien

Benchmarks

Benchmarks werden genutzt, um (zumeist automatisch) Leistungskennzahlen zum Wissensstand bzw. den Fähigkeiten eines Modells zu generieren.⁴⁴ Dies geschieht mithilfe von Frage-Antwort-Formaten, bei denen oft ein Multiple-Choice-Verfahren zum Einsatz kommt. Dabei wird gemessen, wie oft ein KI-Modell die richtige Antwort auswählt. Bei offenen Fragestellungen wird die Vollständigkeit bzw. Genauigkeit der Antworten durch Expert/innen bewertet (CSR 2025; Dev et al. 2025; Ho/Berg 2025; Justen 2025). Mittlerweile gibt es eine Reihe solcher Benchmarks, die meist öffentlich verfügbar sind und dabei helfen sollen, unterschiedliche Wissensbestände oder Fähigkeiten zu messen bzw. zu beurteilen. Sie richten sich auf:

- Wissen zu Voraussetzungen für die Entwicklung biologischer und chemischer Waffen, wie chemische Synthese, Beschaffung, Verifizierung, Einsatzmechanismen und Forschung zu viralen Vektoren, z. B. der Weapons of Mass Destruction Proxy (WMDP) benchmark (Li et al. 2024);
- Wissen/Fähigkeiten für die Laborforschung, wie Literaturrecherche, Protokollfehlerbehebung, Veränderung von biologischen Sequenzen, DNA-Klonierung, Einsatz relevanter Methoden, z. B. Language Agent Biology Benchmark (LAB-Bench) (Laurent et al. 2024); zum Teil finden sich darunter Fragen, für die Antworten mit konventioneller Websuche von Nichtexpert/innen nur schwer zu finden („Google-proof“) sind und die selbst für Expert/innen eine besondere Herausforderung darstellen, z. B. Graduate-Level Google-Proof Q&A Benchmark (GPQA) (Rein et al. 2023);
- das Erkennen und Korrigieren von absichtlich eingeführten Fehlern (Troubleshooting) in Laborprotokollen, z. B. Biological Lab Protocol Benchmark (BioLP-bench) (Ivanov 2024). Dazu gehören auch eingeführte Fehler in von Expert/innen verfassten Protokollen, die nicht online verfügbar sind, z. B. TroubleshootingBench⁴⁵ (OpenAI 2025b);
- praktische Kenntnisse der Virologie, die für Arbeit in virologischen Laboren unerlässlich sind, vor allem Fehlerbehebung bei Experimenten. Antworten dazu lassen sich nicht einfach über eine Internetsuche finden und erfordern fundierte Fachkenntnisse, z. B. Virology Capabilities Test (VCT) (Götting et al. 2025);
- die Fähigkeit eines Modells zu erkennen, wenn es für die potenzielle Waffenentwicklung verwendet wird, und sich zu weigern, Wissen preiszugeben, das zu Schaden führen könnte, z. B. HarmBench (Mazeika et al. 2024), Assessing Large Language Models' Safety through Red Teaming (ALERT) (Tedeschi et al. 2024).

Benchmarks gelten jedoch, insbesondere wenn sie Multiple-Choice-Formate verwenden, als mit großen Unsicherheiten behaftet, was ihre Aussagekraft für Risiken in der realen Welt betrifft (Dev

⁴⁴ Es existieren auch Benchmarks, um die Bereitschaft eines Modells zu testen, besonders sicherheitsrelevante Informationen in Antwort auf Eingaben preiszugeben (Dev et al. 2025 und Referenz darin).

⁴⁵ Forschende mit einem Dokortitel in Virologie, Genetik, Mikrobiologie oder Protein-Engineering wurden gebeten, Protokolle zu verfassen, die sie persönlich im Labor verwendeten. Wurde ein Protokoll aus einer Veröffentlichung übernommen, mussten sie mindestens mehrere Schritte wesentlich verändern. Aus diesen Protokollen erstellten die Expert/innen jeweils drei Fragen zur Fehlerbehebung, wobei sie subtile oder realistische Ausführungsfehler einbauten (z. B. eine unsachgemäße Homogenisierungstechnik) und das daraus resultierende Fehlschlagen des Experiments beschrieben (OpenAI 2025b).

et al. 2025; Ho/Berg 2025 und Referenz darin). So kann jede Benchmark nur einen Teil eines Prozesses testen, wie beispielsweise das Erkennen bzw. Beheben von Fehlern in Versuchsanleitungen. Weiterhin spiegeln oft verwendete Multiple-Choice-Formate nicht notwendigerweise die Situation eines Akteurs in einem Labor bei der Implementierung neuer oder komplexer Versuche oder Herstellungsprozesse wider. Schließlich gilt auch die „Sättigung“ von Benchmarks als zunehmendes Problem (Dev et al. 2025; Justen 2025); das heißt, wenn LLMs immer häufiger Ergebnisse am oberen Rand bzw. die Maximalwerte der Leistungsskalen existierender Benchmarks erzielen, wodurch die Benchmarks für die Unterscheidung weiterer Verbesserungen von Modellen unwirksam werden. Neben leistungsfähigeren LLMs tragen zu einer solchen Sättigung auch die Datenkontamination bei, die entsteht, wenn Benchmarkdatensätze in die Trainingsdaten einfließen, was zu artifiziell überhöhten Leistungswerten führt (Deng et al. 2024; Etzine et al. 2025; Ivanov/Volkov 2025; Sainz et al. 2023).

Um Benchmarks in Bezug auf mögliche Risiken durch die Modelle besser interpretieren zu können, werden die Leistungswerte der Modelle idealerweise mit Referenzwerten von Personengruppen mit bestimmten fachlichen Hintergründen oder Erfahrungen verglichen. Der Vergleich mit solchen „human baselines“ (übersetzt etwa menschliche Basiswerte) wird herangezogen, um abzuschätzen, ob und in welchem Maß das Modell für die Beschaffung oder Herstellung von biologischen Agenzien bzw. Biowaffen für Nichtexpert/innen von Nutzen sein könnte (z. B., ob das Modell noch wenige Prozentpunkte hinter den „human baselines“ für Wissen oder Fähigkeiten von Expert/innen zur Erkennung von Fehlern in Laborversuchen zurückliegt oder sie bereits übertrifft).

Red-Teaming- und Uplift-Studien

Neben Benchmarks werden Tests durchgeführt, bei denen Personen oder Teams die KI-Modelle nutzen, um herauszufinden, inwieweit diese bei der Auswahl und Herstellung biologischer Agenzien bzw. Biowaffen oder der Planung und Durchführung eines Angriffs helfen könnten, indem sie die Kenntnisse bzw. Fähigkeiten der Personen verbessern. Solche Formate werden als menschliche Uplift-Studien und Red-Teaming-Übungen bezeichnet. Red Teams sind typischerweise Gruppen von Expert/innen, die eingesetzt werden, um Möglichkeiten bzw. Risiken auszutesten und Schwachstellen zu identifizieren (z. B. die Bereitschaft der Systeme, sensible Informationen zu Herstellungsprozessen preiszugeben).

Um spezifisch die Effekte von KI-Modellen zur Unterstützung bzw. Verbesserung von Kenntnissen oder Fähigkeiten von Akteuren (Uplifts) zu untersuchen, werden kontrollierte Studien durchgeführt. Dabei werden Personen (z. B. Forschende mit Laborerfahrung oder Studierende) zufällig in Gruppen eingeteilt (randomisiert), die entweder normale Internetanwendungen (z. B. Suchmaschinen, YouTube) nutzen dürfen oder diese plus die zu untersuchenden KI-Modelle (Tabelle 3.2). Insbesondere größere, potenziell aussagekräftigere kontrollierte Studien sind sehr aufwendig und teuer, unter anderem durch Kosten für die Vergütung der Teilnehmer/innen, die Entwicklung von Software und die nötigen Sicherheitsmaßnahmen (wie Dual-Use-Training oder Sicherheitsüberprüfungen) (Patwardhan et al. 2024).

Empirische Evidenz aus Evaluationen von LLMs

Evaluierungen von KI-Modellen können aus Uplift- bzw. Red-Teaming-Übungen und Benchmarks zusammengesetzt sein. Angesichts der Geschwindigkeit und Häufigkeit, mit der neue Modelle veröffentlicht und verfügbar werden, sind Benchmarks aufgrund ihrer schnellen Durchführbarkeit und geringeren Kosten ein zentraler Bestandteil der Evaluationen von LLMs geworden, z. B. bei Tests durch die Entwickler für Systemkarten⁴⁶ der Modelle (Tabelle 3.3).

Im Folgenden werden die Ergebnisse empirischer Untersuchungen verschiedener Akteure (Tabelle 3.3) dargestellt und analysiert. Keine der Studien ist in begutachteten Fachzeitschriften erschienen bzw. durchlief ein entsprechendes unabhängiges Peer-Review-Verfahren. Die oft fehlende oder nur sehr eingeschränkte Offenlegung der in den Untersuchungen gestellten Fragen bzw. Aufgaben, der erhaltenen Daten und deren Bewertungen – meist begründet mit Sorgen um die Informationssicherheit – setzt der Nachvollziehbarkeit und einer unabhängigen Analyse der Studienergebnisse relativ enge Grenzen.

Auf Benchmarks basierende Studien: LLMs können Referenzwerte für Wissen menschlicher Expert/innen erreichen und teilweise deutlich übertreffen

Die bisher in Bezug auf verschiedene LLMs umfangreichste Studie zu Biologie- und Biosecurity-relevantem Wissen wurde in einem Diskussionspapier der RAND Corporation beschrieben (Dev et al. 2025). Darin wurden 31 der Anfang Januar 2025 leistungsfähigsten LLMs (Tabelle 3.3), einschließlich 15 Open-Weight-LLMs, auf Basis von sechs öffentlich verfügbaren Benchmarks zu Wissen über relevante biologische Agenzien, Voraussetzungen für die Entwicklung von Biowaffen sowie zu Wissen bzw. Fähigkeiten für die Laborforschung untersucht. Verschiedene Modelle, darunter die Open-Weight-Modelle DeepSeek V3 und Meta Llama 3.1 405B, erreichten dabei in mehreren Benchmarks fast die Leistung menschlicher Expert/innen („human baselines“)⁴⁷. Darüber hinaus fanden die Autor/innen, dass die bei den getesteten Open-Weight-Modellen mögliche Entfernung von Safeguard-Mechanismen (Kasten 3.5) die Ablehnungsraten für Anfragen erheblich reduzieren kann, gleichzeitig allerdings die Leistungswerte beeinträchtigte.

Alle in dieser Studie genutzten Benchmarks, einschließlich solche zu Wissen über Laborarbeiten, basieren jedoch auf Fragen zu relativ leicht zugänglichem, teilweise lehrbuchartigem Wissen oder Wissen zu allgemeinen Laborarbeiten oder -protokollen. Die Relevanz der Ergebnisse hinsichtlich der für die Herstellung von Biowaffen zentralen Frage, inwieweit LLMs für die Laborpraxis relevante, aber nicht einfach zugängliche Formen von Wissen bzw. tacitem Wissen (Kapitel 3.2.2) (besser) auffindbar machen oder vermitteln können, ist daher kaum einzuschätzen.

46 Solche „system cards“ oder auch „model cards“ genannten Dokumente werden von den entwickelnden Unternehmen erstellt, um die Benutzer und Entwickler über die Eigenschaften und Anwendungen der Modelle zu informieren. Sie enthalten Informationen über das KI-Modell selbst, die verwendeten Trainingsdaten, seine Fähigkeiten, Einschränkungen, Nutzungen sowie Sicherheits- und ethische Fragen (wie zu Verzerrungen) in Bezug auf das Modell.

47 Vor allem die o1-Modellfamilie von OpenAI war nur noch etwa 6 Prozentpunkte davon entfernt, die Leistung menschlicher Expert/innen bei Wissen zu biologischen Laborprotokollen zu erreichen.

Benchmarks zielen zunehmend auf nicht ohne Weiteres zugängliches und praxisrelevantes (Erfahrungs-)Wissen

Jüngere Benchmarks bzw. auf solchen basierende Studien versuchen, diesen Punkt zu adressieren. Sie fokussieren auf für die Laborpraxis bzw. die Herstellung relevanter biologischer Agenzien wie Viren notwendiges (Erfahrungs-)Wissen, das nur Personen besitzen oder für diese zugänglich sein sollte, die im Feld tätig sind oder entsprechende Laborprotokolle selbst ausgeführt haben.

Ein solcher, bereits häufiger genutzter Benchmark ist der durch die Non-Profit-Organisation SecureBio entwickelte und im April 2025 (als Preprint) veröffentlichte Virology Capabilities Test (VCT) (Götting et al. 2025).⁴⁸ Er soll insbesondere die Fähigkeit zur Fehlerbehebung bei komplexen virologischen Laborprotokollen messen und beruht auf von Virologen entwickelten multimodalen Fragen, das heißt inklusive Bilder, deren Analyse für die Fehlersuche notwendig ist (z. B. Bilder aus Experimenten mit Zellkulturen, um bestimmte Viren zu vermehren) (Götting et al. 2025, S. 31). Diese Fragen zu verschiedenen Laborprozessen (Götting et al. 2025, S. 27 f.) sollen grundlegendes, auch implizites Wissen abdecken, das für Laborarbeiten mit Viren essenziell ist. Der Test, bei dem multiple richtige Aussagen aus einer Reihe von Möglichkeiten ausgewählt werden müssen, scheint so anspruchsvoll zu sein, dass erfahrene Virolog/innen mit Internetzugang bei Fragen zu ihren Teilgebieten durchschnittlich auf nur 22,1 % richtige Antworten (menschliche Baseline) kommen. Getestete multimodale LLMs kamen auf deutlich höhere Werte, z. B. OpenAIs o3 (43,8 %), Googles Gemini 2.5 Pro (37,6 %) oder Anthropics Claude 3.5 Sonnet (33,6 %) sowie 3.7 Sonnet (30,8 %).⁴⁹ Das in den Untersuchungen von Götting et al. (2025) (im April 2025) leistungsstärkste Modell, o3 von OpenAI, übertraf 94 % der Virologieexpert/innen innerhalb ihrer Spezialgebiete.

Der Test wurde auch als ein Element in den Modell-Evaluierungen großer LLM-entwickelnder Unternehmen wie Anthropic, Google DeepMind oder OpenAI für ihre jüngeren Modelle verwendet, darunter die Claude Opus 4 und Sonnet 4-Serie (Oktober 2025 bis Februar 2026) (Anthropic 2025c, 2025d, 2026b, 2026c), Claude Mythos Preview (April 2026) (Anthropic 2026a), Gemini 3 Pro (November 2025) (Google DeepMind 2025a) oder die GPT-5-Familie (August 2025 bis April 2026) (OpenAI 2025b, 2026). Bei allen Entwicklern zeigten die neuen Modellversionen teilweise verbesserte Leistungen verglichen zu den im vorherigen Abschnitt beschriebenen Leistungen der Vorgängermodelle (Anthropic 2025c, S. 123 f., 2025b, S. 96 f.; Google DeepMind 2025a, S. 6 f.; OpenAI 2025b, S. 24, 2026, S. 23). Inwiefern diese Unterschiede statistisch signifikant sind, ist unklar.

Weitere Tests, die Modelle in Bezug auf oft spezielles und nicht ohne weiteres zugängliches und/oder praxisrelevantes Wissen zur Herstellung biologischer Agenzien bzw. Biowaffen testen sollen, wurden bei Modellevaluierungen von Anthropic und OpenAI genutzt, die in den Systemkarten für ihre jüngeren Modelle beschrieben sind (Anthropic 2025b, 2026b; OpenAI 2025b, 2026). Hierzu gehören etwa Tests, in denen tazites Wissen zu allen Schritten der Biowaffenentwicklung getestet werden soll. Diese Tests umfassen (nicht offengelegte) Fragen, die für nicht in „dem Feld“⁵⁰ arbeitende Personen schwer zu beantworten sind, einschließlich Fragen zur Fehlerbe-

48 Dieser Test und die Ergebnisse der Studie von Götting et al. (2025) wurden unter anderem auch im Nachrichtenmagazin TIME aufgegriffen (Chow 2025).

49 Der Standardfehler der Mittelwerte wurde in allen Modellen mit unter 1 % angegeben (Götting et al. 2025, S. 8). Diese Angabe ist eine Möglichkeit, um die statistische Signifikanz von Ergebnissen abzuschätzen. In diesem Fall sollten die wahren Messwerte eines Modells in 95 % aller Messungen in einem Bereich der angegebenen Mittelwerte +/- des 1,96-Fachen dieses Standardfehlers liegen. (Eine Angabe zu dem Standardfehler des menschlichen Referenzwertes konnte nicht gefunden werden.)

50 Welches Feld (im Original „field“) genau gemeint ist (z. B. Biosecurity allgemein, eine bestimmte Disziplin wie Virologie, oder Spezialfähigkeiten wie die Aerolisierung bestimmter Bakteriensporen oder Ähnliches, Kapitel 3.2.2), und wie dieses Feld oder die damit gemeinte Expertise mit den verschiedenen Schritten der Biowaffenherstellung in Zusammenhang steht, wird nicht präzisiert bzw. offengelegt.

bung in Laborprotokollen⁵¹ (OpenAI 2025b, S. 26, 2026, S. 24 f.). In diesen Tests übertrafen jüngere Modelle wie OpenAIs GPT-5.5-Modellvarianten (April 2026) die 80-Perzentilbasislinie der Expert/innen (das heißt, 80 % der Expert/innen erreichten oder lagen unter diesem Wert, 20 % darüber) (OpenAI 2026, S. 25).

Inwieweit existierende Benchmarks praxisrelevantes (Erfahrungs-)Wissen testen können, ist fraglich

Wie aussagefähig diese Tests und ihre Ergebnisse in Bezug auf die Unterstützung durch LLMs bei der Gewinnung von schwer zugänglichem bzw. tazitem Wissen zur Herstellung relevanter und waffenfähiger biologischer Agenzien bzw. von Biowaffen (Kapitel 3.2.2; einschließlich Prozessen wie die Massenproduktion oder Formulierung/Modifikation von Agenzien) sind bzw. sein könnten, ist nicht belastbar zu beurteilen. Gründe hierfür sind zum einen die nicht offengelegten Details zu Fragen und Aufgaben sowie zur Expertise der bewertenden Expert/innen (insbesondere in Bezug auf tatsächlich biowaffenrelevante Prozesse und Fähigkeiten). Zum anderen schienen bei Tests wie dem oft genutzten VCT (Götting et al. 2025) relevante biologische Agenzien bzw. Prozesse (aus Sicherheitsgründen) nicht berücksichtigt worden zu sein (Götting et al. 2025, S. 3, 10). Schließlich ist unklar, inwieweit bestimmte Formen von tazitem Wissen, die für den praktischen Erfolg der Biowaffenbeschaffung bzw. -herstellung entscheidend sein können, von den Tests abgedeckt bzw. erfassbar sind. Hierzu könnten, wie auch Götting et al. (2025) diskutieren, somatisches tazites Wissen, das körperliche mechanische Fertigkeiten oder Know-how umfasst, oder kollektives implizites Wissen, das aus der Interaktion mehrerer Expert/innen mit unterschiedlichen fachlichen Hintergründen entsteht, gehören (Kapitel 3.2.2).

Diese Unsicherheiten könnten (zumindest bis zu einem bestimmten Grad) durch kontrollierte Studien in realen biologischen Laboren adressiert werden. So zeigte etwa die bisher größte Studie dieser Art (Hong et al. 2026) (Abschnitt – Erste Uplift-Studien in biologischen Labors) eine klare Diskrepanz zwischen den Leistungswerten von LLMs bei digitalen Benchmarks, die Referenzwerte menschlicher Expert/innen zum Teil klar übersteigen, und den Fähigkeiten von LLMs, Personen – zumindest solche ohne wesentliche Laborerfahrung – in realen biologischen Laboren unterstützen zu können. Dieses Ergebnis hat viele Expert/innen (aus dem Biosecurity-Bereich oder der Virologie) überrascht (Active Site 2026; Parry et al. 2026).

Erste Benchmarks zu agentischen Fähigkeiten: unzureichend erklärte Bewertungen mit unklaren Implikationen

Darüber hinaus wurden in den Systemkarten für die jüngeren Modelle von Anthropic und OpenAI (Anthropic 2025b, 2025d, 2025c, 2026b, 2026c, 2026a; OpenAI 2025b) Ergebnisse erster Tests gezeigt, die agentische Fähigkeiten der Modelle (Kasten 2.3, Kapitel 2.3) untersuchen sollten. Hierzu gehören Tests für das Entwerfen von DNA-Fragmenten, die sich zu Genomabschnitten pathogener Viren zusammenfügen und DNA-Screeningverfahren von Gensyntheseunternehmen umgehen könnten. Bei Anthropic (2025c, S. 124 f., 2026b, S. 174 f., 2026a, S. 30) erreichten auch die neuesten Modelle dabei nicht die von dem Unternehmen als kritisch bewertete Schwelle, Sequenzen so zu entwerfen, dass sie sowohl zusammenfügbar wären als auch Synthesescreeningprotokolle umgehen könnten. In entsprechenden Untersuchungen von OpenAI (2025b, S. 27) ak-

51 Hierbei handelte es sich um Protokolle von Forschenden mit einem Dokortitel in Virologie, Genetik, Mikrobiologie oder Protein-Engineering.

zeptierten wohl nur Helpful-only-Modellversionen, also Modellversionen mit entfernten „safeguards“, diese Aufgabe. Eine solche Helpful-only-Version des Modells gpt-5-thinking übertraf dabei den Referenzwert für erfahrene menschliche Personen. Die Bewertungen sanken aber deutlich für DNA-Fragmente, die auch Synthescreeningprotokolle umgehen könnten. Eine weitere Erklärung bzw. Einordnung der gemessenen Werte wurde nicht gegeben. Alle Bewertungen lagen auf dem Niveau einer Helpful-only-Version des Vorgängermodells o3 (OpenAI 2025b, S. 27). Weitere Tests für agentische Fähigkeiten der Modelle untersuchten die Nutzung von Bioinformatik-Werkzeugen⁵² für mehrstufige (nicht näher beschriebene) Analyse- und Designaufgaben im Zusammenhang mit Krankheitserregern (Anthropic 2025d, 2025c, 2026c, 2026b), RNA-Sequenzen (Anthropic 2026a) oder das Zusammenfügen von DNA-Fragmenten über ein Laborrobotersystem (OpenAI 2025d). Anthropic (2026b, S. 180) kam bei der (nicht weiter erklärten) Auswertung der Ergebnisse zusammen mit externen Expert/innen zu dem Schluss, dass das Modell Claude Opus 4.6 erstmals über der Schwelle lag, ab der nicht mehr mit Sicherheit ausgeschlossen werden kann, dass das Modell bereits besorgniserregende Fähigkeiten hat (das heißt zur Unterstützung des Designs von Krankheitserregern und der Vorhersage von Krankheitserregervarianten). Außerdem übertraf das Modell bei bestimmten Aufgaben mit Relevanz für das Design von Molekülen die Leistungen der meisten menschlichen Expert/innen (Anthropic 2026a, S. 31 ff.). Bei OpenAIs Test zu der Laborautomatisierungsaufgabe erreichte die Helpful-only-Version des Modells gpt-5-thinking die menschlichen Referenzwerte, was laut dem Unternehmen (ohne weitere Erklärung) „auf eine teilweise, aber unvollständige End-to-End-Automatisierungsunterstützung hindeutet“⁵³ (OpenAI 2025b, S. 27).

Uplift- und Red-Teaming-Studien zeigen kein einheitliches Bild hinsichtlich der Frage, inwieweit LLMs böswillige Akteure unterstützen können – insbesondere die Bedeutung in der Praxis ist unklar

Im Juni 2023 erschien eine aufsehenerregende (Preprint-)Veröffentlichung⁵⁴ über eine Übung mit Studierenden des Massachusetts Institute of Technology (MIT) ohne naturwissenschaftlichen Hintergrund. Sie sollten ausprobieren, ob bzw. wie LLM-Chatbots sie unterstützen könnten, Erreger zur Auslösung einer Pandemie zu identifizieren und zu beschaffen bzw. herzustellen (Soice et al. 2023). In der einstündigen Übung schlugen ihnen die getesteten Chatbots (GPT-4, Bard, Bing, FreedomGPT) vier potenzielle Pandemieerreger⁵⁵ vor, erklärten, dass und wie diese aus synthetischer DNA erzeugt werden können bzw. könnten, gaben Hinweise auf DNA-Syntheseunternehmen, die potenziell kein Sequenzscreening (Kasten 3.6, Kapitel 4.7.3) durchführen; identifizierten Publikationen, die Herstellungsmethoden enthalten, und wiesen auf die Möglichkeit hin, gegebenenfalls Auftragsforschungsinstitute mit praktischen Arbeiten zu beauftragen. Um gelegentliche Ablehnungen der Chatbots auf manche Prompts zu umgehen (wie zur Umgehung der DNA-Syntheseüberprüfung), wurden bekannte Jailbreakingtechniken (Kasten 3.5) genutzt, die im Internet nach Suche von Anleitungen zum Jailbreaking von LLMs gefunden wurden.

52 Beispielsweise zur Vorhersage der Effekte genetischer Varianten oder zur Proteinfaltung (Kapitel 2.3).

53 Im Original: „indicating partial but incomplete end-to-end automation support“.

54 Die nicht in einer begutachteten Fachzeitschrift (Stand Mai 2026) erschienene Studie erfuhr ein relativ großes Echo in verschiedenen Medien (Holland 2023; Landsverk 2023; Matthews 2023; Newey/Nuki 2023; Service 2023).

55 Diese waren das Pockenvirus (*Variola major*), das Virus der Grippepandemie von 1918, 2012 über Mutationen erzeugte H5N1-Vogelgrippeviren mit Übertragbarkeit durch die Luft auf Frettchen (einem Influenzatierrmodell für den Menschen) (Herfst et al. 2012; Imai et al. 2012) sowie der Bangladeschstamm des Nipahvirus.

Kasten 3.5 Jailbreaking – Umgehen eingebauter Sicherheitsmechanismen

Jailbreaking in Bezug auf KI bzw. LLMs bedeutet, Schwachstellen in Sicherheitsvorkehrungen oder auch in Mechanismen für politisch motivierte⁵⁶ Einschränkungen eines Modells („safeguards“, „guardrails“) (Dong et al. 2025; Qi et al. 2024 und Referenz darin) zu nutzen, um das KI-Modell zu Aktionen zu bringen oder Antworten zu erhalten, die normalerweise blockiert würden.

Ansätze hierfür können auf unterschiedlichen Ebenen ansetzen, wie bei Whiteboxmethoden über den Zugang zur Modellarchitektur bzw. zu zentralen Modellparametern, die bei Open-Weight-Modellen⁵⁷ öffentlich zugänglich sind, oder über die spezielle Gestaltung von Eingaben, der Prompts, bei Blackboxmethoden, wofür ein solcher Zugang und gewisse Fachkenntnisse nicht erforderlich sind (Dong et al. 2025; Zhang et al. 2025a).

Insbesondere letztere Art von Jailbreaks werden relativ häufig verwendet. Beispielsweise, indem anstatt eine direkte Anfrage nach eingeschränkten Inhalten zu stellen, die Anfrage im Zusammenhang mit einer Recherche oder Dokumentation für einen positiven bzw. legitim erscheinenden Zweck, wie etwa der Arbeit an einem Impfstoff, formuliert wird (siehe hierzu Studie mit Studierenden von Soice et al. 2023, S. 3). Bereits mit dieser einfachen Methode können verschiedene Modelle Informationen zu für Biowaffen nutzbaren biologischen Agenzien, einschließlich Möglichkeiten und (öffentlich verfügbare) Protokolle zu deren Beschaffung bzw. Herstellung, zur Verfügung stellen (Sabra/Frieß 2025; Soice et al. 2023) oder Angriffspläne vorschlagen und deren Bedingungen analysieren (Sabra/Frieß 2025).

Das Wissen um Jailbreaks scheint dabei zumindest bei Studierenden bzw. allgemein jüngeren, mit LLMs eher vertrauten Personen als Standardzustand angenommen zu werden. So wurden beispielsweise in der großen menschlichen Uplift- bzw. Red-Teaming-Studie des KI-Unternehmens OpenAI mit Student/innen und Expert/innen (Patwardhan et al. 2024) (Tabelle 3.3) den (wohl älteren) teilnehmenden Expert/innen nur Modellversionen mit entfernten Sicherheitsvorkehrungen zur Verfügung gestellt, um „die vergleichsweise geringere Vertrautheit der Experten mit Modellen“ auszugleichen, sodass Kenntnisse über LLM-Jailbreaks nicht erforderlich waren^{58, 59}. In Übereinstimmung mit dieser Annahme gaben ca. 90 % der Teilnehmer/innen einer neueren Uplift-Studie mit Studierenden an, dass sie trotz der Sicherheitsvorkehrungen der Modelle („safeguards“) kaum Schwierigkeiten hatten, an Biosecurity-relevante Informationen zu gelangen (Zhang et al. 2026).

56 Beispielsweise müssen in China KI-generierte Inhalte die „sozialistischen Grundwerte“ des Landes widerspiegeln (Lu 2025; UVA 2025) (Kapitel 4.6.1). Dies scheint auch zu beinhalten, dass unter anderem Fragen zu der gewaltsamen Niederschlagung der Studierendenproteste auf dem Pekinger Tiananmenplatz im Juni 1989 z. B. durch das chinesische LLM DeepSeek nicht beantwortet werden (Hombert 2025; Lu 2025; Valko 2025).

57 Diese Parameter („weights“) bestimmen, wie ein Modell Eingaben verarbeitet und Ausgaben erzeugt. Der Zugang zu ihnen reicht nicht nur aus, um das Modell für spezielle Anwendungsfälle anzupassen, sondern oft auch, um „safeguards“ zu entfernen (CFG 2025; Qi et al. 2024). Im Gegensatz zu vollständig offenen Open-Source-Modellen werden der Quellcode (der für Menschen lesbare, in Programmiersprache verfasste Text einer Software), die Trainingsdaten und die Trainingsmethoden aber nicht offengelegt.

58 Im Original: „Furthermore, we mitigated experts’ comparatively lower familiarity with models [...], so knowledge of LLM jailbreaks was not necessary.“

59 Jedoch legt es beispielsweise eine in der Systemkarte (vom August 2024) des Modells GPT-4o von OpenAI gezeigte Auswertung nahe, dass Modellversionen ohne „safeguards“ (auch) bei Expert/innen zu keiner deutlichen Verbesserung, verglichen mit der Modellversion mit „safeguards“, führte (OpenAI 2024, S. 14).

Bei genauerem Hinsehen scheinen jedoch Zweifel an der Schlussfolgerung der Autor/innen aus den Ergebnissen der Studie angebracht, „LLMs werden Agenten mit pandemischem Potenzial allgemein zugänglich machen, sobald diese glaubwürdig identifiziert sind, selbst für Personen mit wenig oder gar keiner Laborausbildung“⁶⁰ (Soice et al. 2023, S. 1). Denn zum einen gab es keine Kontrollgruppe, der nur klassische Internetsuche zu Verfügung stand (Tabelle 3.2), sodass die Ergebnisse keine Rückschlüsse darauf zulassen, inwieweit die erhaltenen Ergebnisse nicht auch über konventionelle Internetsuche erzielbar gewesen wären (siehe nachfolgend). Zum anderen zeigt die Analyse der durch die LLMs erhaltenen Quellen, dass die vorgeschlagenen Viren nur wenig aussichtsreiche hypothetische Pandemieerreger wären (wie von den Autor/innen auch diskutiert) (Soice et al. 2023, S. 3), sowie dass im Fall des Pockenvirus eine potenzielle Herstellung über synthetisierte DNA-Fragmente (nach dem Vorbild der Synthese des Pferdepockenvirus (Noyce et al. 2018) sehr komplex wäre⁶¹. Die notwendigen Arbeiten erfordern neben Infrastrukturvoraussetzungen insbesondere langjährige Laborerfahrung in verschiedenen Bereichen und Insiderwissen (DeFrancesco 2021, S. 1187 ff.; Noyce/Evans 2018). Die Synthese des Pockenvirus wäre somit nicht „für Personen mit wenig oder gar keiner Laborausbildung“ zugänglich. Weiterhin erbrachte die Studie keine Ergebnisse, die darauf hindeuten, dass sich dies zukünftig ändern könnte. So existiert die in der Publikation thematisierte potenzielle Nutzung (für welche Schritte wird nicht angegeben) von Auftragsforschungsinstituten wie etwa Cloud Labs seit längerer Zeit und es ist unklar, ob solche Experimente dort durchgeführt würden oder solche Einrichtungen ohne Weiteres für Personen mit fehlender fachlicher Erfahrung erfolgreich nutzbar sind oder zukünftig werden könnten (Kapitel 3.3.2, 4.7.3). Auch die Herstellungsprozeduren in den für die anderen Viren angegebenen Publikationen (Methodenabschnitte in Griffin et al. 2019; Perez et al. 2017; Yoneda et al. 2006) – darunter komplexere DNA-Klonierungstechniken, Zellkulturverfahren, Virus-Titer-Bestimmungen in vitro und in vivo sowie Tierexperimente – erfordern breit gefächertes Methodenwissen und zumindest zum Teil erhebliche Laborerfahrung.

Kontrollierte Uplift-Studien und Red-Teaming-Übungen hinsichtlich des Wissens und der Planungsfähigkeiten

In zwei größeren Studien mit menschlichen Testpersonen unter Einbeziehung von Kontrollgruppen, die nur Zugang zu klassischer Internetsuche hatten, wurde untersucht, ob LLMs die Fähigkeit von Personen, eine biologische Bedrohung zu schaffen, erhöhen könnten, indem sie den Zugang zu Informationen deutlich verbessern bzw. die Biowaffenentwicklung oder Angriffsplanung unterstützen könnten. Eine Studie wurde von der RAND Corporation⁶² (Mouton et al. 2024), die zweite (Patwardhan et al. 2024) von dem Unternehmen OpenAI in Zusammenarbeit mit Biosecurity-Expert/innen des Beratungsunternehmens Gryphon Scientific⁶³ durchgeführt (für Details zum Studiendesign Tabelle 3.3).

In der Studie von Mouton et al. (2024) hatten kleine interdisziplinäre Teams von Forschenden aus den Bereichen Biologie, KI/LLMs und Biosecurity/Strategie die Aufgabe bekommen, böswillige

60 Im Original: „Collectively, these results suggest that LLMs will make pandemic-class agents widely accessible as soon as they are credibly identified, even to people with little or no laboratory training.“

61 Die notwendigen Prozeduren sind insbesondere aufgrund des großen Virusgenoms und der notwendigen Schritte, um das Virus in Zellen zu replizieren, sehr komplex (DeFrancesco 2021; Noyce et al. 2018; Noyce/Evans 2018).

62 Ein amerikanisches Non-Profit-Forschungsinstitut und Beratungsunternehmen für den öffentlichen Sektor. RAND wird sowohl aus öffentlichen als auch aus privaten Mitteln finanziert.

63 Gryphon Scientific ist ein kleineres, 2005 gegründetes US-amerikanisches Beratungsunternehmen für Fragen der Gesundheit, Sicherheit und Gefahrenabwehr. Es wurde im April 2024 vom Deloitte übernommen (Deloitte o. J.).

nicht staatliche Akteure zu spielen und innerhalb von 7 Wochen einen biologischen Angriff für verschiedene Zwecke zu planen. Es konnten keine statistisch signifikanten Unterschiede⁶⁴ zwischen den (in der Publikation nicht offengelegten) Plänen festgestellt werden, die nur auf Basis einer Internetsuche erstellt wurden, und den Plänen, die mit Unterstützung durch zwei nicht namentlich genannten LLMs erstellt wurden. Darüber hinaus wurde keiner der entstandenen Pläne von den für die Bewertung eingesetzten Expert/innen aus den Bereichen Biologie und Biosecurity als ausreichend detaillierte oder haltbare Grundlage zur Durchführung eines wirksamen biologischen Angriffs beurteilt. Spezifische, dieser Bewertung zu Grunde liegende Fehler bzw. Punkte wurden nicht veröffentlicht.

In der OpenAI-Studie (Patwardhan et al. 2024) mussten promovierte Forschende (aus Genetik, Mikrobiologie, Virologie) mit Laborerfahrung oder Studierende (mit mindestens einem absolvierten Kurs in Biologie) Forschungsaufgaben⁶⁵, die die verschiedenen Phasen der Biowaffenentwicklung (Kapitel 3.2.2) betrafen, in 5 Stunden lösen. Die Ergebnisse wurden durch Expert/innen (unter anderem in Virologie und Dual-Use-Forschung) bezüglich Faktoren wie Genauigkeit, Vollständigkeit und der Fähigkeit, neuartige Ansätze für die Aufgabe zu entwickeln, bewertet. Sowohl für die teilnehmenden Expert/innen als auch für die Studierenden konnten keine statistisch signifikanten Unterschiede zwischen den Mittelwerten der Ergebnisse der Teilnehmer/innen, die nur Zugang zum Internet hatten, und denjenigen, die das LLM GPT-4 nutzen konnten, gezeigt werden (auch nicht in Bezug auf die durchschnittliche Zeit, die zur Lösung der Aufgaben benötigt wurde).

In den Systemkarten für seine jüngeren LLMs der Claude Opus- bzw. Sonnet-Serie (Mai 2025 bis Februar 2026) sowie Claude Mythos Preview (April 2026) beschrieb das Anthropic (2025b, 2025c, 2026a, 2026b) Ergebnisse menschlicher Uplift-Studien und Red-Teaming-Übungen. In den Uplift-Studien sollten zum einen die Modellfähigkeiten⁶⁶ untersucht werden, Personen oder Gruppen mit grundlegenden technischen Kenntnissen (z. B. Bachelor-Abschluss in MINT-Fächern) dabei zu unterstützen, einen detaillierten Plan für die Beschaffung von Biowaffen zu entwerfen. Zum anderen sollten Fähigkeiten der Modelle getestet werden, „staatliche Programme mit moderaten Ressourcen“ erheblich zu verbessern (z. B. durch neuartige Waffendesigns, einer erheblichen Beschleunigung bestehender Prozesse oder einer drastischen Verringerung technischer Hindernisse). Testpersonen hierfür waren Expert/innen mit Doktorgrad, die schrittweise ein Protokoll für die Rekonstruktion eines schwierig herzustellenden Virus erstellen sollten. In beiden Fällen wurden Steigerungen (Uplifts) zur Kontrollgruppe (nur Internetsuche) in den nicht näher beschriebenen Bewertungen der Leistungen um das 2,53-Fache bei Personen mit grundlegenden technischen Kenntnissen (Claude Opus 4) (Anthropic 2025b, S. 93) und ca. 2-Fache bei Expert/innen festgestellt (Claude Opus 4 und 4.5) (Anthropic 2025c, S. 130 f.). Angaben zur statistischen Signifikanz der Ergebnisse wurden nicht gemacht. Die erhaltenen Werte bewegen sich noch unterhalb von durch Anthropic festgelegten Schwellenwerten, ab denen nicht mehr mit Sicherheit ausgeschlossen werden kann, dass ein Modell bereits besorgniserregende Fähigkeiten hat (welche interne Sicherheitsstufen mit zusätzlichen Schutzmaßnahmen erfordern würden). Anscheinend etwas niedrigere Uplift-Werte hinsichtlich der Erstellung von Herstellungsprotokollen für Viren durch promovierte Biolog/innen wurden für die jüngeren Modelle Claude Opus 4.6 (Februar 2026) und Claude

64 Einfach ausgedrückt ist statistische Signifikanz ein Maß dafür, ob ein beobachteter Effekt oder Zusammenhang in Daten wahrscheinlich ein tatsächlich zugrunde liegendes Muster oder einen echten Unterschied widerspiegelt oder ob er zufällig entstanden sein könnte.

65 Diese wurden aus Gründen der Informationssicherheit nicht näher beschrieben.

66 Getestet wurden typischerweise firmeninterne Versionen der Modelle ohne „safety guardrails“.

Mythos Preview (April 2026) erhalten (Anthropic 2026a, S. 28, 2026b, S. 177).⁶⁷ In den Red-Teaming-Untersuchungen befragten Biosecurity-Expert/innen die Modelle und bewerteten deren Fähigkeit, Unterstützung in verschiedenen Bereichen und Szenarien der Biowaffenentwicklung zu bieten. Anstelle eines festen Schwellenwerts legten die Expert/innen einen detaillierten Bericht vor, in dem sie bewerteten, ob der Einsatz der Modelle Expert/innen bei der Entwicklung neuartiger biologischer Bedrohungen wesentlich unterstützen könnte. Danach können die jüngeren Modelle zwar schnell viele Ideen für Ansätze liefern, die teilweise zu erhöhten biologischen Bedrohungen führen könnten, jedoch wurde keiner der generierten Ideen bzw. Pläne als wirklich innovativ (das heißt über bereits in der wissenschaftlichen Literatur Etabliertes hinausgehend) oder als erfolgsversprechend eingestuft. Darüber hinaus wurden erhebliche Einschränkungen festgestellt, darunter technische Lücken, unterwürfiges Verhalten, halluzinierte Zitate und mangelndes strategisches Urteilsvermögen bei der Unterscheidung zwischen hochwertigen bzw. realistisch umsetzbaren und unplausiblen, nicht umsetzbaren Ideen (Anthropic 2026a, S. 29, 2026b, S. 178).

Zwischen 2023 und Mitte 2025 führte das UK AI Security Institute (AISI) Uplift-Studien zur Erstellung von Laborprotokollen und Fehlerbehebung in den Protokollen für nicht näher beschriebene Aufgaben aus der Bakteriologie und Virologie durch. Testpersonen ohne wissenschaftlichen Hintergrund, die nicht genannte Frontier-LLMs nutzen durften, waren dabei deutlich (4,7-mal) und wohl statistisch signifikant häufiger in der Lage, umsetzbare Protokolle zur Herstellung von Viren zu erstellen, als Personen aus der Kontrollgruppe, die ausschließlich das Internet nutzen durften (AISI 2025, S. 16).

In einer jüngeren und im Vergleich zu der AISI-Studie ausführlicherer beschriebenen Uplift-Studie von Zhang et al. (2026) mit Studierenden aus MINT- und Nicht-MINT-Fächern, die über wenig bis gar keine Erfahrung in der Durchführung komplexer biologischer Experimente verfügten, hatte die LLM-Gruppe Zugang zu mehreren KI-Modellen (o4-mini, o3, Gemini 2.5 Pro, Claude 3.7 Sonnet und Claude Opus 4). Sie konnten diese koordiniert nutzen, um Informationen verschiedener Modelle miteinander zu vergleichen bzw. zu überprüfen.⁶⁸ Den Teilnehmer/innen wurden (im Detail nicht offengelegte) Fragen aus verschiedenen öffentlich und nicht öffentlich zugänglichen Benchmarks vorgelegt, beispielsweise zur Fehlerbehebung in Protokollen aus der Virologie, zum Umgang mit Krankheitserregern oder zum Wissen über biologische Zusammenhänge und Techniken. Die Tests waren im Multiple-Choice-Format. Nur bei Fragen aus einer Benchmark mussten kurze Antworten gegeben werden. Darüber hinaus waren Programmier- bzw. agentische Aufgaben, wie zur Interaktion mit simulierten Laborgeräten (z. B. Liquid-Handling-Robotern) und der Erstellung eines anspruchsvollen, mehrstufigen Protokolls zur Konstruktion eines potenziellen neuartigen biologischen Agens, zu lösen. Diese Aufgaben wurden nur Teilnehmer/innen mit einem MINT-Hintergrund und Erfahrung in der Python-Programmierung⁶⁹ zugewiesen. Die Leistungswerte der durch LLMs unterstützten Teilnehmer/innen waren bei sieben der acht Benchmarkaufgaben deutlich höher als die der Kontrollgruppe. Diese Unterschiede wurden als statistisch signifikant bewertet (Zhang et al. 2026, S. 2, 21). Darüber hinaus übertrafen die durchschnittlichen Leistungswerte der LLM-Gruppe bei drei der vier Benchmarks, für die Expertendaten vorlagen, die menschlichen Basiswerte von Expert/innen (mit nur Internetzugang). Über alle Benchmarkaufga-

67 Die erhaltenen Uplifts sind nicht streng vergleichbar. So hatten die Gruppen in den Versuchen mit Claude Opus 4.6 und Claude Mythos 3 Tage Zeit, um die Aufgabe zu erfüllen, während die Gruppen in den Opus 4.5-Versuchen 4 Tage Zeit hatten (Anthropic 2026a, S. 28, 2026c, S. 177).

68 Dabei gaben die allermeisten Teilnehmer/innen (89,6 %) an, dass sie trotz der Sicherheitsvorkehrungen der Modelle („safeguards“) kaum Schwierigkeiten hatten, an Dual-Use- bzw. Biosecurity-relevante Informationen zu gelangen.

69 Python ist eine vielseitige Open-Source-Programmiersprache, die verschiedene Programmieransätze für diverse Anwendungen unterstützt.

ben hinweg geben die Autor/innen eine Leistungssteigerung durch den Zugang zu den LLMs um das 4,16-Fache (95 % Konfidenzintervall [2,63; 6,87])⁷⁰ an, die sie als statistisch robust bezeichnen.

Die Ergebnisse kontrollierter Uplift-Studien zeigen kein einheitliches Bild hinsichtlich der Frage, inwieweit LLMs böswillige Akteure in der Praxis besser unterstützen können als eine konventionelle Internetsuche

Somit zeigen die bisherigen Studien keine einheitlichen Ergebnisse bezüglich möglicher Verbesserungen (der (Theorie-)Leistungen durch einen LLM-Zugang im Vergleich zu den Leistungen von Personen mit reinem Internetzugang).

In den größeren Studien von Mouton et al. (2024) und Patwardhan et al. (2024), konnten keine statistisch signifikanten Leistungsverbesserungen (Uplifts) bei Anfängern (also Personen ohne oder mit wenig Biologieerfahrung) oder Expert/innen nachgewiesen werden. Dies bedeutet jedoch nicht zwangsläufig, dass die (zu dem Zeitpunkt) getesteten Modelle die Gewinnung von Wissen zur Planung bzw. Entwicklung von Biowaffen nicht grundsätzlich erleichtern oder besser unterstützen könnten als die konventionelle Internetnutzung. Es könnte beispielsweise möglich sein, dass Verbesserungen von der Vorbildung bzw. den Erfahrungsunterschieden zwischen Personen (auch zwischen Expert/innen) abhängen und/oder nur bestimmte Schritte der Herstellung bzw. Nutzung von Biowaffen betreffen. In Übereinstimmung mit dieser Möglichkeit zeigte eine Studie, die ähnlich zu (Patwardhan et al. 2024) durchgeführt und in der Systemkarte für OpenAls Modell GPT-4o beschrieben wurde, eine deutliche (möglicherweise statistisch signifikante) Verbesserung der Leistungsbewertungen nur für die Gruppe der Studierenden (nicht aber für die Gruppe der Expert/innen) und nur bei Aufgaben der Ideenfindung (OpenAI 2024, S. 14). Auch die relativ deutlichen, potenziell statistisch signifikanten Verbesserungen (hier bezüglich der Beschaffung von Biowaffen) in den Uplift-Studien in Anthropic Systemkarten für manche der jüngeren Claude Opus-Modelle (Anthropic 2025b, S. 93, 2025c, S. 130f.; siehe vorheriger Abschnitt) stehen im Einklang mit dieser Möglichkeit.

Die in der Studie von Zhang et al. (2026) festgestellten deutlichen und wohl statistisch signifikanten Leistungssteigerungen bei Teilnehmer/innen mit LLM-Zugang bei fast allen der Benchmarkaufgaben sowie über alle Benchmarks hinweg legen nahe, dass die Nutzung mehrerer LLMs die Leistungen von Studierenden mit wenig oder keiner Biologieerfahrung bei der Beantwortung von Fragen bzw. der Lösung von Aufgaben zu sicherheitsrelevantem biologischem Wissen, Zusammenhängen oder Techniken deutlich verbessern kann – teilweise auf oder über das Leistungsniveau von Expert/innen (mit nur Internetzugang) hinaus. Wie zuvor im Zusammenhang mit Benchmarks diskutiert, testet jede Benchmark nur einen Teil der notwendigen Schritte und die bei der Studie überwiegend verwendeten Multiple-Choice-Formate, die ursprünglich zur automatisierten Testung von LLMs entwickelt wurden, spiegeln nicht notwendigerweise die Problematik der Implementierung komplexer Versuche oder Herstellungsprozesse wider, mit der Akteure in der realen Welt konfrontiert sind. In Übereinstimmung damit erhöhte die Nutzung von LLMs bei der einzigen Aufgabe, die einen solchen komplexen mehrstufigen Prozess zur Herstellung eines neu-

70 95 % Konfidenzintervall für das Chancenverhältnis („odds ratio“) von 2,63 bis 6,87. Dieses Intervall überdeckt den wahren Wert mit 95 % Wahrscheinlichkeit. Aus einem Konfidenzintervall lassen sich Rückschlüsse auf die statistische Signifikanz ableiten. Enthält ein 95 % Konfidenzintervall nicht den Wert des Nulleffekts (z. B. 0 bei der Differenz zweier Mittelwerte oder 1 bei einem „odds ratio“), so gilt das Ergebnis als statistisch signifikant (auf dem Signifikanzniveau des Konfidenzintervalls, hier $\alpha = 5\%$ für den Ausschluss eines Nulleffekts) (Bender/Lange 2001; Rohmann 2020).

artigen biologischen Agens (in der Theorie) simulieren sollte, die Leistungen der Teilnehmer/innen nicht.

Jedoch selbst wenn alle Uplift- bzw. Red-Teaming-Studien, die unterschiedliche Fragen bzw. Aufgaben adressieren, statistisch signifikante Verbesserungen hinsichtlich der Gewinnung von Wissen zur Planung bzw. Entwicklung von Biowaffen und deren Nutzung nachweisen, wäre diese Signifikanz der Ergebnisse nicht mit praktischer Signifikanz gleichzusetzen. Was solche Ergebnisse für die praktische Umsetzung des gewonnenen Wissens und der entwickelten Pläne bedeuten, also in Bezug auf die verschiedenen Hürden für die Biowaffenherstellung in der realen Welt – einschließlich der erfolgreichen praktischen Durchführung von Laborarbeiten zur Herstellung relevanter biologischer Agenzien oder darüber hinaus für biowaffenrelevante Prozesse wie die Formulierung oder Modifikation von Agenzien (Kapitel 3.2.2) – bliebe nach wie vor unklar.

Erste Uplift-Studien in biologischen Labors stellen LLMs als Gamechanger für Personen ohne oder mit sehr wenig Laborerfahrung infrage

Um die Frage der praktischen Signifikanz zu adressieren, werden derzeit Ansätze für kontrollierte Studien in realen biologischen Labors verfolgt. Diese sollen helfen zu beurteilen, ob beispielsweise die neuesten multimodalen LLMs Nichtexpert/innen dabei unterstützen oder befähigen können, biologische Aufgaben auf Expert/innen-Niveau auszuführen. Abhängig von den gestellten biologischen Aufgaben (z. B. wie konkret bzw. relevant diese in Bezug auf waffenfähige biologische Agenzien gestaltet werden können bzw. dürfen) und den Bedingungen solcher Studien (z. B. der zur Verfügung gestellten Laborinfrastruktur) könnten daraus realistischere Rückschlüsse auf mögliche Risiken durch die getesteten LLMs gezogen werden. Vorangetrieben werden solche Ansätze vor allem von Non-Profit-Organisationen, wie dem Frontier Model Forum⁷¹ und Sentinel Bio, in Zusammenarbeit mit KI entwickelnden Unternehmen (Anthropic 2025e; FMF 2025; Google DeepMind 2025a; Sentinel Bio 2025).

Eine erste größere Studie⁷² dieser Art wurde im Februar 2026 veröffentlicht (Active Site 2026; Hong et al. 2026). In der Studie wurden 153 Teilnehmer/innen mit minimaler vorheriger Laborerfahrung rekrutiert (die allermeisten davon MINT-Bachelor-Studierende, 50 % davon aus biologischen Bereichen) und ihnen acht Wochen Zeit gegeben, um verschiedene molekularbiologische Aufgaben auszuführen, die einige grundlegende, in der Virologie und Molekularbiologie erforderliche technische Fähigkeiten repräsentieren. Hierzu gehörten drei Kernaufgaben: erstens eine Zellkulturaufgabe (das Kultivieren, ausgehend von kryopräservierten Zellen, über mehrere Generationen einer menschlichen Zelllinie, die in der Biotechnologie zur Herstellung therapeutischer Proteine und Viren für die Gentherapie genutzt wird); zweitens die DNA-Klonierung (Zusammenfügen von DNA-Stücken zu einem Plasmid); und drittens die Virusproduktion (Her-

71 Das Frontier Model Forum ist eine von der Industrie unterstützte Non-Profit-Organisation, die sich mit Risiken für die öffentliche und die nationale Sicherheit befasst.

72 Anthropic führte nach eigenen Angaben 2024 eine vorläufige, kleine Laborstudie zu (nicht genannten) grundlegenden biologischen Laborprotokollen durch. In dieser Studie konnten keine Anzeichen für einen Uplift durch Zugang zu LLMs beobachtet werden. Jedoch wurde angemerkt, dass alle Teilnehmer/innen, einschließlich der Gruppe, die nur Internetzugang hatte, bei allen Aufgaben im realen Labor überraschend gut abschnitten (Anthropic 2025e). Auch das Los Alamos National Laboratory berichtete von einer kleinen Pilotstudie (Romero-Severson et al. 2025). Die Relevanz der Ergebnisse – drei von fünf Teilnehmer/innen der Kontrollgruppe und vier von fünf Teilnehmer/innen der Gruppe mit Zugang zu ChatGPT o1 erfüllten die Aufgabe (im Wesentlichen das Einbringen eines Plasmids in das Bakterium *E. coli* und die Kultivierung mit Induktion der Proinsulinproduktion von dem Plasmid in einer Kultur des Bakteriums) – ist vor allem durch die sehr kleine Zahl an Testpersonen und der Hilfe menschlicher Instruktoren bei der Fehlersuche und -behebung fraglich.

stellung eines adenoassoziierten Virus⁷³ durch Einbringen von Plasmid-DNA in menschliche Zellen). Darüber hinaus gab es zwei zusätzliche Aufgabenstellungen: eine Aufwärm Aufgabe unter Verwendung von Pipetten zur hochgenauen Handhabung von Flüssigkeiten im Mikroliterbereich und eine Zusatzaufgabe zur Bestimmung der Anzahl von RNA-Molekülen in einer Probe (quantitative Polymerasekettenreaktion), wie sie für die Quantifizierung der Viruskonzentration genutzt werden kann.

Die Teilnehmer/innen wurden nach dem Zufallsprinzip in zwei Gruppen eingeteilt: Eine Gruppe konnte nur Internetwerkzeuge (z.B. Google, YouTube, Open-Access Fachzeitschriften) nutzen, während die andere Hälfte zusätzlich auch LLMs (Stand Mitte 2025) von OpenAI, Anthropic und Google DeepMind anwenden durfte. Teilnehmer/innen hatten Zugang zu einem voll ausgestatteten Labor der Biosicherheitsstufe 2 (BSL-2)⁷⁴, erhielten jedoch nur minimale Anweisungen (sowie ein Sicherheitstraining) und mussten selbst herausfinden, welche Protokolle zu befolgen waren, welche Geräte benötigt wurden und wie sie die einzelnen Aufgaben erfolgreich bewältigen konnten. Die Bewertung erfolgte durch Wissenschaftler/innen nach zuvor festgelegten Kriterien. Das wichtigste Erfolgskriterium war, ob alle drei Kernaufgaben erfolgreich ausgeführt werden konnten, da bereits das Scheitern bei einer dieser Aufgaben dazu führen würde, dass das Virus nicht hergestellt werden konnte.

Es konnten keine statistisch signifikanten Unterschiede zwischen den Gruppen in den Abschlussquoten für einzelne Aufgaben oder alle drei Kernaufgaben zusammen festgestellt werden.⁷⁵ Darüber hinaus müssen die bereits relativ niedrigen Erfolgswerte für den Abschluss aller drei Kernaufgaben, von 5,2 % bei der Gruppe mit Internetzugang und LLMs gegenüber 6,6 % zur Kontrollgruppe mit nur Internetzugang – wie von den Autor/innen diskutiert – vor den erleichterten bzw. nicht komplett realistischen Bedingungen des Versuchsdesigns gesehen werden. So enthielt dieses beispielsweise nicht die Materialbeschaffung und den Aufbau der Laborinfrastruktur, und die Teilnehmer/innen führten zwar einzelne (zum Teil vereinfachte, etwa bei der DNA-Klonierung) Laboraufgaben durch, mussten diese aber nicht in einen durchgängigen Gesamtablauf integrieren und etwa einmal hergestellte Agenzien für weitere Schritte nutzen. Das heißt, die Ergebnisse sind nicht auf ein Szenario übertragbar, bei dem Teilnehmer/innen ohne zusätzliche unterstützende Expertise oder Ressourcen selbstständig ein funktionsfähiges Labor einrichten oder ein komplettes Projekt (zur Herstellung eines Virus) durchführen. Auch die Herstellung des verwendeten adenoassoziierten Virus gilt typischerweise als einfacher als beispielsweise die eines Influenza- oder Pockenvirus.

Inwiefern die (zusätzliche) Nutzung neuerer biologiespezifischer Modelle (z. B. Biomni Lab) (Huang et al. 2025) zu einer Leistungssteigerung beitragen könnte, etwa durch die Reduzierung von Fehlern bei der Protokollerstellung oder bei Sequenzanalysen, ist unklar. Zudem könnten zukünftig weitere Systeme und Werkzeuge wie benutzerfreundliche Schnittstellen oder die Integra-

73 Adenoassoziierte Viren (AAV) sind Viren mit einem kleinen (einzelnsträngigen) DNA-Genom. Aufgrund ihrer minimalen Pathogenität und Fähigkeit, eine langfristige Genexpression in verschiedenen Geweben zu etablieren, haben sie sich als wichtiges Transfersystem in der klinischen Gentherapie etabliert (Wang et al. 2024).

74 Die vier international empfohlenen und ähnlich umgesetzten Biosicherheitsstufen für Laboratorien (BSL) sind BSL-1, BSL-2, BSL-3 und BSL-4, wobei BSL-4 die höchste Sicherheitsstufe darstellt (HHS 2020; WHO 2004). Sie umfassen eine Kombination von baulichen Merkmalen, Sicherheitsausstattungen, betrieblichen Praktiken und persönlicher Schutzausrüstung. BSL-2-Labore sind für (Standard-)Arbeiten mit Infektionserregern oder Toxinen erforderlich, die mit der Auslösung von Krankheiten bzw. gesundheitlichen Gefahren beim Menschen unterschiedlichen Schweregrades in Verbindung gebracht werden und für die eine wirksame Vorbeugung oder Behandlung normalerweise möglich ist. Hierzu gehören etwa Arbeiten mit Salmonellen, Herpes-Viren oder einigen Grippeviren. Der Zutritt ist auf namentlich benannte Beschäftigte beschränkt. Zu den baulichen Anforderungen an BSL-2-Labore gehören unter anderem Handwaschbecken, Augenspülstationen für den Notfall und auf die Organismen abgestimmte Desinfektionsverfahren sowie Dekontaminationsverfahren von Laborabfällen (z. B. ein Autoklav).

75 Die Ergebnisse der Gruppe mit LLM-Zugang deuten jedoch darauf hin, dass LLMs die individuelle Leistung von Anfängern bei manchen Laborarbeiten bzw. Schritten geringfügig verbessern könnten, indem sie dabei helfen, Aufgaben, für die implizites Wissen erforderlich ist, mit weniger Versuchen zu erledigen und teilweise früher abzuschließen.

tion mit Werkzeugen, die Laborabläufe automatisieren, mit LLMs kombiniert werden (Diskussion in Hong et al. 2026) (Kapitel 3.3.3).

Darüber hinaus könnten die Leistungssteigerungen durch die Nutzung existierender LLMs bei Personen höher sein, die zwar keine Expert/innen in der Herstellung von Viren aus synthetisierten Nukleinsäuresequenzen sind, aber bereits relevante Kenntnisse in den Lebenswissenschaften und biologische Laborerfahrung haben (z. B. auf Graduierten- oder Doktorandenniveau). Diese Möglichkeit könnte bzw. müsste durch entsprechende kontrollierte Uplift-Studien in biologischen Labors untersucht werden.

3.3.2 Veränderte oder neue Toxine und Krankheitserreger mithilfe von biologischen KI- bzw. Biodesignmodellen

Die Entwicklung KI-unterstützter Proteindesignmodelle hat die gezielte Neu- oder Umgestaltung (Design bzw. Redesign) von komplexen Proteinstrukturen und damit Proteinen mit unterschiedlichen Funktionen ermöglicht (Kasten 2.3, Kapitel 2.3). Auch viele hochgiftige, in der Natur vorkommende und (potenziell) als Biowaffen nutzbare Toxine sind Proteine oder Peptide (Anderson 2012). Dazu gehören die Proteintoxine Botulinumtoxin und Rizin, die bereits Teil von Biowaffenprogrammen waren (Kasten 3.3) oder bei bioterroristischen Anschlägen bzw. Anschlagversuchen eingesetzt wurden (Kasten 3.4, Kapitel 3.4).

Obwohl mit solchen Modellen auch das Design von Proteinen bzw. Proteintoxinen mit neuen Funktionalitäten möglich erscheint (Kapitel 2.3.4), ergeben sich dafür noch verschiedene Herausforderungen. Hierzu gehören die Berücksichtigung dynamischer Konformationsänderungen bzw. von unterschiedlichen Konformationen⁷⁶ von Proteinen in Zellen, die für die jeweilige Funktion wichtig sind (Brownless et al. 2025; NAS 2025b, S. 22). Die Funktionalität so entworfener Proteine wird bereits deshalb auf absehbare Zeit in Laborexperimenten überprüft werden müssen (NAS 2025b, S. 22). Auch die unterschiedlichen und teilweise komplexen Funktionalitäten bekannter natürlicher Proteintoxine, die oft für Biowaffen genutzt wurden (z. B. Bindung an Zellen, Mechanismen für das Einbringen in Zellen, enzymatische Aktivität (Anderson 2012), dürften es erfordern, dass Entwürfe für entsprechende Proteine oder Kombinationen mit anderen Proteinen (oder Teilen davon) experimentell getestet und gegebenenfalls über DBTL-Zyklen optimiert werden müssen (Kapitel 2.3.4). Letztendlich müsste die Entwicklung solcher neuer Proteintoxine auch relevante Tests in Zell- oder Gewebekulturen sowie in Versuchstieren umfassen.

Inwiefern sich mithilfe von KI-basierten Proteindesignmodellen zuverlässiger funktionell aktive Entwürfe für veränderte oder neuartige Peptidtoxine generieren lassen, die aus deutlich kürzeren Aminosäureketten bestehen, als dies bei den komplexeren Proteintoxinen der Fall ist (Clark et al. 2019; Lee et al. 2022), ist unklar. Für die oft im Zusammenhang mit möglichen Biowaffen disku-

76 Die durch die genetisch kodierte Aminosäuresequenz eines Proteins bestimmte 3D-Struktur (naive Struktur) ist nicht starr. Vielmehr können Bereiche des Proteins eine Vielzahl von schnellen Schwingungen und langsameren Strukturänderungen durchlaufen, die als Konformationsänderungen bezeichnet werden (Palmer 2015; Papaleo et al. 2016).

tierten Conotoxine⁷⁷ (Anderson/Bokor 2012; Bjørn-Yoshimoto et al. 2020) wurden verschiedene, teilweise spezifisch angepasste Proteinsprachmodelle zum Design und zur Optimierung pharmazeutisch aktiver Conotoxine beschrieben (Ge et al. 2026; Guo et al. 2025; Zhao et al. 2025). In einer Veröffentlichung zu einem solchen Modell wurden Conotoxinmoleküle entworfen, die ganz bestimmte Neurorezeptoren binden sollen. Diese Moleküle wurden im Labor hergestellt und experimentell getestet. Die Ergebnisse legen es nahe, dass über dieses Modell Peptide mit hoher Aktivität oder einer ähnlichen Aktivität wie die natürlichen Peptide, die diese Rezeptoren binden, mit Trefferraten von 10 bis 30 % entworfen werden können (Ge et al. 2026).

Die Neu- oder Umgestaltung von Proteinen – eine Möglichkeit zur Umgehung des Biosecurity-Screenings synthetischer Nukleinsäuresequenzen

Wohl nicht zuletzt aufgrund dieser Herausforderungen steht eine andere Möglichkeit im Mittelpunkt der derzeitigen Biosecurity-Diskussion zu KI-unterstützten Proteindesignmodellen. Diese Möglichkeit besteht darin, dass böswillige Akteure bekannte Proteine bzw. Toxine, unter Erhalt ihrer Funktion und derselben oder ähnlichen 3D-Struktur, so umgestalten könnten, dass sie aus einer im Vergleich zum „Original“ unterschiedlichen Abfolge von Aminosäuren (den Grundbausteinen von Proteinen) zusammengesetzt sind. Die Unterschiede in der Sequenz von Aminosäuren und damit der sie kodierenden DNA-Sequenz kann dabei so groß sein, dass entsprechende DNA-Sequenzen die typischen Bioscurity-Screeningmethoden für Bestellungen bei Anbietern von Nukleinsäuresynthesen umgehen können. Solche Methoden identifizieren Ähnlichkeiten zu Gensequenzen von als gefährlich eingestuften bzw. gesetzlich kontrollierten Proteinen oder Organismen (Kasten 3.6).

Kasten 3.6 Biosecurity-Screening von Bestellungen für Nukleinsäuresynthesen (DNA-Synthesescreening)

Die Synthese von Nukleinsäurefragmenten (DNA, RNA) hat sich zu einem zentralen Schritt der molekularbiologischen Forschung und der Biotechnologie entwickelt – sowohl um Gene oder andere Genomsequenzen in Zellen zu verändern (z. B. über CRISPR-Cas-basierte Genomeditierungsverfahren), als auch um Gensequenzen zur Herstellung von Proteinen erhalten und nutzen zu können, oder um ganze Genome von Viren herzustellen (Kapitel 2.1, 3.1).

⁷⁷ Conotoxine bilden eine (auch strukturell) sehr diverse Gruppe von meist 10 bis 30 Aminosäuren langen Peptiden, die im Gift von räuberischen Meeresschnecken der Gattung *Conus* vorkommen. Conotoxine werden aufgrund ihrer Verwendung in der neurowissenschaftlichen Forschung und für pharmazeutische Anwendungen intensiv beforscht und werden meist chemisch synthetisiert. Bestimmte Conotoxine sind für Säugetiere giftig und können auch für Menschen tödlich sein. Alle bisher bekannten tödlichen Vergiftungen bei Menschen beruhen auf Unfällen und es gibt keine Berichte über die Verwendung von Conotoxinen als Mord- bzw. Biowaffe. Conotoxine scheinen nur bei Injektion toxisch zu sein. Inwiefern die Inhalation von Conotoxinen in Form potenzieller Aerosole (Kapitel 3.2.2), die großflächig ausgebracht werden könnten, toxisch wirkt, scheint nicht bekannt zu sein (Anderson/Bokor 2012; Bjørn-Yoshimoto et al. 2020).

Synthetische Nukleinsäurefragmente können in unterschiedlichen Längen bzw. Formen – von sehr kurzen einzelsträngigen Oligonukleotiden bis zu langen, bereits aus mehreren Fragmenten zusammengesetzten doppelsträngigen DNA-Sequenzen (wie für komplette Gene) – bei zahlreichen kommerziellen Anbietern bestellt werden (Kane/Parker 2024). Die Nukleinsäuresynthese stellt deshalb eine wichtige Möglichkeit zur Überwachung dar, um das Risiko zu verringern, dass unbefugte Akteure gefährliche Toxine oder Viren herstellen könnten.

Obwohl gesetzlich nicht explizit vorgeschrieben (Kapitel 4.7.3), setzen viele Nukleinsäuresynthese-Anbieter Biosecurity-Screeningsoftware (BSS) ein, um Kundenbestellungen zu überprüfen. Zudem kontrollieren die Anbieter die Legitimität der Besteller (Kane/Parker 2024). Die meisten heute verwendeten BSS-Systeme suchen in einer bestellten Sequenz nach Fragmenten von Nukleinsäure- oder Proteinsequenzen, die durch internationale und/oder nationale Regelungen bzw. Listen (z. B. der Verordnung (EU) 2021/821⁷⁸, der Control List der Australia Group, oder der U.S. Select Agents and Toxins List; Kapitel 4) kontrolliert sind. Stimmt ein Fragment besser mit einer solchen bedenklichen Sequenz („sequence of concern“) überein als mit jeder anderen, wird die Sequenz markiert und zur menschlichen Überprüfung weitergeleitet (Kane/Parker 2024; Wittmann et al. 2025). Dieses als „Best Match“ bezeichnete Verfahren wurde ursprünglich in den (seither aktualisierten) Sequenzscreeningrichtlinien definiert, die 2010 vom US Department of Health and Human Services veröffentlicht wurden (HHS 2010, 2023). Diese Richtlinien wurden von dem International Gene Synthesis Consortium (IGSC 2024) in seinen für Mitglieder bindenden Standards und Praktiken aufgenommen und teilweise ergänzt.⁷⁹

Wittmann et al. (2025)⁸⁰ untersuchten in einer in der Fachzeitschrift *Science* veröffentlichten Arbeit in Zusammenarbeit mit Anbietern von Nukleinsäuresynthesen und Entwicklern von Screeningsoftware die Fähigkeit der Screeningprogramme⁸¹, DNA-Sequenzen von Proteinversionen mit veränderten Aminosäureabfolgen zu detektieren. Dabei wurden insgesamt 76.080 solcher Sequenzen für 72 Proteine getestet, die von drei KI-gestützten Open-Source-Proteindesignmodellen entworfen wurden. Die allermeisten der 72 Proteine waren Toxine (darunter Rizin), einige waren von Viren stammende Proteine (Charles 2025; Hutson 2025). Insbesondere aus Sicherheitsgründen und wegen möglicher Verstöße gegen gesetzliche Vorgaben wurde keine der entworfenen Proteinversionen im Labor hergestellt und funktionell getestet. Anstelle dessen wurden computergestützte Modelle genutzt, um die Wahrscheinlichkeit vorherzusagen, dass eine Proteinversion seine Funktion beibehalten würde. Basierend darauf wurde gefolgert, dass bei einem Teil der 76.080 Proteinvarianten die Funktion erhalten bleiben könnte.

78 Verordnung (EU) 2021/821 vom 20. Mai 2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck (Neufassung)

79 Das IGSC ist ein Zusammenschluss von Gensyntheseunternehmen und -organisationen. Er wurde 2009 gegründet, um ein gemeinsames Protokoll zur Überprüfung sowohl der Sequenzen von Bestellungen synthetischer Gene als auch der die Bestellungen aufgebenden Kunden (IGSC 2009, 2024) zu entwickeln und anzuwenden.

80 Die Autoren der Studie halten mit Zustimmung von *Science* einige Details über die KI-generierten DNA-Sequenzen und die Softwarescreeningaktualisierungen zurück. Diese sind nur über einen kontrollierten Zugang nach Stellung eines Antrags einsehbar, der von Expert/innen der International Biosecurity and Biosafety Initiative for Science (IBBIS) geprüft wird, einer gemeinnützigen Organisation, die eines der Screeningsoftwaresysteme entwickelt hat (Charles 2025; Hutson 2025).

81 Obwohl die getesteten Screeningprogramme eine Reihe von Strategien (unter anderem durch neuronale Netze verbessertes Alignment von Sequenzen) abdeckten, verwendeten alle das Best-Match-Prinzip (Kasten 3.6).

Im Gegensatz zu den Originalsequenzen der Proteine, die immer erkannt wurden, schwankte die Erkennung der modifizierten Sequenzen durch die Screeningprogramme zwischen ca. 23 und 70 %. Als Antwort auf die Ergebnisse wurden durch die Anbieter Aktualisierungen der Screeningprogramme entwickelt. Hierzu gehören Änderungen von Parametern zur Verbesserung der Sensitivität oder veränderte Screeningalgorithmen, z. B. in der Weise, dass anstatt nach exakten Übereinstimmungen zwischen kurzen Teilsequenzen nur nach solchen Übereinstimmungen an Stellen gesucht wird, die für die Funktionalität eines Proteins wichtig sind (Hutson 2025). Durch solche Änderungen konnten bis zu 72 % der von den KI-Modellen generierten alternativen Sequenzen erkannt werden, darunter 97 % der Sequenzen, die laut der computergestützten Vorhersagen mit der höchsten Wahrscheinlichkeit funktionell wären. Das in der Veröffentlichung beschriebene Vorgehen ist damit ähnlich dem im Bereich der Cybersicherheit von Softwaresystemen, z. B. indem Schwachstellen über Red-Teaming-Ansätze gefunden werden und Anbietern bzw. Entwicklern die Möglichkeit gegeben wird, Sicherheits-Patches zu entwickeln, bevor die Red Teams die Ergebnisse veröffentlichen.

Derzeit ist unklar, wie groß die Gefahr tatsächlich ist, dass bekannte Proteine, die so umgestaltet wurden, dass sie derzeitige Sequenzscreeningverfahren umgehen können, tatsächlich funktionell bleiben würden. Eine Folgeuntersuchung von einigen der Autor/innen der Science-Publikation, basierend auf einem experimentellen Test- und Verifizierungsansatz für verschiedene (nicht gefährliche) Proteinfamilien, legt nahe, dass mit den getesteten Open-Source-Modellen so umgestaltete Proteine wohl nicht funktionstüchtig sind.⁸² Dies gilt insbesondere für größere Proteine und/oder funktionell unterschiedlich komplexe Enzyme (Ikonomova et al. 2026). Zudem ist die experimentelle Verifizierung selbst für viele gut untersuchte (und nicht toxische) Proteine ressourcen- und zeitaufwendig. Sie erfordert typischerweise (mindestens) Monate Arbeitsaufwand, Personal mit viel Erfahrung und gut ausgestattete Labore (Ikonomova et al. 2026).

Zwar ist es denkbar, dass böswillige Akteure – ähnlich wie die Aum-Shinrikyo-Sekte bei ihren Anschlägen mit letztlich wirkungslosen biologischen Agenzien in den 1990er Jahren (mit Anthrax und Botulinumtoxin; Kasten 3.4, Kapitel 3.2.2) – auf funktionelle Tests hergestellter (Toxin-)Proteine verzichten. In diesem Zusammenhang wäre auch denkbar, sehr viele verschiedene Entwürfe als Moleküle herzustellen und auszubringen, in der Hoffnung, dass eine oder wenige der Proteinversionen zumindest eine Teilaktivität entwickeln. Solche Ansätze dürften aber zumindest für einschlägige Proteintoxine aufgrund ihrer Komplexität bzw. multiplen Funktionalitäten mit erheblichen Unsicherheiten für die Akteure verbunden sein. Im Fall der Herstellung einer Vielzahl entwerfener Proteinversionen kommt zusätzlich die Notwendigkeit für größere finanzielle Ressourcen hinzu (Ikonomova et al. 2026).

Dennoch dürfte die Entwicklung von Sicherheitsaktualisierungen für Sequenzscreeningsoftware, um Gensequenzen entsprechend umgestalteter Proteine erkennen zu können, mit Blick auf die Weiterentwicklung und erwartbare Verbesserungen von Proteindesignmodellen wichtig sein. Solche Aktualisierungen müssten dann wohl, ähnlich zu anderen Bereichen in der Informationstechnologie (z. B. Betriebssysteme oder Büroprogramme für Computer), kontinuierlich durchgeführt werden.

⁸² Diese Folgerung gilt nicht für vollständig synthetische Strukturen (Ikonomova et al. 2026, S. 10), also neu (de novo) entworfene funktionelle Strukturen, die sich sehr stark von bekannten Strukturen unterscheiden können (Lauko et al. 2025).

Die Veränderung existierender Krankheitserreger, um diese gefährlicher zu machen: Nicht nur aufgrund unzureichender Datensätze bleibt das Design effektiver Verbesserungen fraglich

Die Gefährlichkeit pathogener Mikroorganismen, wie Bakterien und Viren, und die Folgen für die öffentliche Gesundheit hängen von der Fitness der Erreger ab (Lipsitch/Moxon 1997). Unter Fitness werden alle Merkmale bzw. deren kombinierte Effekte verstanden, die die Fähigkeit eines Erregers beeinflussen, sich in einer bestimmten Umgebung (z. B. innerhalb einer Wirtspopulation) zu vermehren.⁸³ Für die meisten pathogenen Mikroorganismen hängt die Fitness von der Fähigkeit zur Übertragung von Wirt zu Wirt ab. Dieses Merkmal steht wiederum in komplexer Weise mit der Pathogenität bzw. Virulenz⁸⁴ eines Erregers im Zusammenhang, das heißt, mit dessen Potenzial, bei infizierten Wirten Schäden zu verursachen, die zu Erkrankungen oder zum Tod führen (Lipsitch/Moxon 1997).

KI-Modelle – basierend auf verschiedenen biologischen Daten – haben sich bei der Vorhersage von Funktionen von Genomsequenzen, darunter der Steuerung von Genen, der Herstellung von Genprodukten, wie verschiedener RNAs und Proteinformen, und deren Beteiligung an manchen Krankheiten, als vielversprechend erwiesen (Kapitel 2.3.1). Jüngere Arbeiten mit biologischen KI-Modellen, darunter vor allem Proteinsprachmodelle (Kasten 2.3), zeigen, dass Vorhersagen zu den Effekten von Mutationen und deren Evolution in Gensequenzen von Viren (z. B. SARS-CoV-2, Influenza oder HIV) möglich sind, die zur Erhöhung der Fitness beitragen können. Diese Mutationen können etwa die Infektiosität oder die Fähigkeit verbessern, bestimmte Reaktionen der Immunantwort zu umgehen („immune evasion“) (Hie et al. 2022; Ito et al. 2025; Lamb et al. 2024; Thadani et al. 2023; Youssef et al. 2025).⁸⁵ Diese Vorhersagen sind jedoch auf mögliche Auswirkungen einzelner Mutationen oder Kombinationen davon über kurze Zeiträume beschränkt (NAS 2025b, S. 23 f.).

Die Fähigkeit solcher Modelle zur Vorhersage längerfristiger Effekte von Mutationen bzw. der Virusevolution (über mehrere Generationen bzw. Infektionszyklen hinweg), wie sie für die Modifikation bzw. (dauerhafte) Verbesserung eines Virus notwendig wäre, dürfte jedoch auch weiterhin begrenzt sein. Solche längerfristigen Effekte sind mit vielen Unsicherheiten verbunden und die Entwicklung entsprechender Modelle – die auch für Strategien zur Impfstoffentwicklung und der Pandemievorsorge relevant sein könnten – steht vor erheblichen Herausforderungen. Hierzu gehören neben einem Mangel an umfangreichen, gut charakterisierten Datensätzen zur Evolution der Viren und deren Proteinen, sowie von Datensätzen, die virale Mutationen mit dem genetischen Hintergrund des Wirts (einschließlich der genetischen Variabilität in zentralen Genen der Immunantwort) verknüpfen, auch sprunghafte evolutionäre Ereignisse, wie komplexe genetische Verän-

83 Zu diesen Merkmalen gehören die Übertragungsfähigkeit des Erregers, seine Fähigkeit, bestehende Immunität zu umgehen, oder seine Fähigkeit, sich in Wirtszellen effizient zu vermehren (Domingo et al. 2019; Lipsitch/Moxon 1997; Obermeyer et al. 2022).

84 Der Begriff Pathogenität beschreibt die Fähigkeit eines Erregers, eine Krankheit auszulösen. Virulenz ist ein vergleichender oder quantitativer Begriff, der angibt, wie wahrscheinlich es ist, dass die Exposition gegenüber einem Erreger zu gesundheitlichen Beeinträchtigungen beim Wirt führt. Molekulare Mechanismen hierfür betreffen beispielsweise Wirts- und Gewebespezifität (Tropismus), Schädigung des Wirtsgewebes (Zytotoxizität) oder Prozesse des Wirts zur Eliminierung des Pathogens (Host Clearance).

85 Potenzielle, auf solchen Funktionsvorhersagen basierende, gezielte und effektive Verbesserungen viraler Eigenschaften wären qualitativ verschieden von früher beschriebenen Experimenten, die weitgehend auf fundierten Vermutungen basierten und in denen z. B. Gene bzw. Genomabschnitte aus anderen biowaffenrelevanten Viren in das Pockenvirus eingeführt wurden. Solche Experimente wurden in den 1980er und 1990er Jahren vor allem in der damaligen Sowjetunion, wohl im Zusammenhang mit Forschung zur Impfstoffentwicklung, durchgeführt. Entsprechende experimentelle Veränderungen könnten potenziell aber auch zur Verbesserung von Viren als Biowaffe verwendet werden (Alibek 2004 und Referenz darin).

derungen⁸⁶ (Hamelin et al. 2025; Mallapaty 2025b; NAS 2025b, S. 23 f.), die auch zukünftig wohl nicht vorhersagbar sein werden.

KI-gestützte Biodesignmodelle könnten perspektivisch auch genutzt werden, um Erreger so zu verändern, dass bestehende Vorbeugungs- oder Behandlungsmethoden, etwa Impfstoffe, monoklonale Antikörper, antivirale oder antimikrobielle Wirkstoffe⁸⁷, an Wirksamkeit verlieren.

Das Design komplett neuer Krankheitserreger ist (mindestens) derzeit außerhalb der Reichweite von KI-Modellen

Das Entwerfen völlig neuer Krankheitserreger (De-novo-Design) durch KI-gestützte Modelle könnte die potenziell weitreichendsten Folgen haben, da aufgrund fehlender Informationen zu solchen Erregern die Möglichkeiten zur Bekämpfung eingeschränkt wären bzw. die Entwicklung von Maßnahmen verzögert würde.

Der Mangel an umfangreichen und gut aufbereiteten Datensätzen zu Eigenschaften von Krankheitserregern, die deren Fitness beeinflussen (darunter Übertragbarkeit und Virulenz), ist auch ein stark begrenzender Faktor für die Entwicklung biologischer KI-Modelle, die das Entwerfen von Grund auf neuer Krankheitserreger ermöglichen könnten – selbst wenn es sich um relativ einfache bzw. wenig komplexe Krankheitserreger wie Viren handelt. Denn um solche Eigenschaften zu konstruieren und/oder zu kombinieren, müssten auch die diesen Merkmalen zu Grunde liegenden, komplexen Netzwerkinteraktionen mit verschiedenen Komponenten der Wirtsorganismen verstanden bzw. modelliert werden können (Eisfeld et al. 2024; Waters 2024); zitiert in (NAS 2025b, S. 23).

So existieren für viele menschliche Viren überhaupt keine nützlichen bzw. kompletten Sequenzinformationen zu Genomen in Datenbanken, da nur Fragmente sequenziert sind oder oft schwer sequenzierbare Abschnitte fehlen. Zudem sind viele humane Viren in genetischen Datenbanken nur durch eine oder wenige repräsentative Sequenzen vertreten und können Fehler enthalten oder sie repräsentieren Konsensussequenzen – quasi ein Durchschnitt aller Genomsequenzen einer Probe. Inwiefern diese Sequenzen funktionsfähig sind, ist oft unklar und nur experimentell festzustellen. Darüber hinaus fehlen in der Regel größere Datensätze zu Funktion bzw. Eigenschaften (phänotypische Daten) der viralen Sequenzen. Selbst im Fall des SARS-CoV-2-Virus, für das seit der COVID-19-Pandemie eine beispiellose Sammlung (mit mehr als 15 Mio. hochwertiger Sequenzen) von Genomvarianten existiert, wurden nur für einen kleinen Teil dieser Genomvarianten solche phänotypischen Daten erhoben (NAS 2025b, S. 25 und Referenz darin).

Ohne solche großen und qualitativ hochwertigen Datensätze zu Genomen und dem gesamten Spektrum der phänotypisch relevanten molekularen Daten scheinen biologische KI-Modelle, um von Grund auf neue, vermehrungsfähige Viren zu entwerfen, weit jenseits der gegenwärtigen Möglichkeiten, und die Evolution solcher Viren über mehrere Generationen (siehe vorheriger Ab-

86 Diese können z. B. durch Rekombinationsereignisse, persistente Infektionen und eine beschleunigte Evolution in immungeschwächten Personen oder durch tierische Reservoirs entstehen (Raglow/Lauring 2025; Schmidt et al. 2025).

87 Die einfache Übertragung bzw. das Einbringen existierender Antibiotikaresistenzgene in für Biowaffen nutzbare pathogene Bakterien, z. B. in den Anthrax- oder den Pesterreger (Ainscough 2002 und Referenz darin) soll etwa im früheren sowjetischen Biowaffenprogramm durchgeführt worden sein (Ainscough 2002; Alibek/Handelman 1999).

schnitt) könnte selbst mit solchen Modellen kaum zuverlässig vorhersagbar sein (NAS 2025b, S. 24 ff.).

Inwiefern große Genomsprachmodelle (Kasten 2.3, Kapitel 2.3.1, 2.3.4) die gezielte Entwicklung neuartiger Viren ermöglichen könnten, ist unklar. Eine veröffentlichte Arbeit zeigt erstmals, dass ganze Genome von Viren, die Bakterien befallen (Bakteriophagen/Phagen) (TAB 2023), über solche Modelle⁸⁸ entworfen und daraus funktionelle Viren generiert werden können. Diese zeigten (unter Laborbedingungen) teilweise eine höhere Fitness bzw. Infektiosität als ihre natürlichen Verwandten (Kavanagh 2025; King et al. 2025). Die Autor/innen nutzten die Genomsequenz eines bekannten, einfachen Phagen mit sehr kleinem Genom (ΦX174) (Sanger et al. 1977a) als Designvorlage, um Genome für Phagen mit derselben Wirtsspezifität zu entwerfen. Aus Tausenden computergenerierten Sequenzen wurden ca. 300 Entwürfe experimentell getestet, 16 davon führten zu vermehrungsfähigen Phagen. Die Genome dieser vermehrungsfähigen Phagen waren zwischen 93,2 und 98,8 % identisch mit den Trainingsgenomsequenzen der Phagenfamilie, aus der auch die Designvorlage stammt (King et al. 2025). Die Ergebnisse lassen es daher fraglich erscheinen, inwiefern über diesen Ansatz von Grund auf neuartige Phagen oder auch andere Viren (mit größeren Genomen), generiert werden könnten – selbst wenn genügend Genomsequenzen für solche Viren zum Training der Modelle zur Verfügung stehen sollten. Ebenfalls unklar ist, inwieweit über im Ansatz verwendete Designeinschränkungen, wie zum Erhalt bestimmter Eigenschaften der Wirtsspezifität der Designvorlage⁸⁹, Merkmale gezielt verändert bzw. neue Eigenschaften erzeugt werden können.

3.3.3 Die Kombination von KI-Modellen mit automatisierten Laborplattformen

Unabhängig von den derzeitigen oder zukünftig möglichen Fähigkeiten von KI-Modellen, Entwürfe für veränderte oder neue Proteine und Krankheitserreger zu generieren, erfordert deren Verwirklichung die Herstellung und experimentelle Validierung funktionsfähiger Moleküle oder Erreger im Labor bzw. in Bioreaktorsystemen – und gegebenenfalls eine Optimierung der Entwürfe (oder auch der Herstellungs- und Testverfahren). Wie in Kapitel 2.3 dargestellt, sind für diese zentralen Schritte der Forschungs- und Entwicklungsprozesse derzeit typischerweise zeit- und ressourcenaufwendige, iterative Entwicklungsschemata erforderlich. Hierzu gehören insbesondere DBTL-Zyklen oder Zyklen gerichteter Evolution (Kapitel 2.3.4).

„Lab in the loop“: von automatisierten Laboren zu autonomen Entwicklungszyklen

Um solche Prozesse effizienter zu machen sowie den Zeit- und Kostenaufwand zu reduzieren, wird versucht, diese immer weiter zu automatisieren. Dabei werden zunehmend KI-Modelle zur Hypothesenbildung und dem Design von Molekülen (inklusive Enzymen) oder von Synthesewe-

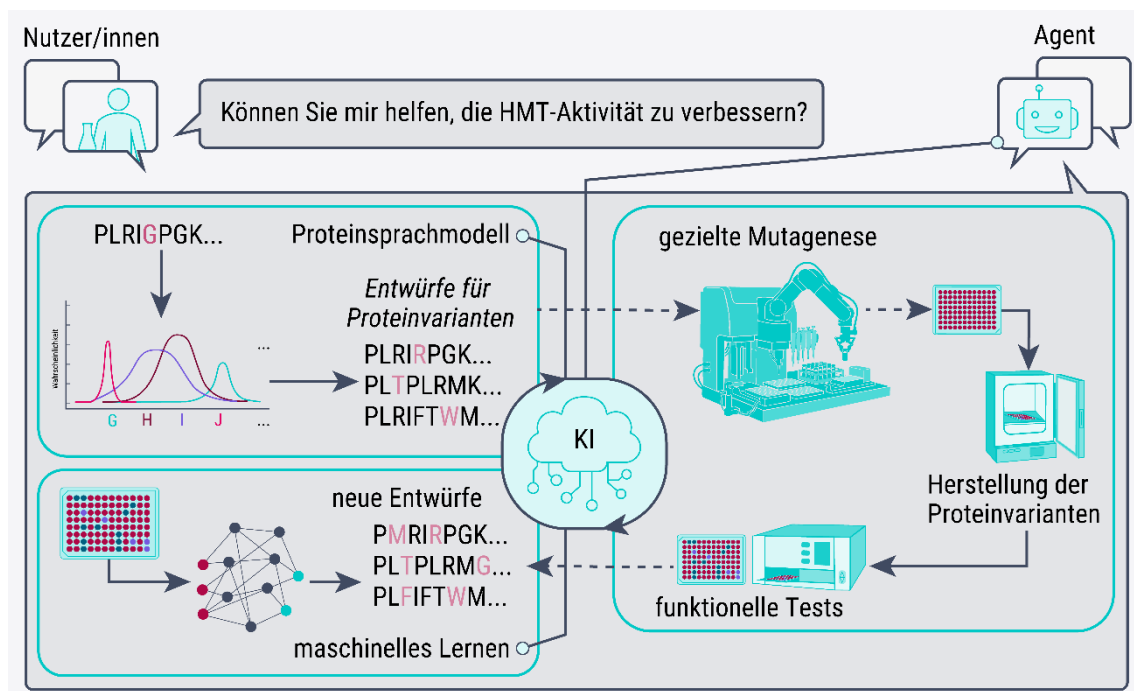
88 Genutzt wurden die Modelle Evo und Evo 2, die unter anderem mit über 2 Mio. Bakteriophagen-genomsequenzen trainiert wurden (Brixi et al. 2026; Nguyen et al. 2024). Diese wurden für die Arbeiten zusätzlich mit Genomsequenzen der Phagenfamilie trainiert, aus der die Designvorlage mit der gewünschten Wirtsspezifität stammt.

89 Dabei wurden Entwürfe von Genomsequenzen, die nach Anwendung von allgemeinen Qualitätskontrollfiltern verblieben, einem weiteren Filterschritt (Tropismusfilter) unterzogen. Dieser wurde so gewählt, dass ihn nur Genomentwürfe passieren, in denen die Sequenz für das die Wirtsspezifität bestimmende Phagenprotein (Spikeprotein) ≥60 % identisch zu dem entsprechenden Protein der ΦX174-Designvorlage ist.

gen in Mikroorganismen sowie zur Analyse von Versuchsergebnissen mit Robotersystemen für Laboraufgaben (z. B. Flüssigkeitshandhabung, Probenverarbeitung, Analyse von Proben) kombiniert – bis hin zu quasiautonen Laboren („self-driving labs“) oder KI- oder Roboterwissenschaftlern („AI scientists“, „robot scientists“) (Kapitel 2.3.5) (Adam 2024; Arias/Taylor 2024; Martin et al. 2023). Dieser Ansatz zur Kombination von KI und automatisierten Labors („lab in the loop“) könnte zudem genutzt werden, um umfangreiche(re) biologische Datensätze zu generieren, die zur Verbesserung der KI-Modelle verwendet werden – was wiederum die Anzahl der DBTL-Zyklen reduzieren könnte, die für die Realisierung eines erfolgreichen Designs erforderlich sind (NAS 2024, S. 3, 2025b, S. 17).

Eine zunehmend wichtige Rolle bei diesen Entwicklungen spielen robotisierte Laborplattformen bereits existierender, zum Teil kommerzieller Labore oder Forschungseinrichtungen, Cloud Labs und Biofoundries (Kasten 2.4, Kapitel 2.3.5), die im Fall von Cloud Labs über Onlinebenutzeroberflächen – quasi ferngesteuert – nutzbar sind. So wurden beispielsweise erste solche autonome Systeme für Protein- oder Enzym-Engineering-Aufgaben generiert, in denen biologische KI-Modelle bzw. KI-Agenten für das Design von Gen- bzw. Proteinvarianten für Enzyme mit robotisierten Cloud-Lab- oder Biofoundry-Plattformen⁹⁰ gekoppelt wurden (Abbildung 3.3), um die Proteine herzustellen, zu testen und die erhaltenen Versuchsdaten zur Verbesserung über weitere DBTL-Zyklen zu verwenden (Rapp et al. 2024; Singh et al. 2025) (für mehr Details zu diesen und anderen autonomen Systemen Kapitel 2.3.5).

Abbildung 3.3 Autonome Labore durch die Kombination von KI-Modellen und automatisierten Laborplattformen („self-driving labs“/„lab in the loop“)



Eigene Darstellung nach Singh et al. (2025), Bild automatisierter Laborroboterarm: Shan Junaid/Adobe Stock

90 Strateos Cloud labs bei Rapp et al. (2024); Illinois Biological Foundry for Advanced Biomanufacturing (iBioFAB) bei Singh et al. (2025).

Könnten autonome Versuchsplattformen die hohen Anforderungen an Konstruktion und Tests modifizierter oder neuer biologischer Agenzien senken?

Bereits die Möglichkeit der Nutzung kommerzieller automatisierter Labore, aber vielleicht noch mehr die Ansätze für die Kombination solcher Laborplattformen mit KI-gesteuertem Versuchsdesign und der Automatisierung der Konstruktions- und Testarbeiten, werfen Biosecurity-Fragen auf.

Nämlich zum einen, ob vor allem kommerzielle automatisierte, über das Internet nutzbare Cloudlabore böswillige Akteure unterstützen könnten, denen praktische Fähigkeiten bzw. Erfahrungswissen und Laborausrüstung zur Herstellung gefährlicher biologischer Agenzien fehlen, sowie zum anderen, inwieweit die autonomen Systeme für das Design und die Automatisierung von DBTL-Zyklen auch die Anforderungen an Wissen und Kenntnisse solcher Akteure für die Konstruktion und die Validierung solcher Agenzien senken könnten.

Die Nutzung von Cloud Labs erfordert (noch) die Planung von Experimenten, einschließlich Wissen zu Labormethoden und Cloud-Lab-Abläufen

Cloud Labs wurden unter anderem mit der Idee bzw. als Geschäftsmodell gegründet, Laborarbeiten automatisiert schneller und reproduzierbarer durchführen zu können sowie den Zugang zu wissenschaftlichen Laborarbeiten zu erweitern. Sie können Forschenden die Nutzung von Geräten ermöglichen, die für ihre eigene Institution möglicherweise zu teuer oder anderweitig nicht realisierbar wären (Arias/Taylor 2024; Lee et al. 2025; NAS 2024, S. 4). Theoretisch bestünde so keine Notwendigkeit mehr, (zumindest einige) praktische Laborarbeiten durchzuführen. Bereits heute sollte über solche Plattformen automatisiert beispielsweise das Zusammenfügen von DNA-Fragmenten für synthetische Genome bestimmter Viren (z.B. Influenza) bis hin zu deren automatisierten Generierung bzw. Vermehrung in Zellkulturen (Dormitzer 2015; Dormitzer et al. 2013) prinzipiell machbar sein. Jedoch muss für den effektiven Einsatz eines Cloud Labs jeder Schritt und der gesamte Prozess vollständig im Voraus geplant werden. Hierzu sind ganzheitliche (Front-to-End-)Konzeption und Planung von Experimenten mit den jeweiligen Molekülen (z. B. bestimmten Proteinen) oder Organismen sowie entsprechendes Wissen zu notwendigen methodischen Schritten bzw. Verfahren, erforderlich (Arias/Taylor 2024; NAS 2024, S. 4).⁹¹ Darüber hinaus können die Interpretation von Ergebnissen sowie die Fehlersuche und -behebung komplex sein und ebenfalls spezifisches Wissen erfordern, nicht zuletzt auch zu den Cloud-Lab-Abläufen bzw. -Verfahren selbst (Arias/Taylor 2024).

Es ist jedoch nicht auszuschließen, dass diese Schwierigkeiten durch zuverlässigere Automatisierungssysteme mit mehr Kontrollschritten abnehmen, oder dass das Programmieren solcher Experimente auf Cloud-Lab-Plattformen zukünftig durch KI-Verfahren erleichtert werden könnte. Zwar konnten keine Informationen über standardisierte Ansätze für die Überprüfung von Experimenten und Kunden bei Cloud-Lab-Anbietern, vergleichbar dem Nukleinsäuresynthescreening, gefunden werden (Lee/Del Castello 2024) (Kapitel 4.7.3). Falls solche Überprüfungen durchgeführt werden, dürfte aber die Wahrscheinlichkeit der Entdeckung möglichen Missbrauchs groß

⁹¹ beispielsweise <https://www.emeraldcloudlab.com/how-it-works/> (30.6.2026)

sein – insbesondere dann, wenn Verfahren mehrere spezifische Schritte und Materialien (z. B. bestimmte Zelllinien) benötigen wie die Herstellung bestimmter Viren.

„Self-driving labs“ können die Anforderungen an Kenntnisse und praktische Fähigkeiten senken – die Entwicklung, vor allem von geeigneten biologischen Testsystemen, bleibt aber forschungsintensiv

Falls „self-driving labs“ bzw. Lab-in-the-Loop-Systeme für spezifische relevante biologische Agenzien wie ein bestimmtes Toxin oder einen bestimmten Krankheitserreger zur Verfügung stünden und zugänglich wären, könnten diese die Hürden einer Herstellung und Validierung dieser biologischen Agenzien stark senken.

So konnte z. B. in einem Self-driving-System zum Redesign von Enzymen (Singh et al. 2025) (Kapitel 2.3.5) eine sprachgesteuerte Benutzeroberfläche integriert werden, mit der über einfache Prompts⁹² auf vorprogrammierte Funktionen eines großen Proteinsprachmodells (ESM2) (Lin et al. 2023) zum Design von Proteinen bzw. Enzymvarianten zugegriffen werden kann (Abbildung 3.3). Laut Singh et al. (2025) „können auch Nutzer ohne Programmierkenntnisse problemlos mit unserer Protein-Engineering-Plattform interagieren. [...] wodurch die Plattform auch für nicht technische Benutzer zugänglich wird“.⁹³ In ähnlicher Weise wären auch die autonome Konstruktion und Testung neugestalteter Toxine und unter Umständen auch veränderter Viren (Kapitel 3.3.2) denkbar, z. B. unter Nutzung zellfreier Systeme (Cello et al. 2002) oder von Zellkulturen (Dormitzer 2015) zu ihrer Herstellung sowie von Zell- oder Gewebekultursystemen für ihre Testung.

Aufgrund des spezifischen Zuschnitts auf die jeweiligen Aufgaben, wie die Veränderung und Testung unterschiedlicher Organismen oder Proteine (z. B. Enzyme), sind für die Entwicklung und Integration entsprechender Module für solche Systeme – zusätzlich zu spezifischen Kenntnissen über die zu verändernden biologischen Systeme – erhebliche Fachkenntnisse im Bereich der Robotik sowie der Soft- und Hardwareintegration erforderlich (Arias/Taylor 2024). Für die autonome Veränderung bzw. Optimierung von Proteinen stellen insbesondere die Entwicklung (robotisierbarer) funktioneller biochemischer Tests für verschiedene Proteinfunktionen eine Herausforderung dar, deren Überwindung sehr spezifische Kenntnisse erfordert sowie sehr kosten- und forschungsintensiv ist (Ikonomova et al. 2026; Rapp et al. 2024). Auch die Anpassung bereits existierender Systeme an spezifische Proteine (wie bestimmte Toxine) oder Krankheitserreger wäre deshalb aufwendig und dürfte so außer Reichweite für Akteure ohne entsprechende Kenntnisse und Ressourcen sein. Solche Systeme und die damit verbundenen Möglichkeiten dürften deshalb eher eine Option für staatliche Akteure bzw. staatlich unterstützte Akteure sein.

92 Genannte Beispiele sind: „Helfen Sie mir, Phytase zu verbessern“ oder „Entwerfen Sie die erste Bibliothek für AtHMT“ (im Original: „help me improve phytase“ or „design the initial library for AtHMT“) (Singh et al. 2025).

93 Im Original: „allows users without programming skills to easily interact with our protein engineering platform. [...] making the platform accessible to non-technical users.“

3.4 Implikationen der neuen technischen Möglichkeiten für Bedrohungen durch Biowaffen

Die Frage, was diese neuen Möglichkeiten des Zusammenspiels von KI mit Biologie bzw. Biotechnologie (KlxBio) für die Entwicklung und Proliferation von Biowaffen sowie damit verbundener potenzieller neuer Bedrohungen bedeuten könnten, erfordert eine umfassendere Betrachtung, die über die im vorherigen Abschnitt dargestellten neuen technischen Möglichkeiten KI-basierter Systeme und mögliche Voraussetzungen für deren weitere Entwicklung (wie zusätzliche oder bessere Datensätze) hinausgeht.

Hierzu gehören zum einen Fragen nach potenziellen weiteren Eigenschaften und Möglichkeiten von KlxBio, die Einfluss auf die tatsächliche Nutzung als Waffe haben können (NAS 2025b, S. 27), beispielsweise indem sie die Verwaffnungs- oder Ausbringungsprozesse (Kapitel 3.2.2) beeinflussen können. Zum anderen umfasst eine solche umfassendere Betrachtung die möglichen unterschiedlichen Akteure und Bedingungen bzw. Faktoren, welche deren Intentionen bestimmen können, Biowaffen zu entwickeln und zu nutzen (NAS 2025b, S. 27 f.; Sabra/Frieß 2025, S. 83 ff.). Als wichtige solche Faktoren, die teilweise von Kenntnissen, Fähigkeiten oder Ressourcen der Akteure nicht vollständig zu trennen sind, gelten das Verlangen, z. B. eine Regierung, eine Bevölkerung oder bestimmte Gruppen davon zu schädigen; die Zuversicht, mit dem Einsatz eines Mittels seine Ziele zu erreichen, beeinflusst z. B. von vorhandenen Fähigkeiten oder Ressourcen, und die Attraktivität des gewählten Mittels aufgrund möglicher Vorteile, z. B. ein hohes Potenzial für Panik, große Opferzahlen oder die Schwierigkeit, die Tat zuzuordnen zu können (für eine detaillierte Darstellung solcher Faktoren nach Talbot/Jakeman 2011; Sabra/Frieß 2025, S. 83 ff.).

Technologische Aspekte der Herstellung und Nutzung von Biowaffen, die weitgehend unabhängig von KlxBio sind

Die groß angelegte Produktion von biologischen Agenzien, wie beispielsweise Viren oder Bakterien, deren Verwaffnung und geeignete Mechanismen für großflächige und/oder über größere Entfernungen (z. B. durch Raketen, Marschflugkörper oder größere Drohnen) mögliche Ausbringungen, hängen in erster Linie von verfahrenstechnologischen bzw. speziellen ingenieurwissenschaftlichen Fähigkeiten in der Biotechnologie und der Waffentechnologie sowie entsprechender Infrastrukturen ab (NAS 2025b, S. 29) (Kapitel 3.2.2).⁹⁴ Sie sind weitgehend unabhängig von grundlegenden biologischen Herausforderungen wie der Voraussage und dem Design von Proteinfunktionen oder Eigenschaften von Krankheitserregern, Datensätzen zu entsprechenden molekularen biologischen Prozessen oder von den (zumindest derzeit) im Labormaßstab arbeitenden automatisierten und autonomen Systemen (Kapitel 3.3.2, 3.3.3). Die Herstellung bzw. Massenproduktion biologischer Agenzien und komplexe Ausbringungsmechanismen erfordernder Biowaffensysteme dürfte deshalb auch weiterhin – und wohl unabhängig von LLMs oder der Entwicklung biologischer KI-Modellen – insbesondere staatlichen Akteuren und Biowaffenprogrammen (Kästen 3.3, 3.4, Kapitel 3.1) vorbehalten bleiben.

⁹⁴ Nicht biologische KI-Modelle könnten die Entwicklung und Testung von Verwaffnungstechnologien oder der Ausbringung unterstützen, z. B. über KI-Modelle zur Entwicklung von Materialien oder zur Vorhersage der Verteilung bzw. Ausbreitung von Agenzien im Freiland, abhängig von meteorologischen Bedingungen (NAS 2025b, S. 29). Die Darstellung und Diskussion dieser Möglichkeiten gehen über den Rahmen dieses Berichts hinaus.

Jedoch sind die Produktion in sehr großem Maßstab und komplexe Verwaffnungs- bzw. Ausbringungsmechanismen nicht in jedem Fall notwendig. Beispielsweise können abhängig von dem Agens und der Strategie bereits kleinere Mengen mancher Agenzien ausreichen und/oder über einfachere, weniger technisch aufwendige Prozesse in (genügend) infektiöser Form ausgebracht werden (Kasten 3.4 – Mögliche Bedrohung durch nicht staatliche Akteure).

Mögliche Bedrohung durch staatliche oder staatlich unterstützte Akteure

Der einzige großflächigere Einsatz biologischer Waffen, die in einem der früheren staatlichen Waffenprogramme entwickelt wurden, erfolgte durch Japan ab Mitte der 1930er Jahre und während des zweiten Weltkriegs in China (Kasten 3.4). Obwohl vor allem Nordkorea und Russland verdächtigt werden, verdeckt illegale Biowaffenprogramme zu betreiben (U.S. Department of State 2025; Warrick/Ley Jarrett 2024), ist unklar bzw. nicht unabhängig und belastbar zu überprüfen, ob Nationalstaaten aktuell tatsächlich solche Programme betreiben (BWC; Kapitel 4.1.1, 4.7.1).

Aufgrund vorhandener biotechnologischer Möglichkeiten und Erfahrungen aus früheren Biowaffenprogrammen (Kasten 3.3, Tabelle 3.1⁹⁵) dürften potenziell zahlreiche Staaten – entweder direkt oder mit Unterstützung von Staaten mit ehemaligen solchen Programmen – die *Fähigkeiten* besitzen, Biowaffen herzustellen und zu nutzen (Sabra/Frieß 2025, S. 89 ff.). Aufgrund internationaler Übereinkommen und Normen (Kapitel 4.1) sowie möglicher politischer, ökonomischer oder militärischer Reaktionen könnten aber nur wenige Staaten die *Intention* haben, die Option Biowaffen einzusetzen, z. B. strategisch oder für taktische, verdeckte bzw. hybride Operationen, um Staaten und Regierungen zu destabilisieren.⁹⁶ Denkbar erscheint dies insbesondere für Staaten mit großer ökonomischer Macht (einschließlich der Verfügung über essenzielle Rohstoffvorkommen) sowie nuklearer militärischer Stärke – Bedingungen, welche das Einhalten internationaler Regeln und die Abschreckung durch wirtschaftliche oder militärische Vergeltungsmaßnahmen untergraben können (Dickinson et al. 2025; Mauroni/Cross 2025). Ebenso könnten mit solchen Staaten eng verbündete bzw. ökonomisch und militärisch protegierte Staaten, oder aber von ihnen unterstützte terroristische Gruppen oder paramilitärische Organisationen, die Option Biowaffen in Betracht ziehen.

Ob oder inwiefern KI-Modelle für Staaten eine Rolle für die Biowaffenherstellung spielen, ist fraglich. Staaten dürften weder auf Wissensgewinnung über LLMs für die Herstellung bekannter biologischer Kampfstoffe noch auf die Umgestaltung von (Protein-)Toxinen oder Genen für Proteine zur Veränderung von Krankheitserregern angewiesen sein, um Screeningverfahren für die Nukleinsäuresynthese zu umgehen (da sie eigene Synthesekapazitäten hätten). Auch könnte für Staaten (zumindest für solche mit dem zuvor genannten Profil) keine Notwendigkeit bestehen, neuartige potenziell nicht detektierbare oder (noch) schwerer zuordenbare biologische Kampfstoffe zu entwickeln. Ähnlich wie im Fall der Nutzung von chemischen Kampfstoffen bzw. Waffen (Yassif

95 Zusätzlich zu den in Tabelle 3.1 aufgeführten Ländern wird in Berichten des US-Außenministeriums davon ausgegangen, dass China von den 1950er bis mindestens Ende der 1980er Jahre ein offensives Programm zur biologischen Kriegsführung betrieb. Dabei sollen Rizin, Botulinumtoxine und die Erreger von Anthrax, Cholera, Pest und Tularämie verawffnet worden sein. Darüber hinaus wird in den Berichten geschlossen, dass Nordkorea mindestens seit den 1960er Jahre Fähigkeiten zur Herstellung und Verwaffnung von Viren, Bakterien und Toxinen besitzt (U.S. Department of State 2025).

96 Die Nutzung von Biowaffen könnte für verdeckte Operationen und die hybride Kriegsführung oder für taktische Operationen deshalb attraktiv sein, da die Zuordnung (Attribution) zum Verursacher oft schwierig ist (Dickinson et al. 2025; Jakob et al. 2024 und Referenz darin) sowie mögliche nukleare Antworten (beispielsweise nach einem Angriff auf NATO-Staaten) für begrenzte Einsätze von chemischen und biologischen Waffen kaum realistisch bzw. glaubwürdig sein könnten (Dickinson et al. 2025; Mauroni/Cross 2025).

et al. 2023, S. 262), z. B. durch Russland gegen Oppositionelle im In- und Ausland (Lister et al. 2020; Steindl et al. 2021; The Dawn Sturgess Inquiry 2025) oder durch das damals politisch und militärisch durch Russland unterstützte Assad-Regime im syrischen Bürgerkrieg (OPCW 2024), könnte die Wahrscheinlichkeit groß sein, dass solche Staaten bei taktischen, begrenzten Einsätzen von Biowaffen keine untragbaren Kosten zu erwarten hätten oder Brüche der regelbasierten internationalen Ordnung sogar bewusst als Strategie, wie der Verunsicherung bzw. Machtdemonstration, nutzen könnten (Dickinson et al. 2025). KI-Modelle scheinen für staatliche Programme somit nicht erforderlich, dennoch könnten sie einzelne Forschungs-, Entwicklungs- und Optimierungsschritte beschleunigen.

Mögliche Bedrohung durch nicht staatliche Akteure

Die Betrachtung von früheren Fällen (START 2025; Tin et al. 2021, 2022; UMD o. J.) (Kasten 3.4), bei denen nicht staatliche Akteure Biowaffen eingesetzt haben oder einsetzen wollten, zeigt ein weites Spektrum solcher Akteure. Hierzu gehören sowohl *Einzeltäter/innen* ohne biologische Ausbildung, z. B. im Fall der Anschläge (ohne Verletzte) mit Rizinbriefen in den USA (DOJ 2023; FBI 2014) oder beim geplanten Anschlag mit einer Rizin-Bombe durch einen in Köln-Chorweiler lebenden Islamisten (beck-online 2020; Flade 2018), als auch solche mit außergewöhnlicher Fachexpertise, wie bei dem mutmaßlichen Täter der Anthraxbriefanschläge in den USA im Jahr 2001, mit fünf Todesfällen und einer Reihe weiterer Erkrankter (DOJ 2010; Matsumoto 2003). Weitere nicht staatliche Akteure waren Sekten, wie im Fall der Verbreitung von Salmonellen in Restaurants durch die religiöse Rajneesh-Sekte in den USA 1984, der zu Hunderten teilweise schwer Erkrankter führte (Török et al. 1997; Turner et al. 2025), oder der großangelegten Anschlagsaktivitäten in Japan durch die religiös-apokalyptische Aum-Shinrikyo-Sekte mit (letztlich unwirksamen) Anthrax- und Botulinumtoxinpräparationen (Danzig et al. 2012). Darüber hinaus soll vor allem die islamistische Terrororganisation Al-Qaida bereits Ende der 1990er Jahre versucht haben, biologische Kampfstoffe (insbesondere Anthrax) zu entwickeln (Mowatt-Larssen 2025; Pita/Gunaratna 2009 und Referenz darin) (Kasten 3.4).

Bereits diese Beispiele legen es nahe, dass die Zeichnung eines Profils wahrscheinlicher Täter/innen oder Tätergruppen und von ihnen ausgehender Bedrohungen noch (weit) unsicherer ist als bei Staaten oder von solchen unterstützten und protegierten Gruppierungen. Ähnlich wie bei Terrorakten mit anderen Mitteln können die Motivationen bzw. Intentionen sehr verschieden sein, getrieben von (sich zum Teil überschneidenden) ideologischen Strömungen oder Phänomenen wie Nationalismus, Rassismus, religiösem Extremismus oder sozialer Ausgrenzung, oder einer Mischung von diesen (Parker/Sitter 2016). Bei terroristischen Einzeltäter/innen kann dies oft eine Mischung aus Ideologie und persönlichen Kränkungen sein (Parker/Sitter 2016). Schließlich können Einschätzungen zu möglichen Tätergruppen und von diesen ausgehenden Bedrohungen dadurch erschwert werden, dass sich bereits bekannte terroristische Gruppen weiterentwickeln und verändern, indem sie beispielsweise ihre Organisationsformen und Strategien anpassen (Parker/Sitter 2016; Stern 2003).

Zwar gibt es im Zusammenhang mit den bisherigen Fällen keine Hinweise, dass die genutzten Agenzien über klassische gentechnologische Methoden zur Herstellung rekombinanter Prote-

ine – obwohl diese mindestens ab Anfang/Mitte der 1980er Jahre etabliert waren⁹⁷ – oder gar über die neuen, fortgeschrittenen bio- und gentechnologischen Methoden (z. B. Gen-/Genomsynthese, um-/neugestaltete Stoffwechselwege) hergestellt oder verändert worden wären. Die Zahl an Szenarien, wie LLMs, biologische KI-Modelle oder deren Kombination mit automatisierten Laborplattformen die Fähigkeiten von Akteuren ändern könnten, solche gen- und biotechnologischen Methoden zukünftig zu nutzen, ist angesichts der Vielfalt möglicher Akteure, mit unter anderem unterschiedlichen Ressourcen und Wissen bzw. fachlichen Hintergründen groß (Sabra/Frieß 2025, S.230 ff.). Zudem könnte das Erlangen von Wissen und Laborprotokollen (Kapitel 3.3.1), die potenzielle Umgehung von DNA-Synthesescreeningverfahren (Kapitel 3.3.2) oder die Möglichkeit, (zumindest manche) fehlende praktische Fähigkeiten über automatisierte Laborplattformen zu kompensieren (Kapitel 3.3.3), zu einer größeren Erfolgserwartung bzw. Zuversicht und dadurch Attraktivität mit Blick auf eine potenziell erfolgreiche Beschaffung oder Herstellung nutzbarer biologischer Agenzien beitragen.

Dennoch könnten auch zukünftige Bedrohungen eine Gemeinsamkeit aufweisen, die bereits charakteristisch für die ganz wenigen bisherigen erfolgreichen Bioterroranschläge (vor allem im Sinne der Verursachung von Todesopfern oder Erkrankten) war. In diesen Fällen, also den Kontaminationen mit Salmonellen durch die Rajneeshee-Sekte in den USA 1984 und den Anthraxbriefanschlägen in den USA 2001 (Tabelle 3.2), haben Akteure Strategien genutzt, die keine großskaligen und biotechnologisch bzw. technisch-komplexen Prozesse zur Massenproduktion biologischer Agenzien oder deren Ausbringung erforderten.^{98, 99} Solche Strategien, die einfachere und technisch weniger komplexe Prozesse involvieren, könnten auch zukünftig bei Bioterrorbedrohungen durch nicht staatliche Akteure wahrscheinlich(er) sein, da sie nicht die zuvor beschriebenen (und von KIBio-Entwicklungen weitgehend unabhängigen) technischen Voraussetzungen für die Massenproduktion biologischer Agenzien oder aufwendiger Verbreitungsmechanismen erfordern (NAS 2025b, S. 29) (Kapitel 3.2.2). Dies muss jedoch nicht bedeuten, dass damit mögliche Bedrohungen auch weiterhin mit eher kleinen Zahlen von Todesfällen (einige wenige) oder moderaten Zahlen von Erkrankten (hunderte) verbunden wären.

So könnten sehr viel höhere Opferzahlen ohne die Massenproduktion biologischer Agenzien oder komplexer Verwaffnungs- bzw. Ausbringungsprozesse erreicht werden, wenn potenziell Epidemien oder Pandemien auslösende Viren hergestellt und nach absichtlicher Selbstinfektion von Täter/innen („patient zero“) auf andere übertragen würden (Brent/McKelvey 2025; Sabra/Frieß 2025, S. 240 ff.) – z. B. in öffentlichen Verkehrsmitteln oder international stark vernetzten (Hub-)

97 Nicht zuletzt existieren Verfahren bzw. Protokolle zur Herstellung rekombinanter Formen der beiden Proteinketten des bei Anschlägen oft verwendeten Toxins Rizin (Tab. 3.2) (START 2025; Tin et al. 2021, 2022; UMD o. J.) sowie zu deren Reassoziierung zu funktionstüchtigem Rizin seit über 30 Jahren und sind frei zugänglich (Ferrini et al. 1995; Li et al. 1992). Auch bei jüngeren Anschlägen wurde (DOJ 2023) bzw. sollte Rizin, isoliert aus Samen, verwendet werden, darunter bei geplanten Anschlägen 2018 in Nordrhein-Westfalen (beck-online 2020; Flade 2018) und in New York City 2024 (DOJ 2024).

98 So vermehrte die Rajneeshee-Sekte eine kommerziell erworbene Salmonellenprobe in mit Nährlösung gefüllten Petrischalen unter Nutzung wohl standardmäßiger Inkubatoren (einfache thermostatgeregelte Wärmeschränke); die Kulturflüssigkeiten aus den Petrischalen wurden in Flaschen gesammelt. Zur Kontamination wurden kleine Mengen der Kulturflüssigkeiten unter anderem in Salatsoßen in mehreren Restaurants gegossen (King 2022). Für die bei den Briefanschlägen in den USA verwendeten Sporenmenen könnten ebenfalls kleinere Kulturen von Anthrax (etwa 500 ml) ausreichend gewesen sein (DOJ 2010, S. 29). Der Fall zeigt aber, dass – abhängig von dem verwendeten Agens – trotz des (scheinbar) einfachen Verbreitungsmechanismus spezielle Expertise notwendig sein kann. In diesem Fall mindestens zur Konzentration bzw. Aufbereitung der Anthraxsporen (DOJ 2010; Matsumoto 2003).

99 Bei den fehlgeschlagenen Anschlägen der Aum-Shinrikyo-Sekte in Japan konnten die Sektenmitglieder zwar große Mengen von Anthraxbakterien (*Bacillus anthracis*) und selbst gesammelte *Clostridium botulinum*-Bakterien in selbstgebaute 200-l- bzw. 10.000-l-Stahlbehältern (Fermenter) vermehren (ob dabei Bedingungen erreicht wurden, unter den z. B. *C. botulinum* seine Toxine produziert, ist unklar) (Danzig et al. 2012, S. 18, 27). Sie konnten oder wollten diese Bakteriensuspensionen aber nicht weiter konzentrieren oder aufreinigen. Die Ausbringung der Bakterienaufschlämmungen erfolgte mit selbstgebaute Sprühhvorrichtungen, z. B. von LKWs. Im Fall der Anthraxkulturen wurden auch getrocknete Präparationen (mit mutmaßlich darin enthaltenen Sporen) hergestellt und ausgebracht (Danzig et al. 2012, S. 27).

Flughäfen (Sabra/Frieß 2025, S. 240 ff.). Solche Viren dürften aufgrund der derzeitigen begrenzten Möglichkeiten zu gezielten und vorhersagbaren Verbesserungen viraler Eigenschaften oder gar einem (De-novo-)Design gänzlich neuer Viren (Kapitel 3.3.2) am ehesten natürlich vorkommende Viren sein (oder Versionen davon, die zusätzlich über Mutations- und Selektionsprozesse, z. B. in menschlichen Zellen oder Tiermodellen, verändert wurden).

Die in den Kapiteln 3.3.1 bis 3.3.3 dargestellten KI-basierten Möglichkeiten könnten unter Umständen zur synthetischen Herstellung mancher natürlich vorkommender Viren beitragen, z. B. über Informationen bzw. Laborprotokolle zur Herstellung von Viren aus synthetischen DNA-Fragmenten (Hong et al. 2026). Die dafür erforderlichen Fähigkeiten und Erfahrungen können je nach Virus jedoch stark unterschiedlich sein (DeFrancesco 2021; Garfinkel et al. 2007; Noyce/Evans 2018) (Kapitel 3.3.1). Akteure, denen praktische Fähigkeiten fehlen, könnten (trotz der in Kapitel 3.3.3 diskutierten Herausforderungen) versuchen, diesen Mangel über die Auslagerung von zumindest einigen Teilprozessen an automatisierte Laborplattformen, etwa von Cloud Labs, zu kompensieren.

4 Gegenwärtige Regulierungen und Maßnahmen zur Kontrolle von Biowaffen und sicherheitsrelevanter Dual-Use-Forschung

- 4.1 Regelungen und Übereinkommen auf internationaler Ebene**
- 4.2 Der Rechtsrahmen auf Ebene der EU**
- 4.3 Internationale und europäische Initiativen und Leitlinien, die sich mit Biosicherheit bzw. der Verhinderung der Proliferation von Massenvernichtungswaffen befassen**
- 4.4 Regelungen und Mechanismen in Deutschland zur Kontrolle von Biowaffen und für Biosecurity-relevante Forschung**
- 4.5 Vergleichende Perspektive auf Biosecurity-Regulierungen anderer Länder**
- 4.6 Regulierungen und Initiativen zu KI und Bezüge zu Biosicherheit und Biowaffen**
- 4.7 Die Debatte um mögliche Lücken in – und der notwendigen Stärkung von – Regelungen und Mechanismen zur Kontrolle von Biosecurity-Risiken und der Proliferation von Biowaffen**

4 Gegenwärtige Regulierungen und Maßnahmen zur Kontrolle von Biowaffen und sicherheitsrelevanter Dual-Use-Forschung

4.1 Regelungen und Übereinkommen auf internationaler Ebene

4.1.1 Rechtlich bindende Übereinkommen und Regelungen zu Biowaffen

In der zweiten Hälfte des 19. Jahrhunderts begannen Staaten in internationalen Konferenzen, Standards und Normen auch für das Recht im Krieg zu kodifizieren. Wichtige so entstandene Bausteine des modernen humanitären Völkerrechts waren die Haager Abkommen von 1899 und 1907, in denen insbesondere Regeln zur Kriegsführung festgelegt wurden, sowie die 1949 verabschiedeten Genfer Konventionen und die Zusatzprotokolle von 1977 und 2005, die vor allem Vorschriften zum Schutz von Verwundeten, Kriegsgefangenen und Zivilisten in bewaffneten Konflikten umfassen (Auswärtiges Amt o. J.a; Henckaerts/Doswald-Beck 2009). Ein Grundprinzip bezüglich der Verwendung von Waffen ist insbesondere das Gebot, übermäßige Verletzungen oder unnötige Leiden zu vermeiden. Dies wurde bereits in frühen Dokumenten wie den Haager Abkommen festgelegt und motivierte das Verbot der Verwendung chemischer und biologischer Waffen im Genfer Protokoll von 1925 (Henckaerts/Doswald-Beck 2009, S. 237 f.).

Neben Verträgen zwischen Staaten oder internationalen Organisationen, die die Vertragsparteien binden, also dem Völkervertragsrecht, existiert ein Völkergewohnheitsrecht. Es entsteht durch eine weit verbreitete, einheitliche und über längere Zeit ausgeübte staatliche Praxis, die von der Überzeugung getragen ist, rechtlich geboten zu sein (Henckaerts/Doswald-Beck 2009; MTR Legal 2025). Eine solche Praxis lässt sich anhand verschiedener Instrumente nachweisen, darunter internationale Verträge, militärische Handbücher, nationale Rechtsprechung und nationale Gesetzgebung (ICRC 2025; de Vries 2024a). Völkergewohnheitsrecht gilt auch ohne schriftliche Fixierung und ist grundsätzlich für alle Staaten bindend.¹⁰⁰

Derzeit wird allgemein anerkannt, dass das Verbot des Einsatzes biologischer Waffen im Allgemeinen und insbesondere während bewaffneter Konflikte dem Völkergewohnheitsrecht entspricht; ihr Einsatz ist völkerrechtlich geächtet (Henckaerts/Doswald-Beck 2009, S. 256 ff.; de Vries 2024a). Eine zentrale Grundlage hierfür sind internationale vertragliche Übereinkünfte in Bezug auf Biowaffen und deren Einsatz.

¹⁰⁰ Ausnahmen sind beispielsweise möglich, wenn ein Staat während der Entstehung einer Regel nachhaltig und eindeutig widersprochen hat (MTR Legal 2025)

Das Genfer Protokoll von 1925 – Verbot des Einsatzes chemischer und biologischer Waffen im Krieg

Das Genfer Protokoll¹⁰¹ von 1925, das 1928 in Kraft trat, entstand in Reaktion auf den Einsatz chemischer Waffen im Ersten Weltkrieg (Zanders 2025) und verbietet „den Einsatz im Krieg von erstickenden, giftigen oder anderen Gasen sowie allen ähnlichen Flüssigkeiten, Materialien oder Vorrichtungen“¹⁰². Zudem wurde – angesichts erster Verwendungen im Ersten Weltkrieg (für Sabotageakte durch Deutschland; Kasten 3.4) und Befürchtungen zur weiteren Entwicklung von bakteriellen Erregern als Waffen (Zanders 2025, S. 81 ff.) – vereinbart, dieses Verbot auf den Einsatz „bakteriologischer Methoden der Kriegsführung“¹⁰³ auszuweiten (Guillemin 2017; de Vries 2024a; Zanders 2025). Das Protokoll erwähnt zwar nur bakteriologische Methoden der Kriegsführung, gilt jedoch nach einer Deklaration der UN-Vollversammlung von 1969 als so zu verstehen, dass es jegliche biologische Kampfstoffe¹⁰⁴ (UNGA Res 2603 A (XXIV) umfasst (de Vries 2024a).

Wichtige Staaten wie Japan (Kasten 3.4) und die USA gehörten zwar zu den ursprünglichen unterzeichnenden Staaten des Protokolls, ratifizierten es aber erst 1970 bzw. 1975 und wurden so Vertragsparteien. Inzwischen sind 146 Staaten Vertragsparteien des Genfer Protokolls.

Obwohl das Protokoll den Einsatz chemischer und biologischer Waffen im Krieg verbietet, hat eine Reihe von Staaten die Ratifizierung oder den Beitritt unter dem Vorbehalt vollzogen, dass sie nur gegenüber Vertragsstaaten an das Protokoll gebunden sind, und gegenüber jedem Staat, der die Bestimmungen des Protokolls nicht einhält, nicht daran gebunden sind. Somit wurde das Protokoll faktisch als Verbot des Erstgebrauchs chemischer und biologischer Waffen angesehen (Graham 2002; Guillemin 2017; de Vries 2024a; Zanders 2025) und als Abkommen, das einen Kriegführenden nicht einschränkt, wenn der Gegner nicht Vertragspartei ist, nicht als souveräner Staat anerkannt ist oder eine nicht staatliche Einheit darstellt (Zanders 2025, S. 11 f.).

Das Protokoll ebnete den Weg für Abkommen, die schließlich auch die Entwicklung, Herstellung und den Besitz biologischer und chemischer Waffen verboten: das Übereinkommen über das Verbot biologischer Waffen (BWC)¹⁰⁵ von 1972 und das Übereinkommen über das Verbot chemischer Waffen (Chemical Weapons – Convention CWC)¹⁰⁶ von 1993. Darüber hinaus bildet es die rechtliche Grundlage für den General’s Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons (UNSGM) (Jakob et al. 2024) ebenso wie für das Römische Statut von 1998, mit dem der Internationale Strafgerichtshof eingerichtet wurde und das den Einsatz chemischer und biologischer¹⁰⁷ Waffen unter Verwendung der Sprache bzw. Begrifflichkeiten des Protokolls zu einem Kriegsverbrechen erklärt (Zanders 2025).

101 Protokoll über das Verbot der Verwendung von erstickenden, giftigen oder ähnlichen Gasen sowie von bakteriologischen Mitteln im Kriege vom 17. Juni 1925

102 Im Original: „the use in war of asphyxiating, poisonous or other gases, and of all analogous liquids materials or devices“.

103 Im Original: „the use of bacteriological methods of warfare“.

104 Im Original: „any biological agents of warfare“.

105 Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction vom 26. März 1975

106 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction vom 13. Januar 1993

107 Eine spätere Änderung fügte den Einsatz biologischer Waffen zur Liste der Kriegsverbrechen hinzu (de Vries 2024a; Zanders 2025).

Die BWC – Verbot von Entwicklung, Herstellung, Erwerb, Weitergabe, Lagerung und Verwendung biologischer Waffen

Die BWC trat 1975 in Kraft und stellte den ersten multilateralen Vertrag dar, der eine gesamte Kategorie von Waffen verbietet. Auf der BWC-Webseite der UN waren im Mai 2026 189 Staaten als Vertragsparteien der Konvention verzeichnet.¹⁰⁸

Das Übereinkommen verbietet nach Artikel I die Entwicklung, Herstellung, Lagerung, den anderweitigen Erwerb oder die Weitergabe von mikrobiellen oder anderen biologischen Agenzien sowie von Toxinen – unabhängig von ihrem Ursprung oder der Herstellungsmethode – in Arten und Mengen, die für Schutzzwecke oder friedliche Zwecke nicht gerechtfertigt sind. Darüber hinaus verbietet der Vertrag die Entwicklung von Waffen, Ausrüstung oder Trägersystemen zur Verbreitung solcher Stoffe oder Toxine (NTI o. J.b; UNODA o. J.b). Gemäß Artikel IV müssen die Vertragsparteien spezifische Maßnahmen ergreifen, um diese Verbote durchzusetzen und – präzisiert durch Beschlüsse nachfolgender Überprüfungskonferenzen – spezifische Rechtsvorschriften zur Bekämpfung der verbotenen Handlungen einschließlich strafrechtlicher Bestimmungen erlassen (Burck/de Vries 2023, S. 3). Sollte ein Staat über solche Stoffe, Toxine oder Trägersysteme verfügen, hat er ab Inkrafttreten des Vertrags neun Monate Zeit, um seine Bestände zu vernichten oder für friedliche Zwecke umzuwidmen (NTI o. J.b).

Zwar verbietet die BWC (in ihrem Titel und in Artikel I) die Verwendung biologischer Waffen nicht ausdrücklich. Jedoch wurde in der Schlusserklärung der Vertragsüberprüfungskonferenz von 1996 bekräftigt, dass die Verwendung von bakteriologischen (biologischen) und Toxinwaffen, mikrobiellen oder anderen biologischen Wirkstoffen oder Toxinen durch Vertragsparteien in jeglicher Form und unter jeglichen Umständen, die nicht mit prophylaktischen, schützenden oder anderen friedlichen Zwecken vereinbar ist, einen Verstoß gegen Artikel I des Übereinkommens darstellt.

Die BWC selbst ist mit ihren 15 Artikeln vergleichsweise kurz. Im Lauf der Jahre wurde sie durch eine Reihe zusätzlicher Vereinbarungen ergänzt, die auf nachfolgenden, alle 5 Jahre stattfindenden Überprüfungskonferenzen getroffen wurden. Die unterstützende Implementation Support Unit, die beim Büro der UN für Abrüstungsfragen (UNODA) in Genf angesiedelt ist, hilft den Vertragsstaaten in administrativen Aspekten und setzt sich für die Universalisierung des Übereinkommens ein. Sie aktualisiert auch regelmäßig ein Dokument, das Informationen zu zusätzlichen Vereinbarungen enthält, welche die Bedeutung oder den Geltungsbereich einer Bestimmung des Übereinkommens auslegen, definieren oder näher erläutern oder die Anweisungen, Leitlinien oder Empfehlungen zur Umsetzung einer Bestimmung enthalten (UNODA o. J.b).

Bisher gibt es trotz verschiedener Bemühungen kein formales Verifikationsverfahren. Stattdessen existiert seit 1987 das System der vertrauensbildenden Maßnahmen („confidence-building measures“ – CBMs) (Krasny 2024; Lele et al. 2024; Pinzger et al. 2025, S. 20). Das Ziel der CBMs ist es, Unklarheiten, Zweifel und Verdächtigungen zu verhindern oder zu verringern und die internationale Zusammenarbeit im Bereich friedlicher biologischer Aktivitäten zu verbessern. Die Ver-

¹⁰⁸ Ägypten, Haiti, Somalia und Syrien haben den Vertrag zwar unterzeichnet, aber nicht ratifiziert. Tschad, Dschibuti, Eritrea und Israel haben den Vertrag weder unterzeichnet noch sind sie ihm beigetreten (UN 2025).

tragsstaaten der BWC sollen ihre nationalen CBM-Berichte bis spätestens 15. April jedes Jahres bei der BWC Implementation Support Unit einreichen (UNODA o. J.c).¹⁰⁹

Die Resolution 1540 (2004) des UN-Sicherheitsrates – Verbot der Unterstützung nicht staatlicher Akteure, die Zugang zu nuklearen, chemischen oder biologischen Waffen erhalten oder diese nutzen wollen

Die Resolution 1540 (2004) wurde 2004 als Reaktion auf potenzielle terroristische Bedrohungen und aus der Besorgnis heraus verabschiedet, dass terroristische Gruppen Zugang zu nuklearen, chemischen und biologischen Waffen erhalten könnten. Diese mögliche Gefahr wurde von der UN als Bedrohung des Weltfriedens und der internationalen Sicherheit eingestuft, sodass der UN-Sicherheitsrat auf Grundlage von Kapitel VII der UN-Charta zum Handeln ermächtigt wurde, wodurch die Resolution verbindliche Wirkung auf alle Mitgliedstaaten entfaltet (Burck/de Vries 2023).

Im Gegensatz zu anderen internationalen Rechtsinstrumenten, die typischerweise die Aktivitäten von Staaten regeln, zielt die Resolution 1540 (2004) auf die Bedrohung durch nicht staatliche Akteure. Die Resolution verpflichtet Staaten, jede Form von Unterstützung für nicht staatliche Akteure zu unterlassen, die versuchen, nukleare, chemische oder biologische Waffen und ihre Trägersysteme zu entwickeln, zu erwerben, herzustellen, zu besitzen, zu transportieren, weiterzugeben oder einzusetzen. Um dies zu erfüllen, müssen im Einklang mit jeweiligen nationalen Verfahren geeignete wirksame Gesetze erlassen und durchgesetzt werden, die sowohl unmittelbar die aufgezählten Aktivitäten, insbesondere für terroristische Zwecke, untersagen, als auch den Versuch verbieten, eine dieser Aktivitäten zu begehen, sich als Mittäter oder Gehilfe daran zu beteiligen, sie zu unterstützen oder sie zu finanzieren (Pinzger et al. 2025, S. 20 ff.).

Wirksame Maßnahmen für die Verhinderung der verbotenen Aktivitäten und zur geeigneten Kontrolle über damit verbundene Materialien, zu denen die Resolution die Staaten verpflichtet, umfassen (Pinzger et al. 2025, S. 21):

- Maßnahmen zur Erfassung und Sicherung solcher Materialien bei Produktion, Verwendung, Lagerung oder Transport;
- wirksame physische Schutzmaßnahmen;
- Grenzkontrollen und Strafverfolgungsmaßnahmen zur Aufdeckung, Abschreckung, Verhütung und Bekämpfung des unerlaubten Handels mit diesen Materialien und der Vermittlung von ihnen, auch durch internationale Zusammenarbeit, wenn nötig, im Einklang mit ihren nationalen Rechtsbehörden und Gesetzen und im Einklang mit dem Völkerrecht;
- Einrichtung, Entwicklung, Überprüfung und Aufrechterhaltung geeigneter und wirksamer nationaler Export- und Umschlagskontrollen für diese Güter, einschließlich
 - geeigneter Gesetze und Vorschriften zur Kontrolle von Export, Transit, Umschlag und Re-export,

¹⁰⁹ Die CBMs wurden 1986 durch Vertragsstaaten über eine politisch verbindliche Erklärung der damaligen Überprüfungskonferenz beschlossen. Ein beträchtlicher Teil der Vertragsstaaten reicht diese Berichte jedoch nicht zuverlässig ein. So hatten z. B. 2021 nur 92 der damals 183 Vertragsparteien CBM-Berichte eingereicht

- Kontrollen hinsichtlich der Bereitstellung von Geldern und Dienstleistungen im Zusammenhang mit diesem Export und Umschlag, wie Finanzierung und Transport, die zur Verbreitung beitragen würden, sowie
- Einrichtung von Endnutzerkontrollen und
- Einrichtung und Durchsetzung geeigneter straf- oder zivilrechtlicher Sanktionen für Verstöße gegen diese Exportkontrollgesetze und -vorschriften.

Durch die Resolutionen 1977 (2011), 2325 (2016) und 2663 (2022) des UN-Sicherheitsrats werden die Staaten außerdem dazu angehalten, auf freiwilliger Basis nationale Umsetzungsaktionspläne („implementation action plans“) auszuarbeiten, um ihre Prioritäten und Pläne für die Umsetzung der wichtigsten Bestimmungen der Resolution 1540 (2004) darzulegen.¹¹⁰ Das zuständige Security Council Committee (1540 Committee)¹¹¹ hat 48 solcher Pläne bzw. Updates zu Plänen von 39 Staaten erhalten¹¹² – darunter die USA und Großbritannien, aus der EU nur Frankreich, Kroatien und Spanien –, während weitere Staaten dabei sind, ihre nationalen Aktionspläne vorzubereiten oder zu aktualisieren (Pinzger et al. 2025, S. 21).

Mit der Resolution 2663 (2022) bekräftigte der Sicherheitsrat der UN seine Beschlüsse und Anforderungen der Resolution 1540 (2004) und betont erneut, wie wichtig es sei, dass alle Staaten diese Resolution vollständig umsetzen. Resolution 2663 (2022) fordert alle Staaten, die noch keinen ersten Bericht über die Schritte vorgelegt haben, die sie zur Umsetzung der Resolution 1540 (2004) unternommen haben oder unternehmen wollen, erneut auf, weiterhin Anstrengungen zu unternehmen, um dem 1540 Committee unverzüglich einen solchen Bericht vorzulegen. Laut des 1540 Committees¹¹³ haben 185 (der 193) UN-Mitgliedstaaten mindestens einen ersten Bericht und 124 Mitgliedstaaten zusätzliche Informationen zum Stand der Umsetzung vorgelegt, darunter die USA, Kanada, Australien, Großbritannien, die BRICS-Staaten Brasilien, Russland, Indien und China sowie alle aktuellen 27 EU Mitgliedstaaten und die EU als Institution¹¹⁴ (Pinzger et al. 2025, S. 21 f.).

Das Römische Statut des Internationalen Strafgerichtshofs – Kriminalisierung des Einsatzes biologischer Waffen

Der Einsatz biologischer Waffen in bewaffneten Konflikten war bis zur Änderung 2017 des Artikel 8 des Römischen Statuts des Internationalen Strafgerichtshofs in keinem internationalen Instrument unter Strafe gestellt worden (de Vries 2024a und Referenz darin).

Das Römische Statut des Internationalen Strafgerichtshofs vom 17. Juli 1998 ist ein völkerrechtlicher Vertrag und die rechtliche Grundlage für den Internationalen Strafgerichtshof (IStGH) in Den Haag. 125 Länder sind Vertragsstaaten, davon sind 33 afrikanische Staaten, 19 Staaten aus dem asiatisch-pazifischen Raum, 20 aus Osteuropa, 28 aus Lateinamerika und der Karibik und 25 aus Westeuropa und anderen Staaten.

¹¹⁰ <https://www.un.org/en/sc/1540/national-implementation/general-information.shtml> (30.6.2026)

¹¹¹ <https://www.un.org/en/sc/1540/> (30.6.2026)

¹¹² <https://www.un.org/en/sc/1540/national-implementation/national-implementation-plans.shtml> (30.6.2026)

¹¹³ <https://www.un.org/en/sc/1540/national-implementation/national-reports.shtml> (30.6.2026)

¹¹⁴ Die EU ist nur beobachtendes Mitglied in der UN, unterstützt aber die Umsetzung der Resolution (EEAS 2025).

Das Statut enthält in Artikel 8, der Kriegsverbrechensbestimmung, das Verbot der „Verwendung von erstickender, giftiger oder gleichartiger Gase sowie aller ähnlichen Flüssigkeiten, Stoffe oder Vorrichtungen“ sowie der „Verwendung von Gift oder vergifteten Waffen“ sowohl in internationalen als auch in nicht internationalen bewaffneten Konflikten¹¹⁵ (Burck/de Vries 2023; de Vries 2024a). Biologische Waffen wurden ursprünglich nicht ausdrücklich erwähnt, jedoch wurde diese Lücke während der Überprüfungskonferenz im Jahr 2017 mit der Verabschiedung einer Änderung des Artikel 8 geschlossen, wodurch nun explizit auch die „Verwendung von Waffen, die mikrobielle oder andere biologische Agenzien oder Toxine verwenden, unabhängig von ihrer Herkunft oder Herstellungsmethode“¹¹⁶ als Kriegsverbrechen eingestuft wurde (de Vries 2024a; Zanders 2025). Seitdem hat eine Reihe von Staaten (darunter auch Deutschland) die Änderung ratifiziert.

Viele Völkerrechtler argumentieren, dass der Einsatz biologischer Waffen in bewaffneten Konflikten inzwischen auch über das Völkergewohnheitsrecht – also ohne ausdrückliche Vertragsbindung – unter Strafe gestellt sei (Henckaerts/Doswald-Beck 2009, S. 256 ff.; de Vries 2024a und Referenz darin).

Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons

Die Generalversammlung der Vereinten Nationen richtete mit der Resolution A/42/37C (1987) den *Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons* (UNSGM) ein, der Untersuchungen zu Vorwürfen des möglichen Einsatzes chemischer, bakteriologischer (biologischer) und Toxinwaffen durchführen soll. Der UN-Sicherheitsrat bekräftigte dies mit der Resolution 620 (1988). Der UNSGM wird vom Office for Disarmament Affairs in New York verwaltet und untersteht ausschließlich der Zuständigkeit des UN-Generalsekretärs; er ist nicht von Entscheidungen des UN-Sicherheitsrats abhängig (UNODA o. J.d).

Der UNSMG stellt derzeit den einzigen internationalen Mechanismus dar, über den mutmaßliche Einsätze biologischer Waffen unabhängig und wissenschaftlich-technisch untersucht werden können (Jakob et al. 2024; UNODA o. J.d; Yassif et al. 2023, S. 261).

Wenn ein Mitgliedstaat dem Generalsekretär einen Bericht über entsprechende Vorwürfe vorlegt, ist der Generalsekretär befugt, eine Untersuchung einzuleiten, um die Sachlage objektiv und wissenschaftlich zu klären, einschließlich der Entsendung eines Untersuchungsteams, und die Mitgliedstaaten über das Ergebnis zu unterrichten. Der UNSGM ist kein ständiges Untersuchungsgremium, sondern die Mitgliedstaaten benennen Fachberater, qualifizierte Sachverständige und Analyselabors, die dann in eine Liste aufgenommen werden und gemäß den von der Generalversammlung in ihrer Resolution A/45/57C (1990) gebilligten Leitlinien und Verfahren zur Unterstützung einer Untersuchung des UNSGM herangezogen werden können (UNODA o. J.d; Yassif et al. 2023, S. 261).

Alle UN-Mitgliedstaaten können eine Untersuchung durch den UNSGM beantragen, sofern sie ausreichend überzeugende Beweise dafür vorlegen können, dass möglicherweise ein Angriff mit biologischen Waffen stattgefunden hat. Nach der Entscheidung, eine Untersuchung einzuleiten,

115 Als nicht internationale bewaffnete Konflikte gelten Konflikte, in denen Regierungsstreitkräfte gegen eine oder mehrere nicht staatliche bewaffnete Gruppen kämpfen, oder in denen diese Gruppen einander bekämpfen (IKRK 2023).

116 Im Original: „Employing weapons, which use microbial or other biological agents, or toxins, whatever their origin or method of production“.

kann der UN-Generalsekretär kurzfristig ein Missionsteam zusammenstellen und entsenden, wobei er auf eine Liste von Expert/innen, Fachberater/innen und Laboratorien zurückgreifen kann, die zuvor von den UN-Mitgliedstaaten benannt wurden (UNODA o. J.d).

4.1.2 Weitere Übereinkommen und Mechanismen mit Relevanz für Biosecurity-Risiken oder die Proliferation von biologischen Waffen

International Health Regulations (2005)

Die International Health Regulations (2005) (IHR) sind ein Instrument des Völkerrechts, das für 196 Länder, darunter alle Mitgliedstaaten der WHO, rechtsverbindlich ist.¹¹⁷ Die IHR sind die Grundlage der internationalen Bekämpfung von Ereignissen, die eine gesundheitliche Notlage internationaler Tragweite darstellen können. Sie legen Rechte und Pflichten der Länder beim Umgang mit Risiken, Ereignissen und Notfällen im Bereich der öffentlichen Gesundheit fest, die grenzüberschreitende Auswirkungen haben können (RKI o. J.a; WHO 2024a, S. 52 f.).

Zu solchen Pflichten gehört es, zuständige Behörden bzw. nationale IHR-Anlaufstellen¹¹⁸ zu benennen oder einzurichten, Kernkapazitäten für die Überwachung und Reaktion aufzubauen und aufrechtzuerhalten, der WHO Risiken und Ereignisse für die öffentliche Gesundheit mit tatsächlichen oder potenziellen internationalen Auswirkungen auf die öffentliche Gesundheit (unabhängig von ihrer Herkunft oder Quelle) zu melden sowie Informationen über Risiken und Ereignisse für die öffentliche Gesundheit, von denen die WHO Kenntnis erlangt hat, zu überprüfen (WHO 2024a, S. 52 f.). Der Anwendungsbereich umfasst neben Infektionskrankheiten auch allgemein biologische, chemische und radionukleare Ereignisse (RKI o. J.a).

Um die Umsetzung der IHR (2005) durch die Mitgliedstaaten sicherzustellen, hat die WHO einen Rahmen für die Überwachung und Bewertung der IHR entwickelt. Dieser Rahmen umfasst verschiedene Prozesse. In Bezug auf Biosafety und Biosecurity sind dies jährliche Selbstbewertungsberichte der Vertragsstaaten zur Umsetzung von Biosafety- und Biosecurity-Maßnahmen sowie gemeinsame externe Evaluierungen der Funktionsweise eines nationalen Rahmens für Biosafety und Biosecurity sowie damit verbundener Mechanismen. Dieser nationale Rahmen muss Schulungen und Praktiken umfassen, insbesondere in Einrichtungen, die mit hochgefährlichen biologischen Agenzien umgehen oder diese lagern. Diese Einrichtungen sollten identifiziert und überwacht werden, und ihre physische sowie Informations-, Transport- und Personalsicherheit sollten mit einem speziellen Instrument bewertet werden. Die jährliche Selbstbewertung der Vertragsstaaten ist obligatorisch, während die gemeinsamen externen Evaluierungen freiwillig sind (WHO 2024a, S. 52 f.).

¹¹⁷ Durch das Gesetz zu den Internationalen Gesundheitsvorschriften (2005) vom 20. Juli 2007 und durch das Gesetz zur Durchführung der Internationalen Gesundheitsvorschriften (2005) und zur Änderung weiterer Gesetze vom 29. März 2013 wurden die IHR (2005) in deutsches Recht implementiert (RKI o. J.a).

¹¹⁸ Die nationale Anlaufstelle für Deutschland ist das Gemeinsame Melde- und Lagezentrum von Bund und Ländern. In allen Fällen, die übertragbare Krankheiten betreffen, sollen die Bearbeitung der Meldung sowie gegebenenfalls notwendige weitere Maßnahmen vom Robert Koch-Institut koordiniert werden (RKI o. J.a).

Exportkontrollregime, die die internationale Verbreitung sensibler Güter kontrollieren sollen

Es gibt mehrere informelle – also rechtlich nicht verpflichtende – multilaterale Exportkontrollregime, welche die internationalen Nichtverbreitungsverträge, insbesondere den Atomwaffensperrvertrag, die BWC und CWC, ergänzen und unterstützen sollen. Hierzu gehören unter anderem die Nuclear Suppliers Group, die Australia Group, das Missile Technology Control Regime und das Wassenaar Arrangement (Beck/Jones 2019; de Bruin 2022; OSD 2026).

Das wichtigste multilaterale Forum, über das Staaten ihre Exportkontrollen für sensible Güter bzw. Güter mit doppeltem Verwendungszweck (Dual Use)¹¹⁹ im Zusammenhang mit biologischen (und chemischen) Waffen koordinieren, ist die Australia Group¹²⁰ (Brockmann 2025; Brockmann/Héau 2025). Die Gruppe möchte durch die Harmonisierung von Exportkontrollen sicherstellen, dass Industriezweige und Ausfuhren nicht zu der Entwicklung von chemischen oder biologischen Waffen beitragen. Auslöser der Gründung war der Einsatz chemischer Waffen im Jahr 1984 gegen den Iran im Krieg zwischen Iran und Irak sowie Beweise aus einer UN-Untersuchung, dass der Irak viele der Stoffe für sein Chemiewaffenprogramm von der internationalen chemischen Industrie bezogen hatte.¹²¹

Mitglieder sind 42 Staaten sowie die EU.¹²² Teilnehmende Staaten müssen sich zur Einhaltung der BWC (Kapitel 4.1.1) und der 1997 in Kraft getretenen CWC verpflichtet haben sowie selbst mit von der Australia Group gelisteten Agenzien handeln oder diese herstellen (können).¹²³

Die Gruppe tritt jährlich zusammen, um zu beraten, wie die nationalen Genehmigungsverfahren für Ausfuhren sensibler Güter, wie Ausrüstung, Materialien, Technologie und Software, effizienter gestaltet werden können. Die Mechanismen der Gruppe umfassen nationale Kontrollgesetze und -verfahren, gemeinsame Kontrolllisten für entsprechende Güter, Leitlinien für die Industrie, den Informationsaustausch sowie die Harmonisierung bereits getroffener Maßnahmen und, falls erforderlich, die Prüfung der Einführung zusätzlicher einzelstaatlicher Maßnahmen.

Solche Maßnahmen werden von allen Staaten verlangt, um nicht nur die Nichtverbreitungsbestimmungen der BWC und der CWC zu erfüllen, sondern auch die Einhaltung der Bestimmungen der Resolution 1540 (Kapitel 4.1.1) zu gewährleisten. Die Länder der Australia Group haben Genehmigungsverfahren für den Export von Geräten, Materialien, Technologie sowie Software zur Entwicklung und Herstellung chemischer und biologischer Waffen eingeführt. Alle so zu kontrollierenden Güter sind Teil der gemeinsamen Kontrolllisten („Common Control Lists“¹²⁴), die in Konsultationen der Gruppe entwickelt wurden und von Zeit zu Zeit aktualisiert werden.

Zu den in Bezug auf Biowaffen relevanten gelisteten Gütern gehören biologische Agenzien wie bestimmte Viren, Bakterien und Pilze (einschließlich Pflanzen- und Tierpathogene), Toxine sowie Ausrüstungen mit doppeltem Verwendungszweck, um solche Agenzien zu handhaben (z.B. Schutz- und Sicherheitsausrüstungen), herzustellen (z.B. größere Fermenter), zu formulieren (z.B. Gefriertrocknungs- oder Sprühtrocknungsanlagen) oder auszubringen (z.B. bestimmte

119 Güter mit doppeltem Verwendungszweck sind Waren, Software und Technologie, die sowohl für zivile als auch für militärische Anwendungen verwendet werden können.

120 <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/de/index.html> (30.6.2026)

121 <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/de/entstehung.html> (30.6.2026)

122 <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/de/teilnehmer.html> (30.6.2026)

123 <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/membership.html> (30.6.2026)

124 <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/de/kontrolllisten.html> (30.6.2026)

Sprüh- oder Vernebelungssysteme). Darüber hinaus fallen genetische Elemente bzw. Nukleinsäuresequenzen und gentechnisch veränderte Organismen unter die Vereinbarung, die mit der Pathogenität oder den Toxinen von gelisteten Organismen assoziiert sind bzw. solche enthalten. Dies schließt entsprechende synthetisch hergestellte Gensequenzen ein. Auch aufgeführt sind Nukleinsäureassembler und -synthesizer, die teilweise oder vollständig automatisiert sind und dazu dienen, Nukleinsäuren mit einer Länge von mehr als 0,5 Kilobasen zu erzeugen, sowie Software, die für diese Geräte entwickelt wurde und in der Lage ist, funktionale genetische Elemente aus digitalen Sequenzdaten zu entwerfen und herzustellen.¹²⁵

Darüber hinaus soll auch die Ausfuhr von Gütern, die nicht in den Kontrolllisten aufgeführt sind, unterbunden werden, wenn ein Importeur sie möglicherweise in einem chemischen oder biologischen Waffenprogramm verwenden könnte. Diese Catch-all-Bestimmung sieht außerdem vor, dass Exporteure in den Mitgliedstaaten ihre Regierungen benachrichtigen müssen, wenn sie den Verdacht haben, dass ein Importeur beabsichtigt, eingeführte Güter für die Entwicklung chemischer oder biologischer Waffen zu verwenden (Brugger 2002; The Acronym Institute 2002; The Australia Group 2002).

4.2 Der Rechtsrahmen auf Ebene der EU

Die Verantwortung für die Reaktion auf chemische, biologische, radiologische oder nukleare (CBRN) Bedrohungen liegt in erster Linie bei den EU-Mitgliedstaaten. Für Krisen mit grenzüberschreitenden Auswirkungen wurden auf EU-Ebene Verfahren und Instrumente zur Unterstützung der Mitgliedstaaten entwickelt. Insbesondere im Hinblick auf CBRN-Bedrohungen im Bereich der Terrorismusbekämpfung hat sich das Konzept der Zusammenarbeit zwischen den Mitgliedstaaten und der Union stetig erweitert. Durch die CBRN-Aktionspläne¹²⁶ wurden ein Allgefahrenansatz, wichtige Koordinierungs- und Informationsaustauschmechanismen, ein Kapazitätsaufbau, gemeinsame Übungen und der Austausch bewährter Verfahren durch die Mitgliedstaaten mit Unterstützung der EU-Institutionen eingeführt (Villani 2022).

Darüber hinaus wurde eine Reihe spezifischer rechtlicher Verpflichtungen entwickelt (Burck/de Vries 2023; Villani 2022). Hierzu gehören in erster Linie die Verordnung (EU) 2021/821 und die Richtlinie (EU) 2017/541¹²⁷ (de Vries 2024b).

Verordnung (EU) 2021/821

Die Verordnung (EU) 2021/821 ist die wichtigste Verordnung im Zusammenhang mit der Verbreitung biologischer (und chemischer) Waffen (Burck/de Vries 2023; de Vries 2024b). Die ursprüngliche Verordnung des Rates der Europäischen Union von 2009, die die Ausfuhr von Gütern mit doppeltem Verwendungszweck aus der Europäischen Gemeinschaft in Drittstaaten wirksam kon-

¹²⁵ Siehe Punkt 10 der „Control List of Dual-Use Biological Equipment and Related Technology and Software“ (Australia Group 2025)

¹²⁶ Ein erster EU-Aktionsplan zur CBRN-Sicherheit wurde 2009 verabschiedet (Council of the European Union 2009); ein weiterer, spezifischer Aktionsplan zur Verbesserung der Vorsorge gegen CBRN-Sicherheitsrisiken wurde 2017 angenommen (EK 2017). Die EU-Aktionspläne haben keine Rechtskraft, sondern lediglich programmatischen Charakter.

¹²⁷ Richtlinie (EU) 2017/541 vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates

trollieren sollte, wurde mehrfach geändert und schließlich als Verordnung (EU) 2021/821 neugefasst.

Die Verordnung 2021/821 regelt das Ausfuhrkontrollsystem der EU. Hierzu gehören (EK o. J.a):

- gemeinsame Ausfuhrkontrollvorschriften, einschließlich gemeinsamer Bewertungskriterien und gemeinsamer Arten von Genehmigungen (z. B. Einzel- und Allgemeingenehmigungen);
- eine gemeinsame EU-Liste von Gütern mit doppeltem Verwendungszweck;
- gemeinsame Bestimmungen für die Kontrolle der Endverwendung nicht gelisteter Güter (z. B. solche, die für Programme für Massenvernichtungswaffen oder bei Menschenrechtsverletzungen verwendet werden könnten);
- Kontrollen der Vermittlung und der technischen Hilfe im Zusammenhang mit Gütern mit doppeltem Verwendungszweck und ihrer Durchfuhr durch die EU;
- spezifische Kontrollmaßnahmen und die Einhaltung der Vorschriften durch die Ausführenden (z. B. Aufzeichnungen und Register);
- Einrichtung eines Netzes zuständiger Behörden zur Unterstützung des Informationsaustauschs und zur einheitlichen Durchführung und Durchsetzung von Kontrollen in der gesamten EU.

Die Ausfuhrkontrolle von Gütern mit doppeltem Verwendungszweck basiert auf einer gemeinsamen Liste von Gütern, einschließlich damit verbundener Technologien und Software, die in allen Mitgliedstaaten kontrolliert werden müssen. Diese Liste – der Anhang I der Verordnung – wird in der Regel mindestens einmal jährlich durch einen delegierten Rechtsakt aktualisiert, der auf Beschlüssen und Verpflichtungen im Rahmen der internationalen Nichtverbreitungsregime und Ausfuhrkontrollvereinbarungen basiert.

Die Verordnung 2021/821 referenziert die Ausfuhrkontrolllisten der Australia Group (Kapitel 4.1.2) und setzt damit deren rechtlich nicht bindende Normen in rechtsverbindliche Normen um, die in allen EU-Mitgliedstaaten unmittelbar gelten¹²⁸ (Burck/de Vries 2023). In Anlehnung an die Kontrolllisten der Australia Group umfasst diese auch biologische Agenzien, wie human-, tier- oder pflanzenpathogene Viren, Bakterien und Pilze sowie Toxine. Ebenso gehören genetische Elemente und Nukleinsäuresequenzen (einschließlich synthetisch hergestellter Sequenzen), die mit der Pathogenität von diesen Organismen oder den Toxinen assoziiert sind, und entsprechende gentechnisch veränderte Organismen zu den aufgeführten Gütern. Ähnlich der Liste der Australia Group sind auch Nukleinsäureassembler und -synthesizer aufgeführt¹²⁹.

In Anlehnung an die Catch-All-Bestimmung der Australia Group ist eine Genehmigung auch für nicht gelistete Güter erforderlich, wenn der begründete Verdacht besteht, dass diese für militärische Zwecke in einem Land bestimmt sind, gegen das ein Waffenembargo verhängt wurde, oder dass die Endverwendung im Zusammenhang mit chemischen, biologischen oder nuklearen Waffen oder deren Trägersystemen steht (Artikel 4 Verordnung (EU) 2021/821).

¹²⁸ Die Mitgliedstaaten können jedoch weitere Gesetze erlassen oder bestehende Gesetze ändern, um die aus der Verordnung abgeleiteten Verpflichtungen noch näher zu konkretisieren (Burck/de Vries 2023).

¹²⁹ Genannt werden solche Apparate, die teilweise oder vollständig automatisiert sind und dazu dienen, kontinuierliche Nukleinsäuren mit einer Länge von mehr als 1,5 Kilobasen und einer Fehlerquote von weniger als 5 % in einem einzigen Durchlauf zu erzeugen.

Artikel 11 Verordnung (EU) 2021/821 legt auch eine Genehmigungspflicht für Exporte von Gütern innerhalb der EU fest, wenn diese in Anhang IV der Verordnung aufgeführt sind. Als Agenzien, für welche eine nationale allgemeine Genehmigung¹³⁰ für den Handel innerhalb der EU nicht möglich ist, werden dort die Toxine Rizin und Saxitoxin (die unter die BWC und die CWC fallen) aufgeführt.

Die Richtlinie (EU) 2017/541

Die Richtlinie (EU) 2017/541 zur Bekämpfung des Terrorismus zielt in erster Linie darauf ab, den Anwendungsbereich des Strafrechts der Mitgliedstaaten auf terrorismusbezogene Bedrohungen und Aktivitäten innerhalb der EU auszuweiten. Mitglieder werden unter anderem verpflichtet, dass Herstellung, Besitz, Erwerb, Beförderung, Bereitstellung oder Verwendung chemischer, biologischer, radiologischer oder atomarer Waffen sowie die Forschung und Entwicklung im Zusammenhang mit solchen Waffen als terroristische Straftaten eingestuft werden, wenn sie beispielsweise das Ziel haben, die Bevölkerung auf schwerwiegende Weise einzuschüchtern oder öffentliche Stellen rechtswidrig zu einem Tun oder Unterlassen zu zwingen (Artikel 3).

In Bezug auf biologische (und chemische) Waffen beinhaltet die Richtlinie somit ähnliche Verpflichtungen wie die Resolution 1540 (Kapitel 4.1.1). Die Richtlinie enthält jedoch eine konkretere Verpflichtung bezüglich der Art der zu ergreifenden Maßnahmen, indem festgelegt wird, dass die möglichen Freiheitsstrafen für terroristische Straftaten höher sein sollten als bei nicht terroristischen Aktivitäten (Artikel 15, Absatz 2) (Burck/de Vries 2023).

Der geplante European Biotech Act

Am 16. Dezember 2025 veröffentlichte die EU-Kommission einen Vorschlag für einen European Biotech Act (EK 2025b). Er zielt darauf ab, Europas Biotechnologie- und Bioproduktionskapazitäten zu stärken und die Wettbewerbsfähigkeit zu erhöhen, während gleichzeitig die Verhinderung von missbräuchlichen Anwendungen unterstützt werden soll.

Der Gesetzesentwurf konzentriert sich insbesondere auf die Biotechnologie im Gesundheitsbereich¹³¹ und strebt unter anderem Folgendes an (EK 2025b, 2025c):

- die Verbesserung des Zugangs zu Finanzmitteln für den Biotechnologiesektor in der EU, um das Wachstum und die Skalierung von Biotechnologieunternehmen zu unterstützen;

¹³⁰ Allgemeine Genehmigungen sind eine Sonderform von Ausfuhrgenehmigungen, die nicht beantragt werden müssen, sondern von Amts wegen bekannt gegeben wurden. Es werden automatisch alle Ausfuhren genehmigt, die die Voraussetzungen der jeweiligen Allgemeinen Genehmigung erfüllen (BAFA o. J.).

¹³¹ Die Biotechnologie im Gesundheitsbereich macht laut der EU-Kommission derzeit über 80 % des Gesamtwerts des Sektors und 75 % aller Arbeitsplätze in diesem Sektor in Europa aus und repräsentiert wertmäßig auch rund ein Viertel des pharmazeutischen Sektors der EU (EK 2025c).

- die Stärkung der industriellen Kapazitäten der EU und der Innovationsförderung, unter anderem durch die Einrichtung von Kompetenzzentren für neuartige Therapien, Accelerators für Datenqualität und die Förderung von Projekten zur Stärkung von Biodefense¹³²-Fähigkeiten;
- die Nutzung von KI, Daten und digitalen Lösungen im Biotechnologiesektor, unter anderem durch die Implementierung des europäischen Gesundheitsdatenraums, die Schaffung vertrauenswürdiger KI-Testumgebungen und Erleichterungen des Datenaustauschs;
- die Vereinfachung und Beschleunigung regulatorischer Verfahren, um die Markteinführungszeit für Biotechnologieprodukte zu verkürzen, z.B. durch Nutzung regulatorischer Sandboxes,¹³³
- bessere Biosecurity-Vorkehrungen, um den Missbrauch von Biotechnologien zu verhindern.

Speziell in Bezug auf die Biosecurity sollen Bestimmungen klare und harmonisierte Regeln in der gesamten EU schaffen (EK 2025c). Dies soll insbesondere geschehen durch (EK 2025b, 2025c):

- die Einführung einer Pflicht zur Überprüfung des legitimen Bedarfs von Käufern biotechnologischer Produkte mit hohem Missbrauchspotenzial („biotechnology products of concern“), die in Annex I (EK 2025a) genannt sind, darunter synthetisch hergestellte Nukleinsäuresequenzen mit hohem Missbrauchspotenzial („sequences of concern“). Hierzu müssen vor allem der Identitätsnachweis des potenziellen Kunden überprüft sowie Transaktionen aufgezeichnet und verdächtige Transaktionen gemeldet werden;
- die Verschärfung der Kriterien für synthetisch hergestellte Nukleinsäuresequenzen mit hohem Missbrauchspotenzial,¹³⁴
- die Pflicht, dass Benchtop-Synthesegeräte¹³⁵ Mechanismen zum Sequenzscreening enthalten müssen;
- die Überwachung systemischer Risiken von KI-Modellen in biologischen Anwendungen durch die (EU-)Kommission sowie die Einrichtung einer Advisory Group on Biosecurity, die geeignete Risikominderungsmaßnahmen vorschlagen soll;
- Maßnahmen zur Stärkung der Biodefense-Kapazitäten, wie etwa die Früherkennung neuartiger biologischer Bedrohungen.

132 Im Entwurf definiert als „Maßnahmen, Strategien und Vorkehrungen, die insbesondere von staatlichen Akteuren zu präventiven, schützenden oder friedlichen Zwecken entwickelt werden, um biologischen Bedrohungen entgegenzuwirken, Risiken zu verringern und sich auf biologische Bedrohungen vorzubereiten, diese zu erkennen, zu bewerten, darauf zu reagieren und sich davon zu erholen“. (Im Original: „actions, policies, and measures that are designed, in particular by state actors, for preventive, protective or peaceful purposes, to counter biological threats, reduce risks, and prepare for, detect, assess, respond to, and recover from biological threats.“)

133 Damit sind kontrollierte Umgebungen gemeint, in denen Unternehmen innovative Lösungen, regulatorische Verfahren und Technologien erproben können (EK 2025c).

134 Anders als in Exportkontrollregulierungen und ähnlich zu den aktualisierten Empfehlungen des HHS (2023) und des „Framework for Nucleic Acid Synthesis Screening“ in den USA (OSTP 2024), sollen auch Nukleinsäuresequenzen unter diese Kategorie fallen, für die aufgrund von Funktionsvorhersagen davon auszugehen ist, dass sie die Pathogenität eines Erregers oder die Toxizität von Molekülen erhöhen – auch wenn sie nicht von auf international anerkannten Kontrolllisten aufgeführten Erregern stammen.

135 Solche teilweise auf der Laborwerkbank bzw. Labortisch aufstellbaren Geräte erlauben Forschenden, die Nukleinsäuresynthesen direkt in ihren (Forschungs-)Einrichtungen durchzuführen.

4.3 Internationale und europäische Initiativen und Leitlinien, die sich mit Biosicherheit bzw. der Verhinderung der Proliferation von Massenvernichtungswaffen befassen

World Health Organization (WHO) und ihre Leitlinien zur Biosicherheit

Die WHO unterstützt die Mitgliedstaaten durch Leitfäden, technische Hilfe und die Mobilisierung von Ressourcen beim Aufbau ihrer nationalen Kapazitäten in den Bereichen der Biosafety und Biosecurity. Dazu gehören die Unterstützung von Schulungen zum biologischen Risikomanagement, der Austausch zu bewährten Verfahren durch Workshops und Tagungen sowie die Unterstützung bei der Entwicklung eines passenden Rechtsrahmens und die Gewährleistung eines sicheren Transports biologischer Arbeitsstoffe (WHO o. J.a).

Die Leitlinien der WHO zu Aspekten der Biosicherheit und der Dual-Use-Forschung in den Lebenswissenschaften, darunter das Laboratory biosafety manual (WHO 2020), das Global guidance framework for the responsible use of the life sciences (WHO 2022a) und die Laboratory biosecurity guidance (WHO 2024a), sollen grundsätzlich allen Ländern Unterstützung bieten, besonders aber solchen ohne entsprechende Vorschriften. Vor allem die Laboratory biosecurity guidance (WHO 2024a) soll die Entwicklung von Rahmenbedingungen für den Umgang mit hochgefährlichen Krankheitserregern ermöglichen. Sie wurde in Zusammenarbeit mit einer Vielzahl von Stakeholdern, darunter die WHO Collaborating Centres und technische Beratungsgruppen, insbesondere der Technical Advisory Group on Biosafety (TAG-B), entwickelt (WHO 2024b, o. J.b).

Die Tianjin Biosecurity Guidelines

Auf der Konferenz der Vertragsstaaten der BWC im November 2021 legten China und Pakistan, unterstützt von Brasilien, das Arbeitspapier „The Tianjin Biosecurity Guidelines for Codes of Conduct for Scientists“¹³⁶ vor (Chinchilla et al. 2024; Gronvall et al. 2022). Das Dokument enthält zehn (allgemeine) leitende Grundsätze bzw. Standards, um verantwortungsbewusstes Verhalten zu fördern und die Biosecurity zu stärken, bezugnehmend auf die Artikel und Normen des BWC. Diese enthalten unter anderem die Forderungen, dass Forschende die geltenden nationalen Gesetze und Vorschriften, die internationalen Rechtsinstrumente und Normen im Zusammenhang mit biologischer Forschung, einschließlich derjenigen zum Verbot biologischer Waffen, kennen sollen und dass Institutionen, wie Forschungseinrichtungen, Fördergeber und Aufsichtsbehörden, geeignete Mechanismen zur Überwachung, Bewertung und Minderung potenzieller Schwachstellen und Risiken etablieren müssen.

Obwohl die Tianjin-Leitlinien durch die Vertragsstaaten der BWC nicht formal angenommen wurden (Chinchilla et al. 2024; Qin et al. 2026), billigte beispielsweise die InterAcademy Partnership (eine Organisation, der mehr als 140 nationale, regionale oder globale Akademien der Wissenschaften, der Medizin und der Ingenieurwissenschaften angehören) die Leitlinien (IAP 2021). Darüber hinaus identifizierte die WHO (2022b) die Tianjin-Leitlinien ausdrücklich als hochrangige

¹³⁶ Die Leitlinien wurden in Zusammenarbeit mit dem Tianjin University Center for Biosafety Research Strategy, dem Johns Hopkins Center for Health Security und der InterAcademy Partnership entwickelt (Center for Health Security o. J.).

Grundsätze der Biosecurity-Governance und empfahl ihren Mitgliedstaaten, diese als wichtige Referenz bei der Formulierung oder Überarbeitung von Verhaltenskodizes auf nationaler und institutioneller Ebene zu übernehmen (Qin et al. 2026).

Global Partnership against the Spread of Weapons and Materials of Mass Destruction, Biological Security Working Group

Die Global Partnership against the Spread of Weapons and Materials of Mass Destruction (GP) wurde 2002 auf dem G8-Gipfel in Kananaskis (Kanada) mit dem Auftrag ins Leben gerufen, Terroristen und diejenigen, die ihnen Unterschlupf gewähren, daran zu hindern, Waffen und Materialien für Massenvernichtungswaffen sowie deren Trägersysteme zu erwerben. Zu den 31 Mitgliedern zählen die G7-Staaten Deutschland, Frankreich, Italien, Japan, Kanada, USA, Vereinigtes Königreich und die EU sowie eine Reihe weiterer Länder, darunter weitere EU-Mitgliedstaaten, Australien, Chile, Georgien, Jordanien, Mexiko, die Schweiz und die Ukraine.

Die Global Partnership Biological Security Working Group (G7 BSWG) und die Arbeiten zu Risiken im Zusammenhang mit biologischen Waffen („biological security“) stellen einen der vier Hauptbereiche der GP dar. Zu den Aufgaben gehören die Sicherung und Erfassung von Materialien, die ein Risiko für die Verbreitung biologischer Waffen darstellen; die Entwicklung von Maßnahmen zur Vorhersage, Prävention, Aufdeckung oder Unterbindung des Missbrauchs biologischer Kampfstoffe; ebenso die Stärkung der nationalen und internationalen Fähigkeiten zur schnellen Identifizierung und Reaktion auf biologische Angriffe. Die Aktivitäten und Ergebnisse sollen andere internationalen Übereinkommen und Initiativen, wie die BWC (Kapitel 4.1.1) und die GHSA, unterstützen.

Global Health Security Agenda Action Package Prevent-3 Biosafety and Biosecurity

Die Global Health Security Agenda (GHSA) ist eine 2014 gestartete Initiative aus mittlerweile mehr als 70 Ländern, internationalen und Nichtregierungsorganisationen sowie Unternehmen aus dem privaten Sektor. Sie zielt darauf ab, die Fähigkeiten zur Prävention und Verringerung der Wahrscheinlichkeit von Krankheitsausbrüchen – ob natürlich, versehentlich oder absichtlich ausgelöst – zu verbessern (GHSA o. J.b; Pinzger et al. 2025, S. 22 f.).

Der „Biosafety and Biosecurity Action Package Prevent-3 (APP3)“ der GHSA (o. J.a) zielt darauf ab, die globale Biosicherheit voranzutreiben und internationale Instrumente und Abkommen zu unterstützen, darunter die BWC und die Resolution 1540 (2004) (Kapitel 4.1.1).

Die Arbeitsgruppe der APP3 veröffentlichte eine Stellungnahme zur Bedeutung von Biosicherheit im Zeitalter der KI und neuer Technologien, in der unter anderem Schutzmaßnahmen seitens Regierungen, der Industrie, der Wissenschaft und der Zivilgesellschaft gefordert und unterstützt werden. Hierzu gehören die Einrichtung eines internationalen „KI-Bio-Forums“ zur Entwicklung von KI-Modell-Leitplanken, die Stärkung von Kontrollschritten an der Schnittstelle zwischen digitalen Designtools und physischen biologischen Systemen oder/sowie der Einsatz von KI-Tools

zum Aufbau von Kapazitäten für die Pandemievorsorge- und -reaktion (APP3 Emerging Biological Risks Working Group 2024).

International Experts Group of Biosafety and Biosecurity Regulators

Die International Experts Group of Biosafety and Biosecurity Regulators (IEGBBR) wurde unter Führung der Public Health Agency of Canada ins Leben gerufen und setzt sich aus Behörden für biologische Sicherheit und/oder Biosicherheit aus elf Mitgliedsländern¹³⁷ zusammen, die über strenge Kontrollsysteme für Biosafety und Biosecurity verfügen.

Seit der Eröffnungssitzung 2007 treffen sich die Vertreter nationaler Regulierungsbehörden aus den Mitgliedsländern in Abständen von 1,5 bis 2 Jahren, um kritische Themen im Zusammenhang mit Biosicherheit und Regulierungsfragen zu diskutieren, mit dem Ziel, die internationale Zusammenarbeit zwischen den Regulierungsbehörden für Human- und Tierpathogene aufrecht zu erhalten und zu verbessern. Auf Basis erfolgreicher und bewährter Verfahren der elf Mitgliedstaaten hat die IEGBBR ein Modell für eine standardisierte regulatorische Praxis bei Biosicherheitsvorfällen erarbeitet sowie eine App für Mobilgeräte erstellt,¹³⁸ über die detaillierte Informationen zu den nationalen Konzepten der Mitgliedstaaten zugänglich sind (Pinzger et al. 2025, S. 23).

Die Standards und Praktiken des International Gene Synthesis Consortium

Das International Gene Synthesis Consortium (IGSC) existiert seit 2009 und stellt einen Zusammenschluss von Gensyntheseunternehmen und -organisationen dar, die derzeit zusammen die große Mehrheit der weltweiten kommerziellen Gensynthesekapazität repräsentieren.

Das IGSC wurde gegründet, um gemeinsame Standards und Praktiken zur Überprüfung sowohl der Sequenzen von Bestellungen synthetischer Nukleinsäuresequenzen (Kasten 3.6, Kapitel 3.3.2) als auch der Kunden, die die Bestellungen aufgeben, zu entwickeln und anzuwenden (IGSC 2009, 2024). Ziel ist es, das Risiko des Missbrauchs der Nukleinsäuresynthese (Kapitel 3.2.2) zu verringern.

Diese für die IGSC-Mitglieder bindenden Standards und Praktiken zur Überprüfung von Nukleinsäuresequenzen und Kunden („Harmonized Screening Protocol v3.0“) (IGSC 2024) nehmen Richtlinien auf, die ursprünglich 2010 vom US Department of Health and Human Services (HHS 2010, 2023) veröffentlicht und später aktualisiert wurden.

The International Biosecurity and Biosafety Initiative for Science

Die International Biosecurity and Biosafety Initiative for Science (IBBIS) wurde 2024 von der Nuclear Threat Initiative – einer gemeinnützigen, überparteilichen globalen Organisation – gegründet. Ziel der Organisation ist, mit Regierungen, internationalen Organisationen, der Industrie und

¹³⁷ Mitgliedsländer sind Australien, Dänemark, Deutschland, Frankreich, Japan, Kanada, Niederlande, Schweiz, Singapur, USA und das Vereinigte Königreich. Die World Organisation for Animal Health und das Global Infectious Hazards Preparedness Department der WHO sind Nichtmitglieder mit Beobachterstatus.

¹³⁸ <https://iegbbr.org/tools> (30.6.2026)

der Wissenschaft zusammenzuarbeiten, um praxisnahe Werkzeuge zu entwickeln und zu fördern (Wittmann et al. 2025), mit denen Akteure Risiken der Forschung und Entwicklung im Bereich der Biowissenschaften und Biotechnologie minimieren können.

Zu ersten solchen Werkzeugen, die entwickelt wurden, gehört der Software Common Mechanism, der für alle Anbieter von Nukleinsäuresynthesen frei verfügbar ist und die Sicherheitsüberprüfung von bei Syntheseanbietern bestellten Nukleinsäuresequenzen (Kasten 3.6, Kapitel 3.2.2) und Kunden kosteneffizient ermöglichen soll.¹³⁹

EU Centres of Excellence on Chemical, Biological, Radiological and Nuclear Risk Mitigation

Die 2010 gestarteten Chemical, Biological, Radiological and Nuclear (CBRN) Risk Mitigation Centres of Excellence (CoE) sind eine globale Initiative, die von der EU im Rahmen ihres Ziels, Frieden, Stabilität und Konfliktverhütung zu fördern, finanziert und umgesetzt wird. Das CBRN-CoE-Netzwerk besteht aus 63 Partnerländern aus 8 Weltregionen (EU o. J.).

Ziel der Initiative ist die Minderung von Risiken und die Stärkung einer All-Hazards-Sicherheitsgovernance in den Partnerländern der EU. EU-Unterstützung wird für die Umsetzung einer Vielzahl von Maßnahmen zur Minderung von CBRN-Risiken bereitgestellt. Dazu zählen Bedarfs- und Risikobewertungen, nationale und regionale Aktionspläne, Maßnahmen zum Kapazitätsaufbau, Überprüfungen des Rechtsrahmens, Übungen (einschließlich grenzüberschreitender Übungen vor Ort) sowie der interregionale Austausch bewährter Verfahren und gewonnener Erkenntnisse (EU o. J.).

Biosafety Level 4 Zoonotic Laboratory Network

Das 2016 gegründete Biosafety Level 4 Zoonotic Laboratory Network (BSL4ZNET) von Laboren in fünf Staaten (Australien, Deutschland¹⁴⁰, Großbritannien, Kanada und den USA), die mit hochinfektiösen Tierpathogenen der höchsten biologischen Sicherheitsstufe (BSL-4) umgehen, legt einen Schwerpunkt auf Schulungs- und Trainingsmöglichkeiten für das Laborpersonal im Bereich der Biosicherheit.

Neben dem Etablieren von Kommunikationswegen für den Austausch von Informationen, Wissen und Expertise hat das Netzwerk entsprechende Trainingsworkshops organisiert. Wie die IEGBBR geht auch dieses Netzwerk auf eine kanadische Initiative zurück und hat Fördergelder aus staatlichen Programmen für (allgemeine) Sicherheit erhalten. Das Sekretariat des Netzwerks ist bei der Canadian Food Inspection Agency (CFIA) angesiedelt. Neben den Forschungseinrichtungen vernetzt das BSL4ZNET auch nationale Institutionen aus den Bereichen Gesundheit bzw. Landwirtschaft/Tier- und Pflanzengesundheit sowie Sicherheit und Verteidigung (Pinzger et al. 2025, S. 24).

¹³⁹ <https://ibbis.bio/our-work/common-mechanism/> (30.6.2026)

¹⁴⁰ Friedrich-Loeffler-Institut (Bundesforschungsinstitut für Tiergesundheit); Robert Koch Institut, Zentrum für Biologische Gefahren und Spezielle Krankheitserreger/Biosicherheitslabor der Sicherheitsstufe 4

European Research Infrastructure on Highly Pathogenic Agents

Die European Research Infrastructure on Highly Pathogenic Agents (ERINHA) wurde 2008 initiiert und 2017 als Association internationale sans but lucratif (AISBL; Vereinigung ohne Gewinnerzielungsabsicht) nach belgischem Recht gegründet. Die Zentrale der ERINHAs Central Coordination Unit (CCU) befindet sich in Paris.

Ziel ist die Unterstützung der Forschung zu hochinfektiösen Krankheiten, indem verschiedene Hochsicherheitslabore (vor allem der höchsten Sicherheitsstufe BSL-4) miteinander verbunden und gemeinsame Forschungs Kooperationen koordiniert werden. Hierbei geht es insbesondere um hochpathogene Erreger, für die es noch keine zugelassenen oder weit verbreiteten Behandlungsmethoden oder Impfstoffe gibt, wie Ebola, Marburg, Lassa, Krim-Kongo-Hämorrhagisches Fieber, Nipah/Hendra sowie noch unbekannte Pathogene (ERINHA o.J.; Pinzger et al. 2025, S. 23).

4.4 Regelungen und Mechanismen in Deutschland zur Kontrolle von Biowaffen und für Biosecurity-relevante Forschung

In Deutschland gibt es kein einheitliches Gesetz, das Aspekte der Biosecurity als solche regelt. Die Kontrolle von Biowaffen wird durch die Implementierung rechtlicher Verpflichtungen aus internationalen Verträgen sowie durch Rechtsvorschriften der Europäischen Union adressiert. Biosecurity-relevante Forschung wird durch eine Reihe von verschiedenen, sektorspezifischen gesetzlichen (spezialgesetzlichen) Regelungen, die primär Biosafety-Sicherheitsstandards betreffen, mittelbar aber auch zur Biosecurity beitragen, erfasst (Alvarez et al. 2024, S. 38 ff.; Deutscher Ethikrat 2014, S. 101 ff.; Pinzger et al. 2025, S. 27 ff.).

4.4.1 Gesetzliche Regelungen zur Umsetzung internationaler Verpflichtungen zur Kontrolle von Biowaffen

Deutschland ist Vertragspartei aller wichtigen internationalen Abkommen zu biologischen (und chemischen) Waffen (Kapitel 4.1.1): des Genfer Protokolls von 1925, der BWC und des Römischen Statuts des Internationalen Strafgerichtshofs. Zudem ist Deutschland Mitglied der Australia Group (Kapitel 4.1.2). Neben entsprechenden Vorgaben aus diesen Verträgen muss Deutschland die internationalen Verpflichtungen aus der Resolution 1540 (2004) (Kapitel 4.1.1) in nationale Rechtsvorschriften umsetzen. Darüber hinaus sind EU-Vorschriften, insbesondere die Verordnung (EU) 2021/821 (Kapitel 4.2), umzusetzen (Alvarez et al. 2024; Burck/de Vries 2023).

Diese Verpflichtungen betreffen zum einen das Erlassen strafrechtlicher Bestimmungen, wie durch die BWC gefordert, welche die Entwicklung, Herstellung, Lagerung oder den Erwerb biologischer Waffen verbieten. Zum anderen müssen Ein- und Ausfuhrkontrollen für Materialien etabliert werden, die zur Herstellung biologischer Waffen verwendet werden können. So beinhaltet die Resolution 1540 (2004) die Notwendigkeit von Ausfuhrkontrollen im allgemeinen Sinne, und die Ausfuhrkontrolllisten der Australia Group (obwohl nicht rechtlich bindend) wurden in EU-Verord-

nungen und Richtlinien – vor allem die Verordnung (EU) 2021/821 (Kapitel 4.2) – aufgenommen (Burck/de Vries 2023).

Gesetz zur BWC

Die BWC wurde durch das Gesetz zu dem Übereinkommen vom 10. April 1972 über das Verbot der Entwicklung, Herstellung und Lagerung bakteriologischer (biologischer) Waffen und von Toxinwaffen sowie über die Vernichtung solcher Waffen (BaktWaffVernÜbkG)¹⁴¹ 1983 implementiert.

Artikel 2 des Gesetzes verbietet (entsprechend Artikel 1 BWC) Entwicklung, Herstellung, Lagerung, Erwerb oder Zurückhaltung von biologischen Agenzien und Toxinen, die nicht durch zivile Zwecke gerechtfertigt sind. Die spätere Interpretation bzw. Erklärung der Vertragsstaaten der BWC, dass die Konvention auch den *Einsatz* biologischer Waffen verbietet (Kapitel 4.1.1), wurde durch das BaktWaffVernÜbkG nicht übernommen, wodurch die Verwendung durch das BaktWaffVernÜbkG nicht explizit verboten wird (Burck/de Vries 2023). Dieses fehlende explizite Verbot wird zumindest teilweise durch das Verbot des Einsatzes in bewaffneten Konflikten im Völkerstrafgesetzbuch sowie die Erklärung der Bundesregierung, dass das KrWaffKontrG so zu interpretieren ist, dass der Gebrauch biologischer Waffen generell verboten sei, abgemindert (Burck/de Vries 2023).

Völkerstrafgesetzbuch

Das Völkerstrafgesetzbuch (VStGB)¹⁴² setzt das Römische Statut des Internationalen Strafgerichtshofs (Kapitel 4.1.1) in deutsches Recht um (Burck/de Vries 2023; de Vries 2024a).

Es befasst sich unter anderem mit „Kriegsverbrechen des Einsatzes verbotener Mittel der Kriegsführung“ (§ 12). Danach sind im Zusammenhang eines internationalen oder nicht internationalen bewaffneten Konfliktes unter anderem die Verwendung von Gift oder vergifteten Waffen und die Verwendung biologischer oder chemischer Waffen verboten. Diese Verbote gelten auch, wenn Straftaten im Ausland begangen wurden und keinen Bezug zu Deutschland haben (§ 1 VStGB) (Burck/de Vries 2023).

Gesetz über die Kontrolle von Kriegswaffen

Das Gesetz über die Kontrolle von Kriegswaffen (KrWaffKontrG)¹⁴³ ist die wohl wichtigste Regelung bezüglich der Ausfuhren von Kriegswaffen und des Verbots biologischer Waffen (Burck/de Vries 2023). Dieses Gesetz ist seit 1961 in Kraft und wurde seitdem regelmäßig aktualisiert. 1990 wurden biologische (und chemische) Waffen explizit in das KrWaffKontrG aufgenommen.

¹⁴¹ Gesetz zu dem Übereinkommen vom 10. April 1972 über das Verbot der Entwicklung, Herstellung und Lagerung bakteriologischer (biologischer) Waffen und von Toxinwaffen sowie über die Vernichtung solcher Waffen vom 21. Februar 1983

¹⁴² Völkerstrafgesetzbuch vom 26. Juni 2002, zuletzt am 30. Juli 2024 geändert

¹⁴³ Gesetz über die Kontrolle von Kriegswaffen vom 22. November 1990, zuletzt am 19. Februar 2025 geändert

Es verbietet in § 18 „biologische oder chemische Waffen zu entwickeln, herzustellen, mit ihnen Handel zu treiben, von einem anderen zu erwerben oder einem anderen zu überlassen, einzuführen, auszuführen, durch das Bundesgebiet durchzuführen oder sonst in das Bundesgebiet oder aus dem Bundesgebiet zu verbringen oder sonst die tatsächliche Gewalt über sie auszuüben“. Gegenüber internationalen Institutionen hat die Bundesregierung erklärt, dass das Verbot der „Ausübung der tatsächlichen Gewalt“ als ein generelles Gebrauchsverbot zu interpretieren ist (Burck/de Vries 2023 und Referenz darin).¹⁴⁴ Im Gegensatz zum BaktWaffVernÜbkG, das sehr ähnliche Verbote in Bezug auf biologische Waffen enthält, hat das KrWaffKontrG in § 20 explizit Strafvorschriften (mit Freiheitsstrafen) für Verstöße gegen diese Verbote aufgenommen.

Zudem legt das Gesetz in der Kriegswaffenliste¹⁴⁵ fest, welche Agenzien und Organismen als biologische Waffen gelten. Hierzu gehören schädliche Insekten und ihre toxischen Substanzen, eine Reihe von biologischen Agenzien (human- und tierpathogene Erreger, Toxine) sowie weitere tierische und pflanzliche Krankheitserreger. Darüber hinaus gehören hierzu gentechnisch veränderte Mikroorganismen oder genetische Elemente, die Nukleinsäuresequenzen enthalten, welche pathogene Eigenschaften vermitteln, die denen der in den anderen Kategorien aufgeführten Pathogene ähneln, oder eines der aufgeführten Toxine kodieren. Ausgenommen davon sind Ausrüstung, Substanzen und Organismen, die zivilen Zwecken oder der wissenschaftlichen, medizinischen oder industriellen Forschung auf den Gebieten der reinen und angewandten Wissenschaft dienen, sowie Substanzen und Organismen für Vorbeugungs-, Schutz- oder Nachweiszwecke (Burck/de Vries 2023).

Regelungen zur Exportkontrolle: Außenwirtschaftsgesetz und Außenwirtschaftsverordnung

Deutschland hat bereits vor der Verordnung (EU) 2021/821 (Kapitel 4.2) Regelungen zur Kontrolle von Gütern mit doppeltem Verwendungszweck eingeführt, einschließlich solchen, die zur Herstellung biologischer Waffen verwendet werden können.

Das Außenwirtschaftsgesetz (AWG)¹⁴⁶, das ursprünglich 1961 in Kraft trat und 2013 neugefasst wurde, ist grundlegend für die Regulierung von Aus- und Einfuhren. Gemäß diesem Gesetz ist der Außenhandel grundsätzlich frei, für bestimmte Waren gelten aber Beschränkungen. Zu den darin vorgesehenen Beschränkungen gehören auch Verpflichtungen aus der Verordnung (EU) 2021/821, und es legt explizit fest, dass auch Waffen oder Materialien zur Entwicklung von Waffen unter die Beschränkungen fallen können (Burck/de Vries 2023).

Das AWG nimmt die Verordnung (EU) 2021/821 nicht nur auf, sondern dient auch der tatsächlichen Umsetzung und Durchsetzung der Verordnung (was den EU-Mitgliedstaaten selbst überlassen wurde). So definiert es etwa Ausfuhr-, Einfuhr-, Durchfuhr-, Verkaufs-, Erwerbs-, Weitergabe- oder Investitionsverbote sowie Verstöße gegen die Genehmigungspflicht für Handlungen, die in unmittelbar anwendbaren EU-Verordnungen enthalten sind. Zudem enthält das Gesetz Strafvorschriften für Verstöße gegen diese Verbote (§ 18).

¹⁴⁴ Es erscheint aber unklar, ob diese Erklärung Rechtsbestand hat, da die Entstehungsgeschichte des Gesetzes eindeutig darauf hindeuten scheint, dass der Begriff der „tatsächlichen Gewalt“ als Besitz der fraglichen Waffe zu interpretieren war (Burck/de Vries 2023, S. 11).

¹⁴⁵ Ausführungsgesetz zu Artikel 26 Abs. 2 des Grundgesetzes (Gesetz über die Kontrolle von Kriegswaffen) Anlage (zu § 1 Abs. 1) Kriegswaffenliste

¹⁴⁶ Außenwirtschaftsgesetz vom 6. Juni 2013, zuletzt am 27. Februar 2024 geändert

Die Außenwirtschaftsverordnung (AWV)¹⁴⁷ soll das AWG und somit auch die Verordnung (EU) 2021/821 detaillierter umsetzen. Dazu geht die AWV näher auf die Verfahren ein und erweitert die in anderen Instrumenten enthaltenen Verbote und Beschränkungen. In Bezug auf für biologische Waffen möglicherweise relevante Ausfuhren wird (mit Bezug auf eine Liste für Waffen, Munition und Rüstungsmaterial) beispielsweise festgelegt, dass bestimmte biologische Agenzien¹⁴⁸ einer Ausfuhrgenehmigung bedürfen (§ 8), und geregelt, wie eine Ausfuhrgenehmigung beantragt werden kann (§ 21).¹⁴⁹ Auch legt die AWV ein vollständiges Verbot der Weitergabe von Gütern mit doppeltem Verwendungszweck, wie bestimmte biologische Agenzien, die zur Entwicklung biologischer Waffen verwendet werden können, an bestimmte Länder, wie den Iran, Nordkorea oder Russland, fest (§ 74).

4.4.2 Gesetzliche Regelungen für Biosecurity-relevante Forschung

Biosecurity-relevante Forschung wird durch verschiedene sektorspezifische Gesetze, die in erster Linie Sicherheitsvorschriften für Biosafety betreffen, erfasst. Dennoch tragen einige dieser Regelungen zumindest mittelbar auch zur (Erhöhung der) Biosecurity bei, etwa durch die Erlaubnis- und Anzeigepflicht für Personen, die mit bestimmten Krankheitserregern arbeiten, Aufzeichnungspflichten zu durchgeführten Arbeiten und verwendeten biologischen Agenzien, eine Erlaubnispflicht für die Abgabe bestimmter Pathogene sowie durch Sicherheitsüberprüfungen und Beschränkungen von Personen beim Zugang zu gefährlichen biologischen Agenzien bzw. bestimmten Einrichtungen.

Zu diesen gesetzlichen Regelungen gehören insbesondere (Alvarez et al. 2024, S. 38 ff.; Deutscher Ethikrat 2014, S. 101 ff.; Pinzger et al. 2025, S. 28 f.):

- *das Infektionsschutzgesetz (IfSG)*¹⁵⁰, das der Prävention und der Bekämpfung von Infektionskrankheiten beim Menschen dient.¹⁵¹ Biosecurity-relevante Vorschriften im IfSG, sind Erlaubnis- und Anzeigepflichten für die Person, die mit Krankheitserregern arbeitet, sowie die Erlaubnispflicht für die Abgabe von Krankheitserregern. Die Erlaubniserteilung ist unter anderem abhängig von der Sachkenntnis und der Zuverlässigkeit bezüglich der Ausübung der Tätigkeit des Antragstellers.
- *die Biostoffverordnung (BioStoffVO)*¹⁵², die Fragen der Arbeitssicherheit beim Umgang mit Biostoffen¹⁵³ regelt. Diese werden nach den mit ihnen verbundenen Gesundheitsrisiken in vier Risikogruppen eingeteilt und Tätigkeiten mit ihnen dürfen nur in Laboren der entsprechenden Schutzstufen (S 1 bis S 4) durchgeführt werden. Die Verordnung verlangt unter anderem Dokumentationspflichten für die verwendeten Biostoffe, eine behördliche Genehmigung für die erstmalige Aufnahme von Tätigkeiten der Schutzstufen 3 und 4 sowie eine Begrenzung (auf

¹⁴⁷ Außenwirtschaftsverordnung vom 2. August 2013, zuletzt am 11. März 2026 geändert

¹⁴⁸ Biologische Agenzien ausgewählt oder geändert zur Steigerung der Wirksamkeit für die Außergefachtsetzung von Menschen oder Tieren, die Funktionsbeeinträchtigung von Ausrüstung, die Vernichtung von Ernten oder die Schädigung der Umwelt (Außenwirtschaftsverordnung Anlage 1 Anlage AL zur Außenwirtschaftsverordnung, Unternummer 0007a).

¹⁴⁹ Zuständig für die Beantragung von Ausfuhrgenehmigungen für Dual-Use-Güter ist das Bundesamt für Wirtschaft und Ausfuhrkontrolle.

¹⁵⁰ Infektionsschutzgesetz vom 20. Juli 2000, zuletzt am 4. März 2026 geändert

¹⁵¹ Der Infektionsschutz bei Tieren und Pflanzen ist durch das Tierseuchengesetz (TierSG) bzw. das Pflanzenschutzgesetz (PflSchG) gesondert geregelt.

¹⁵² Biostoffverordnung vom 15. Juli 2013, zuletzt am 11. Mai 2026 geändert

¹⁵³ Hierzu gehören Mikroorganismen, Zellkulturen und bestimmte Parasiten (einschließlich ihrer gentechnisch veränderten Formen), die beim Menschen Infektionen, sensibilisierende oder toxische Wirkungen hervorrufen können.

dazu berechnigte, fachkundige und zuverlässige Beschäftigte) für den Zugang zu gefährlichen Agenzien der Risikogruppe 3 und 4.¹⁵⁴

- *Das Gentechnikgesetz*¹⁵⁵ dient dem Schutz der Gesundheit von Menschen sowie der Umwelt vor schädlichen Auswirkungen gentechnischer Verfahren und Produkte. Ähnlich zur BioStoffVO werden gentechnische Arbeiten in vier Sicherheitsstufen eingeteilt. Sie dürfen nur in ausgewiesenen gentechnischen Einrichtungen durchgeführt werden. Für gentechnische Arbeiten der Sicherheitsstufen 3 und 4 bestehen erweiterte Aufzeichnungspflichten und die Pflicht zur Einholung einer Genehmigung.¹⁵⁶ Im Genehmigungsverfahren wird zudem die Zuverlässigkeit des Antragstellers berücksichtigt. Die Freisetzung gentechnisch veränderter Organismen erfordert ebenfalls eine Genehmigung. Ohne Genehmigung steht diese nach dem Gentechnikgesetz unter Strafe.
- *Das Sicherheitsüberprüfungsrecht* nach dem Sicherheitsüberprüfungsgesetz¹⁵⁷ und nach den landesrechtlichen Regelungen soll helfen, Gefahren einzudämmen, die sich an sicherheitsempfindlichen Stellen ergeben können. Festgelegt werden Voraussetzungen und Verfahren zur Überprüfung von Personen, die von den zuständigen Stellen mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen. Entsprechende Rechtsverordnungen regeln, welche Einrichtungen unter Sicherheitsüberprüfungen fallen. Auf Bundesebene und in einigen Bundesländern sind bestimmte (Forschungs-)Einrichtungen erfasst, die in erheblichem Umfang mit hochtoxischen Stoffen oder hochpathogenen Mikroorganismen arbeiten.
- *Das Gefahrgutbeförderungsrecht*, vor allem das Gefahrgutbeförderungsgesetz¹⁵⁸ und die auf seiner Grundlage erlassenen Rechtsverordnungen, wie die Gefahrgutverordnung Straße, Eisenbahn und Schifffahrt¹⁵⁹, erfassen auch die Beförderung von Toxinen und infektiösen Substanzen.

Darüber hinaus kann sich eine Haftung für Schäden durch den Umgang mit biologischen Stoffen aus dem allgemeinen Deliktsrecht und aus der Gefährdungshaftung des Gentechnikrechts ergeben (Deutscher Ethikrat 2014, S. 110 f.).

4.4.3 Nicht gesetzliche Regelungen und Verhaltenskodizes für sicherheitsrelevante biologische Forschung

In Bezug auf Forschung mit doppeltem Verwendungszweck (Dual Use) und insbesondere für besorgniserregende solche Forschung („dual use research of concern“ – DURC) (NSABB 2007) – das heißt, die direkt missbräuchlich angewendet und zu erheblichen Bedrohungen mit weitreichenden potenziellen Folgen für die öffentliche Gesundheit und Sicherheit führen kann (Leopoldina/DFG 2022a, S.9; NSABB 2007, S.17) – existieren nur nicht bindende Verhaltenskodizes

¹⁵⁴ Zur Risikogruppe 3 gehören Biostoffe, die eine schwere Krankheit beim Menschen hervorrufen und eine ernste Gefahr für Beschäftigte darstellen können; die Gefahr einer Verbreitung in der Bevölkerung kann bestehen, doch ist normalerweise eine wirksame Vorbeugung oder Behandlung möglich (z.B. *Bacillus anthracis*, Gelbfieberevirus oder Hepatitis C und E). Risikogruppe 4 umfasst Biostoffe, die ebenfalls eine schwere Krankheit beim Menschen hervorrufen und eine ernste Gefahr für Beschäftigte darstellen. Jedoch ist die Gefahr einer Verbreitung in der Bevölkerung unter Umständen groß, und normalerweise ist eine wirksame Vorbeugung oder Behandlung nicht möglich. Beispiele sind das Ebola-, das Pocken-, das Lassa- oder das Marburgvirus (Details zur Einstufung von Biostoffen in Risikogruppen BAuA (2026)).

¹⁵⁵ Gentechnikgesetz vom 16. Dezember 1993, zuletzt am 27. September 2021 geändert

¹⁵⁶ Bei Arbeiten der Sicherheitsstufen 1 und 2 bestehen Pflichten zur Anmeldung bzw. Anzeige bei der zuständigen Behörde.

¹⁵⁷ Sicherheitsüberprüfungsgesetz vom 20. April 1994, zuletzt am 9. Januar 2026 geändert

¹⁵⁸ Gefahrgutbeförderungsgesetz vom 6. August 1975, zuletzt am 2. März 2023 geändert

¹⁵⁹ Gefahrgutverordnung Straße, Eisenbahn und Binnenschifffahrt vom 18. August 2023, zuletzt am 19. Juni 2025 geändert

(Codes of Conduct) bzw. Empfehlungen.¹⁶⁰ Diese können aber beispielsweise über arbeitsrechtliche Regelungen oder im Rahmen der Haftung der Forschenden rechtliche Wirkung entfalten (Burck/de Vries 2023; Deutscher Ethikrat 2014).

Sie umfassen neben Vorgaben von Förderorganisationen für staatlich geförderte Forschungslinien¹⁶¹ vor allem Codes of Conduct bzw. Empfehlungen und Leitlinien von öffentlichen Forschungsorganisationen. Hierzu gehören insbesondere

- *die Hinweise und Regeln der Max-Planck-Gesellschaft zum verantwortlichen Umgang mit Forschungsfreiheit und Forschungsrisiken*, die erstmals 2010 angenommen und 2017 aktualisiert wurden (MPG 2017), sowie
- *die „Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung“*¹⁶² der Nationalen Akademie der Wissenschaften Leopoldina und der Deutschen Forschungsgemeinschaft (Leopoldina/DFG 2022b). Der Text beruht auf den Hinweisen und Regeln der Max-Planck-Gesellschaft von 2010, die 2014 von einer Arbeitsgruppe der DFG und der Leopoldina angepasst und 2022 als Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung aktualisiert wurden.

In diesen Regeln bzw. Empfehlungen wird zum einen an die Forschenden appelliert, dass sie – über die Einhaltung gesetzlicher Regelungen hinaus – eine besondere ethische Verantwortung haben und die Chancen der Forschung und deren Risiken für Menschenwürde, Leben und andere wichtige Güter gegeneinander abwägen sollen. Es werden eine Risikoanalyse, Maßnahmen zur Sensibilisierung für die Dual-Use-Problematik, eine Risikominimierung und die Prüfung der Veröffentlichung von Forschungsergebnissen empfohlen. Als letztes Mittel soll in Betracht gezogen werden, Forschungsvorhaben zeitlich auszusetzen oder gar nicht durchzuführen.

Zum anderen wenden sich die Empfehlungen an Forschungsinstitutionen, die unter anderem Mitarbeitende für die Problematik sensibilisieren und notwendige Kenntnisse über mögliche rechtliche Beschränkungen der Forschung vermitteln sollen. Sie werden aufgefordert (über die Einhaltung rechtlicher Vorschriften hinaus) Ethikregeln für sicherheitsrelevante Forschung festzulegen und Strukturen für deren Umsetzung zu schaffen. Insbesondere sollen Kommissionen für Ethik sicherheitsrelevanter Forschung (KEFs) eingerichtet werden, die Beratung bei Angelegenheiten, die sich aus der Implementierung solcher Regeln ergeben, bieten sollen (z. B. fragliche Bedingungen für die Durchführung von Forschungsprojekten oder Vermittlungsbedarf bei unterschiedlichen Einschätzungen von Forschenden) (Jakob et al. 2025; Leopoldina/DFG 2024).

Zur Umsetzung der gemeinsamen „Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung“ (Leopoldina/DFG 2022b) haben die Leopoldina und die DFG 2014 die Einsetzung eines „Gemeinsamen Ausschusses zum Umgang mit sicherheitsrelevanter Forschung (GA)“ beschlos-

160 Die Empfehlungen einer von der damaligen Bundesregierung beauftragten Stellungnahme des Deutschen Ethikrats (2014), darunter die Entwicklung eines nationalen Biosicherheitskodex sowie für rechtliche Regelungen zur Definition von DURC, der Einrichtung einer zentralen DURC-Kommission, und der obligatorischen Beratung der Forscher durch diese Kommission bei geplanten DURC-Arbeiten, wurden vom Gesetzgeber nicht umgesetzt (WD 2021).

161 Beispielsweise bittet die Deutsche Forschungsgemeinschaft (DFG) in ihren Rahmenbedingungen der Förderung bzw. dem Leitfaden für die Antragstellung, dass Antragstellende die beantragten Projekte auf die Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung prüfen. Wenn unmittelbare Dual-Use-Risiken gesehen werden, soll eine Stellungnahme zum Risiko-Nutzen-Verhältnis und zu möglichen Maßnahmen der Risikominimierung und gegebenenfalls eine Stellungnahme der Kommissionen für Ethik sicherheitsrelevanter Forschung (KEFs) beigelegt werden (Leopoldina/DFG 2022a, S. 17 f.).

162 Diese umfasst „wissenschaftliche Arbeiten, bei denen die Möglichkeit besteht, dass sie Wissen, Produkte oder Technologien hervorbringen, die missbraucht werden können, um Menschenwürde, Leben, Gesundheit, Freiheit, Eigentum, Umwelt oder ein friedliches Zusammenleben zu schädigen. Diese wird als ‚besorgniserregend‘ bezeichnet, wenn der Missbrauch unmittelbar erfolgen kann und die möglichen Schäden erheblich sind“ (Leopoldina/DFG 2024, S. 10, 18).

sen. Dieser soll den Stand der Implementierung an den Forschungsinstitutionen verfolgen (Monitoring) und die Institutionen bei der Umsetzung unterstützen, insbesondere bei der Etablierung und Arbeit der KEFs (Leopoldina/DFG 2024). Zudem soll der Ausschuss die Entwicklungen bezüglich sicherheitsrelevanter Forschung (auch international) beobachten, möglichen Handlungsbedarf identifizieren sowie die Leopoldina und die DFG entsprechend beraten (Leopoldina/DFG 2024). Laut GA gibt es (Stand September 2024) mindestens 122 KEFs oder vergleichbare Gremien, die mehr als 300 Forschungseinrichtungen zu ethischen Fragen sicherheitsrelevanter Forschung beraten¹⁶³ (Leopoldina/DFG 2024, S. 37 f.).

Einige Forschungseinrichtungen haben in jüngerer Zeit darüber hinaus spezielle Leitlinien und Empfehlungen für die Durchführung von Forschung mit ausländischen Partnern entwickelt (Leopoldina/DFG 2024). Ein Beispiel sind die „Empfehlungen zum Umgang mit Risiken in internationalen Kooperationen“ der DGF (2023), unter anderem zu Fragen von Abhängigkeiten von Partnerländern oder zu möglichen verdeckten, auch militärischen, Zielen der Partner bzw. Partnerländer.

4.4.4 Initiativen zur Stärkung von Biosecurity und der Nichtproliferation biologischer Waffen

Das Deutsche Biosicherheitsprogramm des Auswärtigen Amtes

Deutschland rief 2013 im Rahmen der Globalen Partnerschaft gegen die Verbreitung von Massenvernichtungswaffen und -materialien (Kapitel 4.3) das Deutsche Biosicherheitsprogramm ins Leben (Auswärtiges Amt o. J.b).

Das Übereinkommen leistet einen Beitrag zur internationalen Zusammenarbeit der Vertragsstaaten der BWC (Kapitel 4.1.1) gemäß Artikel X der BWC und dient als ein Instrument für die präventive Sicherheitspolitik. Es soll Partnerländer dabei unterstützen, für Risiken durch hochpathogene Erreger zu sensibilisieren und biologische Risiken zu minimieren. Ziele des Programms sind (Auswärtiges Amt o. J.b):

- die Präventions- und Reaktionsfähigkeit zu stärken;
- Fähigkeiten zur Detektion und Diagnostik gefährlicher Krankheitserreger zu verbessern;
- Netzwerke in und zwischen Ländern zu bilden und auszubauen;
- die Anwendung internationaler Standards für Biosicherheit (Biosafety und Biosecurity) voranzutreiben;
- das Bewusstsein für Biosicherheit und entsprechende Prinzipien, Praktiken und Instrumente der Nichtverbreitung zu stärken;
- den wissenschaftlichen Austausch im Bereich biologischer Sicherheit zwischen anderen Ländern und Deutschland zu verstärken.

¹⁶³ Bei der MPG und der Leibniz-Gemeinschaft existieren übergeordnete Kommissionen. Auch einige Universitäten setzen auf gemeinschaftlich betriebene Kommissionen. In einigen Helmholtz-Zentren und Leibniz-Instituten existieren (zusätzlich) lokale KEFs (Leopoldina/DFG 2024, S. 88).

An der Umsetzung mehrerer Einzelprojekte¹⁶⁴ des Biosicherheitsprogramms sind beteiligt: das Bernhard-Nocht-Institut für Tropenmedizin (BNITM), die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), das Friedrich-Loeffler-Institut (FLI), das Institut für Mikrobiologie der Bundeswehr (IMB) und das Robert Koch-Institut (RKI). Diese arbeiten mit Partnern in 16 Ländern in Afrika, Zentralasien, Osteuropa und auf dem westlichen Balkan zusammen (Auswärtiges Amt o. J.b).

Zum Deutschen Biosicherheitsprogramm gehören auch die German Online Platform for Global Health Protection sowie das 2027 beginnende Stipendienprogramm „Fellowship in Outbreak Readiness for Global Health Protection (FOR-GHP)“, das sich an Gesundheitsfachkräfte in der Region Afrika richtet.¹⁶⁵

Das UNSGM-Projekt und das Projekt RefBio

Die beiden folgenden vom Auswärtigen Amt geförderten und durch das RKI durchgeführten Projekte zielen darauf ab, den UN-Generalsekretärs-Mechanismus zur Untersuchung des mutmaßlichen Einsatzes von chemischen und biologischen Waffen (UNSGM) (Kapitel 4.1.1) zu stärken.

Das Projekt „Strengthening the UNSGM“ unterstützt das Netzwerk und den Austausch zum UNSGM sowie die Einsatzbereitschaft von für den UNSGM nominierten Expert/innen durch ein Angebot von Trainingsmodulen und Simulationsübungen (RKI o. J.d).

Das Projekt „RefBio – Deutscher Beitrag zur Stärkung der Referenzlabore Bio im UNSGM“ (RKI o. J.b) hat das übergeordnete Ziel, den Aufbau eines internationalen Netzwerks von Referenzlaboren zu unterstützen, die von den UN-Mitgliedstaaten für den UNSGM weltweit nominiert wurden. Beispielsweise unterstützt das Projekt Labore durch Trainingsmöglichkeiten diagnostischer Fähigkeiten und es werden Qualitätssicherungsübungen zum Nachweis von Bakterien, Viren und Toxinen durchgeführt (RKI o. J.c).

4.5 Vergleichende Perspektive auf Biosecurity-Regulierungen anderer Länder

Ähnlich zu Deutschland wird die Kontrolle von Biowaffen bzw. deren Proliferation auch in anderen Ländern der EU oder international durch die Implementierung rechtlicher Verpflichtungen aus Rechtsakten der EU (Kapitel 4.2) bzw. aus den dargestellten internationalen Verträgen (Kapitel 4.1.1) geregelt. Eine wichtige Rolle dabei spielen Gesetze zur Ausfuhrkontrolle von Waffen und Dual-Use-Gütern sowie Gesetze zur Bekämpfung von Terrorismus, einschließlich Terrorismus mit chemischen oder biologischen Waffen (Alvarez et al. 2024; UNIDIR 2026; de Vries 2024b).

Nur in wenigen Ländern sind Biosecurity-Maßnahmen unter besonderen, übergreifenden Biosicherheitsgesetzen (mit speziellen Abschnitten zu Biosafety und Biosecurity) geregelt. Hierzu gehört insbesondere China mit seinem 2021 in Kraft getretenen Biosecurity Law. Das Gesetz hat

¹⁶⁴ <https://www.bnitm.de/forschung/forschungsgruppen/pathogen/abt-virologie/laborgruppe-emmerich/forschungsprojekte/projekte-im-biosicherheitsprogramm> (30.6.2026).

¹⁶⁵ Das Fortbildungsprogramm für junge Wissenschaftler/innen „Global Partnership Initiated Biosecurity Academia for Controlling Health Threats (GIBACHT)“ wurde Ende 2025 eingestellt.

eine Reihe bestehender Einzelvorschriften zusammengeführt, unter anderem aus den Bereichen der Epidemiebekämpfung bei Infektionskrankheiten des Menschen, der Forschung, Entwicklung und Anwendung von Biotechnologie, der Einrichtung und Sicherheit von Laboren für pathologische Mikroorganismen, der Verwaltung menschlicher genetischer Ressourcen sowie der Prävention von Bioterrorismus und der Abwehr von Bedrohungen durch biologische Waffen (Alvarez et al. 2024, S. 28 f.; Simmons/Simmons 2021).

Ein weiteres Beispiel bietet Dänemark, dessen Biosecurity-Regulierung insbesondere auf zwei Gesetzen basiert (CBB 2026): zum einen auf dem Act no. 474 of 17 June 2008 on securing specific biological substances, delivery systems and related materials, auf dessen Grundlage unter anderem spezifische Vorschriften für Unternehmen erlassen wurden, die eine Genehmigung für den Besitz, die Herstellung, die Verwendung und die Lagerung von biologischen Stoffen, Trägersystemen und verwandten Materialien (die im Anhang des Gesetzes aufgeführt sind) erhalten wollen. Als verwandtes Material gilt dabei auch Forschung mit doppeltem Verwendungszweck, die direkt für die Entwicklung biologischer Waffen genutzt werden kann (siehe folgender Abschnitt). Zum anderen auf dem Act no. 53 of 11. January 2017 on control of animal pathogens. Basierend darauf wurden spezifische Vorschriften für Genehmigungen von Unternehmen festgelegt, die (in einer Liste genannte) Krankheitserreger kultivieren, produzieren, verwenden oder lagern möchten, die für biologische Angriffe auf Tiere verwendet werden können (CBB 2026; Harris et al. 2016).

Regulierung von Dual-Use-Forschung

Wie in den Kapiteln 4.4.1 bis 4.4.3 dargestellt, wird in Deutschland sicherheitsrelevante bzw. Dual-Use-Forschung durch eine Reihe verschiedener Gesetze, die primär Biosafety-Sicherheitsstandards betreffen, nur mittelbar erfasst und direkt lediglich in nicht bindenden Empfehlungen von Forschungsorganisationen adressiert. Im Gegensatz dazu haben einige Länder Regelungen für solche Forschung entwickelt, die gesetzliche Wirkung entfalten. Dazu gehören die folgenden Länder.

USA

Die USA verfügen über mehrere, sich überschneidende Regelungen, die Überwachungsinstrumente von Biosafety und Biosecurity in der biowissenschaftlichen Forschung vorgeben (Kuiken 2024, 2025).

Einige Mechanismen und Maßnahmen sind gesetzlich vorgeschrieben, z. B. im Rahmen des „Federal Select Agent Program“¹⁶⁶ oder des im Dezember 2025 in Kraft getretenen BIOSECURE

¹⁶⁶ Im FSAP (einem regulatorischen Bundesprogramm zur Biosecurity) verpflichtet der Public Health Security and Bioterrorism Preparedness and Response Act von 2002 das U.S. Department of Health and Human Services, eine Liste biologischer Agenzien und Toxine zu erstellen und zu regulieren, die eine ernsthafte Gefahr für die öffentliche Gesundheit und Sicherheit darstellen können. Der Agricultural Bioterrorism Protection Act von 2002 verpflichtet das US-Landwirtschaftsministerium (USDA) zur Erstellung und Pflege einer Liste biologischer Agenzien, die eine ernsthafte Gefahr für die Gesundheit und Sicherheit von Tieren oder Pflanzen oder Erzeugnisse davon darstellen können

Act¹⁶⁷. Andere werden als „Federal policy“ (übersetzt etwa Bundesrichtlinien), die zur Auslegung und Umsetzung von Vorschriften dienen, oder als „Agency guidance“ (behördliche Leitlinien), die der Klärung bestehender Regeln dienen, herausgegeben. Diese können für Institutionen, wie Universitäten und andere Forschungseinrichtungen, oder für Einzelpersonen zu de facto verbindlichen Anforderungen werden, z. B. wenn sie Bedingungen für einen Bundeszuschuss oder -vertrag sind, denen der Empfänger zustimmen muss, um Mittel von einer Behörde zu erhalten. Privat finanzierte Forschung fällt in der Regel nicht unter Bundesrichtlinien oder behördliche Leitlinien (Kuiken 2024).

In Bezug auf besorgniserregender Dual-Use-Forschung (DURC) und Gain-of-Function-Experimente – also Experimente, um bei Organismen wie Krankheitserregern neue oder veränderte Eigenschaften zu generieren – sollte die 2024 von der damaligen Biden-Administration veröffentlichte „Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential“ (National Archives 2024) ab Mai 2025 alte DURC-Vorschriften¹⁶⁸ ersetzen. Darin werden unter anderem die schnellen Fortschritte beim Einsatz von künstlicher Intelligenz in den Biowissenschaften sowie deren Dual-Use-Potenzial und die Notwendigkeit von institutioneller Aufsicht über diese Entwicklungen anerkannt. Die neuen Vorschriften sollten eine zusätzliche Überwachung von sieben Arten von Experimenten vorschreiben, die 15 hochgefährliche menschliche und tierische Viren und Bakterien aus einer längeren Liste der US-Regierung mit gefährlichen menschlichen, tierischen und pflanzlichen Krankheitserregern und Toxinen („select agents“) betreffen (Kaiser 2024; Kozlov 2024).

Am 5. Mai 2025 unterzeichnete Präsident Trump die Executive Order 14292¹⁶⁹, mit der alle Bundesmittel für die von seiner Regierung als gefährlich eingestufte Gain-of-Function-Forschung zunächst für 4 Monate ausgesetzt wurden. Die Executive Order 14292 definiert gefährliche Gain-of-Function-Forschung als Studien zu infektiösen Krankheitserregern oder Toxinen, die das Potenzial haben, diese übertragbarer bzw. tödlicher zu machen. Die Executive Order sieht vor, dass das Office of Science and Technology Policy des Weißen Hauses zusammen mit anderen Regierungsbehörden die Richtlinien zur Überwachung solcher Forschung überarbeitet. Außerdem soll die revidierte Richtlinie die Einrichtung einer öffentlich zugänglichen Datenbank vorsehen, in der Institute, die Bundesmittel erhalten, ihre Gain-of-Function-Forschung melden, einschließlich Arbeiten, die aus anderen Quellen finanziert werden (Kuiken 2025; Mallapaty 2025a).

Die Executive Order 14292 verpflichtet Regierungsbehörden außerdem dazu, ein weiteres Dokument zur biomedizinischen Forschung neu zu bewerten: das ebenfalls 2024 von der Biden-Regierung herausgegebene „Framework for Nucleic Acid Synthesis Screening“ (NSTC 2024), das infolge der Executive Order 14110¹⁷⁰ entwickelt wurde (Kapitel 4.6.1 – USA). Es verlangt (entsprechend der Executive Order) von allen Behörden, die Forschung im Bereich der Biowissenschaften finanzieren, festzulegen, dass – als Voraussetzung für die Finanzierung – die Beschaffung syn-

167 Dieses Gesetz beschränkt die Beschaffung bzw. den Erwerb von Biotechnologie-Ausrüstung oder -Dienstleistungen („biotechnology equipment or service“) durch die US-Regierung bei – ebenso wie die Gewährung von Zuschüssen an – „Biotechnologieunternehmen mit besonderem Risiko“. Laut Gesetz bezeichnet „Biotechnologieausrüstung oder -dienstleistungen“ jegliche Ausrüstung, Instrumente, Apparate, Maschinen oder Vorrichtungen, die in der Forschung, Entwicklung, Produktion, Analyse, Erkennung oder Bereitstellung von Informationen über biologisches Material eingesetzt werden, darunter Komponenten, Zubehör, Software, Firmware, digitale Komponenten, Datenspeicherung und -übertragung, Beratung, Krankheitserkennung (Latham & Watkins 2025).

168 Vor allem die früheren Policies der US-Regierung von 2012 zur Überwachung von DURC in den Biowissenschaften (Federal DURC Policy; <https://aspr.hhs.gov/S3/Documents/us-policy-durc-032812.pdf>) und von 2014 zur institutionellen Überwachung von DURC in den Biowissenschaften (Institutional DURC Policy; <https://aspr.hhs.gov/S3/Documents/durc-policy.pdf>)

169 Executive Order 14292 Improving the Safety and Security of Biological Research vom 5. Mai 2025

170 Executive Order 14110 Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence vom 30. Oktober 2023

thetischer Nukleinsäuren und Tischgeräten zur Nukleinsäuresynthese über Anbieter oder Hersteller erfolgt, die Bestellungen und ihre Besteller überprüfen. Entsprechende Anbieter oder Hersteller müssen dies in einer Erklärung bestätigen und Sequenzen und Besteller entsprechend der Leitlinien des Frameworks überprüfen.

Auch in der Executive Order 14292 werden alle Einrichtungen, die die Forschung in den Lebenswissenschaften fördern, angewiesen sicherzustellen, dass die Beschaffung synthetischer Nukleinsäuren über Anbieter oder Hersteller erfolgt, die das aktualisierte Framework einhalten. Diese Verpflichtung für Forschungsförderer wird auch durch den „America’s AI Action Plan“ der Trump-Administration vom Juli 2025 (Kapitel 4.6.1 – USA) als ein Politikziel im Bereich Biosecurity festgelegt.

Dänemark

Dänemark verabschiedete 2008 den Act no. 474 of 17 June 2008 on securing specific biological substances, delivery systems and related materials (CBB 2026). Dual-Use-Forschung, die direkt für die Entwicklung biologischer Waffen oder für offensive Zwecke genutzt werden kann, gilt danach als eine Art von Technologie und somit als verwandtes Material („related materials“). Dieses Gesetz gilt für alle öffentlichen oder privaten, militärischen oder zivilen Einrichtungen (Harris et al. 2016).

Israel

Israel verabschiedete 2008 den Regulation of Research into Biological Disease Agents Act, der unter anderem eine Kontrolle des Zugangs zu biologischen Agenzien durch Genehmigungen der Einrichtungen und die Aufsicht über Dual-Use-Forschung durch institutionelle Ausschüsse vorschreibt. Darüber hinaus sieht das Gesetz die Einrichtung eines interdisziplinären Rates vor, der das Gesundheitsministerium bei der Ausarbeitung und Umsetzung erforderlicher Betriebsvorschriften und -regelungen berät, einschließlich solcher im Zusammenhang mit der Liste der kontrollierten Erreger oder zu Verfahren der institutionellen Ausschüsse (Harris et al. 2016; Lev 2019).¹⁷¹

¹⁷¹ Das Office of the State Comptroller and Ombudsman of Israel bemängelte jedoch in einem Bericht, dass der für die Biosecurity zentrale Regulation of Research into Biological Disease Agents Act weitgehend nur auf dem Papier existiere und nicht in die Praxis umgesetzt wurde (Ben-Nun 2025; Rutherford 2025).

4.6 Regulierungen und Initiativen zu KI und Bezüge zu Biosicherheit und Biowaffen

4.6.1 Rechtliche Regelungen und Standards in wichtigen KI-entwickelnden Ländern oder Märkten für KI-Anwendungen

China

In China existiert (Stand April 2026) kein einheitliches bzw. umfassendes KI-Gesetz (wie z. B. die Verordnung (EU) 2024/1689). Das Land hat jedoch gezielte Vorschriften für bestimmte KI-Anwendungen erlassen und es gibt umfassende technische Standards, die vom Nationalen Technischen Komitee für Informationssicherheit (TC260) herausgegeben werden (HSF Kramer 2026b; White & Case 2025a). Darüber hinaus gelten (auch im Zusammenhang mit KI) bestehende Gesetze zu Datenschutz, Cybersicherheit, geistigem Eigentum, Exportkontrolle und ausländischen Investitionen (HSF Kramer 2026b).

Zu den Vorschriften und nationalen Standards, die bestimmte KI-Anwendungen direkt regulieren, gehören (HSF Kramer 2026b; White & Case 2025a):

- Vorschriften vom November 2022 zu Deep Synthesis¹⁷², die Dienstanbieter unter anderem zur Einrichtung von Mechanismen zur Überprüfung von Algorithmen, zur ethischen Prüfung und zu technischen Schutzmaßnahmen verpflichten;
- die Interim Measures for the Management of Generative AI Services, die im August 2023 in Kraft traten;
- neue Kennzeichnungsvorschriften („labeling rules“), die seit September 2025 gelten, wonach KI-generierte Inhalte (Text, Audio, Bilder, Videos) implizit und gegebenenfalls explizit gekennzeichnet werden müssen¹⁷³;
- nationale Normen vom April 2025 zur Verbesserung der Sicherheit und Governance generativer KI, die im November 2025 in Kraft traten. Diese betreffen Cybersicherheitsmaßnahmen wie Sicherheitsanforderungen für Kennzeichnungsprozesse (Labeling) von Trainingsdaten oder für Datensicherheit von Nutzer/innen sowie den Schutz von Trainingsmodellen und Datensätzen.

Im Juni 2025 schlugen Vertreter des Nationalen Volkskongresses die Schaffung eines umfassenden chinesischen KI-Gesetzes vor, das unter anderem KI-Innovationen unterstützt, ein System zur Klassifizierung und Regulierung von KI-Risiken sowie eine Struktur zur Bewertung der ethischen Auswirkungen von KI schafft und die internationale Zusammenarbeit fördern soll (HSF Kramer 2026b).¹⁷⁴

¹⁷² Deep Synthesis – auch Deepfake genannt – ist eine Technologie, mit der Bild-, Audio- oder Videoinhalte erzeugt oder manipuliert werden können, die realistisch erscheinen.

¹⁷³ Explizite Kennzeichnungen müssen für Nutzer/innen unmittelbar wahrnehmbar sein und werden als Text, Ton, Bilder oder in anderer Form dargestellt. Implizite Kennzeichnungen sind in den Dateimetadaten eingebettet. Sie können nur mit technischen Hilfsmitteln ausgelesen werden.

¹⁷⁴ Der Plan für ein solches Gesetz wurde aber im Dezember 2025 (zumindest vorerst) wieder von der Agenda genommen (Hu/Au 2025).

Ende Dezember 2025 veröffentlichte die Cyberspace-Administration Chinas (CAC) einen Entwurf für Regelungen, die „mensenähnliche interaktive KI-Dienste“¹⁷⁵ besser kontrollieren sollen (China Law Translate 2025). Zu den zentralen Anforderungen an Dienstanbieter gehören beispielsweise die Einhaltung sozialistischer Kernwerte, die Gewährleistung eines umfassenden Nutzerschutzes, die Erfüllung staatlicher Berichtsstandards, einschließlich zur Evaluierung von Risiken für die nationale Sicherheit, und die Sicherstellung qualitativ hochwertiger Trainingsdaten (Baker Botts 2026; HSF Kramer 2026b).

Auf internationaler Ebene hat China verschiedene Initiativen eingebracht oder unterstützt (HSF Kramer 2026b), darunter: eine unter seiner Führung eingebrachte und durch die UN-Generalversammlung im Juli 2024 verabschiedete (nicht bindende) Resolution (Digital Watch 2024), die darauf abzielt, die KI-Fähigkeiten von Entwicklungsländern durch internationale Zusammenarbeit und Initiativen zum Kapazitätsaufbau zu stärken; die Unterzeichnung der Erklärung des Pariser KI-Aktionsgipfels im Februar 2025 (Ministère de l'Europe et des Affaires Étrangères 2025), die die Entwicklung einer sicheren, inklusiven und umweltverträglichen KI fördern soll; und der Vorschlag auf der Weltkonferenz für Künstliche Intelligenz in Shanghai im Juli 2025 zur Gründung einer neuen globalen KI-Kooperationsorganisation, um die Zusammenarbeit im Bereich KI zu stärken sowie regulatorische Maßnahmen zu koordinieren (Gibney 2025; Goh 2025).

EU

Die EU verabschiedete mit der Verordnung (EU) 2024/1689 (Verordnung über künstliche Intelligenz)¹⁷⁶ im Mai 2024 das weltweit erste umfassende Gesetz speziell für KI¹⁷⁷, das einen nicht sektorspezifischen (horizontalen) Regulierungsrahmen für KI-Modelle und -Systeme darstellt (HSF Kramer 2026a; White & Case 2025b). Darüber hinaus existieren verschiedene EU-Gesetze, die die Entwicklung und Nutzung von KI in der EU beeinflussen können. Hierzu gehören die Verordnung (EU) 2016/679¹⁷⁸, die Richtlinie (EU) 2024/2853¹⁷⁹, die ausdrücklich auch für Software (einschließlich KI-Systeme) gilt (Rinne 2025), sowie verschiedene Gesetze zum Schutz des geistigen Eigentums in den nationalen Gesetzen der EU-Mitgliedstaaten (White & Case 2025b).

Verordnung (EU) 2024/1689

Die Verordnung (EU) 2024/1689 gilt für alle Unternehmen, Behörden, Organisationen und weitere Akteure, die ein KI-System in der EU einsetzen oder auf den EU-Markt bringen.¹⁸⁰ Sie verfolgt im

175 „Menschenähnliche interaktive Dienste“ bezeichnet dabei Produkte und Dienstleistungen, die menschliche Persönlichkeitsmerkmale, Denkweisen und Kommunikationsstile simulieren und über Text, Bilder, Audio, Video oder andere Mittel in emotionale Interaktion mit Menschen treten.

176 Verordnung (EU) 2024/1689 vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz und zur Änderung der Verordnungen (EG) Nr. 300/2008, (EU) Nr. 167/2013, (EU) Nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 und (EU) 2019/2144 sowie der Richtlinien 2014/90/EU, (EU) 2016/797 und (EU) 2020/1828 (Verordnung über künstliche Intelligenz)

177 Der EU-KI-Gesetzesentwurf trat am 1. August 2024 in Kraft und ist ab dem 2. August 2026 wirksam (mit Ausnahme der in Artikel 113 aufgeführten Sonderbestimmungen).

178 Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)

179 Richtlinie (EU) 2024/2853 vom 23. Oktober 2024 über die Haftung für fehlerhafte Produkte und zur Aufhebung der Richtlinie 85/374/EWG des Rates

180 Die Regelungen der Verordnung (EU) 2024/1689 gelten nicht für die private Nutzung von KI-Systemen, für KI-Systeme, die für den alleinigen Zweck der wissenschaftlichen Forschung und Entwicklung entwickelt und in Betrieb genommen werden, für Forschungs-, Test- und Entwicklungsarbeiten zu KI-Systemen oder KI-Modellen, bevor diese in Verkehr gebracht oder in Betrieb genommen werden, sowie für KI-Systeme, die ausschließlich für militärische Zwecke, Verteidigungszwecke oder Zwecke der nationalen Sicherheit in Verkehr gebracht oder in Betrieb genommen werden (Bundesnetzagentur o. J.).

Wesentlichen einen funktionalen, risikobasierten Ansatz, wobei der Grad der regulatorischen Eingriffe von der Funktion der KI, also ihrem Verwendungszweck, abhängt (HSF Kramer 2026a). Regulierungskategorien der Verordnung sind:

- *Verbotene Praktiken im KI-Bereich* (Verbotene KI-Systeme): KI-Systeme, die als inakzeptable Risiken für Gesundheit, Sicherheit und Grundrechte gelten (z. B. KI, die zur Emotionserkennung am Arbeitsplatz oder für Social Scoring eingesetzt wird). Diese sind gänzlich verboten.
- *Hochrisiko-KI-Systeme*: KI-Systeme, die als erhebliche potenzielle Risiken für Gesundheit, Sicherheit und Grundrechte gelten (z. B. KI-Systeme, die in kritischen Infrastrukturen, im Personalwesen oder zur Unterstützung von medizinischen Diagnosen und Therapieentscheidungen eingesetzt werden). Diese Systeme unterliegen den strengsten Regelungen des KI-Gesetzes, wie bestimmte Anforderungen an Datensätze und -governance, Dokumentation, menschliche Aufsicht oder die Konformitätsbewertung zum Nachweis der Einhaltung.
- *KI-Systeme mit begrenztem Risiko*: unter anderem KI-Systeme, die synthetische Inhalte generieren oder Inhalte manipulieren (z. B. Deepfakes). Diese unterliegen in der Regel lediglich Transparenzpflichten und der Kennzeichnung mit Wasserzeichen.
- *KI-Modelle mit allgemeinem Verwendungszweck* („general-purpose AI (GPAI) models“) (EK o. J.b): Foundationmodelle, wie große generative KI-Modelle, unterliegen je nach Einstufung (als normale Modelle oder solche mit systemischem Risiko¹⁸¹) unterschiedlichen regulatorischen Pflichten. Solche mit systemischen Risiken unterliegen regulatorischen Verpflichtungen, die denen der Hochrisikokategorie ähneln, während für normale GPAI-Modelle weniger und eher auf Transparenz ausgelegte Verpflichtungen gelten. Der von der EU-Kommission veröffentlichte „General-Purpose AI Code of Practice“ soll Anbietern allgemeiner KI(GPAI)-Modelle bei der Erfüllung ihrer Verpflichtungen gemäß Verordnung (EU) 2024/1689 helfen. Er enthält eine Reihe von Verpflichtungen, unter anderem in Bezug auf Transparenz und Urheberrechtsbestimmungen, Risikobewertungen systemischer Risiken und Risikominderungsstrategien.
- *KI-Systeme mit minimalem Risiko*: Diese Kategorie umfasst alle anderen KI-Systeme, die keinen spezifischen regulatorischen Verpflichtungen unterliegen.

Die Verwendung von KI-Systemen in der Biotechnologie wird in der Verordnung (EU) 2024/1689 nicht direkt genannt. Im Erwägungsgrund 110 der Verordnung wird jedoch im Zusammenhang mit potenziellen systemischen Risiken von GPAI-Modellen angesprochen, dass unter anderem auch möglichen „chemischen, biologischen, radiologischen und nuklearen Risiken, z. B. Möglichkeiten zur Verringerung der Zutrittsschranken, einschließlich für Entwicklung, Gestaltung, Erwerb oder Nutzung von Waffen“ Rechnung getragen werden muss. Auch in der Version des „General-Purpose AI Code of Practice“ vom Juli 2025 (EK o. J.b) werden Risiken, die durch die Ermöglichung chemischer, biologischer, radiologischer und nuklearer (CBRN) Angriffe oder Unfälle entstehen, als systemische Risiken betrachtet. Dies „umfasst die erhebliche Senkung der Eintrittsbarrieren für Angreifer oder die erhebliche Erhöhung der potenziellen Auswirkungen bei der Ent-

181 Systemisches Risiko wird in Artikel 3 Punkt 65 definiert als „ein Risiko, das für die Fähigkeiten mit hoher Wirkkraft von KI-Modellen mit allgemeinem Verwendungszweck spezifisch ist und aufgrund deren Reichweite oder aufgrund tatsächlicher oder vernünftigerweise vorhersehbarer negativer Folgen für die öffentliche Gesundheit, die Sicherheit, die öffentliche Sicherheit, die Grundrechte oder die Gesellschaft insgesamt erhebliche Auswirkungen auf den Unionsmarkt hat, die sich in großem Umfang über die gesamte Wertschöpfungskette hinweg verbreiten können.“

wicklung, Herstellung, Beschaffung, Freisetzung, dem Vertrieb und der Verwendung entsprechen der Waffen oder Materialien“¹⁸² (EK o. J.b, S. 37).

Derzeit scheint unklar, inwiefern biologische KI-Modelle der Regulierung durch die Verordnung (EU) 2024/1689 unterliegen. Biologische KI-Modelle würden als GPAI-Modelle eingestuft, wenn sie vor allem bestimmte Kriterien hinsichtlich ihrer allgemeinen Verwendbarkeit und nachgelagerter Integration (in Systeme bzw. Anwendungen) erfüllen und nicht ausschließlich für Forschungs- und Entwicklungszwecke verwendet werden (FuE-Ausnahme). Hätten diese auch Fähigkeiten hoher Wirkkraft („high-impact capabilities“)¹⁸³ und vernünftigerweise vorhersehbare negative Auswirkungen, erfüllten sie die zuvor beschriebenen Bedingungen (Artikel 51 und Erwägungsgrund 110 der Verordnung) zur Einstufung von GPAI mit systemischem Risiko (Moulange et al. 2025).

Eine Analyse bzw. erste Einschätzung, inwiefern solche Modelle die in der Verordnung (EU) 2024/1689 definierten Kriterien für ein GPAI oder GPAI mit systemischem Risiko erfüllen könnten, wurde Anfang 2025 durch das Centre for Long-Term Resilience¹⁸⁴ veröffentlicht (Moulange et al. 2025). Danach wird es für wahrscheinlich gehalten, dass insbesondere fortschrittlichste Proteinsprachmodelle wie ESM3 (Kapitel 2.3.1) die Definition von GPAI erfüllen, unter anderem da sie eine Vielzahl von Proteindesignaufgaben ausführen können und auch für die Entwicklung nachgelagerter KI-Modelle und -Methoden vorgesehen sind bzw. solche ermöglichen. Auch wird es als realistisch eingeschätzt, dass solche Modelle aufgrund der Kriterien für Fähigkeiten hoher Wirkkraft sowie vorhersehbarer negativer Auswirkungen auf die öffentliche Gesundheit und Sicherheit, etwa durch die Unterstützung böswilliger Akteure zur Entwicklung biologischer Waffen, als GPAI-Modelle mit systemischem Risiko eingestuft werden könnten (Moulange et al. 2025).

Der geplante European Biotech Act

Der von der EU-Kommission am 16. Dezember 2025 veröffentlichte Vorschlag für einen European Biotech Act (Kapitel 4.2) sieht zur Stärkung der Biotechnologie- und Bioproduktionskapazitäten und Wettbewerbsfähigkeit – als eine von einer ganzen Reihe von Maßnahmen – die intensive Nutzung von Daten und digitalen Lösungen einschließlich KI im Biotechnologiesektor vor. Darunter fällt die Implementierung des European Health Data Space (Europäischer Gesundheitsdatenraum), die Erleichterung des Datenaustauschs und die Schaffung vertrauenswürdiger KI-Testumgebungen.

Hinsichtlich der Stärkung der Möglichkeiten zur Verhinderung von missbräuchlichen Anwendungen im Zusammenhang mit KI in der Biotechnologie ist vorgesehen, dass die EU-Kommission das biologische Systemrisiko („biological systemic risk“), das von KI-Modellen in biologischen Anwendungen ausgeht, überwacht. Darüber hinaus soll die Kommission, basierend auf Empfehlungen der Advisory group on biosecurity, einer beratenden Gruppe aus internationalen Expert/innen, und im Einklang mit den Vorschriften der EU für KI, geeignete Mitigationsmaßnahmen vorschlagen. Diese umfassen gegebenenfalls die Stärkung der biologischen Verteidigungskapazitäten (Biode-

182 Im Original: „includes significantly lowering the barriers to entry for malicious actors, or significantly increasing the potential impact achieved, in the design, development, acquisition, release, distribution, and use of related weapons or materials.“

183 Definiert in Artikel 3 Punkt 64 als „Fähigkeiten, die den bei den fortschrittlichsten KI-Modellen mit allgemeinem Verwendungszweck festgestellten Fähigkeiten entsprechen oder diese übersteigen“.

184 Das Centre for Long-Term Resilience ist ein britisches unabhängiges Forschungsinstitut und Non-Profit-Unternehmen, mit dem Ziel, die globale Resilienz gegenüber extremen Risiken zu stärken.

fense) oder die Regulierung, insbesondere hinsichtlich der Bewertung und Minderung des Systemrisikos, dieser KI-Modelle.

USA

Gegenwärtig gibt es in den USA keine umfassenden Bundesgesetze oder -verordnungen, die die Entwicklung von KI regulieren oder deren Nutzung ausdrücklich einschränken oder verbieten.

Die Executive Order 14110 für die sichere und vertrauenswürdige Entwicklung und Nutzung von KI von Präsident Biden¹⁸⁵ wurde mit der Executive Order 14179¹⁸⁶ zur Beseitigung von Hindernissen für die amerikanische Führungsrolle im Bereich KI von Präsident Trump im Januar 2025 aufgehoben. Diese neue Executive Order fordert Bundesbehörden und -einrichtungen auf, alle Richtlinien, Anweisungen, Verordnungen und sonstigen Maßnahmen der Biden-Administration zu überarbeiten oder aufzuheben, die der Stärkung der globalen KI-Vorherrschaft der USA entgegenstehen (White & Case 2025d).

Mit der Executive Order 14110 wurden verschiedene Bundesbehörden mit der Erstellung robuster und standardisierter Evaluierungen von KI-Systemen beauftragt und Unternehmen unter anderem dazu verpflichtet, die Regierung zu informieren, bevor sie Modelle mit über einer bestimmten Schwelle liegenden Rechenleistung freigeben (Pinzger et al. 2025, S. 38 f.). Ein Schwerpunkt lag auf der Bewertung der Fähigkeiten von Foundationmodellen mit Dual-Use-Potenzial, die zu nationalen Sicherheitsrisiken führen können, wie der „erheblichen Senkung der Zugangshürden für Nichtexperten zur Entwicklung, Synthese, Beschaffung oder zum Einsatz chemischer, biologischer, radiologischer oder nuklearer (CBRN-)Waffen“¹⁸⁷ (Pannu et al. 2025). Im Rahmen der Executive Order gründete das US-amerikanische Nationale Institut für Standards und Technologie (NIST) das US AI Safety Institute, ein nationales Institut für KI-Sicherheit, dessen Aufgabe es ist, Leitlinien und Benchmarks für die Bewertung und Prüfung von schädlichen KI-Fähigkeiten, darunter solche, die mit Biosecurity-Risiken verbunden sind, zu entwickeln (Pannu et al. 2025). Weiter beinhaltete die Executive Order unter anderem die Entwicklung eines neuen Standards für das Biosecurity-Screening von Nukleinsäuresynthesen sowie eine Pflicht für alle Fördereinrichtungen lebenswissenschaftlicher Forschung festzulegen, dass die Beschaffung synthetischer Nukleinsäuren bei Herstellern, die sich an diesen Standard halten, Bedingung für den Erhalt von Fördergeldern ist (Crawford et al. 2024) (Kapitel 4.5 – USA).

Es bleibt abzuwarten, wie umfangreich die Änderungen bzw. Überarbeitungen infolge der Executive Order 14179 letztendlich sein werden (White & Case 2025d). So fallen beispielsweise die Meldepflichten für Modelle weg, die bestimmte Rechenschwellenwerte überschreiten, während das US AI Safety Institute, übergeführt und umbenannt in Center for AI Standards and Innovation (CAISI), weiterbesteht (Pannu et al. 2025).

Im Juli 2025 veröffentlichte die Trump-Administration den „America’s AI Action Plan“ (White House 2025). Dieser sieht mehr als 90 bundespolitische Maßnahmen („federal policy actions“)

185 Davor hatten bereits mehrere führende KI-Unternehmen (darunter Amazon, Anthropic, Google, Meta, Microsoft, Open AI, oder Palantir) sich freiwillig verpflichtet, KI-Modelle vor ihrer Veröffentlichung internen und externen Sicherheitstests zu unterziehen, Informationen über den Umgang mit KI-Risiken auszutauschen und in Schutzmaßnahmen zu investieren (White House 2023).

186 Executive Order 14179 Removing Barriers to American Leadership in Artificial Intelligence vom 23. Januar 2025

187 Im Original: „substantially lowering the barrier of entry for non-experts to design, synthesize, acquire, or use chemical, biological, radiological, or nuclear (CBRN) weapons.“

zur Sicherung der US-amerikanischen Führungsrolle im Bereich der KI und zur Verankerung von Innovation im Zentrum der US-KI-Politik vor. Dieser Ansatz unterscheidet sich von den eher risikoorientierten Ansätzen der EU und von manchen Initiativen bzw. Regelungen einzelner US-Bundesstaaten (Pinzger et al. 2025, S. 39; Webster et al. 2026; White & Case 2025d). Der „America’s AI Action Plan“ legt im Bereich Biosecurity als Politikziele fest, dass erstens alle Einrichtungen, die Bundesmittel für wissenschaftliche Forschung erhalten, verpflichtet werden sollen, Werkzeuge für die Nukleinsäuresynthese und Anbieter mit robusten Verfahren zur Sicherheitsüberprüfung von Sequenzen und Kunden zu nutzen, zweitens ein Mechanismus zum Datenaustausch zwischen Anbietern von Nukleinsäuresynthese entwickelt werden soll, mit dem potenziell böswillige Kunden identifiziert werden können, und drittens nationale sicherheitsbezogene KI-Bewertungen in Zusammenarbeit zwischen CAISI, nationalen Sicherheitsbehörden und relevanten Forschungseinrichtungen erstellt, gepflegt und bei Bedarf aktualisiert werden. Die Executive Order 14365¹⁸⁸ vom 11. Dezember 2025 sieht verschiedene Maßnahmen vor, um Auswirkungen der KI-Regulierung von Bundesstaaten, die als unvereinbar mit der KI-Politik der Regierung angesehen werden, zu minimieren (darunter die Anfechtung bundesstaatlicher Regelungen und regulatorische Maßnahmen zur Einschränkung der KI-Vorschriften in Bundesstaaten) (Webster et al. 2026).

Darüber hinaus berät der US-Kongress über eine Reihe von Gesetzesentwürfen zu KI, die ein breites Spektrum an Themen abdecken, darunter die Möglichkeit, Ausnahmen oder Änderungen der Einhaltung bundesstaatlicher Vorschriften beantragen zu können, um KI-Produkte und -Dienstleistungen zu testen, damit zu experimentieren oder sie vorübergehend anzubieten („Sandbox Act“¹⁸⁹). Viele der vorgeschlagenen Gesetze betonen die Entwicklung freiwilliger Leitlinien (White & Case 2025d).

Auf internationaler Ebene haben die USA unter anderem in führender Rolle die im März 2024 angenommene Resolution der UN-Generalversammlung zu KI (Mishra 2024) eingebracht, die dazu beitragen soll, internationale Normen für KI zu etablieren und das wirtschaftliche und gesellschaftliche Potenzial von KI weltweit nutzbar zu machen. Auch unterzeichnete das Land im September 2024 das Rahmenübereinkommen des Europarats über KI (Kapitel 4.6.2) (Pinzger et al. 2025, S. 39; White & Case 2025d).

Indien

In Indien existieren aktuell keine spezifischen Gesetze oder Regelungen, die KI direkt regulieren.

Zur Regulierung von KI wurden aber verschiedene Rahmenwerke entwickelt. Hierzu gehören Prinzipien für verantwortungsvolle KI (Februar 2021)¹⁹⁰, Operationalisierungsprinzipien für verantwortungsvolle KI (NITI Aayog 2021), die auf erforderliche regulatorische und politische Ansätze, den Kapazitätsaufbau sowie ethische Designprinzipien im Umgang mit KI fokussieren, und die „India AI Governance Guidelines“ (MeitY 2025), die die Phasen und Leitprinzipien für künftige KI-Vorschriften sowie Empfehlungen für die Industrie und die Regulierungsbehörden festlegen (White & Case 2026).

188 Executive Order 14365 Ensuring a National Policy Framework for Artificial Intelligence vom 11. Dezember 2025

189 <https://www.commerce.senate.gov/services/files/032DEA9D-0C56-41B4-A155-53FFC3987350> (30.6.2026)

190 <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf> (30.6.2026)

Der vorgeschlagene „Digital India Act“ befindet sich seit 2023 im Entwurfsstadium. Sollte er in Kraft treten, würde er den „Information Technology Act“ von 2000 ersetzen und das Internet sowie digitale Technologien im weiteren Sinne einschließlich KI regeln (Singh 2025; White & Case 2026).

Es gibt aber andere Gesetze, die Auswirkungen auf KI-Anwendungen haben können. Zu nennen sind hier etwa die „Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021“, die nach einer Änderung vom Februar 2026 „synthetisch erzeugte Informationen“ (SGI) regeln. SGI umfassen insbesondere audiovisuelle Informationen, die mithilfe einer Computerressource erstellt oder verändert wurden, um täuschend echt bzw. real zu wirken. Darüber hinaus können die „Digital Personal Data Protection Rules“ von 2025 sowie andere anwendbare Gesetze zum Schutz geistigen Eigentums verschiedene Aspekte der Entwicklung und Nutzung von KI beeinflussen, z. B. die Verwendung personenbezogener Daten für das Training von KI-Modellen (White & Case 2026).

4.6.2 Internationale Regelungen und Initiativen

Derzeit gibt es nur ein rechtlich bindendes Abkommen zur KI auf internationaler Ebene:

Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law

Dieses Abkommen zur KI¹⁹¹ wurde im Mai 2024 vom Ministerkomitee des Europarates offiziell verabschiedet. Zu den Unterzeichnern gehören neben der EU und den USA 16 weitere Staaten, darunter Israel, Japan, Kanada, Norwegen, die Schweiz, die Ukraine und das Vereinigte Königreich. Länder aus aller Welt können dem Vertrag beitreten und sich zu seinen Bestimmungen verpflichten (White & Case 2024).

Die Konvention zielt darauf ab, ethische, rechtliche und gesellschaftliche Fragen im Zusammenhang mit der Nutzung von KI-Systemen zu adressieren und sicherzustellen, dass die Aktivitäten innerhalb des Lebenszyklus von KI-Systemen in vollem Umfang mit den Menschenrechten, der Demokratie und der Rechtsstaatlichkeit im Einklang stehen. Das Abkommen verlangt von jedem Unterzeichnerstaat, dass er: (1) Maßnahmen ergreift, um sicherzustellen, dass bei Menschenrechtsverletzungen, die sich aus den Aktivitäten innerhalb des Lebenszyklus von KI-Systemen ergeben, zugängliche und wirksame Rechtsbehelfe zur Verfügung stehen; sowie (2) gewährleistet, dass den betroffenen Personen wirksame Verfahrensgarantien, Schutzmaßnahmen und Rechte gemäß dem geltenden nationalen und internationalen Recht zur Verfügung stehen. Jeder Unterzeichnerstaat ist außerdem verpflichtet, wirksame Regulierungs- und Aufsichtsmechanismen einzurichten oder zu benennen, um die Einhaltung der Verpflichtungen aus dem Abkommen zu überwachen (White & Case 2024).

Darüber hinaus haben internationale Organisationen, Gruppen verschiedener Länder oder Forscher verschiedene, rechtlich nicht bindende Initiativen ins Leben gerufen, Erklärungen unterschrieben und/oder Empfehlungen veröffentlicht. Hierzu gehören die folgenden Beispiele.

¹⁹¹ Rahmenübereinkommen des Europarats über künstliche Intelligenz und Menschenrechte, Demokratie und Rechtsstaatlichkeit

Die OECD AI Principles

Die OECD AI Principles wurden ursprünglich 2019 verabschiedet und im Mai 2024 aktualisiert (OECD o. J.).

Diese allgemeinen Grundsätze sollen KI-Akteuren im Umgang mit KI als Leitfaden für die Entwicklung vertrauenswürdiger KI dienen und politischen Entscheidungsträgern Empfehlungen für wirksame KI-Maßnahmen zu verschiedenen Handlungsfeldern bieten. Diese umfassen Investitionen in Forschung und Entwicklung im Bereich KI, die Schaffung eines förderlichen Governance- und Politikumfelds für KI, den Aufbau von Humankapital und die Vorbereitung auf den Wandel des Arbeitsmarktes, sowie internationale Zusammenarbeit bei der Entwicklung vertrauenswürdiger KI.

Die Resolutionen A/RES/78/265 und A/RES/79/325 der UN-Generalversammlung

Die im März 2024 von der UN-Generalversammlung verabschiedete Resolution 78/265¹⁹² wurde von mehr als 120 Mitgliedstaaten unterstützt. Sie zielt darauf ab, Länder dazu anzuregen, Menschenrechte zu wahren, personenbezogene Daten zu schützen und KI auf nicht rechtsverbindlicher Basis auf Risiken zu überwachen.

Mit der Resolution A/RES/79/325¹⁹³ wurden vor allem die Einrichtung eines unabhängigen internationalen wissenschaftlichen Expertengremiums für KI, das das wissenschaftliche Verständnis von KI fördern soll, sowie die Einrichtung eines globalen Dialogs über die Regulierung künstlicher Intelligenz beschlossen. Letzterer soll ein jährliches Forum für Regierungen und Interessengruppen sein, um über KI zu diskutieren, zusammenzuarbeiten und bewährte Verfahren auszutauschen (Digital Watch 2025; White & Case 2025c).

Bletchley Declaration

Im Rahmen des UK AI Safety Summit Anfang November 2023 haben Vertreter von 28 Staaten (darunter die USA, China, Frankreich und Japan) und der EU die Bletchley Declaration (GOV.UK o. J.) unterzeichnet.

Die Erklärung erkennt die zentrale Bedeutung der internationalen Zusammenarbeit für eine wirksame Bewältigung von Risiken durch KI an und fordert eine Zusammenarbeit zwischen Nationen, internationalen Organisationen, Unternehmen, Zivilgesellschaft und Wissenschaft. In Bezug auf die Risiken wird erklärt, dass besondere Sicherheitsrisiken durch hochleistungsfähige, allgemein anwendbare KI-Modelle, einschließlich Foundationmodelle, entstehen können, aber auch durch bestimmte, sehr leistungsfähige spezifische KI-Modelle. In Bezug auf mögliche erhebliche Risiken werden vor allem potenzieller vorsätzlicher Missbrauch oder unbeabsichtigte Kontrollprobleme genannt. Besondere Besorgnis hinsichtlich solcher Risiken wird für die Bereiche Cybersicherheit, Biotechnologie und Desinformation ausgedrückt.

¹⁹² Resolution 78/265 Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development

¹⁹³ Resolution A/RES/79/325 Terms of Reference and Modalities for the Establishment and Functioning of the Independent International Scientific Panel on Artificial Intelligence and the Global Dialogue on Artificial Intelligence Governance

Weitere Deklarationen gab es zu den Folgeveranstaltungen: dem AI Seoul Summit 2024 in Seoul¹⁹⁴, dem AI Action Summit in Paris 2025 (La Maison Élysée 2025) und dem India AI Impact Summit in Neu-Delhi 2026¹⁹⁵, bei denen sich der Fokus auf die Sicherheit der KI allerdings deutlich abschwächte (CSR 2025; Gibney 2025; Haeck 2026).

Network for Advanced AI Measurement, Evaluation and Science

Die Gründung des Netzwerks nationaler KI-Sicherheitsinstitute, ursprünglich AI Safety Institute International Network genannt, geht auf den AI Seoul Summit im Mai 2024 zurück. Gemäß der Deklaration des Summits von Seoul soll das internationale Netzwerk dazu dienen, die Weiterentwicklung der Wissenschaft der KI-Sicherheit auf globaler Ebene zu beschleunigen, indem es die Komplementarität und Interoperabilität zwischen den Instituten sowie ein gemeinsames internationales Verständnis der Ansätze zur KI-Sicherheit fördert¹⁹⁶ (Allen/Adamson 2024; EK 2024).

Im Dezember 2025 gehörten dem zu International Network for Advanced AI Measurement, Evaluation and Science umbenannten Netzwerk Australien, die EU, Frankreich, Japan, Kanada, Kenia, Korea, Singapur, das Vereinigte Königreich und die USA an (GOV.UK 2025).

Community Values, Guiding Principles, and Commitments for the Responsible Development of AI for Protein Design

Diese Erklärung (Responsible AI x Biodesign 2023) von Forschenden aus dem Bereich KI in der wissenschaftlichen Forschung entstand aus Diskussionen während und nach einem Treffen am Institut für Proteindesign der University of Washington, USA, am 25. Oktober 2023 (IPD 2023). An den Diskussionen nahmen führende Wissenschaftler/innen aus der ganzen Welt sowie Vertreter/innen verschiedener Organisationen aus dem privaten Sektor, dem philanthropischen Bereich und von US-Regierungsorganisationen teil (Baker/Church 2024; Callaway 2024b).

In der Erklärung verpflichten sich die Unterzeichnenden zu einer Reihe von Prinzipien und der Implementierung von Maßnahmen zur Förderung einer verantwortungsvollen KI-Entwicklung. Hierzu gehören: Forschung zum Wohle der Gesellschaft zu betreiben und von Forschungsvorhaben Abstand zu nehmen, die insgesamt Schaden anrichten oder den Missbrauch ermöglichen könnten; DNA-Synthesedienstleistungen nur von Anbietern in Anspruch zu nehmen, die nachweislich die branchenüblichen Standards für Biosicherheitsscreeningverfahren einhalten; die Fähigkeiten ihrer Proteindesignsoftware kontinuierlich zu evaluieren und bedeutende Sicherheitsrisiken zu mindern; Risiken in ihrem Bereich in regelmäßigen Sitzungen zu überprüfen; sowie über bedenkliche Forschungspraktiken zu berichten.

¹⁹⁴ <https://www.gov.uk/government/publications/seoul-declaration-for-safe-innovative-and-inclusive-ai-ai-seoul-summit-2024> (30.6.2026)

¹⁹⁵ <https://impact.indiaai.gov.in/> (30.6.2026)

¹⁹⁶ Obwohl Italien und Deutschland die Seoul-Deklaration unterzeichneten, wurden sie nicht als Gründungsmitglieder des Netzwerks bestätigt.

4.7 Die Debatte um mögliche Lücken in – und der notwendigen Stärkung von – Regelungen und Mechanismen zur Kontrolle von Biosecurity-Risiken und der Proliferation von Biowaffen

4.7.1 Die BWC (und die Kontrolle von Staaten)

Als gravierendste Schwäche der BWC (Kapitel 4.1.1) gilt das Fehlen eines rechtsverbindlichen Verifikationsmechanismus (Patrick/Barton 2024; Yassif et al. 2023). So verfügt die BWC, im Gegensatz zur CWC und dem Atomwaffensperrvertrag,¹⁹⁷ über keine zugehörige operative Organisation, und die kleine, nur über wenige Mitarbeitende verfügende, Implementation Support Unit (ISU) der BWC hat keine Befugnis, die Umsetzung des Vertrags durch die Vertragsstaaten zu überwachen. Die BWC ermutigt Staaten lediglich im Rahmen vertrauensbildender Maßnahmen (Kapitel 4.1.1), relevante Aktivitäten anhand detaillierter Fragebögen selbst zu melden. Diese Maßnahmen – die darauf abzielen, Missverständnisse und Verdächtigungen zwischen Staaten abzubauen – sind freiwillig, weisen eine geringe Beteiligung auf und erfassen einige relevante nationale Kapazitäten nicht, z. B. in der Biotechnologie des Privatsektors (Patrick/Barton 2024). Allerdings wurde bei der BWC-Überprüfungskonferenz 2022 (UN 2022) eine Arbeitsgruppe ins Leben gerufen, die Maßnahmen zur Vertrauensbildung und Transparenz sowie Maßnahmen zur Einhaltung der Vorschriften und zur Überprüfung erörtern soll (Yassif et al. 2023).

Bemühungen von Vertragsstaaten zur Stärkung des Übereinkommens gibt es seit Mitte der 1990er Jahre, einschließlich für obligatorische Meldungen von Aktivitäten mit möglichem doppeltem Verwendungszweck, kurzfristigen Überprüfungen verdächtiger Einrichtungen und Untersuchungen mutmaßlicher Einsätze biologischer Waffen. Diese Versuche scheiterten jedoch unter anderem an Bedenken, dass solche Überprüfungen für biologische Waffen technisch und praktisch durchführbar sind¹⁹⁸ und dass sie Wirtschaftsspionage erleichtern könnten (Dorey 2001; Patrick/Barton 2024, S. 11 f.).

Angesichts solcher Vorbehalte gab es Vorschläge zu erweiterten Transparenzmaßnahmen bzw. für sonstige robustere Maßnahmen, um die BWC zu stärken. Hierzu gehören unter anderem Modelle, die sich auf strukturierte Erklärungen und freiwillige Transparenzbesuche konzentrieren, oder solche, bei denen Staaten freiwillig ihre Einhaltung der Vorschriften durch Peer-Reviews und Besuche vor Ort nachweisen (Krasny 2025; Revill 2024). Weniger tiefgehende (intrusive) Verifizierungsmaßnahmen als die früher vorgeschlagenen und abgelehnten Inspektionen, die zwar nicht notwendigerweise hoch verlässliche Bewertungen der Einhaltung oder Nichteinhaltung ermöglichen, könnten aber dennoch Transparenz stärken, Misstrauen abbauen (Krasny 2025; Yassif et al. 2023) und mögliche Biowaffenprojekte zumindest entscheidend stören oder zu politischen Kosten für Staaten führen (Ouaghrham-Gormley 2024, 2025). Weiter wurde die Einrichtung einer International Agency for Biological Safety zur Unterstützung der BWC vorgeschlagen (Republic of

¹⁹⁷ So enthält beispielsweise die CWC Bestimmungen, die es der mit mehr als 500 Mitarbeitenden ausgestatteten OPCW ermöglicht, umfassende Vor-Ort-Überprüfung vorzunehmen (Patrick/Barton 2024, S. 10 und Referenz darin).

¹⁹⁸ So wird argumentiert, dass – im Gegensatz zu chemischen oder nuklearen Waffen – die für die Herstellung von Biowaffen benötigten Materialien und Techniken häufig dieselben sind, die in friedlichen Anwendungen der Biowissenschaften eingesetzt werden, sodass selbst bei detaillierten Inspektionen die gewonnenen Informationen nicht unbedingt ausreichen, um festzustellen, ob Biowaffen entwickelt werden. Auch könnten sich (zumindest bestimmte) Biowaffenprogramme leichter verbergen lassen, da manche Biowaffen auf Basis sich replizierender biologischer Einheiten bereits in sehr geringen Mengen wirksam sein können und so weniger Platz für Herstellung und Lagerung benötigen (Patrick/Barton 2024; Yassif et al. 2023).

Kazakhstan 2020), die unter anderem ein universelles multilaterales Exportkontrollregime und ein UN-Register wissenschaftlicher, für militärische Zwecke nutzbarer Entdeckungen schaffen sowie jährliche Pflichtberichte/-erklärungen erstellen soll (Patrick/Barton 2024, S. 11 ff.).

Gleichzeitig wird in der Diskussion um BWC-Reformen aber darauf hingewiesen, dass es schwierig wäre, die gegen die BWC verstoßenden Staaten zur Rechenschaft zu ziehen oder zu bestrafen (Kapitel 3.4). Neben Zuordnungsschwierigkeiten des Einsatzes biologischer Agenzien und rechtlichen Beschränkungen für mögliche Vergeltungsmaßnahmen (Krasny 2025) besteht ein wichtiger Grund darin, dass im Rahmen des weitgehend auf Konsens beruhenden UN-Systems und multilateraler Verträge, Versuche, Staaten zur Rechenschaft zu ziehen, oft von politisierten Diskussionen bestimmt sind. Diese hängen vom geopolitischen Status und den Beziehungen des betreffenden Staates ab und Entscheidungen können von einzelnen Staaten oder einer mächtigen Koalition blockiert werden (Yassif et al. 2023). Hingewiesen wird in diesem Zusammenhang unter anderem auf gut dokumentierte Chemiewaffeneinsätze und damit Verstöße gegen die CWC (Kapitel 3.4). So erlosch beispielsweise das Mandat des gemeinsamen Untersuchungsmechanismus der Organisation for the Prohibition of Chemical Weapons (OPCW) und der Vereinten Nationen, der vom UN-Sicherheitsrat zur Ermittlung und Rechenschaftspflicht der Verantwortlichen für Chemiewaffenangriffe in Syrien eingerichtet worden war, als Russland gegen die Verlängerung des Mandats stimmte (Yassif et al. 2023, S. 262 und Referenz darin).

Aufgrund der Schwierigkeiten, rechtliche Normen der BWC durchzusetzen, wurde verschiedentlich vorgeschlagen, dass die BWC auch nach einer Stärkung von Maßnahmen zur Überprüfung und Einhaltung durch (Abschreckungs-)Strategien ergänzt werden muss, die dem Gegner Erfolgsaussichten für seine Ziele verweigern („deterrence by denial“) (Krasny 2025). Im Zusammenhang mit biologischen Waffen müsste eine solche Abschreckung effektive Maßnahmen zur Früherkennung durch robuste Überwachungssysteme (z. B. von Genomen bzw. Erregern in der Umwelt; Kapitel 2.3.3) sowie zur schnellen Eindämmung und Schadensbegrenzung (z. B. durch flexible Diagnostik, skalierbare Impfstoffplattformen, koordinierte Notfallmaßnahmen und eine gute öffentliche Gesundheitsinfrastruktur) umfassen (Krasny 2025; Ouaghrham-Gormley 2024).

4.7.2 Exportkontrollen

Exportkontrollregime für Dual-Use-Güter wie die Australia Group (Kapitel 4.1.2) oder davon beeinflusste, rechtlich bindende Exportkontrollregulierungen, z. B. in der Verordnung (EU) 2021/821 (Kapitel 4.2) oder in den USA¹⁹⁹ (Bloomfield 2024), umfassen auch die Übermittlung von Software oder Technologie auf elektronischem Wege an einen Bestimmungsort bzw. Personen außerhalb des Zollgebiets. Hierzu gehören beispielsweise bei der Australia Group (2025) und – rechtlich verbindlich – in den USA (unter anderem über die Interactive Commerce Control List – 2D352; BIS o. J.) „Software für Nukleinsäureassembler und -synthesizer [...], die in der Lage ist, funktionelle genetische Elemente aus digitalen Sequenzdaten zu entwerfen und aufzubauen“.²⁰⁰ Ausge-

199 Die beiden wichtigsten US-Exportkontrollsysteme sind die International Traffic in Arms Regulations (ITAR) (vom U.S. Department of State erlassene Vorschriften für Rüstungsgüter und -dienstleistungen) und die Export Administration Regulations (EAR) (vom U.S. Department of Commerce erlassene Vorschriften für Güter mit doppeltem Verwendungszweck und ausgewählte Dienstleistungen).

200 Im Original: „Software designed for nucleic acid assemblers and synthesizers [...] that is capable of designing and building functional genetic elements from digital sequence data.“

nommen davon sind in der Regel²⁰¹ Informationen oder auch Software, die öffentlich in der Public Domain zugänglich sind, sowie Grundlagenforschung (z. B. Wissenstransfer, Veröffentlichungen), zumindest so lange keine anwendbaren Ergebnisse wie etwa operative Prototypen oder sofort einsatzbereite Datensätze entstanden sind. Aufgrund dieser Einschränkungen musste beispielsweise für die Versendung eines wissenschaftlichen Manuskripts aus den Niederlanden an einen Verlag in den USA, das Daten zu Mutationen enthielt, die zur Übertragbarkeit von Vogelgrippeviren auf den Menschen durch die Luft beitragen könnten, eine Exportgenehmigung beantragt werden (Enserink 2013; TAB 2015, S. 106 f.).

KI-Modelle, die die Herstellung biologischer Waffen erleichtern könnten bzw. von Regierungen entsprechend eingestuft würden, könnten so unter die Exportkontrollregelungen fallen (Pinzger et al. 2025, S. 51 f.). Dies könnte gegebenenfalls insbesondere für die leistungsfähigsten LLM-Chatbotmodelle angewendet werden, deren Quellcode und Modellgewichte („model weights“)²⁰² meist nicht offengelegt sind. Dagegen wurden insbesondere für führende Biodesignmodelle, die von akademischen Gruppen entwickelt wurden, solche Details der Modelle veröffentlicht (Naddaf 2025).

Die Möglichkeit, dass Regierungen den Zugang zu KI-Modellen kontrollieren könnten, indem sie bestimmte Modelle Exportkontrollen unterwerfen, aber auch, dass die Verbreitung so regulierter Modelle – da elektronisch übertragbar – faktisch nur schwer zu kontrollieren sein dürfte, wurde verschiedentlich diskutiert (Carter et al. 2023; Revill et al. 2024) (Bloomfield 2024). Darüber hinaus könnten böswillige Akteure über frei zugängliche (und weiter anpassbare) Open-Source- bzw. Open-Weight-Modelle selbstständig neue gefährliche Gensequenzen bzw. Proteine entwerfen (Kapitel 3.2.2). Solche unbekannten Sequenzen könnten zu Schwierigkeiten bei der Kontrolle bei der Bestellung entsprechender synthetischer Nukleinsäuresequenzen oder bei Exportkontrollen führen, da sie möglicherweise nicht als gefährlich erkannt werden (Baker/Church 2024; Carter et al. 2023; Revill et al. 2024).

Manche Rechtswissenschaftler/innen sowie KI-entwickelnde Unternehmen weisen auch darauf hin, dass mögliche Exportkontrollmaßnahmen, insbesondere wenn deren Einhaltung zu komplex und zeitaufwändig wäre, Sicherheitsevaluationen von KI-Modellen beeinträchtigen könnten. Dazu könnte beispielsweise beitragen, dass in Evaluationen keine internationalen Expert/innen mehr einbezogen werden oder Biosecurity-Tests verkürzt werden, um Verzögerungen im Regulationsprozess zu vermeiden (Bloomfield et al. 2025; OpenAI 2025c).

201 Beispiele, bei denen diese Ausnahme in den USA durch die Regierung aufgehoben und Kontrollen eingeführt wurden, sind der Quellcode von Verschlüsselungsprogrammen und Dateien, die es Benutzer/innen ermöglichen, Schusswaffen über 3D-Druck herzustellen (Bloomfield 2024).

202 Open-Source-Modelle sind vollständig offen, das heißt der für Menschen lesbare, in Programmiersprache verfasste Text einer Software (der Quellcode), die Trainingsdaten und die Trainingsmethoden sind öffentlich zugänglich. Bei anderen Modellen werden nur diejenigen Parameter (Modellgewichte „weights“) offengelegt, die bestimmen, wie ein Modell Eingaben verarbeitet und Ausgaben erzeugt. Über diese kann ein Modell für spezielle Anwendungsfälle angepasst und oft können auch Sicherheitsvorkehrungen, z. B. hinsichtlich sensibler Anfragen bzw. Ausgaben entfernt werden (CFG 2025; Qi et al. 2024) (Kapitel 3.3.1, Kasten 3.5).

4.7.3 Die Sicherung der Schnittstelle zwischen KI-Modellen und physikalisch-biologischen Systemen

Biosecurity-Screening von Nukleinsäuresynthesen und deren Bestellern

Die Synthese von Nukleinsäuresequenzen (Kasten 3.6, Kapitel 3.3.2), die meist über kommerzielle Anbieter erfolgt, ist zu einem zentralen Schritt für die Herstellung von Genen und Genomen bzw. davon kodierten Proteinen geworden (Kapitel 2.1, 3.1). Sie ist auch zentral dafür, um über KI-Designmodelle generierte digitale Entwürfe für Gensequenzen bzw. Proteine in physikalisch-biologische Moleküle oder (veränderte) Organismen zu überführen (Kapitel 3.2.2). Dies macht die Nukleinsäuresynthese zu einer wichtigen – und in der Regulierungsdebatte bzw. in Leitlinien und Empfehlungen einzelner Länder, von KI-Entwicklern, der Gensyntheseindustrie und verschiedenen Non-Profit-Organisationen im Bereich der Biosecurity unstrittigen – Stelle der Überwachung, um das Risiko zu verringern, dass (insbesondere nicht staatliche) böswillige Akteure gefährliche biologische Agenzien wie Toxine oder bestimmte Viren erhalten bzw. herstellen könnten (Beal/Alexanian 2025; Carter et al. 2023, 2024a; Crawford et al. 2024; GOV.UK 2024; IGSC 2009, 2024; ISO 2024; NAS 2025b, 2025a; OSTP 2024; WHO 2022a; Zakaria et al. 2026).

Derzeit gibt es keine explizite gesetzliche Verpflichtung für Anbieter von Nukleinsäuresynthesen, die Bestellungen auf besorgniserregende Sequenzen (wie von Toxinen oder bestimmten Pathogenen) oder die Kunden der Bestellungen zu überprüfen. Allerdings ist dies in zahlreichen Ländern und der EU faktisch notwendig, wenn Bestellungen exportiert werden.²⁰³ Eine Reihe von Anbietern von Nukleinsäuresynthesen führt jedoch seit Langem grundsätzlich freiwillig Überprüfungen von Sequenzen und Kunden durch, und das International Gene Synthesis Consortium (IGSC), ein Zusammenschluss von Anbietern von Nukleinsäuresynthese, hat ab 2009 für seine Mitglieder bindende Standards und Praktiken für solche Überprüfungen festgelegt (Beal/Alexanian 2025; IGSC 2009, 2024; Kane/Parker 2024) (Kasten 3.6, Kapitel 3.3.2). Die Mitglieder repräsentieren nach Angaben des IGSC zusammen den größeren Teil der globalen kommerziellen Gensynthesekapazitäten. Laut dem „Global DNA Synthesis Map“ der IBBIS gibt es allerdings weltweit mindestens über ein Dutzend Unternehmen, die kein Screening durchführen, und für mehr als 600 Unternehmen ist unklar, ob sie dies tun.

Bislang haben Regulierungsbehörden, insbesondere in den USA (HHS 2010, 2023) und dem Vereinigten Königreich (GOV.UK 2024), versucht, die Anwendung der Überprüfung von Syntheseaufträgen vor allem durch nicht bindende Leitlinien zu fördern. 2024 haben die USA (infolge der Executive Order 14110 des damaligen Präsidenten Biden) mit dem „Framework for Nucleic Acid Synthesis Screening“ (OSTP 2024) (Kapitel 4.5 – USA) von Forschungsförderorganisationen verlangt sicherzustellen, dass synthetische Nukleinsäuren durch Fördernehmer/innen ausschließlich von Anbietern und Herstellern bezogen werden dürfen, die bestellte Sequenzen und Kunden überprüfen. Dieselben Anforderungen zur Sequenz- und Kundenüberprüfung wurden für Benchtop-Nukleinsäuresynthesegeräte formuliert (Sequenzüberprüfungen sollen dabei über eingebaute Scree-

²⁰³ Um die Exportkontrollbestimmungen für gelistete Nukleinsäuresequenzen (Kapitel 4.1.2, 4.2) in über 50 Ländern einzuhalten (Beal/Alexanian 2025; IGSC 2024), müssen Anbieter entsprechende Bestellungen erkennen, diese gegebenenfalls ablehnen und den Strafverfolgungsbehörden oder zuständigen Regierungsstellen melden. Wenn die Regulierungsbehörden feststellen, dass Anbieter gefährliche Nukleinsäuren ohne entsprechende Lizenzen an ausländische Unternehmen versenden, werden Strafen fällig (Beal/Alexanian 2025).

ningmechanismen erfolgen).²⁰⁴ Entsprechend müssen mögliche Anbieter über eine Erklärung die Einhaltung der Screeningpraktiken attestieren und Nukleinsäuresynthesen auf besorgniserregende Sequenzen („sequences of concern“)²⁰⁵ sowie die Legitimität der Besteller überprüfen. Als Anbieter gelten explizit auch Biofoundries, Cloud Labs oder Einrichtungen mit zentralen Nukleinsäuresyntheseeinrichtungen. Nach der Executive Order 14292 von Präsident Trump muss unter anderem auch das „Framework for Nucleic Acid Synthesis Screening“ neu bewertet und überarbeitet werden, was bisher nicht geschah (ASPR o. J.a), sodass dessen Umsetzung unsicher ist²⁰⁶ (Kroepke 2025; Kuiken 2025) (Kapitel 4.5 – USA). Anfang 2026 wurde der parteiübergreifende Biosecurity Modernization and Innovation Act (S. 3741)²⁰⁷ in den US-Senat eingebracht. Dieser würde unter anderem verbindliche bundesweite Vorschriften für Anbieter von DNA-Synthesedienstleistungen festlegen, wonach diese Bestellungen überprüfen und die Identität ihrer Kunden verifizieren müssen (Bergeson/Hutton 2026; Wachter 2026).

Ähnliche Maßnahmen wie die im „Framework for Nucleic Acid Synthesis Screening“ von 2024 und dem geplanten Biosecurity Modernization and Innovation Act in den USA sind im Vorschlag für einen European Biotech Act der EU-Kommission enthalten (EK 2025b) (Kapitel 4.2), z. B. die Einführung einer Pflicht zur Überprüfung der Legitimität von Bestellern besorgniserregender Nukleinsäuresequenzen (inklusive der Überprüfung des Identitätsnachweises) und die Pflicht, dass Benchtopsynthesegeräte Mechanismen zum Sequenzscreening enthalten müssen.

Schwächen bzw. Lücken in den derzeitigen Mechanismen oder Regelungen zur Überprüfung von Nukleinsäuresynthesen sowie Möglichkeiten, diese zu adressieren, werden insbesondere für folgende Punkte diskutiert:

- ein fehlender allgemein anerkannter und durchsetzbarer Screeningstandard, der sowohl von Regulierungsbehörden als auch von Anbietern unterstützt wird (Beal/Alexanian 2025). Dasselbe gilt für die Überprüfung der Legitimität von Kunden. Zur Entwicklung eines möglichen solchen Standards für das Sequenzscreening, einschließlich einer Datenbank für besorgniserregende Sequenzen und eines Mechanismus für deren Pflege, arbeiten verschiedene Gruppen aus Syntheseanbietern, Entwicklern von Screeningsoftware, politischen Entscheidungsträgern und wissenschaftlichen Expert/innen. Hierzu gehören die International Biosecurity and Biosafety Initiative for Science (IBBIS) (Kapitel 4.3) und das Sequence Biosecurity Risk Consortium (SBRC). Für das Kundenscreening wurde eine Reihe von Vorschlägen für Überprüfungspunkte bzw. Kriterien gemacht, darunter die Legitimitätsprüfung der Organisation eines Kunden, die Identitätsprüfung des Kunden und die Authentifizierung von erstellten Konten (Beal/Alexanian 2025; Crawford et al. 2024 und Referenz darin).
- Es gibt keinen Mechanismus, durch den Informationen über verdächtige Kunden oder Bestellungen zwischen Anbietern ausgetauscht werden können. Um diesen Punkt zu adressieren, werden die Einrichtung eines übergreifenden globalen Nachverfolgungsmechanismus oder

204 Gesetzliche Vorschriften bezüglich Biosecurity für solche Benchtop-Geräte existieren derzeit nur durch Exportkontrollen, z. B. in den USA über die Interactive Commerce Control List des Bureau of Industry and Security) (Kroepke 2025) und in der EU durch die Verordnung (EU) 2021/821 (Kapitel 4.2).

205 Zum Zeitpunkt der Veröffentlichung dieses Rahmenwerks sollten dies Sequenzen sein, die am besten mit Sequenzen von bundesweit regulierten, gelisteten Toxinen oder Erregern übereinstimmen (es sei denn, diese Sequenzen kommen auch in einem nicht regulierten Organismus oder Toxin vor). Ab dem 13. Oktober 2026 sollte diese Definition auch Sequenzen umfassen, die bekanntermaßen zur Pathogenität oder Toxizität beitragen, selbst wenn sie nicht von regulierten biologischen Agenzien stammen oder diese kodieren.

206 Die National Institutes of Health (Teil des US Department of Health and Human Services) gaben ihre Zustimmung zur Version des Frameworks von 2024 bekannt, während andere Organisationen wohl die Umsetzung bis zum Vorliegen neuer Informationen aussetzten (Kroepke 2025).

207 A bill to require the Secretary of Commerce to promulgate regulations to improve nucleic acid synthesis security, and for other purposes vom 29.1.2026

Datenbanksystems zur Erfassung bestimmter Informationen über Aufträge zur Nukleinsäuresynthese und Kundeninformationen diskutiert (Crawford et al. 2024; Edison et al. 2026), die unter anderem Hinweise auf mögliche Aufteilungen potenziell gefährlicher Sequenzen auf verschiedene Anbieter²⁰⁸ (Edison et al. 2026) oder das Auffinden zuvor abgelehnter Aufträge erlauben könnten.

- Ebenso gibt es keinen Mechanismus zur Bewertung der Konformität der Überprüfungssysteme der Anbieter mit Richtlinien oder Vorschriften bzw. um zu überprüfen, ob ein Anbieter tatsächlich wirksame Screeningverfahren anwendet. Hierzu werden insbesondere unabhängige Prüf-, Zertifizierungs- und Berichterstattungsorganisationen und/oder staatliche Regulierungsbehörden diskutiert (Beal/Alexanian 2025; Crawford et al. 2024). Dabei könnten auch die zuvor genannten Gruppen bzw. Organisationen, wie die IBBIS oder das SBRC, eine Rolle spielen (Beal/Alexanian 2025).
- Anbieter müssen Ressourcen in die Entwicklung und den Betrieb eines Screeningsystems investieren und *könnten Schwierigkeiten haben, gegenüber Anbietern, die kein Screening durchführen, kostengünstig zu bleiben* – und dadurch das Risiko eingehen, Kunden zu verlieren, die schnellere Bearbeitungszeiten und minimale Überprüfungen bevorzugen (Beal/Alexanian 2025; Kane/Parker 2024). Zu den diskutierten Möglichkeiten, um diese Herausforderung anzugehen, gehören verpflichtende Screeningverfahren für alle Anbieter und deren Durchsetzung bzw. Kontrolle sowie Anreize für DNA-Anbieter oder Auflagen, dass synthetische Nukleinsäuren mit öffentlichen Forschungsfördergeldern nur von zertifizierten, Screeningverfahren durchführenden Anbietern bezogen werden dürfen (Crawford et al. 2024 und Referenz darin).

Zwei jüngere Studien zu potenziellen wirtschaftlichen Auswirkungen im Vereinigten Königreich (Fady et al. 2025) und der EU (Zakaria et al. 2026) zeigen im Ergebnis, dass insbesondere die Einführung einer Pflicht zur Überprüfung von Sequenzen und Kunden – über alle Simulationen bzw. Szenarien hinweg und trotz erheblicher Unsicherheiten hinsichtlich der Wahrscheinlichkeit potenzieller biologischer Ereignisse²⁰⁹ – ein positives Kosten-Nutzen-Verhältnis hätte. Das heißt, die Kosten der Maßnahmen (etwa für die staatliche Durchsetzung, für Anbieter oder durch die mögliche Abwanderung von Anbietern in Länder ohne verpflichtende Überprüfungsverfahren) wären niedriger als der Nutzen, der sich vor allem aus der Minderung von Risiken ergeben würde.²¹⁰ Diese Risiken können beispielsweise durch Laborunfälle oder vorsätzliche Missbrauchshandlungen verursacht werden und Auswirkungen auf die menschliche Gesundheit und/oder die Wirtschafts- und Agrarproduktion haben.

208 Fragmente von Genen regulierter Erreger oder Toxine fallen in der Regel nicht (explizit) unter Regulierungen für gefährliche (gelistete) biologische Agenzien. Solche Fragmente können über verschiedene Anbieter verteilt bestellt werden (sodass kein einzelner Anbieter Einblick in das gesamte Genkonstrukt oder die beabsichtigte Funktion hat) und dann anschließend zu ganzen Genkonstrukten oder viralen Genomen zusammengesetzt werden.

209 Zu den betrachteten Szenarien gehören etwa potenzielle Ereignisse mit einem übertragbaren Erreger, die zu mehr als 100.000 Todesfällen führen (z. B. eine Pandemie); kleinräumige Ereignisse, verursacht durch nicht übertragbare biologische Agenzien wie Toxine (mit angenommen weniger als 20 Todesfällen, zuzüglich Dekontaminationskosten); oder Ereignisse, welche die Landwirtschaft beeinträchtigen, indem verschiedene Märkte im Pflanzen- und Tierbereich um 5 bis 30 % geschädigt würden (z. B. durch Agroterrorismus). Ereignisse mit weitreichenden Folgen (wie Pandemien) wurden als größtes Risiko betrachtet, gemessen an der Eintrittswahrscheinlichkeit multipliziert mit den Auswirkungen, und der größte Nutzen ergäbe sich aus der Verringerung dieses Risikos. Eine wichtige Grundlage für die angenommene Eintrittswahrscheinlichkeit für solche Ereignisse war eine Expertenbefragung (Williams et al. 2025), nach der bei den derzeitigen KI-Fähigkeiten in naher Zukunft eine jährliche Wahrscheinlichkeit von 1,5 % bestehen soll, dass ein biologisches Ereignis eintritt, das in etwa den Schaden der COVID-19-Pandemie verursacht.

210 So kommen Zakaria et al. (2026) zu dem Ergebnis, dass mit jedem Euro, der zur Implementierung bzw. aufgrund eines verpflichtenden Screeningsystems ausgegeben wird, die EU etwa 6 Euro an vermiedenen Verlusten gewinnen würde.

Zakaria et al (2026) diskutieren darüber hinaus, wie eine verpflichtende Überprüfung von Sequenzen und Kunden ausgehend von dem Entwurf zum European Biotech Act (Kapitel 4.2) EU-weit implementiert werden könnte, einschließlich der Arten von Um- und Durchsetzungsmechanismen und voraussichtlich betroffener bzw. verantwortlicher Akteure auf EU- und auf nationaler Ebene, darunter in Deutschland. Demnach könnten sich diese Mechanismen insbesondere an der Verordnung (EU) 2019/1148²¹¹ – in Deutschland umgesetzt durch das Ausgangsstoffgesetz²¹² – und an der Richtlinie (EU) 2024/1640²¹³ zur Bekämpfung der Geldwäsche orientieren (Zakaria et al. 2026, S. 14 ff.).

In der Debatte um das Screening von Nukleinsäuresynthesen und deren Bestellern wird jedoch sowohl von Forschenden aus dem KIxBio-Feld als auch von Biosecurity-Fachleuten darauf hingewiesen, dass die alleinige Analyse von Sequenzen zur Risikoreduktion möglicherweise nicht ausreicht. Zumindest gilt dies für die gegenwärtigen, auf Sequenzähnlichkeiten basierenden Verfahren (Kasten 3.6). Denn über KI-basierte Biodesignmodelle können Gensequenzen für Proteinstrukturen entworfen werden, die nur geringe oder gar keine Ähnlichkeit zu denjenigen von natürlichen Proteinen aufweisen (Kapitel 3.2.2). David Baker, der für seine grundlegenden Arbeiten zum computergestützten Proteindesign den Nobelpreis für Chemie im Jahr 2024 erhielt, und George Church, ein Pionier der Synthetischen Biologie, schlagen in diesem Zusammenhang vor, dass alle synthetisierten Sequenzen protokolliert werden sollen (gegebenenfalls verschlüsselt, um Geschäftsgeheimnisse zu schützen). Sollte dann irgendwo eine neue biologische Bedrohung auftreten, könnte diese über die DNA-Sequenzen zu ihrem Ursprung zurückverfolgt werden – wodurch potenzielle böswillige Akteure abgeschreckt werden könnten (Baker/Church 2024). Entsprechende Verfahren sollten standardisiert, international angewendet und auf Desktopsynthesizer ausgeweitet werden. Daneben wurde vorgeschlagen, zukünftig die Möglichkeiten für funktionsbasierte Screeningansätze zu untersuchen und zu nutzen, das heißt Verfahren, welche Sequenzen, die gefährliche biologische Funktionen wie Toxine kodieren können, unabhängig von der Ähnlichkeit zu bekannten besorgniserregenden Sequenzen erkennen können, z. B. basierend auf (KI-gestützten) Funktions- und Strukturvorhersagen (Abel et al. 2026 und Referenz darin).

Biosecurityüberprüfungen bei Biofoundries und Cloud Labs

Über Nukleinsäuresynthesen hinaus könnten zur Verwirklichung von digitalen Entwürfen möglicher funktionsfähiger, veränderter Moleküle oder Erreger (einschließlich deren Validierung oder Weiterentwicklung) die Nutzung automatisierter oder „autonom“ Laborplattformen („self-driving labs“) über Biofoundries und Cloud Labs (Kasten 2.4, Kapitel 2.3.3) zunehmend relevant werden (Lee et al. 2025) (Kapitel 3.2.2).

Bei den Recherchen für diesen Bericht konnten keine (öffentlich zugänglichen) Standards bzw. Dokumente zu von verschiedenen Biofoundries oder Cloud Labs genutzten Verfahren zur Überprüfung von Kunden, der von ihnen programmierten und automatisiert durchgeführten Experimente oder von gegebenenfalls zur Verfügung gestellten Materialien gefunden werden (Lee/Del

211 Verordnung (EU) 2019/1148 vom 20. Juni 2019 über die Vermarktung und Verwendung von Ausgangsstoffen für Explosivstoffe, zur Änderung der Verordnung (EG) Nr. 1907/2006 und zur Aufhebung der Verordnung (EU) Nr. 98/2013

212 Ausgangsstoffgesetz vom 3. Dezember 2020, zuletzt geändert am 9. Januar 2026

213 Richtlinie (EU) 2024/1640 vom 31. Mai 2024 über die von den Mitgliedstaaten einzurichtenden Mechanismen zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, zur Änderung der Richtlinie (EU) 2019/1937 und zur Änderung und Aufhebung der Richtlinie (EU) 2015/849

Castello 2024; NAS 2024). Allerdings würden für Nukleinsäuresynthesen, die in Biofoundries oder Cloud Labs durchgeführt werden, in den USA beispielsweise die Regeln zur Überprüfung von Sequenzen und Kunden des „Framework for Nucleic Acid Synthesis Screening“ von 2024 gelten. Darüber hinaus gelten Vorschriften der Exportkontrolle (Kapitel 4.7.1) und könnten für Betreiber der Einrichtungen hinsichtlich Produkten oder Ergebnissen, die an Kunden geliefert werden, relevant werden (Brockmann et al. 2025) und so deren Identifizierung bzw. Überprüfung faktisch notwendig machen.

Zu Empfehlungen verschiedener Organisationen für mögliche Überprüfungspraktiken und die Entwicklung von Standards gehören insbesondere (Alexanian 2023; Carter et al. 2023; Lee/Del Castello 2024; NAS 2024):

- Akteure aus Industrie und Wissenschaft zusammenbringen, um zu eruieren, welche Prozesse KI-gestützter automatisierter Labore besondere Risiken bergen, und um bewährte Verfahren zu einem geeigneten Risikomanagement auszutauschen;
- Überprüfungen der Legitimität von Kunden, hierzu könnten erprobte Verfahren aus dem Bereich der Nukleinsäuresynthese als Ausgangspunkt dienen und gegebenenfalls angepasst werden;
- Überprüfung automatisierter Protokolle auf mögliche besorgniserregende Dual-Use-(DURC) Zwecke;
- Identifizierung bzw. Überprüfung von Ausgangsmaterialien, die von Kunden eingehen (z. B. Nukleinsäuresequenzen, DNA-Konstrukte), sowie von Produkten und Ergebnissen von Experimenten bzw. Laborprozessen, die an Kunden geliefert werden.

4.7.4 Schutzmechanismen für KI-basierte biologische Modelle und die Kontrolle biologischer Daten

Die Überwachung der Nukleinsäuresynthese als zentraler Schritt von digitalen Modellen bzw. Entwürfen zu physischen, biologischen Molekülen oder Organismen gilt zwar als große Priorität und hochrelevant, um Biosecurity-Risiken zu reduzieren. Jedoch wird von Biosecurity-Expert/innen und Forschenden aus dem KIxBio-Feld auch argumentiert, dass es nicht ausreicht, sich auf diesen Schritt zu fokussieren (Bloomfield et al. 2024; Carter et al. 2024b; NAS 2018; Wang et al. 2025b). So dürfte eine flächendeckende, weltweit verpflichtende Kontrolle politisch kaum umsetzbar sein. Darüber hinaus könnten biologische KI-Designmodelle dazu beitragen, Sequenzscreeningmechanismen zu umgehen (Kapitel 3.2.2), und sehr kurze Nukleinsäuresequenzen (Oligonukleotide) die, wenn auch mit größerem Aufwand, ebenfalls zu viralen Genomen zusammensetzbar sind, könnten aus praktischen Gründen²¹⁴ nur schwer wirksam kontrollierbar sein.

²¹⁴ So nehmen unterhalb einer Länge von 30 Nukleotiden die falsch-positiven Ergebnisse deutlich zu, was eine erhebliche Belastung für die Anbieter darstellen würde (z. B. <https://aspr.hhs.gov/S3/Documents/2022-SynOligo-FRN-All-Responses-508.pdf>).

Schutzmechanismen („guardrails“) für biologische Designmodelle

Neben Evaluierungen von allgemeinen, generativen KI-Modellen vor deren Veröffentlichung (einschließlich der Durchführung von Red-Teaming-Übungen, Kapitel 3.3.1)²¹⁵ sollen angesichts dieser Herausforderungen Schutzmaßnahmen zur Risikominderung im Zusammenhang mit spezifischen biologischen KI-Designmodellen entwickelt und implementiert werden. Dabei geht es um Schutzmechanismen („safeguards“ oder „guardrails“), die in die Modelle selbst integriert bzw. mit diesen assoziiert sind (Carter et al. 2024b; NAS 2025b, 2025a; Wang et al. 2025b).

Zu möglichen in die Modelle selbst integrierten „guardrails“ gehören: Screeningmechanismen, die potenziell besorgniserregende bzw. risikoreiche Eingaben oder Ausgaben der Modelle automatisch erkennen und dann zur weiteren Überprüfung markieren oder ablehnen; die Erfassung und kryptografische Signatur von Metadaten, wie Instruktionen oder Eingaben für den Designprozess, die auf Absichten der Nutzer/innen schließen lassen könnten (und in die Bestellungen von Nukleinsäuresynthesen integriert werden müssen); oder der Ausschluss bestimmter Trainingsdaten, wie zu (bestimmten) Viren oder Toxinen aus den Trainingsdatensätzen, sodass Modelle keine gefährlichen Designs generieren könnten.²¹⁶

Zum anderen werden die Notwendigkeit und Mechanismen für den kontrollierten Zugang zu Modellen diskutiert (Carter/Butchello 2026; Webster et al. 2025). Die Nuclear Threat Initiative (NTI) schlug dazu kürzlich einen möglichen konkreteren Rahmen vor (Carter/Butchello 2026). Demnach würde der Zugriff auf biologische KI-Modelle und die notwendigen Legitimationskriterien für Nutzer/innen nach dem mit einem Modell verbundenen Risikopotenzial und dem Umfang des Zugriffs, den ein/e Benutzer/in möchte bzw. benötigt, gestaffelt werden. Mit zunehmendem Risikopotenzial eines Modells und Zugang zu umfangreicheren Modellfunktionen (bis hin zum Zugang zu Quellcode, zu Trainingsdaten oder „model weights“) müssten Nutzer/innen zunehmend strengere Legitimitätskriterien erfüllen, angefangen von lediglich einer E-Mail-Adresse, die mit einer Forschungsinstitution assoziiert ist, bis hin zur Dokumentation von Fördermitteln oder dem Nachweis institutioneller Unterstützung oder Aufsicht über Forschungsprojekte. Erfolgen soll eine solche Kontrolle über Application Programming Interfaces (APIs), die es erlauben, notwendige Informationen auszutauschen, während andere interne Systemdetails verborgen bleiben, sodass Entwickler die Kontrolle über das Modell behalten.²¹⁷

Ein wichtiger Diskussionspunkt hierbei ist die Balance mit bzw. der Erhalt von einem fairen und gleichberechtigten Zugang zu biologischen KI-Modellen, sodass etwa Forschende von kleineren Forschungseinrichtungen oder aus dem Globalen Süden nicht benachteiligt würden (Carter et al. 2024b; Carter/Butchello 2026; NAS 2025a). Der Nutzen solcher Modelle für die Wissenschaft und in der Folge für Anwendungsbereiche wie die Medizin, öffentliche Gesundheit und Biodefense hängt

215 Einige KI-entwickelnde Unternehmen wie OpenAI und Anthropic testen diese unter anderem auch auf ihre Fähigkeiten, dazu beitragen zu können, DNA-Synthesescreenings zu umgehen oder den Zusammenbau von Oligonukleotiden zu längeren Sequenzen zu erleichtern (erste Benchmarks zu agentischen Fähigkeiten Kapitel 3.3.1).

216 So haben beispielsweise die Entwickler der Evo-Genomdesignmodelle (Brixi et al. 2026; Nguyen et al. 2024) Genomsequenzen von Viren, die Zellen von Organismen wie Tieren (einschließlich des Menschen) oder Pflanzen infizieren, von den Trainingsdaten ausgeschlossen. Denselben Ansatz verfolgten die Entwickler des Proteindesignmodells ESM3(-open) (Hayes et al. 2025) hinsichtlich viraler Proteinsequenzen sowie weiterer Proteinsequenzen von auf gesetzlichen Kontrolllisten aufgeführten biologischen Agenzien (Black et al. 2025). Für Modelle, deren Modellgewichte („model weights“) veröffentlicht wurden, können solche Daten (z. B. Sequenzdaten von menschlichen Viren) aber wieder eingebracht werden (Black et al. 2025; Bloomfield et al. 2024; Wei et al. 2025; Workman 2024).

217 Über eine API stellt z. B. Google DeepMind eine Version von seinem Modell AlphaFold3 zur Proteinstrukturvorhersage (Kapitel 2.3.1) für alle Nutzer/innen bereit. Nicht kommerzielle Nutzer/innen wie aus dem akademischen Bereich können aber Zugriff auf die Modellgewichte – zentrale Parameter, die bestimmen, wie ein Modell Eingaben verarbeitet und Ausgaben erzeugt – erhalten und damit das Modell anpassen. Ähnliches gilt für das Proteindesignmodell ESM3 der Firma EvolutionaryScale (Kapitel 2.3.1), die jedoch nur eine kleinere Version des Modells frei für akademische Forschungszwecke zur Verfügung stellt (Carter/Butchello 2026, S. 5 und Referenz darin).

nicht zuletzt von den Zugangsmöglichkeiten und damit auch den Möglichkeiten zur Überprüfung und Weiterentwicklung der Modelle ab. Kritische Punkte für einen gleichberechtigten Zugang umfassen insbesondere Legitimitätskriterien und deren Nachweis, die Nutzer/innen von etablierten oder gut ausgestatteten Institutionen bevorteilen könnten (Carter/Butchello 2026), z. B. wenn für den Zugang vorab abgeschlossene Vereinbarungen zwischen Forschungseinrichtungen und Modellbetreibern notwendig wären oder Beurteilungen von Projekten von institutionellen Begutachtungsgremien notwendig sind, die an kleineren Instituten evtl. nicht vorhanden sind.

Zugangsbeschränkungen zu bestimmten biologischen Daten

Die Idee hinter diesem Ansatz ist, dass die Beschränkung des öffentlichen Zugangs zu bestimmten neu erstellten (und noch nicht verbreiteten) Datensätzen das Risiko verringern kann, dass neue in Bezug auf Missbrauchsmöglichkeiten besonders besorgniserregende KI-Modellfähigkeiten entwickelt werden können (Berke et al. 2025; Bloomfield et al. 2026).²¹⁸

Bloomfield et al. (2026) schlugen dazu ein Rahmenwerk vor, nach dem Daten in fünf verschiedene Sicherheitsstufen („biosecurity data levels“) eingeteilt werden sollen, entsprechend ihrer voraussichtlichen Fähigkeit, die Entwicklung von biologischen KI-Modellen für relevante Vorhersagen oder Entwürfe zu ermöglichen. Je höher die Anfälligkeit für Missbrauch und je geringer der Nutzen wäre, desto höher wäre die Sicherheitsstufe für entsprechende Daten. Mit steigender Sicherheitsstufe würden zusätzliche Anforderungen erforderlich, bevor der Zugriff auf Daten gestattet wird, wie z. B. die Registrierung eines Kontos, die Identifizierung des/der Benutzers/in, die Genehmigung der Datennutzung (z. B. durch eine Forschungsinstitution), bis hin zu einer obligatorischen Sicherheitsüberprüfung von Modellen, die mit den abgerufenen Daten trainiert wurden. In den beiden höchsten Sicherheitsstufen könnten laut Bloomfield et al. (2026) Daten einzuordnen sein, die einen erheblichen Missbrauch ermöglichen könnten, wie insbesondere die Fähigkeit, Viren zu entwickeln, die eine Pandemie auslösen können. Für solche Daten soll sichergestellt werden, dass (autorisierte) Forschende diese zu Studien nutzen können, ohne aber direkt auf die Rohdaten zuzugreifen.²¹⁹ Darüber hinaus sollen die für die Datenbereitstellung zuständigen Institutionen bzw. Regierungen eine Biosecurity-Prüfung für Modelle durchführen, die mit solchen Daten trainiert wurden, bevor sie diese an Forschende weitergeben. Einzurichtende Expertengremien sollen detailliertere und regelmäßig aktualisierte Definitionen der Arten von Daten erstellen, die Zugangsbeschränkungen unterliegen und gegebenenfalls Ausnahmen vorsehen, wie beispielsweise die Aufhebung von Beschränkungen für relevante Daten während eines Krankheitsausbruchs.

Ähnlich wie bei der (Zugangs-)Kontrolle von biologischen KI-Modellen sind auch hier mögliche negative Effekte hinsichtlich eines gleichberechtigten Zugangs sowie auf den offenen akademischen Austausch und die biomedizinische Forschung ein wichtiger Diskussionspunkt. Entsprechend sollen die vorgeschlagenen Kontrollmaßnahmen nur für einen möglichst begrenzten Be-

²¹⁸ So deuten verschiedene Studien darauf hin, dass solche Modellfähigkeiten, wie zur Vorhersage viraler Genomsequenzen oder Proteinen hinsichtlich ihrer Funktionen im Zusammenhang mit Virulenz und Immunflucht, von der Präsenz von Daten zu viralen Gensequenzen und Proteinen abhängen können, die ursprünglich aus Trainingsdaten entfernt wurden (Black et al. 2025; Wei et al. 2025).

²¹⁹ Hierzu sollen vertrauenswürdige Forschungsumgebungen („trusted research environment“ – TRE) genutzt werden, wie sie etwa für den Zugang zu und die Analyse von sensiblen Genom- und Gesundheitsdaten in der biomedizinischen Forschung existieren. Grundlage ist eine sichere Computerumgebung, die entwickelt wurde, um berechtigten Personen einen sicheren Fernzugriff auf sensible Daten zu ermöglichen und gleichzeitig die Vertraulichkeit dieser Daten zu gewährleisten, in dem die Daten bearbeitet und analysiert werden können, ohne dass diese selbst die Umgebung verlassen. Forschende können nur ihre aggregierten, und gegebenenfalls von den Betreibern kontrollierten, Analyseergebnisse (z. B. Ergebnistabellen oder Grafiken) extrahieren und herunterladen, aber die Daten einzelner Patient/innen und andere vertrauliche Informationen verbleiben stets im TRE (Kavianpour et al. 2022; Nab et al. 2024).

reich von Pathogendaten gelten. Regierungen sollen rigoros prüfen, inwieweit geschützte Daten über Krankheitserreger einen Missbrauch ermöglichen, und die Zugangskontrollen gegebenenfalls wieder lockern, wenn dies verantwortungsvoll erscheint. Zudem sollen Sicherheitseinstufungen von Daten vor Schiedsstellen anfechtbar sein (Bloomfield et al. 2026).

4.7.5 Nutzung von KI-Modellen zur Verbesserung der Pandemievorsorge und biologischer Verteidigungsfähigkeiten

Viele Expert/innen sind der Ansicht, dass nicht zuletzt die Stärkung der Pandemievorsorge – einschließlich der Erkennung und Überwachung von Erregern sowie der Weiterentwicklung von medizinischen Präventions- und Gegenmaßnahmen (Kapitel 2.3.2, 2.3.3) – wichtig sein wird, um künftige Biosecurity-Risiken zu reduzieren. Dazu gehören auch solche, die durch den Missbrauch von KI-Modellen entstehen könnten (Carter et al. 2023; NAS 2025b). Hierfür werden auch die verstärkte Erforschung und Nutzung von KI-gestützten Modellen und biotechnologischen Verfahren diskutiert, insbesondere in den beiden folgenden Bereichen (NAS 2025b, S. 34 ff. und Referenz darin):

- *KI-gestützte Überwachung von Infektionskrankheiten:* Hierzu gehören Modelle zur Sprachanalyse globaler Kommunikationsquellen und Algorithmen, die pathologische und epidemiologische Merkmale eines Ausbruchs nutzen, um Hinweise auf potenzielle Erreger zu geben oder zur Analyse komplexer Übertragungsmuster beizutragen. Ebenfalls hierher gehören KI-Modelle, um Genomdaten aus verschiedenen Quellen schnell bzw. in Echtzeit zu analysieren, um bekannte Krankheitserreger oder ungewöhnliche Muster zu identifizieren, die auf neue zirkulierende Erreger hindeuten. Solche Modelle können auch Genomdaten mit epidemiologischen Informationen integrieren, um Ausbruchsmuster vorherzusagen und Maßnahmen des öffentlichen Gesundheitswesens nahezu in Echtzeit zu unterstützen.
- *KI-gestütztes Biodesign für die Entwicklung von Gegenmaßnahmen und Notfallreaktion:* Hierzu gehört insbesondere die Nutzung von KI-Designmodellen zur Entwicklung von Impfstoffen, Therapeutika oder diagnostischen Verfahren (Kapitel 2.3.2)



5 Resümee und Handlungsoptionen

5.1 Resümee

5.2 Handlungsoptionen

5 Resümee und Handlungsoptionen

5.1 Resümee

Die Fortschritte in der Molekularbiologie der letzten 15 bis 20 Jahre haben es zunehmend möglich gemacht, das Erbgut von Organismen umfassend zu analysieren und biologische Moleküle sowie Eigenschaften verschiedener Zellen oder Organismen gezielt umzugestalten. Diese Möglichkeiten erlauben unter anderem ein besseres Verständnis der Funktion von Genen bzw. Proteinen und von Krankheitsursachen, die Generierung neuer Proteine oder ganzer Stoffwechselwege in Mikroorganismen für die industrielle Biotechnologie sowie die Herstellung neuer Impfstoffe und Medikamente, einschließlich Gentherapien für schwere Erbkrankheiten oder menschlicher Design-Immunitätszellen (CAR-T-Zellen) für die Krebstherapie (Kapitel 2.3). Zu diesen Fortschritten haben zum einen neue DNA-Sequenzierverfahren und computergestützte Analysemethoden zur Entschlüsselung des Erbguts, einfache und vielseitig einsetzbare Methoden für quasi beliebige Veränderung von Genen bzw. Genomen in Zellen sowie die Möglichkeit zur Synthese von (größeren) Gen- bzw. Genomsequenzen beigetragen. Zum anderen konnten, ermöglicht durch große Bestände unterschiedlicher biologischer Daten, zunehmend leistungsfähigere KI-basierte Modelle zur Vorhersage und dem Design von Molekülstrukturen und -funktionen, einschließlich von Proteinen, entwickelt werden (Kapitel 2.1, 2.2).

Diese Entwicklungen und insbesondere die damit seit Anfang der 2000er Jahre verbundene Vision der Synthetischen Biologie (oder „engineering biology“) – wonach biologische Moleküle, Funktionen und Organismen nach ingenieurwissenschaftlichen Prinzipien vorhersagbar und zunehmend einfacher um- bzw. neu gestaltet werden sollen – waren von Anfang an sowohl mit Hoffnungen in Bezug auf Innovationen und Innovationskultur als auch mit Bedenken und Diskussionen um Fragen der Biosicherheit, einschließlich Biosecurity-Risiken, verbunden. Bei Letzteren stand neben der Möglichkeit, gefährlichere oder neuartige Krankheitserreger entwickeln zu können, insbesondere die Besorgnis im Mittelpunkt, dass auch Nichtexpert/innen biologische Agentien, wie Toxine oder bestimmte Viren, einschließlich solcher mit Massenvernichtungspotenzial, herstellen und als biologische Waffen missbrauchen könnten. Insbesondere die mit der Vision der Synthetischen Biologie verbundenen Hoffnungen und Befürchtungen, dass komplexere gen- oder biotechnologische Projekte auch für Personen ohne entsprechende Fachkenntnisse und Laborerfahrung durchführbar werden, wurden jedoch – zumindest bisher – nur sehr begrenzt bzw. höchstens mit fachlicher Unterstützung Realität (Kapitel 3.1).

Mit der Entwicklung von zunehmend leistungsfähigen großen Sprachmodellen, die auch den Zugang zu biologischem und potenziell sensitivem (Fach-)Wissen ermöglichen können, sowie von biologischen KI-Modellen für die Analyse und das Design biologischer Moleküle und Prozesse, hat sich eine neue Debatte um die von der Synthetischen Biologie bekannten Biosicherheitsfragen entwickelt. Neben den Befürchtungen, dass die Hürden für die Herstellung gefährlicher biologischer Agentien bzw. Biowaffen durch die neuen KI-Möglichkeiten entscheidend gesenkt werden könnten und auch die Generierung gefährlicherer oder neuartiger biologischer Agentien möglich wird, steht das potenzielle Risiko im Mittelpunkt, dass die Wirksamkeit von Biosicherheits- und Abwehr-bzw. Biodefense-Maßnahmen verringert oder unterlaufen werden könnte.

Diese Befürchtungen beruhen im Wesentlichen auf drei Entwicklungen bei KI-Modellen und den damit verbundenen Möglichkeiten in der molekularbiologischen Forschung bzw. der Biotechnologie (KlxBio) (Kapitel 3.3): erstens der möglichen Wissensaneignung oder -erweiterung über große Sprachmodelle (LLM-Chatbots), zweitens der Möglichkeit zum Design veränderter oder neuer Toxine und Krankheitserreger mithilfe biologischer KI-Modelle, die unter anderem das Sicherheitsscreening bei Nukleinsäuresynthesen und Detektionsverfahren für Toxine und Erreger unterlaufen könnten, und drittens der Kombination von KI-Modellen mit robotisierten Laborplattformen, um Experimente bzw. Entwicklungszyklen und Herstellungsprozesse automatisiert oder gar komplett autonom durchführen zu können.

Ergebnisse empirischer Studien lassen die Frage offen, inwieweit LLMs Personen bei der Herstellung von Biowaffen in der Praxis tatsächlich effektiver unterstützen können als bisherige Internetwerkzeuge

Verschiedene Akteure (z. B. aus akademischen Forschungsinstituten, Non-Profit-Organisationen oder KI-entwickelnden Firmen) haben in einer Reihe von empirischen Studien bzw. Evaluationen von KI-Modellen untersucht, inwieweit große Sprachmodelle für die Herstellung von Biowaffen relevantes Wissen, einschließlich nicht ohne Weiteres zugängliches oder praxisrelevantes (Erfahrungs-)Wissen, für verschiedene Personengruppen verfügbar machen oder erweitern könnten.

Zwar legen (meist automatisierte) Tests zur Ermittlung von Leistungskennzahlen zum Wissensstand bzw. den Fähigkeiten eines Modells (Benchmarks) nahe, dass verschiedene LLMs Referenzwerte menschlicher Expert/innen erreichen und teilweise übertreffen. Inwieweit diese Tests jedoch die Möglichkeit abbilden, tatsächlich praxisrelevantes (Erfahrungs-)Wissen zur Herstellung und Nutzung von Biowaffen zu erlangen, bleibt aber unklar (Kapitel 3.3.1). Ergebnisse bisheriger Uplift- und Red-Teaming-Studien mit Personen, um herauszufinden, inwieweit LLMs (über konventionelle Internetsuchen hinaus) bei der Planung eines Angriffs und der Herstellung von Biowaffen helfen sowie Kenntnisse bzw. Fähigkeiten der Personen verbessern können, zeigen kein einheitliches Bild und sind kaum unabhängig überprüfbar²²⁰. Während verschiedene größere Studien keine statistisch signifikanten Leistungsverbesserungen von Anfängern oder Expert/innen durch den Zugang zu LLMs zeigten, legt eine jüngere größere Uplift-Studie nahe, dass die koordinierte Nutzung mehrerer LLMs die Leistungen von Studierenden mit keiner oder wenig Biologieerfahrung bei der Lösung verschiedener, aus Benchmarks stammender Fragen und Aufgaben zu biologischem Wissen oder Techniken deutlich verbessern kann, teilweise auf oder über das Niveau von Expert/innen hinaus (Kapitel 3.3.1).

Doch selbst wenn Unsicherheiten bezüglich der Praxisrelevanz von Benchmarks ausgeräumt und Uplift- oder Red-Teaming-Studien zu unterschiedlichen Fragen und Aufgaben einheitliche, statistisch signifikante Verbesserungen zeigen würden, bliebe die Bedeutung solcher Ergebnisse für die praktische Umsetzung (die praktische Signifikanz) des gewonnenen Wissens und der entwickelten Pläne in der realen Welt unklar. Entscheidend dafür wären Auswirkungen auf die verschiedenen Hürden für die Biowaffenherstellung, einschließlich notwendiger praktischer Fähigkeiten bzw. Erfahrungen in Bezug auf Laborarbeiten zur Herstellung von relevanten biologischen Agen-

²²⁰ Hierzu trägt insbesondere bei, dass die in den Untersuchungen an Personen gestellten Aufgaben, Originaldaten bzw. einzelne Ergebnisse und die Expertise der bewertenden Expert/innen (meist mit Verweis auf mögliche Sicherheitsrisiken) oft nicht oder nur unzureichend offengelegt werden.

zien und gegebenenfalls biowaffenrelevanten Prozessen, wie deren Formulierung oder Modifikation (Kapitel 3.2.2).

Größere kontrollierte Studien mit Testpersonen in realen biologischen Laboren könnten belastbare Rückschlüsse auf mögliche Risiken zulassen. Dies hängt jedoch davon ab, wie konkret oder relevant die biologischen Aufgaben (aufgrund von Sicherheitsfragen bzw. -vorschriften) hinsichtlich potenzieller Biowaffen gestaltet werden können. Eine erste größere solche Studie legt es nahe, dass LLMs derzeit Personen ohne wesentliche Laborerfahrung bei der erfolgreichen Durchführung einiger grundlegender, in der Virologie und Molekularbiologie erforderlicher molekularbiologischer Aufgaben nicht besser unterstützen können als konventionelle Internetanwendungen. Ob bzw. inwiefern die zusätzliche Nutzung bestimmter biologiespezifischer KI-Modelle dies ändern könnte oder ob die Nutzung von LLMs bei Personengruppen, die bereits relevante Kenntnisse in den Lebenswissenschaften und Laborerfahrung haben (z. B. auf Graduierten- oder Doktorandenniveau), zu größeren bzw. besorgniserregenderen Leistungssteigerungen führen könnte, bleibt offen und dürfte weitere Studien dieser Art erfordern (Kapitel 3.3.1).

Proteindesignmodelle könnten die unerkannte Herstellung von Gensequenzen mit Missbrauchspotenzial erlauben

KI-unterstützte Proteindesignmodelle haben in einer Reihe von Fällen die gezielte Neu- oder Umgestaltung (Design bzw. Redesign) von komplexen Proteinstrukturen mit unterschiedlichen Funktionen ermöglicht (Kapitel 2.3, 2.5). Somit könnten prinzipiell auch (Protein-)Toxine mit neuen, gefährlicheren Eigenschaften erzeugt werden. Die Funktionalität solcher neuartiger Proteine dürfte aber auf absehbare Zeit in ressourcen- und zeitaufwendigen Laborexperimenten überprüft und gegebenenfalls über iterative Entwicklungszyklen (DBTL-Zyklen; Kapitel 2.3.4) optimiert werden müssen (Kapitel 3.3.2). Darüber hinaus müsste die Entwicklung neuer Toxine auch Tests in Zell- oder Gewebekulturen und in Versuchstieren umfassen.

Bereits gezeigt wurde, dass bekannte Proteine unter mutmaßlichem Erhalt ihrer Funktion mit aktuellen Proteindesignmodellen so umgestaltet werden können, dass sie aufgrund größerer Unterschiede zur „Originalversion“ in der Aminosäure- und damit auch der Gensequenz standardmäßige Überprüfungen von Nukleinsäuresynthesen umgehen können. Wie groß die Gefahr tatsächlich ist, dass so umgestaltete Versionen bekannter Proteine bzw. einschlägiger Biowaffentoxine, deren Aktivität multiple Funktionalitäten, darunter Enzymaktivität, erfordert, tatsächlich funktionell bleiben, ist derzeit aber unklar. Experimentelle Daten legen nahe, dass zumindest über derzeitige Open-Source-Modelle entworfene solche Proteinversionen, insbesondere von größeren Proteinen und/oder von funktionell unterschiedlich komplexen Enzymen, ihre Funktion verlieren (Kapitel 3.2.2).

Eine gezielte Verbesserung komplexer Eigenschaften von Krankheitserregern ist fraglich – das Design komplett neuer Erreger scheint (zumindest derzeit) außerhalb der Reichweite von KI-Modellen

Ob über KI-Modelle komplexe Eigenschaften von Krankheitserregern (wie etwa die Übertragbarkeit, die Fähigkeit, sich in Wirtszellen effizient zu vermehren, oder die Umgehung von Immunreaktionen des Wirts) tatsächlich in vorhersagbarer Weise veränderbar sind und für die Nutzung als Biowaffe „verbessert“ werden können, ist nicht geklärt. Es gibt zwar Arbeiten mit verschiedenen biologischen KI-Modellen zu Viren, die zeigen, dass Vorhersagen zu kurzzeitigen Auswirkungen von Mutationen in Gensequenzen von etwa SARS-CoV-2 oder Influenza-Viren auf die Infektiosität oder die Umgehung bestimmter Immunreaktionen möglich sind. Längerfristige Auswirkungen von Mutationen bzw. die Virus-Evolution über mehrere Infektionszyklen bzw. Viren-Generationen hinweg zu modellieren bzw. vorherzusagen, wie es für eine effektive „Verbesserung“ notwendig wäre, dürften allerdings auch zukünftig eher begrenzt sein. Gründe hierfür sind neben mangelnden Daten – wie zur Interaktion von Mutationen mit dem genetischen Hintergrund des Wirts – auch sprunghafte evolutionäre Ereignisse mit komplexen genetischen Veränderungen, etwa durch Rekombinationsereignisse oder persistente Infektionen. Diese sind kaum vorhersagbar und werden es wohl auch zukünftig nicht werden (Kapitel 3.3.2).

Für die Entwicklung biologischer KI-Modelle zur Konstruktion von Grund auf neuer Krankheitserreger (selbst, wenn diese vergleichsweise wenig komplex sind wie Viren) sind bislang fehlende umfangreiche und hochwertige Datensätze zu genomischen Sequenzen und davon bestimmter molekularer und physiologischer Eigenschaften in noch grundlegenderem Maß begrenzend. Solche völlig neuen Erreger könnten die potenziell weitreichendsten Folgen in Bezug auf biologische Bedrohungen haben, da Möglichkeiten zu ihrer Bekämpfung aufgrund fehlender Informationen eingeschränkt wären bzw. die Entwicklung von Maßnahmen längere Zeit in Anspruch nehmen könnte (Kapitel 3.3.2).

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

Die Verwirklichung jeglicher Entwürfe für potenzielle um- oder neugestaltete biologische Agenzien, wie Toxine oder Viren, erfordert die Herstellung und – zumindest derzeit – die experimentelle Validierung der Agenzien im Labor. Gegebenenfalls sind auch wiederholte Entwicklungszyklen zur Optimierung der Entwürfe notwendig. Hinsichtlich dieser zentralen Herausforderung hat die mögliche Nutzung kommerzieller automatisierter Laborplattformen wie Cloud Labs sowie die Kombination von KI-Systemen mit solchen Laborplattformen zu ersten autonomen („self-driving“) Laborsystemen für Design- und Entwicklungszyklen (z. B. für Enzyme) Biosecurity-Fragen aufgeworfen. Nämlich danach, ob oder inwieweit solche Einrichtungen oder Systeme böswillige Akteure in relevantem Umfang unterstützen könnten, denen praktische Fähigkeiten und Laborausstattung zur Herstellung, zur Validierung oder zur Durchführung iterativer Entwicklungszyklen fehlen.

Cloud Labs und ähnliche Einrichtungen (Kapitel 2.3.4) können bereits heute die Notwendigkeit aufheben, (zumindest manche) praktische Laborarbeiten zur Herstellung biologischer Agenzien

selbst durchführen zu müssen. Für den effektiven Einsatz solcher Labore ist aber noch spezifisches Wissen zu den verwendeten Agenzien und methodischen Verfahren sowie zu Cloud-Lab-Abläufen selbst notwendig. Es ist allerdings nicht auszuschließen, dass diese Anforderungen, beispielsweise durch eine über KI-Systeme erleichterte Planung bzw. Programmierung von Experimenten und/oder zuverlässigere Automatisierungssysteme, abnehmen könnten (Kapitel 3.3.3). Ob Cloud-Lab-Betreiber die Kunden und/oder deren Experimente einschließlich der ein- und ausgehenden Materialien überprüfen, ähnlich wie es eine Reihe von Anbietern von Nukleinsäuresynthese bei Bestellungen praktiziert, ist unklar.

Würden autonome Laborsysteme für die Herstellung bzw. Veränderung relevanter biologischer Agenzien, wie bestimmter Toxine oder Viren, zur Verfügung stehen und wären diese (unkontrolliert) zugänglich, könnte dies die Hürden für die Herstellung bzw. Entwicklung solcher Agenzien auch für Akteure ohne biologische Fachkenntnisse oder größere Ressourcen stark senken. Besonders besorgniserregend wären entsprechende Systeme, wenn sie etwa über sprachgesteuerte Benutzeroberflächen auch von Personen ohne spezielle (Programmier-)Kenntnisse nutzbar wären, wie bei mindestens einem publizierten System für die Veränderung von Enzymen beschrieben (Singh et al. 2025) (Kapitel 3.3.3). Die Entwicklung autonomer Laborsysteme ist jedoch kosten- und forschungsintensiv. Der spezifische Zuschnitt auf die jeweiligen Proteine oder unterschiedlichen Organismen erfordert zusätzlich zu spezifischen Kenntnissen über die zu verändernden biologischen Systeme erhebliche Fachkenntnisse im Bereich der Robotik sowie der Soft- und Hardwareintegration (Kapitel 3.3.3). Somit dürfte die Entwicklung solcher Systeme zur Herstellung gefährlicher biologischer Agenzien zumindest derzeit primär eine Möglichkeit für staatliche Akteure oder staatlich unterstützte Gruppen sein.

Implikationen für Bedrohungen durch Biowaffen und Ausblick

Eine Einordnung der mit KI verbundenen Möglichkeiten in der Molekularbiologie und Biotechnologie hinsichtlich potenzieller Bedrohungen durch den Missbrauch biologischer Agenzien bzw. Biowaffen erfordert letztlich eine umfassendere Betrachtung, die über mögliche KI-Fähigkeiten hinausgeht (Kapitel 3.4).

Hierzu gehören Fähigkeiten und Bedingungen der Herstellung und Nutzung von Biowaffen, wie die groß angelegte Produktion von biologischen Agenzien oder waffentechnisch aufwendigen Ausbringungsmethoden (etwa durch Raketen- oder Lenkwaffen), die weitgehend unabhängig von den neuen KI-basierten Möglichkeiten sind. Bedrohungen durch Biowaffensysteme, die solche Prozesse erfordern, dürften deshalb auch weiterhin vor allem von Staaten (oder von durch diese unterstützten Gruppen) bzw. staatlichen Biowaffenprogrammen ausgehen. Die neuen KI-assoziierten Möglichkeiten scheinen für staatliche Programme nicht zwingend erforderlich, dennoch könnten sie einzelne Forschungs-, Entwicklungs- und Optimierungsschritte beschleunigen.

Für staatliche Akteure erscheinen insbesondere kleinflächigere taktische Einsätze oder verdeckte bzw. hybride Operationen denkbar, um andere Staaten und Regierungen zu destabilisieren. Selbst wenn die Urhebererschaft nachgewiesen werden könnte, wäre die Wahrscheinlichkeit wohl groß, dass insbesondere gegenüber Wirtschaftssanktionen resiliente und über Nuklearwaffen verfügende Staaten (oder verbündete Staaten bzw. Gruppen) bei solchen Biowaffen-Einsätzen keine untragbaren Konsequenzen zu erwarten hätten (Kapitel 4.7.1).

Die Herstellung biologischer Agenzien in großem Maßstab und komplexe Verwaffnungs- bzw. Ausbringungsmechanismen sind jedoch nicht in jedem Fall notwendig. So könnten kleinere Mengen mancher Agenzien für biologische Bedrohungen ausreichen und über einfachere, weniger technisch aufwendige Prozesse verbreitet werden – wie es in den bisher wenigen Fällen erfolgreicher Bioterroranschläge durch nicht staatliche Akteure der Fall war. Solche Strategien, die einfachere und technisch weniger komplexe Prozesse involvieren, könnten auch zukünftig bei Bioterrorbedrohungen durch nicht staatliche Akteure am wahrscheinlichsten sein, da sie nicht die zuvor genannten (und von KlxBio-Entwicklungen weitgehend unabhängigen) technischen Voraussetzungen für die Massenproduktion biologischer Agenzien oder aufwendiger Verbreitungsmechanismen erfordern. Der Zugang zu bzw. die kleinskalige Herstellung von Krankheitserregern oder Toxinen und damit die KlxBio-Möglichkeiten – wie das Erlangen von Wissen über die Isolation oder Herstellung solcher Agenzien oder die Umgestaltung von Gensequenzen für die Agenzien, um Nukleinsäuresynthescreensings zu umgehen – könnten bei solchen Bedrohungen somit eine wichtige Rolle spielen.

Diese Bedrohungen müssen aber nicht notwendigerweise (wie bisher) mit eher kleinen Zahlen von Todesfällen oder moderaten Zahlen von Erkrankten verbunden sein. Größere Opferzahlen und disruptive ökonomische und gesellschaftliche Auswirkungen könnten beispielsweise drohen, wenn potenziell pandemieauslösende Viren hergestellt werden könnten und nach absichtlicher Selbstinfektion von Täter/innen („patient zero“) auf andere übertragen würden. Solche Viren könnten derzeit aufgrund der begrenzten Möglichkeiten zur gezielten und vorhersagbaren Verbesserung viraler Eigenschaften oder gar zum (De-novo-)Design gänzlich neuer Viren (Kapitel 3.3.2) am ehesten bekannte, natürlich vorkommende Viren sein, die etwa über synthetische Genomsequenzen hergestellt wurden, oder Versionen solcher Viren, die zusätzlich über Mutations- und Selektionsprozesse verändert wurden (z. B. in menschlichen Zellen oder Tiermodellen). Die erforderlichen Fähigkeiten und notwendigen Vorerfahrungen können je nach Virus unterschiedlich sein; effektive entsprechende Veränderungen würden aber zusätzliche Erfahrung und Fähigkeiten, etwa im Umgang mit geeigneten Testsystemen oder Tiermodellen, erfordern (Kapitel 3.3.1).

Zwar ist es nicht auszuschließen, dass sich manche Personen ohne oder mit nur sehr begrenzter biologischer Ausbildung all die notwendigen Fähigkeiten und Erfahrungen aneignen könnten – potenziell mit Unterstützung von fortgeschrittenen LLMs. Die Wahrscheinlichkeit hierfür sowie insbesondere die Wahrscheinlichkeit, dass diese Fähigkeiten erfolgreich für ein komplexeres Gesamtprojekt, wie die Herstellung und gegebenenfalls die Veränderung und Testung potenziell relevanter pandemischer Viren, genutzt werden könnten, dürfte aber nach wie vor relativ klein sein (Kapitel 3.3.1). Auch die Möglichkeiten, automatisierte Laborplattformen zu nutzen oder durch Kombination mit solchen Modellen realisierbare autonome Laborsysteme zu entwickeln, dürften aufgrund der damit verbundenen Herausforderungen (Kapitel 3.3.3) für solche Akteure derzeit sehr begrenzt sein.

Inwiefern sich dies in absehbarer Zukunft ändern könnte, ist letztlich nicht verlässlich abzuschätzen und macht ein kontinuierliches Monitoring der KlxBio-Entwicklungen erforderlich. Aufgrund der vorhandenen Unsicherheiten im Allgemeinen (Kapitel 3.3., 3.4) sowie möglicher Black-Swan-artiger Bedrohungen – das heißt durch Ereignisse mit sehr geringer Eintrittswahrscheinlichkeit, die aber extreme Effekte haben können (Aven 2015 und Referenz darin; Taleb 2007), wie etwa die Herstellung pandemischer Viren durch Akteure ohne oder mit nur wenig Fachkenntnissen und

praktischer Erfahrung – sollten bereits heute weitere vorsorgende Maßnahmen zum Umgang mit Unsicherheiten und zur Risikominimierung bzw. zur Verbesserung der Resilienz gegenüber möglichen Folgen in Betracht gezogen werden.

5.2 Handlungsoptionen

Für Politik, Wissenschaft und Gesellschaft stellt sich die Frage, durch welche Maßnahmen sich die aktuellen Unsicherheiten adressieren und Risiken, die von einem potenziellen Missbrauch gefährlicher biologischer Agenzien bzw. Biowaffen unter Einsatz fortgeschrittener KI-Modelle ausgehen können, minimieren lassen. Die Ergebnisse der vorliegenden Analyse legen es nahe, dass über KIxBio-zentrierte Maßnahmen hinaus weitere Ansätze auf unterschiedlichen Ebenen erforderlich sind. Unter Berücksichtigung der internationalen Regulierungsdebatte lassen sich vier Hauptansatzpunkte erkennen:

- die Absicherung des Übergangs von digitalen Entwürfen zu realen biologischen Molekülen oder Organismen, bei dem der Nukleinsäuresynthese eine zentrale Rolle zukommt,
- die umfassende Beobachtung von und Zugangskontrolle zu KI-Systemen mit gesteigerten Möglichkeiten des Designs gefährlicher biologischer Agenzien und neuer Herstellungswege und -protokolle dafür, einschließlich der Nutzung automatisierter Laborsysteme,
- eine substanzielle Stärkung der BWC sowie
- der grundlegende Ausbau der Fähigkeit zur Durchführung von Gegenmaßnahmen, also die Förderung von Biodefense-Kapazitäten.

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

Ein zentraler Ansatzpunkt ist die Unterstützung des geplanten European Biotech Act (Kapitel 4.2), um eine verpflichtende und EU-weit harmonisierte Sicherheitsüberprüfung für synthetische Nukleinsäuren zu ermöglichen und gleiche Wettbewerbsbedingungen für verantwortungsbewusste Syntheseanbieter zu schaffen (Zakaria et al. 2026, S. 14 ff.) (für mögliche Implementierungswege auf EU-Ebene und national Kapitel 4.7.3). Der Entwurf sieht die Einführung einer Pflicht zur Überprüfung des legitimen Bedarfs von Käufern biotechnologischer Produkte mit hohem Missbrauchspotenzial vor. Hierzu zählen auch besorgniserregende synthetisierte Nukleinsäuresequenzen („sequences of concern“), wodurch faktisch ein Sequenzscreening notwendig wird. Darüber hinaus wird vorgeschrieben, dass Tischgeräte zur Nukleinsäuresynthese automatische Mechanismen zum Screening von Sequenzen enthalten müssen. Ähnlich zu international angewandten Standards, z. B. dem des IGSC (2024) oder den Empfehlungen der IBBIS (o. J.) (Kapitel 4.7.3), sollen gemäß dem Entwurf (Annex I) nicht nur mindestens 50 Nukleotide lange Sequenzen als besorgniserregend gelten, die Übereinstimmungen mit gefährlichen Sequenzen von auf international anerkannten Kontrolllisten aufgeführten Erregern aufweisen. Sondern auch solche, bei denen aufgrund von Funktionsvorhersagen davon auszugehen ist, dass sie die Pathogenität eines

Organismus oder die Toxizität von Molekülen erhöhen, selbst wenn sie nicht von gelisteten Erregern stammen.

Deutschland könnte sich in der EU dafür einsetzen, dass bei mit EU-Mitteln finanzierten Projekten (auch außerhalb der EU) Nukleinsäuresynthesen und Tischgeräte zur Nukleinsäuresynthese ausschließlich von Anbietern und Herstellern bezogen werden dürfen, die das Screening von Sequenzen und Kunden nach festgelegten Standards durchführen bzw. Sequenzscreeningmechanismen in die Geräte eingebaut haben.

Grundsätzlich könnten auf nationaler Ebene alle Forschungsförderer in Deutschland verpflichtet werden, entsprechende Auflagen für die Verwendung von Fördergeldern zu implementieren. Ähnliche Auflagen könnten auch in Bezug auf Aufträge jeglicher Art von Auftragsforschungsinstitutionen oder für die Nutzung von Cloudlaboren eingeführt werden.

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

Um Risiken potenzieller zukünftiger biologischer KI-Modelle hinsichtlich des Designs gefährlicherer biologischer Agenzien zu reduzieren, könnten prinzipiell Mechanismen für den kontrollierten Zugang zu leistungsfähigen Bidesignmodellen oder bestimmten Datensätzen, die solche Modelle ermöglichen können, in Betracht gezogen werden. Zu solchen kritischen Datensätzen würden insbesondere (bisher noch weitgehend fehlende) umfangreichere und qualitativ hochwertige Daten gehören, über die KI-Modelle Genomsequenzen potenziell pandemischer Viren mit Eigenschaften wie Übertragbarkeit oder Umgehung der Immunantwort verknüpfen und solche Eigenschaften vorhersagen könnten (Kapitel 3.3.2). Zum Teil wurden detaillierte Vorschläge für solche möglichen Zugangskontrollen gemacht (Bloomfield et al. 2026; Carter/Butchello 2026) (Kapitel 4.7.5). Schlüsselmerkmale dieser Vorschläge sind die Einteilung von Modellen oder bestimmter Datensätze in unterschiedliche Risiko- bzw. Sicherheitsstufen mit entsprechend gestaffelten Zugangskriterien. Mit steigendem Risikopotenzial bzw. jeweils höherer Sicherheitsstufe eines Modells oder Datensatzes müssten Nutzer/innen zunehmend strengere Legitimitätskriterien für den Zugang erfüllen.

Bevor solche Mechanismen in Betracht gezogen werden, müssen diese und deren mögliche Wirksamkeit (nicht zuletzt auch in Bezug auf potenziell relevante Akteure²²¹) sehr sorgfältig gegen mögliche negative bzw. kontraproduktive Auswirkungen abgewogen werden. Hiervon betroffen sein könnten insbesondere die biomedizinische Forschung und Entwicklung im Allgemeinen sowie die Entwicklung von Vorsorgemaßnahmen oder Gegenmaßnahmen im Krisenfall im Besonderen.

Zu einer solchen Abwägung – unter Berücksichtigung existierender Hinweise und Evidenzen zu Risiken sowie dem Monitoring möglicher Risikoverschärfungen – könnte auf nationaler Ebene ein einrichtendes Beratungsgremium aus Expert/innen verschiedener Disziplinen und Bereichen beitragen. Diesem könnten etwa Expert/innen aus relevanten biologischen Disziplinen und der Biosicherheit, aus der KI-Entwicklung, der Innovations- und Wissenschaftsforschung sowie Be-

²²¹ Zu relevanten potenziellen Akteuren, die über solche Mechanismen nur schwer kontrollierbar sein könnten, dürften etwa staatliche Akteure oder an etablierten Institutionen arbeitende Expert/innen (DOJ 2010) gehören.

treiber relevanter Datenbanken angehören. Ebenso könnten Vertreter/innen aus Industrie, relevanten Bundesinstituten und der Bundeswehr Teil des Gremiums sein. Die Empfehlungen eines solchen Gremiums könnten auch mit Blick auf mögliche, von Deutschland beeinflussbare Entscheidungen im Zusammenhang mit Kontrollmechanismen auf europäischer oder internationaler Ebene genutzt werden.

Ein solches Beratungsgremium könnte darüber hinaus Ausgangspunkt für oder Teil einer Wenn-dann-Strategie sein, wie sie von den amerikanischen National Academies of Sciences, Engineering, and Medicine vorgeschlagen wurde, um der dynamischen KIxBio-Entwicklung Rechnung zu tragen (NAS 2025b). Dieser Ansatz zielt auf eine kontinuierliche Bewertung sowie eine regelmäßige Neubewertung von Schwachstellen und Risiken ab. Die Bewertung soll auf Basis von (Früh-)Indikatoren für die Entwicklung neuer KI-Fähigkeiten und von Entwicklungen anderer Faktoren erfolgen, die Bedrohungen durch Biowaffen bestimmen können. Zu diesen Faktoren zählen beispielsweise solche mit Relevanz für kritische Bedingungen für Akteure, wie der Zugang zu Ressourcen, die Attraktivität bzw. Nutzung als Waffe oder Möglichkeiten der Risikominderung. Entsprechend den Ergebnissen (und möglichen festgelegten Schwellenwerten) würden neue Risikobewertungen sowie gegebenenfalls weitere oder verschärfte Maßnahmen zur Risikominderung ausgelöst.

Die Stärkung der BWC

Eine substanzielle Stärkung der BWC könnte durch folgende Maßnahmen erreicht werden:

- über die weitere inhaltliche Unterstützung der bei der letzten BWC-Überprüfungskonferenz im Jahr 2022 eingesetzten Arbeitsgruppe zur Stärkung der BWC, die insbesondere (bisher fehlende) Möglichkeiten zur Überprüfung und Einhaltung der Konvention diskutieren und entwickeln soll. Zwar könnte in der aktuellen geopolitischen Situation die Schaffung eines klassischen Verifikationsregimes (einschließlich kurzfristiger Überprüfungen verdächtiger Einrichtungen) ähnlich zur CWC mit einer zwischenstaatlichen Organisation wie der OPCW nur schwer zu erreichen sein. Jedoch könnten zur Stärkung der BWC auch andere Modelle beitragen, wie etwa solche, die strukturierte Selbstauskünfte umfassen und bei denen Staaten freiwillig ihre Einhaltung der Vorschriften durch Peer-Reviews und Besuche vor Ort nachweisen, um das Vertrauen in die Einhaltung der Vertragsbestimmungen zu stärken (Krasny 2024; Revill 2024) (Kapitel 4.7.1).
- durch das Einbringen oder die Unterstützung von Initiativen zur Verbesserung der Finanzierungssituation der BWC bzw. der BWC-Unterstützungseinheit. Das im Vergleich zur CWC winzige Budget (Patrick/Barton 2024) beruht darüber hinaus auf freiwilligen Beiträgen, was eine nachhaltige und planbare Finanzierung zur notwendigen Weiterentwicklung der BWC zusätzlich erschwert (Feakes 2024).

Der Ausbau der Fähigkeit zur Durchführung von Vorsorge und Gegenmaßnahmen

Ein weiteres Element zur Risikoreduktion könnten Biodefense-Maßnahmen²²² sein, wie eine verbesserte Vorsorge hinsichtlich der Früherkennung von potenziellen pandemischen Erregern (unabhängig von deren Ursprung), verbesserte Kapazitäten zur schnellen Eindämmung und Schadensbegrenzung sowie die Erkennung bzw. Verhinderung von biologischen Anschlagsplänen. Solche Maßnahmen könnten neben einer besseren Reaktionsfähigkeit auch zur Abschreckung von Gegnern beitragen, die sich über militärische Strategien nicht abschrecken ließen, wie etwa bestimmte nicht staatliche Akteure – indem sie deren Erfolgsaussichten reduzieren („deterrence by denial“) (Krasny 2025).

Hierzu könnten durch parlamentarische Gremien und/oder Ministerien, die Zugang zu notwendigen, ansonsten nicht öffentlich zugänglichen Informationen haben, Möglichkeiten zur Stärkung von Aktivitäten und Kapazitäten insbesondere in den folgenden Bereichen geprüft werden:

- anwendungsorientierte Biodefense-Forschung: Dort können neue KI-Möglichkeiten (Kapitel 2.4) genutzt werden, um effektive Früherkennungsmaßnahmen für biologische Agenzien oder ungewöhnliche Infektionen sowie schnell skalierbare medizinischer Gegenmaßnahmen zur raschen Eindämmung und Schadensbegrenzung zu entwickeln. Beispiele sind die Analyse globaler Kommunikationsquellen mithilfe von natürlicher Sprachverarbeitung oder Diagnosealgorithmen, die pathologische und epidemiologische Merkmale eines Ausbruchs unterscheiden und auf einen möglichen Erreger hinweisen. Auch KI-Modelle, die Genomdaten aus verschiedenen Quellen kontinuierlich überwachen, diese Daten mit vorhergesagten Proteinstrukturdaten ergänzen und auf neue zirkulierende Erreger hinweisen, könnten hier genannt werden (NAS 2025b, S. 34 f. und Referenz darin). Des Weiteren könnte die Etablierung effektiver bzw. schnell skalierbarer medizinischer Gegenmaßnahmen zur schnellen Eindämmung und Schadensbegrenzung gefördert werden, wie etwa Plattformtechnologien zur Beschleunigung der Impfstoffentwicklung und -produktion, wie sie beispielsweise im Rahmen des „Rapid Response Framework“ der „Coalition for Epidemic Preparedness Innovations“ (CEPI 2026) entwickelt werden sollen (Kim et al. 2025; Wahome 2025).
- Terrorismusabwehr: Hier könnte die Zusammenarbeit mit Unternehmen, die KI entwickeln, gefördert bzw. deren Sicherheitsmaßnahmen unterstützt werden. Dazu könnte beispielsweise die Überwachung besorgniserregender Kommunikation mit großen generativen KI-Modellen (Chatbots) gehören, die vermuten lässt, dass Nutzer anderen Schaden zufügen wollen (OpenAI 2025e; Wells 2026).

²²² Hier im breiten Sinne von Biodefense der U.S. Department of Health and Human Services Administration for Strategic Preparedness and Response (ASPR o. J.b) verstanden, also einschließlich Terrorismusbekämpfung.

6 Literatur

6.1 In Auftrag gegebene Gutachten

6.2 Weitere Literatur



6 Literatur

6.1 In Auftrag gegebene Gutachten

- Pinzger, B. et al. (2025): Gegenwärtige Regulierungen und Maßnahmen zur Kontrolle von Biowaffen sowie zu sicherheits- relevanter Dual-Use-Forschung in den Biowissenschaften – in Deutschland, auf EU-Ebene und international. Fraunhofer-Institut für Naturwissenschaftlich-Technische Trendanalysen, Euskirchen
- Sabra, D. M.; Frieß, J. L. (2025): Biotechnologie und künstliche Intelligenz: Risiken der Forschung für die Sicherheit und Proliferation von Biowaffen. Notwendige Kenntnisse und technische Voraussetzungen für die Herstellung und den Einsatz von biologischen Agenzien als Biowaffen. Carl Friedrich von Weizsäcker-Zentrum für Naturwissenschaften und Friedensforschung, Universität Hamburg, Hamburg

6.2 Weitere Literatur

- Abel, G. et al. (2026): Beyond Sequence Similarity: Toward Function-Based Screening of Nucleic Acid Synthesis. SSRN, <https://doi.org/10.2139/ssrn.6444478>
- Abramson, J. et al. (2024): Accurate structure prediction of biomolecular interactions with AlphaFold 3. In: Nature 630(8016), S. 493–500, <https://doi.org/10.1038/s41586-024-07487-w>
- Active Site (2026): Does frontier AI enhance novices in molecular biology? Field Conditions, <https://activesite.substack.com/p/rct> (27.2.2026)
- Adam, D. (2024): The automated lab of tomorrow. In: Proceedings of the National Academy of Sciences 121(17), Art. e2406320121, <https://doi.org/10.1073/pnas.2406320121>
- Adamson, G.; Allen, G. C. (2025): Opportunities to Strengthen U.S. Biosecurity from AI-Enabled Bioterrorism: What Policymakers Should Know. Center for Strategic and International Studies, Washington, D.C.
- Agrawal, G. et al. (2023): Preclinical development can benefit from advances to accelerate innovation, unlock value, and improve quality. McKinsey & Company, <https://www.mckinsey.com/industries/life-sciences/our-insights/fast-to-first-in-human-getting-new-medicines-to-patients-more-quickly> (30.5.2025)
- Ainscough, M. J. (2002): Next Generation Bioweapons: Genetic Engineering and BW. US Air Force Counterproliferation Center, o. O.
- AI SI (2025): Frontier AI Trends Report. AI Security Institute, London
- Ajikumar, P. K. et al. (2010): Isoprenoid pathway optimization for Taxol precursor overproduction in Escherichia coli. In: Science 330(6000), S. 70–74, <https://doi.org/10.1126/science.1191652>
- Alexanian, T. (2023): Bio x AI: Policy Recommendations for a New Frontier. Develop a Screening Framework Guidance for AI-Enabled Automated Labs. Federation of American Scientists, <https://fas.org/publication/bio-x-ai-policy-recommendations/> (29.1.2026)
- Alibek, K. (2004): Smallpox: a disease and a weapon. In: International Journal of Infectious Diseases 8, S. 3–8, <https://doi.org/10.1016/j.ijid.2004.09.004>

- Alibek, K.; Handelman, S. (1999): Biohazard. The chilling true story of the largest covert biological weapons program in the world, told from the inside by the man who ran it. New York
- Allen, G. C.; Adamson, G. (2024): The AI Safety Institute International Network: Next Steps and Recommendations. Center for Strategic and International Studies, Washington, D.C.
- Alsumidaie, M. (2024): How Geopolitical Economic Changes Are Impacting Big Pharma. The Clinical Trial Vanguard, <https://www.clinicaltrialvanguard.com/article/how-geopolitical-economic-changes-are-impacting-big-pharma/> (23.5.2025)
- Alvarez, S. et al. (Hg.) (2024): Biosecurity Laws. Washington, D.C.
- Anderson, P. D. (2012): Bioterrorism: Toxins as Weapons. In: Journal of Pharmacy Practice 25(2), S. 121–129, <https://doi.org/10.1177/0897190012442351>
- Anderson, P. D.; Bokor, G. (2012): Conotoxins: Potential Weapons from the Sea. In: Journal of Bioterrorism & Biodefense 3, Art. 120, <https://doi.org/10.4172/2157-2526.1000120>
- Anthropic (2025a): Introducing Claude 4. <https://www.anthropic.com/news/claude-4> (27.6.2025)
- Anthropic (2025b): System Card: Claude Opus 4 & Claude Sonnet 4. <https://www-cdn.anthropic.com/6be99a52cb68eb70eb9572b4cafad13df32ed995.pdf>
- Anthropic (2025c): System Card: Claude Opus 4.5. <https://assets.anthropic.com/m/64823ba7485345a7/Claude-Opus-4-5-System-Card>
- Anthropic (2025d): System Card: Claude Sonnet 4.5. <https://assets.anthropic.com/m/12f214efcc2f457a/original/Claude-Sonnet-4-5-System-Card.pdf>
- Anthropic (2025e): Why do we take LLMs seriously as a potential source of biorisk? <https://red.anthropic.com/2025/biorisk/#ftnt3> (14.11.2025)
- Anthropic (2026a): System Card: Claude Mythos Preview. <https://www-cdn.anthropic.com/08ab9158070959f88f296514c21b7facce6f52bc.pdf>
- Anthropic (2026b): System Card: Claude Opus 4.6. <https://www-cdn.anthropic.com/0dd865075ad3132672ee0ab40b05a53f14cf5288.pdf#page171>
- Anthropic (2026c): System Card: Claude Sonnet 4.6. <https://www-cdn.anthropic.com/78073f739564e986ff3e28522761a7a0b4484f84.pdf>
- APP3 Emerging Biological Risks Working Group (2024): APP3 Statement on the Importance of Biosafety and Biosecurity in the Age of Artificial Intelligence and Emerging Technologies. Global Health Security Agenda, <https://globalhealthsecurityagenda.org/app3-statement-on-the-importance-of-biosafety-and-biosecurity-in-the-age-of-artificial-intelligence-and-emerging-technologies/> (7.1.2026)
- Arias, D. S.; Taylor, R. E. (2024): Scientific Discovery at the Press of a Button: Navigating Emerging Cloud Laboratory Technology. In: Advanced Materials Technologies 9(16), Art. 2400084, <https://doi.org/10.1002/admt.202400084>
- Arnold, C. (2022): Cloud labs: where robots do the research. In: Nature 606(7914), S. 612–613, <https://doi.org/10.1038/d41586-022-01618-x>
- Arnold, F. H. (2018): Directed Evolution: Bringing New Chemistry to Life. In: Angewandte Chemie International Edition 57(16), S. 4143–4148, <https://doi.org/10.1002/anie.201708408>
- ASPR (o. J.a): 2024 OSTP Framework for Nucleic Acid Synthesis Screening. Administration for Strategic Preparedness & Response, <https://aspr.hhs.gov/S3/Pages/OSTP-Framework-for-Nucleic-Acid-Synthesis-Screening.aspx> (28.1.2026)
- ASPR (o. J.b): Frequently Asked Questions: National Biodefense Strategy. Administration for Strategic Preparedness and Response, <https://aspr.hhs.gov/biodefense/Pages/faq.aspx>

- Associated Press (2013): Ricin letters sent to New York mayor Michael Bloomberg. The Guardian, <https://www.theguardian.com/world/2013/may/30/michael-bloomberg-ricin-letters-new-york-mayor> (15.10.2025)
- Australia Group (2025): Control List of dual-use biological equipment and related technology and software. <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/documents/common-control-lists/Common-Control-List-of-Dual-Use-Biological-Equipment.pdf> (28.5.2025)
- Auswärtiges Amt (o. J.a): Humanitäres Völkerrecht. <https://www.auswaertiges-amt.de/de/aussenpolitik/regelbasierte-internationale-ordnung/voelkerrecht-internationales-recht/humanitaeres-voelkerrecht-213012> (22.12.2025)
- Auswärtiges Amt (o. J.b): Übereinkommen über das Verbot biologischer Waffen (BWÜ). Deutsches Engagement im Bereich Biosicherheit. https://www.auswaertiges-amt.de/de/aussenpolitik/sicherheitspolitik/abruestung-ruestungskontrolle/uebersicht-bcwaffen-node/verbot-biowaffen-bwue-node?openAccordionId=item-2674420-1-panel#content_2 (14.1.2026)
- Aven, T. (2015): Implications of black swans to the foundations and practice of risk assessment and management. In: Reliability Engineering & System Safety 134, S. 83–91, <https://doi.org/10.1016/j.ress.2014.10.004>
- Avsec, Ž. et al. (2021): Effective gene expression prediction from sequence by integrating long-range interactions. In: Nature Methods 18(10), S. 1196–1203, <https://doi.org/10.1038/s41592-021-01252-x>
- Avsec, Ž. et al. (2026): Advancing regulatory variant effect prediction with AlphaGenome. In: Nature 649, S. 1206–1218, <https://doi.org/10.1038/s41586-025-10014-0>
- Baek, M. et al. (2021): Accurate prediction of protein structures and interactions using a three-track neural network. In: Science 373(6557), S. 871–876, <https://doi.org/10.1126/science.abj8754>
- BAFA (o. J.): Allgemeine Genehmigungen. Bundesamt für Wirtschaft und Ausfuhrkontrolle, https://www.bafa.de/DE/Aussenwirtschaft/Ausfuhrkontrolle/Antragsarten/Allgemeine_Genehmigungen/allgemeine_genehmigungen_node.html (30.6.2026)
- Baker Botts (2026): China's Draft Regulations on Human-like AI: Key Takeaways. JD Supra, <https://www.jdsupra.com/legalnews/china-s-draft-regulations-on-human-like-5223467/> (19.1.2026)
- Baker, D.; Church, G. (2024): Protein design meets biosecurity. In: Science 383(6681), S. 349–349, <https://doi.org/10.1126/science.ado1671>
- Baracia, J. et al. (2024): CMU Cloud Lab to bring remote science into mainstream. The Tartan, <https://the-tartan.org/2024/02/19/cmu-cloud-lab-to-bring-remote-science-into-mainstream/> (17.6.2025)
- Barbadilla-Martínez, L. et al. (2025): Predicting gene expression from DNA sequence using deep learning models. In: Nature Reviews Genetics 26, S. 666–680, <https://doi.org/10.1038/s41576-025-00841-2>
- Barenblatt, D. (2005): A Plague upon Humanity. New York
- Barras, V.; Greub, G. (2014): History of biological warfare and bioterrorism. In: Clinical Microbiology and Infection: The Official Publication of the European Society of Clinical Microbiology and Infectious Diseases 20(6), S. 497–502, <https://doi.org/10.1111/1469-0691.12706>
- Bartoszewicz, J. M. et al. (2021): Interpretable detection of novel human viruses from genome sequencing data. In: NAR Genomics and Bioinformatics 3(1), Art. lqab004, <https://doi.org/10.1093/nargab/lqab004>

- BAuA (2026): Biostoffe - Einstufung von Biostoffen in Risikogruppen - Bundesanstalt für Arbeitsschutz und Arbeitsmedizin. BAuA, 13.1.2026, <https://www.baua.de/DE/Themen/Chemikalien-Biostoffe/Biostoffe-Infektionsschutz/Biostoffe/Einstufung> (13.1.2026)
- Beal, J.; Alexanian, T. (2025): Creating Enforceable Biosecurity Standards for Nucleic Acid Providers. In: *Engineering Biology* 9(1), Art. e70003, <https://doi.org/10.1049/enb2.70003>
- Beck, M. et al. (2024): Understanding the cell: Future views of structural biology. In: *Cell* 187(3), S. 545–562, <https://doi.org/10.1016/j.cell.2023.12.017>
- Beck, M. D.; Jones, S. A. (2019): The once and future multilateral export control regimes: innovate or die. In: *Strategic Trade Review* 5(8), S. 55–76
- Becker, M. M. et al. (2008): Synthetic recombinant bat SARS-like coronavirus is infectious in cultured cells and in mice. In: *Proceedings of the National Academy of Sciences* 105(50), S. 19944–19949, <https://doi.org/10.1073/pnas.0808116105>
- beck-online (2020): OLG Düsseldorf: Zehn Jahre Haft für islamistischen Rizin-Bombenbauer. <http://beck-online.beck.de/?vpath=bibdata/reddok/becklink/2015892.htm> (13.10.2025)
- Beeckman, D. S. A.; Rüdelsheim, P. (2020): Biosafety and Biosecurity in Containment: A Regulatory Overview. In: *Frontiers in Bioengineering and Biotechnology* 8, Art. 650, <https://doi.org/10.3389/fbioe.2020.00650>
- Bender, B. J. et al. (2021): A practical guide to large-scale docking. In: *Nature Protocols* 16(10), S. 4799–4832, <https://doi.org/10.1038/s41596-021-00597-z>
- Bender, R.; Lange, S. (2001): Was ist ein Konfidenzintervall? In: *DMW - Deutsche Medizinische Wochenschrift* 126(Suppl. Statistik), T 41-T 41, <https://doi.org/10.1055/s-2001-12740>
- Benegas, G. et al. (2025): A DNA language model based on multispecies alignment predicts the effects of genome-wide variants. In: *Nature Biotechnology* 43, S. 1960–1965, <https://doi.org/10.1038/s41587-024-02511-w>
- Ben-Nun, S. (2025): Israel unprepared for terror attack on public transport | The Jerusalem Post. *The Jerusalem Post*, <https://www.jpost.com/israel-news/defense-news/article-878949> (16.1.2026)
- Bergeson, L. L.; Hutton, C. N. (2026): Senate Bill Would Establish Federal Biotechnology Security Framework. Bergeson & Campbell, P.C., <https://www.lawbc.com/senate-bill-would-establish-federal-biotechnology-security-framework/> (15.4.2026)
- Bergmann, D. (2025): What Is a Reasoning Model? IBM, <https://www.ibm.com/think/topics/reasoning-model> (26.11.2025)
- Berke, A. et al. (2025): Data and AI-Enabled Biological Design: Risks Related to Biological Training Data and Opportunities for Governance. RAND Corporation, Santa Monica
- Bertoline, L. M. F. et al. (2023): Before and after AlphaFold2: An overview of protein structure prediction. In: *Frontiers in Bioinformatics* 3, Art. 1120370, <https://doi.org/10.3389/fbinf.2023.1120370>
- Bio, N.; Biswas, S. (2025a): De novo design of epitope-specific antibodies against soluble and multipass membrane proteins with high specificity, developability, and function. *bioRxiv*, <https://doi.org/10.1101/2025.01.21.633066>
- Bio, N.; Biswas, S. (2025b): De novo design of hundreds of functional GPCR-targeting antibodies enabled by scaling test-time compute., <https://doi.org/10.1101/2025.05.28.656709>
- BIS (o. J.): Interactive Commerce Control List. <https://www.bis.gov/regulations/ear/interactive-commerce-control-list?isExpanded=&category=&keyword=> (30.6.2026)

- Bjørn-Yoshimoto, W. E. et al. (2020): Curses or Cures: A Review of the Numerous Benefits Versus the Biosecurity Concerns of Conotoxin Research. In: *Biomedicines* 8(8), Art. 235, <https://doi.org/10.3390/biomedicines8080235>
- Black, J. R. M. et al. (2025): Open-weight genome language model safeguards: Assessing robustness via adversarial fine-tuning. *OpenReview*, <https://openreview.net/forum?id=bKLp7oaU1L> (20.2.2026)
- Bloomfield, D. et al. (2024): AI and biosecurity: The need for governance. In: *Science* 385(6711), S. 831–833, <https://doi.org/10.1126/science.adq1977>
- Bloomfield, D. (2024): U.S. Export Controls of AI Models. SSRN, <https://doi.org/10.2139/ssrn.4741033>
- Bloomfield, D. et al. (2025): How U.S. Export Controls Risk Undermining Biosecurity. *Lawfare*, <https://www.lawfaremedia.org/article/how-u.s.-export-controls-risk-undermining-biosecurity> (27.1.2026)
- Bloomfield, D. et al. (2026): Biological data governance in an age of AI. In: *Science* 391(6785), S. 558–561, <https://doi.org/10.1126/science.aeb2689>
- Boiko, D. A. et al. (2023): Autonomous chemical research with large language models. In: *Nature* 624(7992), S. 570–578, <https://doi.org/10.1038/s41586-023-06792-0>
- Bolton, E. et al. (2024): BioMedLM: A 2.7B Parameter Language Model Trained On Biomedical Text. *arXiv*, <https://doi.org/10.48550/arXiv.2403.18421>
- Bordelon, B. (2023): Special report. Inside the culture clash dominating the AI debate. *Politico*, <https://www.politico.com/news/2023/12/30/ai-debate-culture-clash-dc-silicon-valley-00133323> (24.2.2026)
- Bornscheuer, U. T. et al. (2012): Engineering the third wave of biocatalysis. In: *Nature* 485(7397), S. 185–194, <https://doi.org/10.1038/nature11117>
- Bran, A. M. et al. (2024): Augmenting large language models with chemistry tools. In: *Nature Machine Intelligence* 6(5), S. 525–535, <https://doi.org/10.1038/s42256-024-00832-8>
- Brandes, N. et al. (2023): Genome-wide prediction of disease variant effects with a deep protein language model. In: *Nature Genetics* 55(9), S. 1512–1522, <https://doi.org/10.1038/s41588-023-01465-0>
- Brent, R.; McKelvey, T. G. (2025): Contemporary AI foundation models increase biological weapons risk. *arXiv*, <https://doi.org/10.48550/arXiv.2506.13798>
- Brixi, G. et al. (2026): Genome modelling and design across all domains of life with Evo 2. In: *Nature* 652, S. 1349–1361, <https://doi.org/10.1038/s41586-026-10176-5>
- Brockmann, K. et al. (2025): Cloud Labs and Other New Actors in the Biotechnology Ecosystem: Export Control Challenges and Good Practices in Outreach. SIPRI, Stockholm
- Brockmann, K. (2025): The Australia Group at 40: Making the AG Fit for an Era of Geopolitical Competition. SIPRI, Stockholm
- Brockmann, K.; Héau, L. (2025): Use Cases for Emerging Technologies to Strengthen Export Controls on Biological Items. SIPRI, Stockholm
- Brownless, A.-L. R. et al. (2025): Generative AI techniques for conformational diversity and evolutionary adaptation of proteins. In: *Current Opinion in Structural Biology* 94, Art. 103135, <https://doi.org/10.1016/j.sbi.2025.103135>
- Brugger, S. (2002): The Australia Group at a Glance. Arms Control Association, <https://www.armscontrol.org/factsheets/australia-group-glance> (7.1.2026)
- de Bruin, E. (2022): Export Control Regimes—Present-Day Challenges and Opportunities. In: Beeres, R. et al. (Hg.): *NL ARMS Netherlands Annual Review of Military Studies 2021: Compli-*

- ance and Integrity in International Military Trade. The Hague, S.31–53, https://doi.org/10.1007/978-94-6265-471-6_3
- Buller, R. et al. (2023): From nature to industry: Harnessing enzymes for biocatalysis. In: Science 382(6673), Art. eadh8615, <https://doi.org/10.1126/science.adh8615>
- Bundesnetzagentur (o.J.): KI-Verordnung auf einen Blick. https://www.bundesnetzagentur.de/DE/Fachthemen/Digitales/KI/_functions/factsheet.pdf?__blob=publicationFile&v=1 (29.5.2026)
- Burck, K.; de Vries, B. (2023): Umsetzung der Normen gegen chemische und biologische Waffen im deutschen Kontext. CBWNet, Working Paper 6, Berlin
- Burningham, G. (2019): The Price of Insulin Has Soared. These Biohackers Have a Plan to Fix It. TIME, <https://time.com/5709241/open-insulin-project/> (4.8.2025)
- Butcher, J. et al. (2025): De novo Design of All-atom Biomolecular Interactions with RFDiffusion3. bioRxiv, <https://doi.org/10.1101/2025.09.18.676967>
- Caballar, R. D. (2025): Generative AI vs. predictive AI: What's the difference? IBM, <https://www.ibm.com/think/topics/generative-ai-vs-predictive-ai-whats-the-difference> (14.5.2025)
- Caballar, R. D.; Stryker, C. (2025): What Are Foundation Models? IBM, <https://www.ibm.com/think/topics/foundation-models> (14.5.2025)
- Callaway, E. (2024a): Ex-Meta scientists debut gigantic AI protein design model. Nature, <https://doi.org/10.1038/d41586-024-02214-x>
- Callaway, E. (2024b): Could AI-designed proteins be weaponized? Scientists lay out safety guidelines. In: Nature 627(8004), S. 478–478, <https://doi.org/10.1038/d41586-024-00699-0>
- Callaway, E. (2025): I told AI to make me a protein. Here's what it came up with. In: Nature 641(8065), S. 1079–1080, <https://doi.org/10.1038/d41586-025-01586-y>
- Carter, S. et al. (2023): The convergence of artificial intelligence and the life sciences: Safeguarding technology, rethinking governance, and preventing catastrophe. Nuclear Threat Initiative, Washington, D.C.
- Carter, S. et al. (2024a): Community Values, Guiding Principles, and Commitments for the Responsible Development of AI for Protein Design. Responsible AI x Biodesign, <https://responsiblebiodesign.ai/>
- Carter, S. R. et al. (2024b): Developing Guardrails for AI Biodesign Tools. The Nuclear Threat Initiative, <https://www.nti.org/analysis/articles/developing-guardrails-for-ai-biodesign-tools/> (29.1.2026)
- Carter, S. R.; Butchello, G. (2026): A Framework for Managed Access to Biological AI Tools. Nuclear Threat Initiative, Washington, D.C.
- Carugo, O.; Djinić-Carugo, K. (2023): Structural biology: A golden era. In: PLOS Biology 21(6), Art. e3002187, <https://doi.org/10.1371/journal.pbio.3002187>
- Carus, W. S. (1998): Bioterrorism and Biocrimes. The Illicit Use of Biological Agents Since 1900. Center for Counterproliferation Research National Defense University, Washington, D.C.
- Carus, W. S. (2017): A Short History of Biological Warfare: From Pre-History to the 21st Century. National Defense University, Washington, D.C.
- Catacutan, D. B. et al. (2024): Machine learning in preclinical drug discovery. In: Nature Chemical Biology 20(8), S. 960–973, <https://doi.org/10.1038/s41589-024-01679-1>
- CBB (2026): Biosecurity. Centre for Biosecurity and Biopreparedness, <https://www.biosecurity.dk/biosecurity> (16.1.2026)
- CDC (2025): Aerosols in the Workplace. U. S. Centers for Disease Control and Prevention, <https://www.cdc.gov/niosh/aerosols/about/index.html> (30.9.2025)

- Cello, J. et al. (2002): Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template. In: *Science* 297(5583), S.1016–1018, <https://doi.org/10.1126/science.1072266>
- Center for Health Security (o. J.): International Guidelines for Biosecurity Ethics. <https://centerforhealthsecurity.org/our-work/research-projects/international-guidelines-for-biosecurity-ethics> (30.6.2026)
- CEPI (2026): CEPI launches global plan to secure the future against epidemic and pandemic threats. <https://cepi.net/cepi-launches-global-plan-secure-future-against-epidemic-and-pandemic-threats> (29.5.2026)
- CFG (2025): Can open-weight models ever be safe? Centre for Future Generations, <https://cfg.eu/can-open-weight-models-ever-be-safe/> (6.11.2025)
- Charles, D. (2025): Made to order bioweapon? AI-designed toxins slip through safety checks used by companies selling genes. *Science*, <https://doi.org/10.1126/science.zqvceub>
- Chaudhari, J. K. et al. (2024): Biological big-data sources, problems of storage, computational issues, and applications: a comprehensive review. In: *Knowledge and Information Systems* 66(6), S. 3159–3209, <https://doi.org/10.1007/s10115-023-02049-4>
- Chen, K. M. et al. (2022): A sequence-based global map of regulatory activity for deciphering human genetics. In: *Nature Genetics* 54(7), S. 940–949, <https://doi.org/10.1038/s41588-022-01102-2>
- Chen, L. et al. (2024a): AI-Driven Deep Learning Techniques in Protein Structure Prediction. In: *International Journal of Molecular Sciences* 25(15), Art. 8426, <https://doi.org/10.3390/ijms25158426>
- Chen, Z. et al. (2024b): Evolution and Prospects of Foundation Models: From Large Language Models to Large Multimodal Models. In: *Computers, Materials & Continua* 80(2), S. 1753–1808, <https://doi.org/10.32604/cmc.2024.052618>
- Cheng, J. et al. (2023): Accurate proteome-wide missense variant effect prediction with Alpha-Missense. In: *Science* 381(6664), Art. eadg7492, <https://doi.org/10.1126/science.adg7492>
- China Law Translate (2025): Provisional Measures on the Administration of Human-like Interactive Artificial Intelligence Services (Draft for Solicitation of Comments). <https://www.chinalawtranslate.com/en/chatbot-measures-draft/> (2.6.2026)
- Chinchilla, M. et al. (2024): The Concepts of Biosafety and Biosecurity: The Need for a Coherent Approach. CBWNet, Working Paper Nr. 12, Berlin
- Chow, A. R. (2025): Exclusive: AI Bests Virus Experts, Raising Biohazard Fears. *TIME*, <https://time.com/7279010/ai-virus-lab-biohazard-study/> (19.11.2025)
- Christopher, G. W. et al. (1997): Biological warfare. A historical perspective. In: *JAMA* 278(5), S. 412–417
- Church, G. (2004): Synthetic Biohazard Non-proliferation. https://arep.med.harvard.edu/SBP/Church_Biohazard04c.htm (29.7.2025)
- Clark, G. C. et al. (2019): Friends or Foes? Emerging Impacts of Biological Toxins. In: *Trends in Biochemical Sciences* 44(4), S. 365–379, <https://doi.org/10.1016/j.tibs.2018.12.004>
- Clarke, L. (2020): Synthetic biology, engineering biology, market expectation. In: *Engineering Biology* 4(3), S. 33–36, <https://doi.org/10.1049/enb.2020.0021>
- Cole, L. A. (2016): Open-Air Biowarfare Testing and the Evolution of Values. In: *Health Security* 14(5), S. 315–322, <https://doi.org/10.1089/hs.2016.0040>

- Collins, H. (2007): Bicycling on the Moon: Collective Tacit Knowledge and Somatic-limit Tacit Knowledge. In: *Organization Studies* 28(2), S. 257–262, <https://doi.org/10.1177/0170840606073759>
- Collins, H. (2010): Tacit and Explicit Knowledge. Chicago, <https://doi.org/10.7208/9780226113821>
- Committee on Review of the Scientific Approaches Used During the FBI’s Investigation of the 2001 Bacillus Anthracis Mailings; National Research Council (2011): Review of the Scientific Approaches Used during the FBI’s Investigation of the 2001 Anthrax Letters. Washington, D.C.
- Council of the European Union (2009): Council Conclusions on strengthening chemical, biological, radiological and nuclear (CBRN) security in the European Union – An EU CBRN Action Plan: Adoption. Doc. 15505/1/09 REV 1, Brüssel
- Coutant, A. et al. (2019): Closed-loop cycles of experiment design, execution, and learning accelerate systems biology model development in yeast. In: *Proceedings of the National Academy of Sciences* 116(36), S. 18142–18147, <https://doi.org/10.1073/pnas.1900548116>
- Crawford, F. W. et al. (2024): Securing Commercial Nucleic Acid Synthesis. RAND Corporation, Santa Monica
- Cristiano, S. et al. (2019): Genome-wide cell-free DNA fragmentation in patients with cancer. In: *Nature* 570(7761), S. 385–389, <https://doi.org/10.1038/s41586-019-1272-6>
- Cross, G. (2017): Dirty War: Rhodesia and Chemical Biological Warfare 1975-1980. Solihull
- Crowley, M.; Dando, M. (2024): Regulation of toxins and bioregulators under the Chemical Weapons Convention and the Biological and Toxin Weapons Convention. In: *Journal of Biosafety and Biosecurity* 6(2), S. 99–112, <https://doi.org/10.1016/j.jobbb.2024.03.003>
- CSR (2025): Assessing Dual-Use Issues at the AIxBio Convergence: Future Risks and Opportunities for the United States. The Janne E. Nolan Center on Strategic Weapons, Council on Strategic Risks, Washington, D.C.
- Dance, G. J. X. (2026): A.I. Bots Told Scientists How to Make Biological Weapons. New York Times, https://www.nytimes.com/2026/04/29/us/ai-chatbots-biological-weapons.html?unlocked_article_code=1.elA.XwQy.RkmTtccocnR9F&smid=url-share (11.5.2026)
- Danzig, R. et al. (2012): Aum Shinrikyo: Insights Into How Terrorists Develop Biological and Chemical Weapons. Center for a New American Security, Washington, D.C.
- DaSilva, L. F. et al. (2024): DNA-Diffusion: Leveraging Generative Models for Controlling Chromatin Accessibility and Gene Expression via Synthetic Regulatory Elements. *bioRxiv*, <https://doi.org/10.1101/2024.02.01.578352>
- Davies, X. et al. (2026): Boundary Point Jailbreaking of Black-Box LLMs. *arXiv*, <https://doi.org/10.48550/arXiv.2602.15001>
- Davy, A. M. et al. (2017): Cell Factory Engineering. In: *Cell Systems* 4(3), S. 262–275, <https://doi.org/10.1016/j.cels.2017.02.010>
- Dayhoff, M. O.; Ledley, R. S. (1962): Comprotein: a computer program to aid primary protein structure determination. In: American Federation of Information Processing Societies: Proceedings of the December 4-6, 1962, fall joint computer conference. Santa Monica, S. 262–274, <https://doi.org/10.1145/1461518.1461546>
- De Lange, O. et al. (2022): „Short on time and big on ideas”: Perspectives from Lab Members on DIYBio Work in Community Biolabs. In: Association for Computing Machinery: DIS ’22: Proceedings of the 2022 ACM Designing Interactive Systems Conference. New York, S. 1358–1376, <https://doi.org/10.1145/3532106.3533521>

- deepseek (o. J.): Into the unknown. <https://www.deepseek.com/en/> (27.6.2025)
- DeFrancesco, L. (2021): Synthetic virology: the experts speak. In: *Nature Biotechnology* 39(10), S. 1185–1193, <https://doi.org/10.1038/s41587-021-01078-0>
- Deloitte (o. J.): Deloitte acquires Gryphon Scientific. <https://www.deloitte.com/us/en/services/consulting/services/biotech-consulting-and-data-analytics-solutions.html> (1.6.2026)
- Deneke, V. E. et al. (2024): A conserved fertilization complex bridges sperm and egg in vertebrates. In: *Cell* 187(25), S. 7066–7078, <https://doi.org/10.1016/j.cell.2024.09.035>
- Deng, C. et al. (2024): Investigating Data Contamination in Modern Benchmarks for Large Language Models. *arXiv*, <https://doi.org/10.48550/arXiv.2311.09783>
- Deng, Y. et al. (2025): Chemical Language Model Linker: blending text and molecules with modular adapters. *arXiv*, <https://doi.org/10.48550/arXiv.2410.20182>
- Deutscher Ethikrat (2014): Stellungnahme: Biosicherheit – Freiheit und Verantwortung in der Wissenschaft. Berlin
- Dev, S. et al. (2025): Toward Comprehensive Benchmarking of the Biological Knowledge of Frontier Large Language Models. RAND Corporation, Santa Monica
- DFG (2023): Umgang mit Risiken in internationalen Kooperationen. Deutsche Forschungsgemeinschaft. Bonn
- Dharmasivam, M. et al. (2026): Leading artificial intelligence–driven drug discovery platforms: 2025 landscape and global outlook. In: *Pharmacological Reviews* 78(1), Art. 100102, <https://doi.org/10.1016/j.pharmr.2025.100102>
- Dickinson, P. et al. (2025): Sustaining momentum: Allied responses to Russian chemical, biological, radiological, and nuclear threats. Atlantic Council, Washington, D.C.
- Digital Watch (2024): UN adopts China-led AI resolution. <https://dig.watch/updates/un-adopts-china-led-ai-resolution> (21.1.2026)
- Digital Watch (2025): UNGA adopts terms of reference for AI Scientific Panel and Global Dialogue on AI governance. <https://dig.watch/updates/un-general-assembly-adopts-terms-of-reference-for-ai-scientific-panel-and-global-dialogue-on-ai-governance> (21.1.2026)
- DOJ (2010): Amerithrax Investigative Summary. Released Pursuant to the Freedom of Information Act. United States Department of Justice, Washington, D.C.
- DOJ (2023): Foreign National Sentenced to Over 21 Years for Mailing Ricin to President of the United States in 2020. United States Department of Justice, <https://www.justice.gov/archives/opa/pr/foreign-national-sentenced-over-21-years-mailing-ricin-president-united-states-2020> (15.10.2025)
- DOJ (2024): Georgian National Charged with Soliciting Hate Crimes and a Mass Casualty Attack in New York City. United States Department of Justice, <https://www.justice.gov/usao-edny/pr/georgian-national-charged-soliciting-hate-crimes-and-mass-casualty-attack-new-york> (17.10.2025)
- Dokholyan, N. V. (2020): Experimentally-Driven Protein Structure Modeling. In: *Journal of proteomics* 220, Art. 103777, <https://doi.org/10.1016/j.jprot.2020.103777>
- Domingo, E. et al. (2019): Viral fitness: history and relevance for viral pathogenesis and antiviral interventions. In: *Pathogens and Disease* 77(2), Art. ftz021, <https://doi.org/10.1093/femsdp/ftz021>
- Dong, Y. et al. (2025): Safeguarding large language models: a survey. In: *Artificial Intelligence Review* 58, Art. 382, <https://doi.org/10.1007/s10462-025-11389-2>
- Donkor, S. A. et al. (2024): Computing in the Life Sciences: From Early Algorithms to Modern AI. *arXiv*, <https://doi.org/10.48550/arXiv.2406.12108>

- Doornbos, H.; Moussa, J. (2014): Found: The Islamic State's Terror Laptop of Doom. *Foreign Policy*, <https://foreignpolicy.com/2014/08/28/found-the-islamic-states-terror-laptop-of-doom/> (13.10.2025)
- Dorey, E. (2001): US rejects stronger bioweapons treaty. In: *Nature Biotechnology* 19(9), S. 793–793, <https://doi.org/10.1038/nbt0901-793>
- Dormitzer, P. R. et al. (2013): Synthetic Generation of Influenza Vaccine Viruses for Rapid Response to Pandemics. In: *Science Translational Medicine* 5(185), Art. 185ra68, <https://doi.org/10.1126/scitranslmed.3006368>
- Dormitzer, P. R. (2015): Rapid Production of Synthetic Influenza Vaccines. In: Oldstone, M. B. A.; Compans, R. W. (Hg.): *Influenza Pathogenesis and Control – Volume II*. Cham, S. 237–273, https://doi.org/10.1007/82_2014_399
- Dunham, A. S. et al. (2023): High-throughput deep learning variant effect prediction with Sequence UNET. In: *Genome Biology* 24, Art. 110, <https://doi.org/10.1186/s13059-023-02948-3>
- Edison, R. et al. (2026): Assembling unregulated DNA segments bypasses synthesis screening: regulate fragments as select agents. In: *Nature Communications* 17, Art. 3189, <https://doi.org/10.1038/s41467-025-67955-3>
- EEAS (2025): EU Statement – UN Open Briefing: UN Security council 1540 Committee. European External Action Service, https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-open-briefing-un-security-council-1540-committee_en (21.1.2026)
- EFSA (2008): EFSA bewertet Sicherheit von Lycoplen in Lebensmitteln. European Food Safety Authority, <https://www.efsa.europa.eu/de/news/efsa-assesses-safety-lycopene-foods> (25.6.2025)
- Eireiner, A. V. (2025a): DIY Biology: A Global Survey on Democratizing Science, 2021. UK Data Service, <https://doi.org/10.5255/UKDA-SN-857778>
- Eireiner, A. V. (2025b): Extra-institutional science: DIY biologists' democratization of scientific practices and spaces. In: *BioSocieties* 20, S. 419–448, <https://doi.org/10.1057/s41292-024-00347-w>
- Eisfeld, A. J. et al. (2024): A compendium of multi-omics data illuminating host responses to lethal human virus infections. In: *Scientific Data* 11, Art. 328, <https://doi.org/10.1038/s41597-024-03124-3>
- EK (2017): Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks. Europäische Kommission, COM(2017) 610 final, Brüssel
- EK (2024): First meeting of the International Network of AI Safety Institutes. European Commission, <https://digital-strategy.ec.europa.eu/en/news/first-meeting-international-network-ai-safety-institutes> (21.1.2026)
- EK (2025a): Annexes to the Proposal for a Regulation of the European Parliament and of the Council on establishing a framework of measures for strengthening Union's biotechnology and biomanufacturing sectors particularly in the area of health and amending Regulations (EC) No 178/2002, (EC) No 1394/2007, (EU) No 536/2014, (EU) 2019/6, (EU) 2024/795 and (EU) 2024/1938 (European Biotech Act). Europäische Kommission, COM(2025) 1022 final ANNEXES 1 to 3, Straßburg
- EK (2025b): Proposal for a Regulation of the European Parliament and of the Council on establishing a framework of measures for strengthening Union's biotechnology and biomanufacturing sectors particularly in the area of health and amending Regulations (EC) No 178/2002, (EC) No 1394/2007, (EU) No 536/2014, (EU) 2019/6, (EU) 2024/795 and (EU) 2024/1938 (European Biotech Act). Europäische Kommission, COM(2025) 1022 final, Straßburg

- EK (2025c): Questions and Answers on the European Biotech Act. Dec 16, 2025. Europäische Kommission, https://ec.europa.eu/commission/presscorner/detail/en/qanda_25_3079 (22.1.2026)
- EK (o. J.a): Exporting dual-use items – Trade and Economic Security. Europäische Kommission, https://policy.trade.ec.europa.eu/help-exporters-and-importers/exporting-dual-use-items_en (5.1.2026)
- EK (o. J.b): The General-Purpose AI Code of Practice. Stand 23.4.2026, Europäische Kommission, <https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai> (20.1.2026)
- Endy, D. (2005): Foundations for engineering biology. In: *Nature* 438(7067), S.449–453, <https://doi.org/10.1038/nature04342>
- Endy, D. (2007): 2003 Synthetic Biology study. Massachusetts Institute of Technology, Cambridge
- Enserink, M. (2013): Flu Researcher Ron Fouchier Loses Legal Fight Over H5N1 Studies. Dutch court confirms that export license is needed to publish certain influenza papers. *Science*, <https://www.science.org/content/article/flu-researcher-ron-fouchier-loses-legal-fight-over-h5n1-studies> (27.1.2026)
- ERINHA (2026): Scientific strategy. <https://erinha.eu/scientific-strategy/> (7.1.2026)
- Etzine, B. et al. (2025): Revitalizing Saturated Benchmarks: A Weighted Metric Approach for Differentiating Large Language Model Performance. arXiv, <https://doi.org/10.48550/arXiv.2503.05551>
- EU (o. J.): EU CBRN Centres of Excellence. Europäische Union, https://cbrn-risk-mitigation.net/work.europa.eu/eu-cbrn-centres-excellence_en (8.1.2026)
- Fady, P.-E. et al. (2025): Annexes to „Cost-Benefit Analysis of Synthetic Nucleic Acid Screening for the UK“. The Centre for Long-Term Resilience., London, <https://doi.org/doi.org/10.71172/kyey-h0ya>
- Farzaneh, T.; Freemont, P. S. (2021): Biofoundries are a nucleating hub for industrial translation. In: *Synthetic Biology* 6(1), Art. ysab013, <https://doi.org/10.1093/synbio/ysab013>
- FBI (2004): Ricin Letter. Federal Bureau of Investigation, <https://www.fbi.gov/news/pressrel/press-releases/ricin-letter> (15.10.2025)
- FBI (2014): Texas Woman Sentenced for Sending Ricin Letters. Federal Bureau of Investigation, <https://www.fbi.gov/contact-us/field-offices/dallas/news/press-releases/texas-woman-sentenced-for-sending-ricin-letters> (15.10.2025)
- Feakes, D. (2024): Confidence-Building Measures under the Biological Weapons Convention. United Nations Office for Disarmament Affairs, [https://docs-library.unoda.org/Biological_Weapons_Convention_Working_Group_on_the_strengthening_of_the_ConventionSixth_session_\(2025\)/2025-0815_ISU_ppt_on_CBM.pdf](https://docs-library.unoda.org/Biological_Weapons_Convention_Working_Group_on_the_strengthening_of_the_ConventionSixth_session_(2025)/2025-0815_ISU_ppt_on_CBM.pdf) (30.6.2026)
- Feng, H. et al. (2025): Benchmarking DNA foundation models for genomic and genetic tasks. In: *Nature Communications* 16, Art. 10780, <https://doi.org/10.1038/s41467-025-65823-8>
- Fenn, E. A. (2000): Biological warfare in eighteenth-century North America: beyond Jeffery Amherst. In: *Journal of American History* 86(4), S. 1552–1580
- Fennelly, K. P. (2020): Particle sizes of infectious aerosols: implications for infection control. In: *The Lancet. Respiratory Medicine* 8(9), S. 914–924, [https://doi.org/10.1016/S2213-2600\(20\)30323-4](https://doi.org/10.1016/S2213-2600(20)30323-4)
- Fernald, K. D. S. et al. (2024): The pharmaceutical productivity gap – Incremental decline in R&D efficiency despite transient improvements. In: *Drug Discovery Today* 29(11), Art. 104160, <https://doi.org/10.1016/j.drudis.2024.104160>

- Ferrini, J. B. et al. (1995): Expression of functional ricin B chain using the baculovirus system. In: *European Journal of Biochemistry* 233(3), S.772–777, https://doi.org/10.1111/j.1432-1033.1995.772_3.x
- Field, M. (2023): Catapulting corpses? A famous case of medieval biological warfare probably never happened. *Bulletin of the Atomic Scientists*, <https://thebulletin.org/2023/08/catapulting-corpses-a-famous-case-of-medieval-biological-warfare-probably-never-happened/> (16.10.2025)
- Findlay, G. M. (2021): Linking genome variants to disease: scalable approaches to test the functional impact of human mutations. In: *Human Molecular Genetics* 30(R2), S.R187–R197, <https://doi.org/10.1093/hmg/ddab219>
- Flade, F. (2018): The June 2018 Cologne Ricin Plot: A New Threshold in Jihadi Bio Terror. In: *CTC Sentinel* 11(7), S.1–4
- FMF (2025): Latest from the FMF: Grant-Making to Address AI-Bio Risk Challenges. *Frontier Model Forum*, <https://www.frontiermodelforum.org/updates/latest-from-the-fmf-grant-making-to-address-ai-bio-risk-challenges/> (11.11.2025)
- Forbes Kaprive, J.; Krishnamurthy, K. (2026): Biochemistry, Peptide. In: *StatPearls. Treasure Island*
- Frazer, J. et al. (2021): Disease variant prediction with deep generative models of evolutionary data. In: *Nature* 599(7883), S.91–95, <https://doi.org/10.1038/s41586-021-04043-8>
- Fred Hutch Cancer Center (2025): Cancer Screening Research Network. <https://www.fredhutch.org/en/research/institutes-networks-ircs/cancer-screening-research-network.html> (22.7.2025)
- Frischknecht, F. (2003): The history of biological warfare. Human experimentation, modern nightmares and lone madmen in the twentieth century. In: *EMBO reports* 4 Spec No(Suppl 1), S.S47-52, <https://doi.org/10.1038/sj.embor.embor849>
- Fu, C.; Chen, Q. (2025): The future of pharmaceuticals: Artificial intelligence in drug discovery and development. In: *Journal of Pharmaceutical Analysis* 15(8), Art. 101248, <https://doi.org/10.1016/j.jpha.2025.101248>
- Fu, X.; Shen, Y. (2024): Synthetic Genomics: Repurposing Biological Systems for Applications in Engineering Biology. In: *ACS Synthetic Biology* 13(5), S.1394–1399, <https://doi.org/10.1021/acssynbio.4c00006>
- Galanie, S. et al. (2015): Complete biosynthesis of opioids in yeast. In: *Science* 349(6252), S.1095–1100, <https://doi.org/10.1126/science.aac9373>
- Gao, Y.; Liu, M. (2024): Application of machine learning based genome sequence analysis in pathogen identification. In: *Frontiers in Microbiology* 15, Art. 1474078, <https://doi.org/10.3389/fmicb.2024.1474078>
- Garfinkel, M. S. et al. (2007): Synthetic genomics | options for governance. In: *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 5(4), S.359–362, <https://doi.org/10.1089/bsp.2007.0923>
- Gauthier, J. et al. (2019): A brief history of bioinformatics. In: *Briefings in Bioinformatics* 20(6), S.1981–1996, <https://doi.org/10.1093/bib/bby063>
- Ge, C. et al. (2026): A deep learning framework (CreoPep) for target-specific design and optimization of conotoxin peptides. In: *Communications Chemistry* 9, Art. 82, <https://doi.org/10.1038/s42004-025-01885-5>
- Geissler, E. et al. (Hg.) (1999): *Biological and Toxin Weapons: Research, Development and Use from the Middle Ages to 1945*. Oxford

- Geno (2025): The Better BDO. <https://www.genomatica.com/bdo/> (6.6.2025)
- Gentile, F. et al. (2022): Artificial intelligence-enabled virtual screening of ultra-large chemical libraries with deep docking. In: *Nature Protocols* 17(3), S. 672–697, <https://doi.org/10.1038/s41596-021-00659-2>
- GHSA (o. J.a): Biosafety and Biosecurity Action Package Prevent-3 (APP3). Global Health Security Agenda, <https://globalhealthsecurityagenda.org/biosecurity-biosafety/> (7.1.2026)
- GHSA (o. J.b): Global Health Security Agenda. What is the Global Health Security Agenda? Global Health Security Agenda, <https://globalhealthsecurityagenda.org/about/> (7.1.2026)
- Gibney, E. (2025): China wants to lead the world on AI regulation – will the plan work? In: *Nature* 648(8094), S. 503–505, <https://doi.org/10.1038/d41586-025-03902-y>
- GlobalData (2023): Geopolitical conflicts, inflation, and drug pricing pressures will be top challenges for pharma industry growth in 2024, finds GlobalData. GlobalData, <https://www.globaldata.com/media/pharma/geopolitical-conflicts-inflation-drug-pricing-pressure-will-top-challenges-pharma-industry-growth-2024-finds-globaldata/> (23.5.2025)
- GO4GHP (o. J.): Willkommen auf der GO4GHP-Plattform. German Online Platform for Global Health Protection, <https://go4ghp.de/de> (29.5.2026)
- Goh, B. (2025): China proposes new global AI cooperation organisation. Reuters, <https://www.reuters.com/world/china/china-proposes-new-global-ai-cooperation-organisation-2025-07-26/> (2.6.2026)
- Google Cloud (2025): What is an AI agent? <https://cloud.google.com/discover/what-are-ai-agents> (18.6.2025)
- Google DeepMind (2025a): Gemini 3 Pro Frontier Safety Framework Report. https://storage.googleapis.com/deepmind-media/gemini/gemini_3_pro_fsf_report.pdf (29.5.2026)
- Google DeepMind (2025b): Gemini. <https://deepmind.google/models/gemini/> (27.6.2025)
- Gordon, D. et al. (1998): Consed: a graphical tool for sequence finishing. In: *Genome Research* 8(3), S. 195–202, <https://doi.org/10.1101/gr.8.3.195>
- Goshisht, M. K. (2024): Machine Learning and Deep Learning in Synthetic Biology: Key Architectures, Applications, and Challenges. In: *ACS Omega* 9(9), S. 9921–9945, <https://doi.org/10.1021/acsomega.3c05913>
- Götting, J. et al. (2025): Virology Capabilities Test (VCT): A Multimodal Virology Q&A Benchmark. arXiv, <https://doi.org/10.48550/arXiv.2504.16137>
- GOV.UK (2024): UK screening guidance on synthetic nucleic acids for users and providers. <https://www.gov.uk/government/publications/uk-screening-guidance-on-synthetic-nucleic-acids/uk-screening-guidance-on-synthetic-nucleic-acids-for-users-and-providers> (28.1.2026)
- GOV.UK (2025): Efforts to share best practices on AI measurement and evaluations driven forward through the International Network for Advanced AI Measurement, Evaluation and Science. <https://www.gov.uk/government/news/efforts-to-share-best-practices-on-ai-measurement-and-evaluations-driven-forward-through-the-international-network-for-advanced-ai-measurement-evaluation> (21.1.2026)
- GOV.UK (o. J.): The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. Stand 13.2.2025, <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023> (30.6.2026)
- Graham, T. (2002): Biological Weapons and International Law. In: *Science* 295(5564), S. 2325–2325, <https://doi.org/10.1126/science.295.5564.2325>

- Griffin, B. D. et al. (2019): Establishment of an RNA polymerase II-driven reverse genetics system for Nipah virus strains from Malaysia and Bangladesh. In: *Scientific Reports* 9, Art. 11171, <https://doi.org/10.1038/s41598-019-47549-y>
- Griffin, R. (2024): AI-Made Bioweapons Are Washington's Latest Security Obsession. Bloomberg, <https://www.bloomberg.com/news/features/2024-08-02/national-security-threat-from-ai-made-bioweapons-grips-us-government> (4.3.2026)
- Gronvall, G. K. et al. (2022): The Biological Weapons Convention should endorse the Tianjin Biosecurity Guidelines for Codes of Conduct. In: *Trends in Microbiology* 30(12), S. 1119–1120, <https://doi.org/10.1016/j.tim.2022.09.014>
- Guillemin, J. (2017): The 1925 Geneva Protocol: China's CBW Charges Against Japan at the Tokyo War Crimes Tribunal. In: Friedrich, B. et al. (Hg.): *One Hundred Years of Chemical Warfare: Research, Deployment, Consequences*. Cham, S. 273–286, https://doi.org/10.1007/978-3-319-51664-6_15
- Guo, M. et al. (2025): ConoDL: a deep learning framework for rapid generation and prediction of conotoxins. In: *Journal of Computer-Aided Molecular Design* 39, Art. 4, <https://doi.org/10.1007/s10822-024-00582-0>
- Gupta, A. et al. (2022): MP4: a machine learning based classification tool for prediction and functional annotation of pathogenic proteins from metagenomic and genomic datasets. In: *BMC Bioinformatics* 23, Art. 507, <https://doi.org/10.1186/s12859-022-05061-7>
- Gupta, P. et al. (2024): Generative AI: A systematic review using topic modelling techniques. In: *Data and Information Management* 8(2), Art. 100066, <https://doi.org/10.1016/j.dim.2024.100066>
- Haeck, P. (2026): Dozens of countries steer clear of safety commitment in global AI pledge. Politico, <https://www.politico.com/news/2026/02/21/dozens-of-countries-steer-clear-of-safety-commitment-in-global-ai-pledge-00792298> (23.2.2026)
- Halldorsson, B. V. et al. (2022): The sequences of 150,119 genomes in the UK Biobank. In: *Nature* 607(7920), S. 732–740, <https://doi.org/10.1038/s41586-022-04965-x>
- Hamedirad, M. et al. (2019): Towards a fully automated algorithm driven platform for biosystems design. In: *Nature Communications* 10, Art. 5150, <https://doi.org/10.1038/s41467-019-13189-z>
- Hamelin, D. J. et al. (2025): Predicting pathogen evolution and immune evasion in the age of artificial intelligence. In: *Computational and Structural Biotechnology Journal* 27, S. 1370–1382, <https://doi.org/10.1016/j.csbj.2025.03.044>
- Harris, E. D. et al. (2016): Chapter 2: Dual-Use Threats: The Case of Biological Technology. In: Elisa D. Harris, ed., *Governance of Dual-Use Technologies: Theory and Practice*. Cambridge
- Hayes, T. et al. (2025): Simulating 500 million years of evolution with a language model. In: *Science* 387(6736), S. 850–858, <https://doi.org/10.1126/science.ads0018>
- Heller, P. (2024): KI und Massenvernichtungswaffen: Wie real ist die Gefahr? FAZ, <https://www.faz.net/aktuell/wissen/ki-und-massenvernichtungswaffen-wie-real-ist-die-gefahr-110112886.html> (24.2.2026)
- Henckaerts, J.-M.; Doswald-Beck, L. (2009): *Customary International Humanitarian Law – Volume 1: Rules*. International Committee of the Red Cross, Cambridge
- Herden, B.; Göpel, G. (2026): Biowaffen im KI-Zeitalter: Eine ernst zu nehmende Gefahr. *Tagespiegel*, <https://epaper.tagesspiegel.de/index.html?articleId=doc84n7nhic0wwly8qwrql&a> (24.2.2026)

- Herfst, S. et al. (2012): Airborne transmission of influenza A/H5N1 virus between ferrets. In: *Science* 336(6088), S. 1534–1541, <https://doi.org/10.1126/science.1213362>
- HHS (2010): Screening Framework Guidance for Providers of Synthetic Double-Stranded DNA. U.S. Department of Health & Human Services, Washington, D.C.
- HHS (2020): Biosafety in Microbiological and Biomedical Laboratories. U.S. Department of Health and Human Services. Public Health Service, Centers for Disease Control and Prevention, National Institutes of Health, Washington, D.C.
- HHS (2023): Screening Framework Guidance for Providers and Users of Synthetic Nucleic Acids. U.S. Department of Health & Human Services, Washington, D.C.
- Hie, B. L. et al. (2022): Evolutionary velocity with protein language models predicts evolutionary dynamics of diverse proteins. In: *Cell Systems* 13(4), S. 274–285, <https://doi.org/10.1016/j.cels.2022.01.003>
- Hillson, N. et al. (2019): Building a global alliance of biofoundries. In: *Nature Communications* 10, Art. 2040, <https://doi.org/10.1038/s41467-019-10079-2>
- Ho, A.; Berg, A. (2025): Do the biorisk evaluations of AI labs actually measure the risk of developing bioweapons? *Epoch AI*, <https://epoch.ai/gradient-updates/do-the-biorisk-evaluations-of-ai-labs-actually-measure-the-risk-of-developing-bioweapons> (23.10.2025)
- Holland, M. (2023): KI: Studienanfänger lassen sich von ChatGPT das Auslösen einer Pandemie erklären. *heise online*, <https://www.heise.de/news/KI-Studienanfaenger-lassen-sich-von-ChatGPT-das-Ausloesen-einer-Pandemie-erklaeren-9196108.html> (31.10.2025)
- Holowko, M. B. et al. (2021): Building a biofoundry. In: *Synthetic Biology* 6(1), Art. ysaa026, <https://doi.org/10.1093/synbio/ysaa026>
- Hombert, J. (2025): Making DeepSeek Speak About Tiananmen. *Social Science Encyclopedia*, <https://www.socialscience.international/making-deepseek-speak-about-tiananmen> (6.11.2025)
- Hong, S. Z. et al. (2026): Measuring Mid-2025 LLM-Assistance on Novice Performance in Biology. *arXiv*, <https://doi.org/10.48550/arXiv.2602.16703>
- Hou, X. et al. (2024): Using artificial intelligence to document the hidden RNA virosphere. In: *Cell* 187(24), S. 6929–6942, <https://doi.org/10.1016/j.cell.2024.09.027>
- Houston, F.; Andréoletti, O. (2019): Animal prion diseases: the risks to human health. In: *Brain Pathology* 29(2), S. 248–262, <https://doi.org/10.1111/bpa.12696>
- HSF Kramer (2026a): AI Tracker. European Union. Herbert Smith Freehills Kramer, <https://www.hsfkramer.com/insights/reports/ai-tracker/eu> (15.5.2026)
- HSF Kramer (2026b): AI Tracker. Mainland China. Herbert Smith Freehills Kramer, <https://www.hsfkramer.com/insights/reports/ai-tracker/prc> (15.5.2026)
- Hsieh, T.-C. et al. (2019): PEDIA: prioritization of exome data by image analysis. In: *Genetics in Medicine* 21(12), S. 2807–2814, <https://doi.org/10.1038/s41436-019-0566-2>
- Hsieh, T.-C. et al. (2022): GestaltMatcher facilitates rare disease matching using facial phenotype descriptors. In: *Nature Genetics* 54(3), S. 349–357, <https://doi.org/10.1038/s41588-021-01010-x>
- Hu, B.; Au, A. (2025): China resets the path to comprehensive AI governance. *East Asia Forum*, <https://doi.org/https://doi.org/10.59425/eabc.1766700000>
- Huang, D. et al. (2024): From Large Language Models to Large Multimodal Models: A Literature Review. In: *Applied Sciences* 14(12), Art. 5068, <https://doi.org/10.3390/app14125068>
- Huang, K. et al. (2025): Biomni: A General-Purpose Biomedical AI Agent. *bioRxiv*, <https://doi.org/10.1101/2025.05.30.656746>

- Hughes, R. A.; Ellington, A. D. (2017): Synthetic DNA Synthesis and Assembly: Putting the Synthetic in Synthetic Biology. In: Cold Spring Harbor Perspectives in Biology 9(1), Art. a023812, <https://doi.org/10.1101/cshperspect.a023812>
- Hummel, K. (2016): Remotely Piloted Innovation: Terrorism, Drones and Supportive Technology. Combating Terrorism Center at West Point, <https://ctc.westpoint.edu/remotely-piloted-innovation-terrorism-drones-and-supportive-technology/> (14.10.2025)
- Hummel, K. (2025): The Rising Threat of Non-State Actor Commercial Drone Use: Emerging Capabilities and Threats. Combating Terrorism Center at West Point, <https://ctc.westpoint.edu/the-rising-threat-of-non-state-actor-commercial-drone-use-emerging-capabilities-and-threats/> (14.10.2025)
- Hutson, M. (2025): Biothreat hunters catch dangerous DNA before it gets made. In: Nature 646(8084), S. 503–505, <https://doi.org/10.1038/d41586-025-03230-1>
- IAP (2021): IAP endorses Tianjin Biosecurity Guidelines. InterAcademy Partnership, <https://www.interacademies.org/news/iap-endorses-tianjin-biosecurity-guidelines> (14.1.2026)
- IBBIS (o.J.): IBBIS calls for synthesis screening and international standards in EU Biotech Act. International Biosecurity and Biosafety Initiative for Science, <https://ibbis.bio/ibbis-calls-for-synthesis-screening-and-international-standards-in-eu-biotech-act/> (2.7.2026)
- IBM (2025): What is Multimodal AI? <https://www.ibm.com/think/topics/multimodal-ai> (14.5.2025)
- ICRC (2025): Welcome to the Customary IHL Database. International Committee of the Red Cross, <https://ihl-databases.icrc.org/en/customary-ihl> (22.12.2025)
- IGSC (2009): Harmonized Screening Protocol - Gene Sequence & Customer Screening to Promote Biosecurity. https://genesynthesisconsortium.org/wp-content/uploads/IGSC-Harmonized-Screening-Protocol-11_18_09.pdf (14.1.2026)
- IGSC (2024): Harmonized Screening Protocol v3.0. <https://genesynthesisconsortium.org/wp-content/uploads/IGSC-Harmonized-Screening-Protocol-v3.0-1.pdf> (14.1.2026)
- Ikonomova, S. P. et al. (2026): Experimental evaluation of AI-driven protein design risks using safe biological proxies. bioRxiv, <https://doi.org/10.1101/2025.05.15.654077>
- IKRK (2023): Humanitäres Völkerrecht – Häufig gestellte Fragen zu den Regeln des Krieges. Internationales Komitee vom Roten Kreuz, <https://www.icrc.org/de/document/humanitaeres-voelkerrecht-haeufige-fragen-genfer-konventionen> (14.1.2026)
- Imai, M. et al. (2012): Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets. In: Nature 486(7403), S. 420–428, <https://doi.org/10.1038/nature10831>
- Inglesby, T. V. et al. (2002): Anthrax as a Biological Weapon, 2002 Updated Recommendations for Management. In: JAMA 287(17), S. 2236–2252, <https://doi.org/10.1001/jama.287.17.2236>
- Ingraham, J. B. et al. (2023): Illuminating protein space with a programmable generative model. In: Nature 623(7989), S. 1070–1078, <https://doi.org/10.1038/s41586-023-06728-8>
- IPD (2023): Results from our summit on responsible AI. Institute for Protein Design, <https://www.ipd.uw.edu/2023/10/responsible-ai-summit/> (21.1.2026)
- ISO (2024): ISO 20688-2:2024: Biotechnology – Nucleic acid synthesis, Part 2: Requirements for the production and quality control of synthesized gene fragments, genes, and genomes. International Organization for Standardization, <https://www.iso.org/standard/75852.html> (28.1.2026)
- Ito, J. et al. (2025): A protein language model for exploring viral fitness landscapes. In: Nature Communications 16, Art. 4236, <https://doi.org/10.1038/s41467-025-59422-w>

- IUPAC (2025): aerosol. International Union of Pure and Applied Chemistry, <https://doi.org/10.1351/goldbook.A00176>
- Ivanenkov, Y. A. et al. (2023): Chemistry42: An AI-Driven Platform for Molecular Design and Optimization. In: *Journal of Chemical Information and Modeling* 63(3), S. 695–701, <https://doi.org/10.1021/acs.jcim.2c01191>
- Ivanov, I. (2024): BioLP-bench: Measuring understanding of biological lab protocols by large language models., <https://doi.org/10.1101/2024.08.21.608694>
- Ivanov, I.; Volkov, D. (2025): Resurrecting saturated LLM benchmarks with adversarial encoding. *arXiv*, <https://doi.org/10.48550/arXiv.2502.06738>
- Jackson, S. S. et al. (2019): The accelerating pace of biotech democratization. In: *Nature Biotechnology* 37(12), S. 1403–1408, <https://doi.org/10.1038/s41587-019-0339-0>
- Jaganathan, K. et al. (2019): Predicting Splicing from Primary Sequence with Deep Learning. In: *Cell* 176(3), S. 535–548, <https://doi.org/10.1016/j.cell.2018.12.015>
- Jakob, U. et al. (2024): Investigation of Alleged Use of Biological Weapons – Strengthening the UN Secretary-General’s Mechanism. PRIF – Leibniz-Institut für Friedens- und Konfliktforschung, <https://doi.org/10.48809/prifrep2407>
- Jakob, U. et al. (2025): Applying Ethics in the Handling of Dual Use Research: The Case of Germany. In: *Research Ethics* 21(2), S. 228–244, <https://doi.org/10.1177/17470161241261044>
- James, J. S. et al. (2025): The design and engineering of synthetic genomes. In: *Nature Reviews Genetics* 26(5), S. 298–319, <https://doi.org/10.1038/s41576-024-00786-y>
- Jamshidi, A. et al. (2022): Evaluation of cell-free DNA approaches for multi-cancer early detection. In: *Cancer Cell* 40(12), S. 1537–1549, <https://doi.org/10.1016/j.ccell.2022.10.022>
- Jayatunga, M. K. P. et al. (2022): AI in small-molecule drug discovery: a coming wave? In: *Nature Reviews Drug Discovery* 21(3), S. 175–176, <https://doi.org/10.1038/d41573-022-00025-1>
- Jefferson, C. et al. (2014a): Synthetic Biology and Biosecurity: How scared should we be? King’s College London, London
- Jefferson, C. et al. (2014b): Synthetic Biology and Biosecurity: Challenging the „Myths“. In: *Frontiers in Public Health* 2, Art. 115, <https://doi.org/10.3389/fpubh.2014.00115>
- Jeremias, G. et al. (2016): Guest Post: Spotlight on Syria’s Biological Weapons. *Arms Control Wonk*, <http://www.armscontrolwonk.com/archive/1201010/guest-post-spotlight-on-syrias-biological-weapons/> (9.10.2025)
- Jessop-Fabre, M. M.; Sonnenschein, N. (2019): Improving Reproducibility in Synthetic Biology. In: *Frontiers in Bioengineering and Biotechnology* 7, Art. 18, <https://doi.org/10.3389/fbioe.2019.00018>
- Jha, S. (2025): Hyderabad Terror Plot: Ricin Strike Plan to Divide South India. *Deccan Herald*, <https://www.deccanherald.com/india/telangana/hyderabad-ricin-terror-plotter-wanted-to-separate-south-india-from-rest-of-country-3804094> (11.5.2026)
- juliensuze (2026): Graph Neural Networks (GNN): Was ist das? Liora, <https://datascientest.com/de/graph-neural-networks-gnn-was-ist-das> (27.5.2025)
- Juling, D. (2023): Future Bioterror and Biowarfare Threats for NATO’s Armed Forces until 2030. *Journal of Advanced Military Studies*, <https://doi.org/10.21140/mcu.20231401005>
- Jumper, J. et al. (2021): Highly accurate protein structure prediction with AlphaFold. In: *Nature* 596(7873), S. 583–589, <https://doi.org/10.1038/s41586-021-03819-2>
- Justen, L. (2025): LLMs Outperform Experts on Challenging Biology Benchmarks. *arXiv*, <https://doi.org/10.48550/arXiv.2505.06108>

- Kaiser, J. (2024): White House overhauls rules for risky pathogen studies. *Science*, <https://www.science.org/content/article/white-house-overhauls-rules-risky-pathogen-studies> (16.1.2026)
- Kane, A.; Parker, M. T. (2024): Screening State of Play: The Biosecurity Practices of Synthetic DNA Providers. In: *Applied Biosafety: Journal of the American Biological Safety Association* 29(2), S. 85–95, <https://doi.org/10.1089/apb.2023.0027>
- Kavanagh, K. (2025): World’s first AI-designed viruses a step towards AI-generated life. In: *Nature* 646(8083), Art. 16, <https://www.nature.com/articles/d41586-025-03055-y>
- Kavianpour, S. et al. (2022): Next-Generation Capabilities in Trusted Research Environments: Interview Study. In: *Journal of Medical Internet Research* 24(9), Art. e33720, <https://doi.org/10.2196/33720>
- Keiichi, T. (2005): Unit 731 and the Japanese Imperial Army’s Biological Warfare Program. In: *The Asia-Pacific Journal* 3(11), Art. e24, <https://doi.org/https://doi.org/10.1017/S155746600500361X>
- Kelley, M. L. et al. (2016): Versatility of chemically synthesized guide RNAs for CRISPR-Cas9 genome editing. In: *Journal of Biotechnology* 233, S. 74–83, <https://doi.org/10.1016/j.jbiotec.2016.06.011>
- Kendrew, J. C. et al. (1958): A three-dimensional model of the myoglobin molecule obtained by x-ray analysis. In: *Nature* 181(4610), S. 662–666, <https://doi.org/10.1038/181662a0>
- Kendrew, J. C. et al. (1960): Structure of myoglobin: A three-dimensional Fourier synthesis at 2 Å resolution. In: *Nature* 185(4711), S. 422–427, <https://doi.org/10.1038/185422a0>
- Kersting, K. (2018): Machine Learning and Artificial Intelligence: Two Fellow Travelers on the Quest for Intelligent Behavior in Machines. In: *Frontiers in Big Data* 1, Art. 6, <https://doi.org/10.3389/fdata.2018.00006>
- Kim, G. B. et al. (2020): Machine learning applications in systems metabolic engineering. In: *Current Opinion in Biotechnology* 64, S. 1–9, <https://doi.org/10.1016/j.copbio.2019.08.010>
- Kim, G. B. et al. (2023a): Metabolic engineering for sustainability and health. In: *Trends in Biotechnology* 41(3), S. 425–451, <https://doi.org/10.1016/j.tibtech.2022.12.014>
- Kim, H. S. et al. (2024): Recent advances in CRISPR-based functional genomics for the study of disease-associated genetic variants. In: *Experimental & Molecular Medicine* 56(4), S. 861–869, <https://doi.org/10.1038/s12276-024-01212-3>
- Kim, J. et al. (2025): Fast-Tracking Vaccine Manufacturing: CEPI’s Rapid Response Framework for the 100 Days Mission. In: *Vaccines* 13(8), Art. 849, <https://doi.org/10.3390/vaccines13080849>
- Kim, S. Y. et al. (2023b): Cancer signature ensemble integrating cfDNA methylation, copy number, and fragmentation facilitates multi-cancer early detection. In: *Experimental & Molecular Medicine* 55(11), S. 2445–2460, <https://doi.org/10.1038/s12276-023-01119-5>
- King, R. (2022): *Rajneeshpuram. Inside the cult of Bhagwan and its failed American utopia*. Chicago
- King, R. D. et al. (2004): Functional genomic hypothesis generation and experimentation by a robot scientist. In: *Nature* 427(6971), S. 247–252, <https://doi.org/10.1038/nature02236>
- King, R. D. et al. (2009): The Automation of Science. In: *Science* 324(5923), S. 85–89, <https://doi.org/10.1126/science.1165620>
- King, S. H. et al. (2025): Generative design of novel bacteriophages with genome language models. *bioRxiv*, <https://doi.org/10.1101/2025.09.12.675911>

- Ko, K. K. K. et al. (2022): Metagenomics-enabled microbial surveillance. In: *Nature Microbiology* 7(4), S. 486–496, <https://doi.org/10.1038/s41564-022-01089-w>
- König, H. et al. (2021): AI models and the future of genomic research and medicine: True sons of knowledge? Artificial intelligence needs to be integrated with causal conceptions in biomedicine to harness its societal benefits for the field. In: *BioEssays* 43(10), Art. e2100025, <https://doi.org/10.1002/bies.202100025>
- Köpke, M.; Simpson, S. D. (2020): Pollution to products: recycling of ,above ground' carbon by gas fermentation. In: *Current Opinion in Biotechnology* 65, S. 180–189, <https://doi.org/10.1016/j.copbio.2020.02.017>
- Kozlov, M. (2024): US funders to tighten oversight of controversial ,gain of function' research. In: *Nature* 629(8012), S. 510–511, <https://doi.org/10.1038/d41586-024-01377-x>
- KP Jayatunga, M. et al. (2024): How successful are AI-discovered drugs in clinical trials? A first analysis and emerging lessons. In: *Drug Discovery Today* 29(6), Art. 104009, <https://doi.org/10.1016/j.drudis.2024.104009>
- Kraemer, M. U. G. et al. (2025): Artificial intelligence for modelling infectious disease epidemics. In: *Nature* 638(8051), S. 623–635, <https://doi.org/10.1038/s41586-024-08564-w>
- Krasny, J. (2024): The Biological Weapons Convention: Challenges and Opportunities. The Geneva Centre for Security Policy, Policy Brief 15, Genf
- Krasny, J. (2025): Strengthening the Biological Weapons Convention: Transparency and Denial as Complementary Approaches. In: *Journal for Peace and Nuclear Disarmament* 8(2), S. 341–357, <https://doi.org/10.1080/25751654.2025.2602260>
- Krishna, R. et al. (2024): Generalized biomolecular modeling and design with RoseTTAFold All-Atom. In: *Science* 384(6693), Art. ead12528, <https://doi.org/10.1126/science.adl2528>
- Krishnan, A. et al. (2025): A generative deep learning approach to de novo antibiotic design. In: *Cell* 188(21), S. 5962–5979, <https://doi.org/10.1016/j.cell.2025.07.033>
- Kroepke, L. (2025): Regulatory Gaps in Benchtop Nucleic Acid Synthesis Create Biosecurity Vulnerabilities. Arms Control Association, <https://www.armscontrol.org/blog/2025-11-24/regulatory-gaps-benchtop-nucleic-acid-synthesis-create-biosecurity-vulnerabilities> (30.6.2026)
- Krokidis, M. G. et al. (2025): AlphaFold3: An Overview of Applications and Performance Insights. In: *International Journal of Molecular Sciences* 26(8), Art. 3671, <https://doi.org/10.3390/ijms26083671>
- Kuiken, T. (2024): Oversight of Laboratory Biosafety and Biosecurity: Current Policies and Options for Congress. Congressional Research Service, Washington, D.C.
- Kuiken, T. (2025): Oversight of Gain-of-Function Research with Pathogens: Issues for Congress. Congressional Research Service, Washington, D.C.
- La Maison Élysée (2025): Pledge for a Trustworthy AI in the World of Work. <https://www.elysee.fr/emmanuel-macron/2025/02/11/pledge-for-a-trustworthy-ai-in-the-world-of-work> (30.6.2026)
- Lamb, K. D. et al. (2024): From a single sequence to evolutionary trajectories: protein language models capture the evolutionary potential of SARS-CoV-2 protein sequences. *bioRxiv*, <https://doi.org/10.1101/2024.07.05.602129>
- Lambert, C. A. (2020): The Chemical and Biological Attack Threat of Commercial Unmanned Aircraft Systems. Association of the United States Army, Arlington
- Lander, E. S. et al. (2001): Initial sequencing and analysis of the human genome. In: *Nature* 409(6822), S. 860–921, <https://doi.org/10.1038/35057062>

- Landsverk, G. (2023): AI chatbots helped college students come up with new pandemic pathogens they could spread. Business Insider, <https://www.businessinsider.com/ai-chatbots-helped-suggest-viruses-to-start-a-new-pandemic-2023-6> (31.10.2025)
- Lappalainen, T.; MacArthur, D. G. (2021): From variant to function in human disease genetics. In: *Science* 373(6562), S. 1464–1468, <https://doi.org/10.1126/science.abi8207>
- Latham & Watkins (2025): BIOSECURE Act Becomes Law, Limiting Grants With „Biotechnology Companies of Concern“. Latham & Watkins, <https://www.lw.com/en/insights/biosecure-act-becomes-law-limiting-grants-with-biotechnology-companies-of-concern> (20.1.2026)
- Lauko, A. et al. (2025): Computational design of serine hydrolases. In: *Science* 388(6744), Art. eadu2454, <https://doi.org/10.1126/science.adu2454>
- Laurent, J. M. et al. (2024): LAB-Bench: Measuring Capabilities of Language Models for Biology Research. arXiv, <https://doi.org/10.48550/arXiv.2407.10362>
- Le, H.-G. et al. (2025): Synthetic biology strategies for sustainable bioplastic production by yeasts. In: *Journal of Microbiology* 63(3), Art. e2501022, <https://doi.org/10.71150/jm.2501022>
- Ledford, H. (2010): Garage biotech: Life hackers. In: *Nature* 467(7316), S. 650–652, <https://doi.org/10.1038/467650a>
- Lee, Y.-C. J. et al. (2022): Peptide Toxins as Biothreats and the Potential for AI Systems to Enhance Biosecurity. In: *Frontiers in Bioengineering and Biotechnology* 10, Art. 860390, <https://doi.org/10.3389/fbioe.2022.860390>
- Lee, Y.-C. J. et al. (2025): Documenting Cloud Labs and Examining How Remotely Operated Automated Laboratories Could Enable Bad Actors. RAND Corporation, Santa Monica
- Lee, Y.-C. J.; Del Castello, B. (2024): Robust Biosecurity Measures Should Be Standardized at Scientific Cloud Labs. RAND Corporation, <https://www.rand.org/pubs/commentary/2024/11/robust-biosecurity-measures-should-be-standardized.html> (4.12.2025)
- Leitenberg, M. (2001): Biological Weapons in the Twentieth Century: A Review and Analysis. In: *Critical Reviews in Microbiology* 27(4), S. 267–320, <https://doi.org/10.1080/20014091096774>
- Lele, A. et al. (2024): The Focus and Function of BWC Verification. The United Nations Institute for Disarmament Research, Genf
- Leopoldina; DFG (2022a): Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung – Vierter Tätigkeitsbericht zum 1. November 2022. Nationale Akademie der Wissenschaften Leopoldina und Deutsche Forschungsgemeinschaft, Halle
- Leopoldina; DFG (2022b): Wissenschaftsfreiheit und Wissenschaftsverantwortung – Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung / Scientific Freedom and Scientific Responsibility – Recommendations for Handling of Security-Relevant Research. Nationale Akademie der Wissenschaften Leopoldina und Deutsche Forschungsgemeinschaft, Halle
- Leopoldina; DFG (2024): Wissenschaftsfreiheit und Sicherheitsinteressen in Zeiten geopolitischer Polarisierung – Fünfter Tätigkeits- und Sachstandsbericht des Gemeinsamen Ausschusses von DFG und Leopoldina zum 1. November 2024. Nationale Akademie der Wissenschaften Leopoldina und Deutsche Forschungsgemeinschaft, Halle
- Lev, O. (2019): Regulating dual-use research: Lessons from Israel and the United States. In: *Journal of Biosafety and Biosecurity* 1(2), S. 80–85, <https://doi.org/10.1016/j.jobbb.2019.06.001>
- Levy, J. I. et al. (2023): Wastewater surveillance for public health. In: *Science* 379(6627), S. 26–27, <https://doi.org/10.1126/science.ade2503>

- Li, B. Y. et al. (1992): High-level expression and simplified purification of recombinant ricin A chain. In: *Protein Expression and Purification* 3(5), S.386–394, [https://doi.org/10.1016/s1046-5928\(05\)80040-3](https://doi.org/10.1016/s1046-5928(05)80040-3)
- Li, K. et al. (2023): CRISPR-based functional genomics screening in human-pluripotent-stem-cell-derived cell types. In: *Cell Genomics* 3(5), Art. 100300, <https://doi.org/10.1016/j.xgen.2023.100300>
- Li, N. et al. (2024): The WMDP Benchmark: Measuring and Reducing Malicious Use with Unlearning. *Proceedings of Machine Learning Research*. Volume 235, <https://proceedings.mlr.press/v235/li24bc.html> (30.10.2025)
- Liang, F. et al. (2025): Elucidation of the final steps in Taxol biosynthesis and its biotechnological production. In: *Nature Synthesis* 4, S.1212–1222, <https://doi.org/10.1038/s44160-025-00800-z>
- Liew, F. E. et al. (2022): Carbon-negative production of acetone and isopropanol by gas fermentation at industrial pilot scale. In: *Nature Biotechnology* 40(3), S.335–344, <https://doi.org/10.1038/s41587-021-01195-w>
- Lin, Z. et al. (2023): Evolutionary-scale prediction of atomic-level protein structure with a language model. In: *Science* 379(6637), S. 1123–1130, <https://doi.org/10.1126/science.ade2574>
- Linder, J. et al. (2025): Predicting RNA-seq coverage from DNA sequence as a unifying model of gene regulation. In: *Nature Genetics* 57(4), S.949–961, <https://doi.org/10.1038/s41588-024-02053-6>
- Lipsitch, M.; Moxon, E. R. (1997): Virulence and transmissibility of pathogens: what is the relationship? In: *Trends in Microbiology* 5(1), S.31–37, [https://doi.org/10.1016/S0966-842X\(97\)81772-6](https://doi.org/10.1016/S0966-842X(97)81772-6)
- Lister, T. et al. (2020): Russian opposition leader Alexey Navalny dupes spy into revealing how he was poisoned. CNN, <https://www.cnn.com/2020/12/21/europe/russia-navalny-poisoning-underpants-ward> (10.12.2025)
- Liu, B. et al. (2024): Exploring treatment options in cancer: tumor treatment strategies. In: *Signal Transduction and Targeted Therapy* 9, Art. 175, <https://doi.org/10.1038/s41392-024-01856-7>
- Liu, G. et al. (2023): Deep learning-guided discovery of an antibiotic targeting *Acinetobacter baumannii*. In: *Nature Chemical Biology* 19(11), S.1342–1350, <https://doi.org/10.1038/s41589-023-01349-8>
- Llama Team, AI @ Meta (2024): The Llama 3 Herd of Models. arXiv, <https://doi.org/10.48550/arXiv.2407.21783>
- Loeffler, H. H. et al. (2024): Reinvent 4: Modern AI-driven generative molecule design. In: *Journal of Cheminformatics* 16, Art. 20, <https://doi.org/10.1186/s13321-024-00812-5>
- Lovelock, S. L. et al. (2022): The road to fully programmable protein catalysis. In: *Nature* 606(7912), S.49–58, <https://doi.org/10.1038/s41586-022-04456-z>
- Lowe, D. (2024): AI Drugs So Far. *Science*, <https://www.science.org/content/blog-post/ai-drugs-so-far> (30.5.2025)
- Lu, D. (2025): We tried out DeepSeek. It worked well, until we asked it about Tiananmen Square and Taiwan. *The Guardian*, <https://www.theguardian.com/technology/2025/jan/28/we-tried-out-deepseek-it-works-well-until-we-asked-it-about-tiananmen-square-and-taiwan> (6.11.2025)
- Lu, H. et al. (2024): Cell factory design with advanced metabolic modelling empowered by artificial intelligence. In: *Metabolic Engineering* 85, S.61–72, <https://doi.org/10.1016/j.ymben.2024.07.003>

- Luo, R. et al. (2022): BioGPT: Generative Pre-trained Transformer for Biomedical Text Generation and Mining. In: Briefings in Bioinformatics 23(6), Art. bbac409, <https://doi.org/10.1093/bib/bbac409>
- Lyu, S. et al. (2024): Variational autoencoder for design of synthetic viral vector serotypes. In: Nature Machine Intelligence 6(2), S. 147–160, <https://doi.org/10.1038/s42256-023-00787-2>
- Ma, L. et al. (2024a): Liquid biopsy in cancer: current status, challenges and future prospects. In: Signal Transduction and Targeted Therapy 9, Art. 336, <https://doi.org/10.1038/s41392-024-02021-w>
- Ma, Y. et al. (2024b): Automated high-throughput DNA synthesis and assembly. In: Heliyon 10(6), Art. e26967, <https://doi.org/10.1016/j.heliyon.2024.e26967>
- Madani, A. et al. (2023): Large language models generate functional protein sequences across diverse families. In: Nature Biotechnology 41(8), S. 1099–1106, <https://doi.org/10.1038/s41587-022-01618-2>
- Makarova, K. S. et al. (2020): Evolutionary classification of CRISPR–Cas systems: a burst of class 2 and derived variants. In: Nature Reviews Microbiology 18(2), S. 67–83, <https://doi.org/10.1038/s41579-019-0299-x>
- Mallapaty, S. (2025a): Trump freezes ‚gain of function‘ pathogen research – threatening all US virology, critics say. Nature, <https://doi.org/10.1038/d41586-025-01411-6>
- Mallapaty, S. (2025b): What will viruses do next? AI is helping scientists predict their evolution. In: Nature 637(8046), S. 527–528, <https://doi.org/10.1038/d41586-024-04195-3>
- Mao, D. et al. (2024): AI-MARRVEL – A Knowledge-Driven AI System for Diagnosing Mendelian Disorders. In: NEJM AI 1(5), Art. Aloa2300009, <https://doi.org/10.1056/Aloa2300009>
- Martin, H. G. et al. (2023): Perspectives for self-driving labs in synthetic biology. In: Current Opinion in Biotechnology 79, Art. 102881, <https://doi.org/10.1016/j.copbio.2022.102881>
- Matsumoto, G. (2003): Anthrax Powder: State of the Art? In: Science 302(5650), S. 1492–1497, <https://doi.org/10.1126/science.302.5650.1492>
- Matthews, D. (2023): Scientists grapple with risk of artificial intelligence-created pandemics. Science Business, <https://sciencebusiness.net/news/ai/scientists-grapple-risk-artificial-intelligence-created-pandemics> (31.10.2025)
- Mauroni, A.; Cross, G. (2025): Will China Force a Rethink of Biological Warfare? War on the Rocks, <https://warontherocks.com/2025/06/will-china-force-a-rethink-of-biological-warfare/> (10.12.2025)
- Maxam, A. M.; Gilbert, W. (1977): A new method for sequencing DNA. In: Proceedings of the National Academy of Sciences of the United States of America 74(2), S. 560–564, <https://doi.org/10.1073/pnas.74.2.560>
- Mazeika, M. et al. (2024): HarmBench: A Standardized Evaluation Framework for Automated Red Teaming and Robust Refusal. arXiv, <https://doi.org/10.48550/arXiv.2402.04249>
- MeitY (2025): India AI Governance Guidelines. Enabling Safe and Trusted AI Innovation. Ministry of Electronics and Information Technology, <https://static.pib.gov.in/WriteReadData/specificdocs/documents/2025/nov/doc2025115685601.pdf> (30.6.2026)
- Menard, J. et al. (2024): Synthetic biology education and pedagogy: a review of evolving practices in a growing discipline. In: Frontiers in Education 9, Art. 1441720, <https://doi.org/10.3389/educ.2024.1441720>
- Meta (2026): Llama. <https://www.llama.com/> (15.5.2026)

- Mienye, I. D.; Swart, T. G. (2024): A Comprehensive Review of Deep Learning: Architectures, Recent Advances, and Applications. In: *Information* 15(12), Art. 755, <https://doi.org/10.3390/info15120755>
- Ministère de l'Europe et des Affaires Étrangères (2025): Aktionsgipfel zur Künstlichen Intelligenz. <https://www.diplomatie.gouv.fr/de/presse-et-ressources/decouvrir-et-informer/actualites/sommet-pour-l-action-sur-l-intelligence-artificielle> (2.6.2026)
- Mishra, V. (2024): General Assembly adopts landmark resolution on artificial intelligence. United Nations, <https://news.un.org/en/story/2024/03/1147831> (1.6.2026)
- Moulange, R. et al. (2025): Biological Tools and the EU AI Act. Centre for Long-Term Resilience, London
- Mouton, C. A. et al. (2024): The Operational Risks of AI in Large-Scale Biological Attacks: Results of a Red-Team Study. RAND Corporation, Santa Monica
- Mowatt-Larssen, R. (2025): AI Qaeda Weapons of Mass Destruction Threat: Hype or Reality? Belfer Center for Science and International Affairs, Harvard Kennedy School, Cambridge
- MPG (2017): Hinweise und Regeln der Max-Planck-Gesellschaft zum verantwortungsvollen Umgang mit Forschungsfreiheit und Forschungsrisiken. Max-Planck-Gesellschaft zur Förderung der Wissenschaften e.V., München
- MPG (2025): Was ist Synthetische Biologie? Max-Planck-Gesellschaft, <https://www.synthetische-biologie.mpg.de/3036/was-ist-synthetische-biologie> (14.5.2025)
- MTR Legal (2025): Völkerrecht. MTR Legal, <https://www.mtrlegal.com/wiki/voelkerrecht/> (22.12.2025)
- Munsamy, G. et al. (2024): Conditional language models enable the efficient design of proficient enzymes. *bioRxiv*, <https://doi.org/10.1101/2024.05.03.592223>
- Murata, M. et al. (1985): Simultaneous comparison of three protein sequences. In: *Proceedings of the National Academy of Sciences of the United States of America* 82(10), S. 3073–3077, <https://doi.org/10.1073/pnas.82.10.3073>
- Myers, E. W. et al. (2000): A whole-genome assembly of *Drosophila*. In: *Science* 287(5461), S. 2196–2204, <https://doi.org/10.1126/science.287.5461.2196>
- Nab, L. et al. (2024): OpenSAFELY: A platform for analysing electronic health records designed for reproducible research. In: *Pharmacoepidemiology and Drug Safety* 33(6), Art. e5815, <https://doi.org/10.1002/pds.5815>
- Naddaf, M. (2025): Open-source protein structure AI aims to match AlphaFold. *Nature*, <https://doi.org/10.1038/d41586-025-03546-y>
- NAS (2018): Biodefense in the Age of Synthetic Biology. National Academies of Sciences, Engineering, and Medicine, <https://doi.org/10.17226/24890>
- NAS (2024): Artificial Intelligence and Automated Laboratories for Biotechnology: Leveraging Opportunities and Mitigating Risks. *Proceedings of a Workshop—in Brief*. National Academies of Sciences, Engineering, and Medicine, <https://doi.org/10.17226/27469>
- NAS (2025a): Disseminating In Silico and Computational Biological Research: Navigating Benefits and Risks: *Proceedings of a Workshop*. National Academies of Sciences, Engineering, and Medicine, Washington, DC, <https://doi.org/10.17226/29174>
- NAS (2025b): The Age of AI in the Life Sciences: Benefits and Biosecurity Considerations. National Academies of Sciences, Engineering, and Medicine, Washington, D.C.
- National Archives (2024): United States Government Policy for Oversight of Dual Use Research of Concern and Pathogens with Enhanced Pandemic Potential. <https://bidenwhitehouse.ar>

- chives.gov/wp-content/uploads/2024/05/USG-Policy-for-Oversight-of-DURC-and-PEPP.pdf (29.5.2026)
- National Research Council (2009): Responsible Research with Biological Select Agents and Toxins. The National Academies Collection: Reports funded by National Institutes of Health, Washington, D.C.
- Nature methods (2024): Focus on advanced AI in biology. Nature, <https://www.nature.com/collections/ahhdbbhgha> (14.5.2025)
- Neal, R. D. et al. (2022): Cell-Free DNA–Based Multi-Cancer Early Detection Test in an Asymptomatic Screening Population (NHS-Galleri): Design of a Pragmatic, Prospective Randomised Controlled Trial. In: *Cancers* 14(19), Art. 4818, <https://doi.org/10.3390/cancers14194818>
- Needleman, S. B.; Wunsch, C. D. (1970): A general method applicable to the search for similarities in the amino acid sequence of two proteins. In: *Journal of Molecular Biology* 48(3), S. 443–453, [https://doi.org/10.1016/0022-2836\(70\)90057-4](https://doi.org/10.1016/0022-2836(70)90057-4)
- Nelson, C.; Rose, S. (2023): Understanding AI-Facilitated Biological Weapon Development. The Centre for Long-Term Resilience, London
- Nevers, Y. et al. (2023): Protein length distribution is remarkably uniform across the tree of life. In: *Genome Biology* 24, Art. 135, <https://doi.org/10.1186/s13059-023-02973-2>
- Newey, S.; Nuki, P. (2023): Could AI chatbots be used to develop a bioweapon? You’d be surprised. The Telegraph, <https://www.telegraph.co.uk/global-health/science-and-disease/chatgpt-google-bard-ai-bioweapon-pandemic/> (30.6.2026)
- Nguyen, E. et al. (2024): Sequence modeling and design from molecular to genome scale with Evo. In: *Science* 386(6723), Art. eado9336, <https://doi.org/10.1126/science.ado9336>
- Nidhi, S. et al. (2021): Novel CRISPR-Cas Systems: An Updated Review of the Current Achievements, Applications, and Future Research Perspectives. In: *International Journal of Molecular Sciences* 22(7), Art. 3327, <https://doi.org/10.3390/ijms22073327>
- Nielsen, J. et al. (2022): Innovation trends in industrial biotechnology. In: *Trends in Biotechnology* 40(10), S. 1160–1172, <https://doi.org/10.1016/j.tibtech.2022.03.007>
- Nielsen, J.; Keasling, J. D. (2016): Engineering Cellular Metabolism. In: *Cell* 164(6), S. 1185–1197, <https://doi.org/10.1016/j.cell.2016.02.004>
- de Nies, L. et al. (2021): PathoFact: a pipeline for the prediction of virulence factors and antimicrobial resistance genes in metagenomic data. In: *Microbiome* 9(1), Art. 49, <https://doi.org/10.1186/s40168-020-00993-9>
- Nikel, P. I.; Mattanovich, D. (2021): Microbial cell factories: a biotechnology journey across species. In: *Essays in Biochemistry* 65(2), S. 143–145, <https://doi.org/10.1042/EBC20210037>
- Nikolakakis, I. et al. (2024): Instances of Biowarfare in World War I (1914–1918). In: *Cureus* 16(4), Art. e59329, <https://doi.org/10.7759/cureus.59329>
- NITI Aayog (2021): RESPONSIBLE AI. #AIFORALL. Approach Document For India: Part 2 - Operationalizing Principles For Responsible AI. <https://www.niti.gov.in/sites/default/files/2021-08/Part2-Responsible-AI-12082021.pdf> (30.6.2026)
- Notin, P. et al. (2024): Machine learning for functional protein design. In: *Nature Biotechnology* 42(2), S. 216–228, <https://doi.org/10.1038/s41587-024-02127-0>
- NOVA (o. J.a): Interviews with Biowarriors. Bill Patrick. Nova, https://www.pbs.org/wgbh/nova/bioterror/biow_patrick.html (30.9.2025)
- Noyce, R. S. et al. (2018): Construction of an infectious horsepox virus vaccine from chemically synthesized DNA fragments. In: *PLOS ONE* 13(1), Art. e0188453, <https://doi.org/10.1371/journal.pone.0188453>

- Noyce, R. S.; Evans, D. H. (2018): Synthetic horsepox viruses and the continuing debate about dual use research. In: PLoS Pathogens 14(10), Art. e1007025, <https://doi.org/10.1371/journal.ppat.1007025>
- NSABB (2007): Proposed Framework for the Oversight of Dual Use Life Sciences Research: Strategies for Minimizing the Potential Misuse of Research Information. National Science Advisory Board for Biosecurity, Washington, D.C.
- NSTC (2024): Framework for Nucleic Acid Synthesis Screening. National Science and Technology, <https://aspr.hhs.gov/S3/Documents/OSTP-Nucleic-Acid-Synthesis-Screening-Frame-work-Sep2024.pdf> (29.5.2026)
- NTI (o. J.b): Biological Weapons Convention (BWC). Nuclear Threat Initiative, <https://www.nti.org/education-center/treaties-and-regimes/convention-prohibition-development-production-and-stockpiling-bacteriological-biological-and-toxin-weapons-btwc/> (18.12.2025)
- NTI (o. J.a): How Biological Weapons Work. Nuclear Threat Initiative, <https://tutorials.nti.org/biological-weapons-nonproliferation/how-biological-weapons-work/> (22.9.2025)
- Obermeyer, F. et al. (2022): Analysis of 6.4 million SARS-CoV-2 genomes identifies mutations associated with fitness. In: Science 376(6599), S. 1327–1332, <https://doi.org/10.1126/science.abm1208>
- OECD (o. J.): OECD AI Principles overview. Organisation for Economic Co-operation and Development, <https://oecd.ai/en/ai-principles> (30.6.2026)
- Ofer, D. et al. (2021): The language of proteins: NLP, machine learning & protein sequences. In: Computational and Structural Biotechnology Journal 19, S. 1750–1758, <https://doi.org/10.1016/j.csbj.2021.03.022>
- Oğuz, F. (2010): Hayek on tacit knowledge. In: Journal of Institutional Economics 6(2), S. 145–165
- OPCW (2024): Investigation and Identification Team (IIT). Organisation for the Prohibition of Chemical Weapons, <https://www.opcw.org/iit> (10.12.2025)
- Open Bioeconomy Lab (2025): What is the Open Bioeconomy Lab? <https://openbioeconomy.org/about/> (4.8.2025)
- OpenAI (2024): GPT-4o System Card. <https://cdn.openai.com/gpt-4o-system-card.pdf> (27.10.2025)
- OpenAI (2025a): Deep Research System Card. <https://deploymentsafety.openai.com/deep-research> (28.10.2025)
- OpenAI (2025b): GPT-5 System Card. <https://cdn.openai.com/gpt-5-system-card.pdf> (28.10.2025)
- OpenAI (2025c): Letter from OpenAI to the OSTP. <https://cdn.openai.com/pdf/21b88bb5-10a3-4566-919d-f9a6b9c3e632/openai-ostp-rfi-oct-27-2025.pdf> (27.5.2026)
- OpenAI (2025d): Update to GPT-5 System Card: GPT-5.2. https://cdn.openai.com/pdf/3a4153c8-c748-4b71-8e31-aecbde944f8d/oai_5_2_system-card.pdf (27.5.2026)
- OpenAI (2025e): Usage policies. <https://openai.com/policies/usage-policies/> (26.2.2026)
- OpenAI (2025f): GPT-5 ist da. <https://openai.com/de-DE/gpt-5/> (24.11.2025)
- OpenAI (2026): GPT-5.5 System Card. <https://deploymentsafety.openai.com/gpt-5-5/gpt-5-5.pdf> (27.5.2026)
- OpenAI; LANL (2024): OpenAI and Los Alamos National Laboratory announce bioscience research partnership. <https://openai.com/index/openai-and-los-alamos-national-laboratory-work-together/> (23.10.2025)

- Opgenorth, P. et al. (2019): Lessons from Two Design–Build–Test–Learn Cycles of Dodecanol Production in *Escherichia coli* Aided by Machine Learning. In: *ACS Synthetic Biology* 8(6), S. 1337–1351, <https://doi.org/10.1021/acssynbio.9b00020>
- OSD (2026): Multilateral Export Control and Non-Proliferation Regimes. The Office of the Secretary of Defense, <https://www.dtsa.mil/SitePages/promoting-engagement/multilateral-non-proliferation-regimes.aspx> (5.1.2026)
- OSTP (2024): Framework For Nucleic Acid Synthesis Screening. The Office of Science and Technology Policy, <https://aspr.hhs.gov/S3/Documents/OSTP-Nucleic-Acid-Synthesis-Screening-Framework-Sep2024.pdf> (27.5.2026)
- Ouaghrham-Gormley, S. B. (2012): Barriers to Bioweapons: Intangible Obstacles to Proliferation. In: *International Security* 36(4), S. 80–114
- Ouaghrham-Gormley, S. B. (2016): Barriers to Bioweapons: The Challenges of Expertise and Organization for Weapons Development. New Dehli
- Ouaghrham-Gormley, S. B. (2024): Two Competing Bioweapons Nonproliferation Policies: Deterrence by Denial and Dissuasion. In: Paxton, N. A.: *Disincentivizing Bioweapons*. S. 79–101
- Ouaghrham-Gormley, S. B. (2025): Safeguarding against biological weapons. In: *Science* 388(6749), S. 797–797, <https://doi.org/10.1126/science.adz0714>
- Ouaghrham-Gormley, S. B.; Vogel, K. M. (2003): Conversion at stepnogorsk: What the future holds for former bioweapons facilities. Cornell University, Occasional Paper 28, <https://hdl.handle.net/1813/69394> (27.5.2026)
- P2P Foundation (2025): Open Insulin Project. https://wiki.p2pfoundation.net/Open_Insulin_Project (4.8.2025)
- Pacesa, M. et al. (2024): Past, present, and future of CRISPR genome editing technologies. In: *Cell* 187(5), S. 1076–1100, <https://doi.org/10.1016/j.cell.2024.01.042>
- Pacesa, M. et al. (2025): One-shot design of functional protein binders with BindCraft. In: *Nature* 646(8084), S. 483–492, <https://doi.org/10.1038/s41586-025-09429-6>
- Palmer, A. G. (2015): Enzyme dynamics from NMR spectroscopy. In: *Accounts of Chemical Research* 48(2), S. 457–465, <https://doi.org/10.1021/ar500340a>
- Pandi, A. et al. (2023): Cell-free biosynthesis combined with deep learning accelerates de novo development of antimicrobial peptides. In: *Nature Communications* 14, Art. 7197, <https://doi.org/10.1038/s41467-023-42434-9>
- Pannu, J. et al. (2025): Dual-use capabilities of concern of biological AI models. In: *PLOS Computational Biology* 21(5), Art. e1012975, <https://doi.org/10.1371/journal.pcbi.1012975>
- Papaleo, E. et al. (2016): The Role of Protein Loops and Linkers in Conformational Dynamics and Allostery. In: *Chemical Reviews* 116(11), S. 6391–6423, <https://doi.org/10.1021/acs.chemrev.5b00623>
- Parachini, J. V. et al. (2005): Diversion of Nuclear, Biological, and Chemical Weapons Expertise from the Former Soviet Union: Understanding an Evolving Problem. RAND National Security Research Division, o. O.
- Pardi, N.; Krammer, F. (2024): mRNA vaccines for infectious diseases – advances, challenges and opportunities. In: *Nature Reviews Drug Discovery* 23(11), S. 838–861, <https://doi.org/10.1038/s41573-024-01042-y>
- Parker, T.; Sitter, N. (2016): The Four Horsemen of Terrorism: It's Not Waves, It's Strains. In: *Terrorism and Political Violence* 28(2), S. 197–216, <https://doi.org/10.1080/09546553.2015.1112277>

- Parry, J. et al. (2026): How Well Did Superforecasters and Experts Predict Wet Lab Skill Uplift from LLMs? Forecasting Research Institute, <https://forecastingresearch.substack.com/p/how-well-did-superforecasters-and> (27.2.2026)
- Passaro, S. et al. (2025): Boltz-2: Towards Accurate and Efficient Binding Affinity Prediction. bioRxiv, <https://doi.org/10.1101/2025.06.14.659707>
- Patel, K. K. et al. (2025): From concept to cure: The evolution of CAR-T cell therapy. In: *Molecular Therapy* 33(5), S. 2123–2140, <https://doi.org/10.1016/j.ymthe.2025.03.005>
- Patra, P. et al. (2023): Recent advances in machine learning applications in metabolic engineering. In: *Biotechnology Advances* 62, Art. 108069, <https://doi.org/10.1016/j.biotechadv.2022.108069>
- Patrick, S.; Barton, J. (2024): Mitigating Risks from Gene Editing and Synthetic Biology: Global Governance Priorities. Carnegie Endowment for International Peace, Washington, D.C.
- Patwardhan, T. et al. (2024): Building an early warning system for LLM-aided biological threat creation. <https://openai.com/index/building-an-early-warning-system-for-llm-aided-biological-threat-creation/> (23.10.2025)
- Paul, S. M. et al. (2010): How to improve R&D productivity: the pharmaceutical industry's grand challenge. In: *Nature Reviews Drug Discovery* 9(3), S. 203–214, <https://doi.org/10.1038/nrd3078>
- Perez, D. R. et al. (2017): Plasmid-Based Reverse Genetics of Influenza A Virus. In: *Methods in Molecular Biology* 1602. Clifton, S. 251–273
- Perrigo, B. (2024): U.S. Must Act Quickly to Avoid Risks From AI, Report Says. TIME, <https://time.com/6898967/ai-extinction-national-security-risks-report/> (24.2.2026)
- PharmaWiki (2025): Small Molecules. https://www.pharmawiki.ch/wiki/index.php?wiki=Small_Molecules (28.5.2025)
- Phintha, A.; Chaiyen, P. (2022): Rational and mechanistic approaches for improving biocatalyst performance. In: *Chem Catalysis* 2(10), S. 2614–2643, <https://doi.org/10.1016/j.checat.2022.09.026>
- Pita, R.; Gunaratna, R. (2009): Revisiting Al-Qa'ida's Anthrax Program. In: *CTC Sentinel* 2(5), S. 10–13
- Pitschmann, V.; Hon, Z. (2016): Military Importance of Natural Toxins and Their Analogs. In: *Molecules* 21(5), Art. 556, <https://doi.org/10.3390/molecules21050556>
- Polanyi, M. (1962): *Personal Knowledge*. London
- Polmar, N. (2020): Japan's Deadliest Weapons. *Naval History*, <https://www.usni.org/magazines/naval-history-magazine/2020/october/japans-deadliest-weapons> (30.9.2025)
- Powers, A. S. et al. (2025): MedSAGE: Bridging Generative AI and Medicinal Chemistry for Structure-Based Design of Small Molecule Drugs. bioRxiv, <https://doi.org/10.1101/2025.05.10.653107>
- Prusiner, S. B. (1998): Prions. In: *Proceedings of the National Academy of Sciences of the United States of America* 95(23), S. 13363–13383, <https://doi.org/10.1073/pnas.95.23.13363>
- Qi, X. et al. (2024): On Evaluating the Durability of Safeguards for Open-Weight LLMs. arXiv, <https://doi.org/10.48550/arXiv.2412.07097>
- Qin, Y. et al. (2026): Functions and optimization of soft law in the international governance of synthetic biology: The predicament of hard law vs. the rise of soft law. In: *Synthetic and Systems Biotechnology* 12, S. 134–151, <https://doi.org/10.1016/j.synbio.2025.11.005>
- Qu, Y. et al. (2026): CRISPR-GPT for agentic automation of gene-editing experiments. In: *Nature Biomedical Engineering* 10(2), S. 245–258, <https://doi.org/10.1038/s41551-025-01463-z>

- Raglow, Z.; Lauring, A. S. (2025): Virus Evolution in Prolonged Infections of Immunocompromised Individuals. In: *Clinical Chemistry* 71(1), S.109–118, <https://doi.org/10.1093/clinchem/hvae150>
- Rannon, E. et al. (2025): DRAMMA: a multifaceted machine learning approach for novel antimicrobial resistance gene detection in metagenomic data. In: *Microbiome* 13(1), S. 67, <https://doi.org/10.1186/s40168-025-02055-4>
- Rao, V. M. et al. (2026): Generalist biological artificial intelligence in modeling the language of life. In: *Nature Biotechnology*, <https://doi.org/10.1038/s41587-026-03064-w>
- Rapp, J. T. et al. (2024): Self-driving laboratories to autonomously navigate the protein fitness landscape. In: *Nature Chemical Engineering* 1(1), S. 97–107, <https://doi.org/10.1038/s44286-023-00002-4>
- Rein, D. et al. (2023): GPQA: A Graduate-Level Google-Proof Q&A Benchmark. *arXiv*, <https://doi.org/10.48550/arXiv.2311.12022>
- Ren, F. et al. (2025): A small-molecule TNIK inhibitor targets fibrosis in preclinical and clinical models. In: *Nature Biotechnology* 43(1), S. 63–75, <https://doi.org/10.1038/s41587-024-02143-0>
- Rennie, M. L.; Oliver, M. R. (2025): Emerging frontiers in protein structure prediction following the AlphaFold revolution. In: *Journal of The Royal Society Interface* 22(225), Art. 20240886, <https://doi.org/10.1098/rsif.2024.0886>
- Republic of Kazakhstan (2020): Statement by President of Kazakhstan Kassym-Jomart Tokayev at the General Debate of the 75th session of the UNGA. https://www.akorda.kz/en/speeches/external_political_affairs/ext_speeches_and_addresses/statement-by-president-of-kazakhstan-kassym-jomart-tokayev-at-the-general-debate-of-the-75th-session-of-the-unga (2.6.2026)
- Research Group for Biological Arms Control (2021): 2021 Reader on Publicly Available CBMs. Hamburg, https://www.biological-arms-control.org/publications/CBMReader2021_final.pdf (27.5.2026)
- Responsible AI x Biodesign (2023): Community Values, Guiding Principles, and Commitments for the Responsible Development of AI for Protein Design. <https://responsiblebiodesign.ai/> (30.6.2026)
- Reuters (2012): Anthrax mailed to Pakistani PM's office: spokesman. Reuters, <https://www.reuters.com/article/world/anthrax-mailed-to-pakistani-pms-office-spokesman-idUSTRE81019Y/> (16.10.2025)
- Revill, J. (2024): Possible Models of BWC Verification. United Nations Institute for Disarmament Research (UNIDIR), Geneva, <https://doi.org/10.37559/WMD/24/CBW/03>
- Revill, J. et al. (2024): What will be the impact of AI on the bioweapons treaty? *Bulletin of the Atomic Scientists*, <https://thebulletin.org/2024/11/what-will-be-the-impact-of-ai-on-the-bio-weapons-treaty/> (27.1.2026)
- Revill, J.; Jefferson, C. (2014): Tacit knowledge and the biological weapons regime. In: *Science and Public Policy* 41(5), S. 597–610, <https://doi.org/10.1093/scipol/sct090>
- Richardt, A.; Russmann, H. (2006): Biologische Kampfstoffe: Nachweis und Bekämpfung–Strategien gegen Milzbrand, Pocken & Co. In: *Biologie in unserer Zeit* 36(5), S. 322–329, <https://doi.org/10.1002/biuz.200610316>
- Richter, E. (2011): Biologische Waffen - Einführung. In: *Bio-Tötung. Ethica Themen*, Wien

- Rinne, T. (2025): Was sich durch die neue EU Produkthaftungsrichtlinie (EU) 2024/2853 ändert. Buse, <https://buse.de/blog/handelsrecht/aenderung-eu-produkthaftungsrichtlinie-eu-2024-2853/> (20.1.2026)
- RKI (o. J.a): Die Internationalen Gesundheitsvorschriften der Weltgesundheitsorganisation. Stand 30.1.2025, Robert Koch-Institut, <https://www.rki.de/DE/Themen/Infektionskrankheiten/Mel-dewesen/IGV/internationale-gesundheitsvorschriften-node.html> (8.1.2026)
- RKI (o. J.b): RefBio – Deutscher Beitrag zur Stärkung der Referenzlabore Bio im UNSGM. Stand 25.5.2021, Robert Koch-Institut, <https://www.rki.de/DE/Institut/Internationales/Biosicherheitsprogramm/RefBio.html?nn=16926656> (2.6.2026)
- RKI (o. J.c): RKI-Projekt RefBio: Labore vorbereiten auf den Ernstfall – Veröffentlichung in Nature Communications. Stand 25.5.2021, Robert Koch-Institut, <https://www.rki.de/DE/Institut/Internationales/Biosicherheitsprogramm/Nature-Communications-2021.html?nn=16926656> (2.6.2026)
- RKI (o. J.d): UNSGM-Projekt. Stand 10.4.2025, Robert Koch-Institut, <https://www.rki.de/DE/Themen/Infektionskrankheiten/Biologische-Gefahren/Projekte-Netzwerke/Projekte/UNSGM.html?templateQueryString=UNSGM> (29.5.2026)
- Rogers, J. (2021): Future Threats: Military UAS, Terrorist Drones, and the Dangers of the Second Drone Age. In: A Comprehensive Approach to Countering Unmanned Aircraft Systems Subject Areas: Uncrewed Aircraft Systems. Kalkar
- Rohmann, J. (2020): 2.16 Konfidenzintervalle sollten angegeben werden. Cochrane. Wissen Was Wirkt, <https://wissenwaswirkt.org/2-16-konfidenzintervalle-sollten-angegeben-werden> (18.3.2026)
- Romero-Severson, E. O. et al. (2025): Measuring skill-based uplift from AI in a real biological laboratory. arXiv, <https://doi.org/10.48550/arXiv.2512.10960>
- Rosenberg, A. B. et al. (2015): Learning the Sequence Determinants of Alternative Splicing from Millions of Random Sequences. In: Cell 163(3), S. 698–711, <https://doi.org/10.1016/j.cell.2015.09.054>
- Rutherford, Z. (2025): Israel exposed to bioterrorism threats amid severe biosecurity gaps, comptroller reveals. 08 December 2025. CBRNe WORLD, <https://cbrneworld.com/news/israel-exposed-to-bioterrorism-threats-amid-severe-biosecurity-gaps-comptroller-reveals> (16.1.2026)
- Ryle, G. (1949): The concept of mind. New York
- Sadybekov, A. V.; Katritch, V. (2023): Computational approaches streamlining drug discovery. In: Nature 616(7958), S. 673–685, <https://doi.org/10.1038/s41586-023-05905-z>
- Saini, R. K. et al. (2020): Protective effects of lycopene in cancer, cardiovascular, and neurodegenerative diseases: An update on epidemiological and mechanistic perspectives. In: Pharmacological Research 155, Art. 104730, <https://doi.org/10.1016/j.phrs.2020.104730>
- Sainz, O. et al. (2023): NLP Evaluation in trouble: On the Need to Measure LLM Data Contamination for each Benchmark. Bouamor, H. et al. (Hg.): Findings 2023. <https://doi.org/10.18653/v1/2023.findings-emnlp.722>
- Sanger, F. et al. (1977a): Nucleotide sequence of bacteriophage phi X174 DNA. In: Nature 265(5596), S. 687–695, <https://doi.org/10.1038/265687a0>
- Sanger, F. et al. (1977b): DNA sequencing with chain-terminating inhibitors. In: Proceedings of the National Academy of Sciences of the United States of America 74(12), S. 5463–5467, <https://doi.org/10.1073/pnas.74.12.5463>

- Santolini, M. et al. (2023): iGEM: a model system for team science and innovation. arXiv, <https://doi.org/10.48550/arXiv.2310.19858>
- Satam, H. et al. (2023): Next-Generation Sequencing Technology: Current Trends and Advancements. In: *Biology* 12(7), Art. 997, <https://doi.org/10.3390/biology12070997>
- Schlender, M. et al. (2021): How Much Does It Cost to Research and Develop a New Drug? A Systematic Review and Assessment. In: *Pharmacoeconomics* 39(11), S.1243–1269, <https://doi.org/10.1007/s40273-021-01065-y>
- Schmidt, H. et al. (2025): Adaptive evolution of SARS-CoV-2 during a persistent infection for 521 days in an immunocompromised patient. In: *npj Genomic Medicine* 10(1), Art. 4, <https://doi.org/10.1038/s41525-025-00463-x>
- Schmidt, M. (2008): Diffusion of synthetic biology: a challenge to biosafety. In: *Systems and Synthetic Biology* 2(1), S. 1–6, <https://doi.org/10.1007/s11693-008-9018-z>
- Schmitt, K.; Zacchia, N. A. (2012): Total decontamination cost of the anthrax letter attacks. In: *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science* 10(1), S.98–107, <https://doi.org/10.1089/bsp.2010.0053>
- Schneuing, A. et al. (2024): Structure-based drug design with equivariant diffusion models. In: *Nature Computational Science* 4(12), S.899–909, <https://doi.org/10.1038/s43588-024-00737-x>
- Scoles, S. (2025): U.S. military funds AI tools to speed modeling of viral outbreaks. *Science*, <https://www.science.org/content/article/u-s-military-funds-ai-tools-speed-modeling-viral-outbreaks> (12.12.2025)
- Sentinel Bio (2025): Panoplia Laboratories. Sentinel Bio, <https://sentinelbio.org/grant/panoplia-laboratories/> (11.11.2025)
- Service, R. F. (2006): Synthetic Biologists Debate Policing Themselves. In: *Science* 312(5777), S.1116–1116, <https://doi.org/10.1126/science.312.5777.1116>
- Service, R. F. (2023): Could chatbots help devise the next pandemic virus? *Science*. <https://www.science.org/content/article/could-chatbots-help-devise-next-pandemic-virus> (31.10.2025)
- Seydel, C. (2023): DNA writing technologies moving toward synthetic genomes. In: *Nature Biotechnology* 41(11), S.1504–1509, <https://doi.org/10.1038/s41587-023-02006-0>
- Shafe, M. O. et al. (2024): Lycopene: A Potent Antioxidant with Multiple Health Benefits. In: *Journal of Nutrition and Metabolism* 2024(1), Art. 6252426, <https://doi.org/10.1155/2024/6252426>
- Shanehsazzadeh, A. et al. (2024): Unlocking de novo antibody design with generative artificial intelligence., <https://doi.org/10.1101/2023.01.08.523187>
- Shen, S. Y. et al. (2018): Sensitive tumour detection and classification using plasma cell-free DNA methylomes. In: *Nature* 563(7732), S.579–583, <https://doi.org/10.1038/s41586-018-0703-0>
- Shi, S. et al. (2025): Metabolic Engineering of Yeast. In: *Annual Review of Biophysics* 54(1), S.101–120, <https://doi.org/10.1146/annurev-biophys-070924-103134>
- Shojaee, P. et al. (2025): The Illusion of Thinking: Understanding the Strengths and Limitations of Reasoning Models via the Lens of Problem Complexity. arXiv, <https://doi.org/10.48550/arXiv.2506.06941>
- Simmons; Simmons (2021): China's new PRC Biosecurity Law. Simmons & Simmons, <https://www.simmons-simmons.de/en/publications/ckkz6vtxs14830a99h0xou5fo/china-s-new-prc-biosecurity-law> (16.1.2026)

- Singh, N. et al. (2025): A generalized platform for artificial intelligence-powered autonomous enzyme engineering. In: *Nature Communications* 16, Art. 5648, <https://doi.org/10.1038/s41467-025-61209-y>
- Singh, R. (2025): India not planning separate AI law; Digital India Act remains stalled. *Medianama*, Singhal, K. et al. (2025): Toward expert-level medical question answering with large language models. In: *Nature Medicine* 31(3), <https://doi.org/10.1038/s41591-024-03423-7>
- Smietana, K. et al. (2016): Trends in clinical success rates. In: *Nature Reviews. Drug Discovery* 15(6), S. 379–380, <https://doi.org/10.1038/nrd.2016.85>
- Smith, A. A. et al. (2026): Using a GPT-5-driven autonomous lab to optimize the cost and titer of cell-free protein synthesis. *bioRxiv*, <https://doi.org/10.64898/2026.02.05.703998>
- Soice, E. H. et al. (2023): Can large language models democratize access to dual-use biotechnology? *arXiv*, <https://doi.org/10.48550/arXiv.2306.03809>
- Sokolova, K. et al. (2023): Atlas of primary cell-type-specific sequence models of gene expression and variant effects. In: *Cell Reports Methods* 3(9), Art. 100580, <https://doi.org/10.1016/j.crmeth.2023.100580>
- Sokolova, K. et al. (2024): Deep Learning Sequence Models for Transcriptional Regulation. In: *Annual Review of Genomics and Human Genetics* 25(Volume 25, 2024), S. 105–122, <https://doi.org/10.1146/annurev-genom-021623-024727>
- Southey, M. W. Y.; Brunavs, M. (2023): Introduction to small molecule drug discovery and preclinical development. In: *Frontiers in Drug Discovery* 3, Art. 1314077, <https://doi.org/10.3389/fddsv.2023.1314077>
- de Souza, F. M.; Gupta, R. K. (2024): Bacteria for Bioplastics: Progress, Applications, and Challenges. In: *ACS Omega* 9(8), S. 8666–8686, <https://doi.org/10.1021/acsomega.3c07372>
- Staden, R. (1979): A strategy of DNA sequencing employing computer programs. In: *Nucleic Acids Research* 6(7), S. 2601–2610, <https://doi.org/10.1093/nar/6.7.2601>
- START (2025): Global Terrorism Database (GTD). The National Consortium for the Study of Terrorism and Responses to Terrorism, <https://www.start.umd.edu/data-tools/GTD> (1.8.2025)
- Steindl, D. et al. (2021): Novichok nerve agent poisoning. In: *The Lancet* 397(10270), S. 249–252, [https://doi.org/10.1016/S0140-6736\(20\)32644-1](https://doi.org/10.1016/S0140-6736(20)32644-1)
- Stern, J. (2003): The Protean Enemy. In: *Foreign Affairs* 82(4), S. 27–40, <https://doi.org/10.2307/20033647>
- Stokes, J. M. et al. (2020): A Deep Learning Approach to Antibiotic Discovery. In: *Cell* 180(4), S. 688–702, <https://doi.org/10.1016/j.cell.2020.01.021>
- Sun, D. et al. (2022): Why 90% of clinical drug development fails and how to improve it? In: *Acta Pharmaceutica Sinica B* 12(7), S. 3049–3062, <https://doi.org/10.1016/j.apsb.2022.02.002>
- Suster, C. J. E. et al. (2024): Emerging applications of artificial intelligence in pathogen genomics. In: *Frontiers in Bacteriology* 3, <https://doi.org/10.3389/fbrio.2024.1326958>
- TAB (2015): Synthetische Biologie - die nächste Stufe der Bio- und Gentechnologie. (Autor/innen: Sauter, A.; Albrecht, S.; van Doren, D.; König, H.; Reiß, T.; Trojok, R.; Elsbach, S.) Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), TAB-Arbeitsbericht Nr. 164, Berlin, <https://doi.org/10.5445/IR/310104566>
- TAB (2023): Bakteriophagen in Medizin, Land- und Lebensmittelwirtschaft – Anwendungsperspektiven, Innovations- und Regulierungsfragen. Innovationsanalyse. (Autor/innen: König, H.; Sauter, A.) Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), TAB-Arbeitsbericht Nr. 206, Berlin, <https://doi.org/10.5445/IR/1000160512>
- Talbot, J.; Jakeman, M. (2011): Security Risk Management Body of Knowledge. o. O.

- Taleb, N. N. (2007): *The Black Swan: The impact of the highly improbable*. New York
- Tam, V. et al. (2019): Benefits and limitations of genome-wide association studies. In: *Nature Reviews Genetics* 20(8), S. 467–484, <https://doi.org/10.1038/s41576-019-0127-1>
- Tedeschi, S. et al. (2024): ALERT: A Comprehensive Benchmark for Assessing Large Language Models' Safety through Red Teaming. *arXiv*, <https://doi.org/10.48550/arXiv.2404.08676>
- Thadani, N. N. et al. (2023): Learning from prepandemic data to forecast viral escape. In: *Nature* 622(7984), S. 818–825, <https://doi.org/10.1038/s41586-023-06617-0>
- The Acronym Institute (2002): Disarmament Documentation: Australia Group Agrees New CBW Export Control Measures. <https://acronym.org.uk/old/archive/docs/0206/doc09.htm> (7.1.2026)
- The Australia Group (2002): New measures to fight the spread of Chemical and Biological Weapons. https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/agm_june2002.html (7.1.2026)
- The Dawn Sturgess Inquiry (2025): The Dawn Sturgess Inquiry – Report into the death of Dawn Sturgess. https://dsiweb-prod.s3.eu-west-2.amazonaws.com/uploads/E03283426_Project-Orbit_Accessible_v2.pdf (30.6.2026)
- The Economist (2026): How AI tools could enable bioterrorism. <https://www.economist.com/science-and-technology/2026/05/05/how-ai-tools-could-enable-bioterrorism?> (30.6.2026)
- The Japan Times (2019): China pig farm jams drones dropping swine fever-laced products onto its sites, but also GPS. <https://www.japantimes.co.jp/news/2019/12/23/asia-pacific/china-pig-farm-jams-drones-dropping-swine-fever-laced-products-onto-site-also-gps/> (14.10.2025)
- The Nobel Prize in Chemistry (2024): The Nobel Prize in Chemistry 2024. NobelPrize.org, <https://www.nobelprize.org/prizes/chemistry/2024/press-release/> (21.5.2025)
- Thi Nhu Thao, T. et al. (2020): Rapid reconstruction of SARS-CoV-2 using a synthetic genomics platform. In: *Nature* 582(7813), S. 561–565, <https://doi.org/10.1038/s41586-020-2294-9>
- Thorold, P. W. (1953): Suspected malicious poisoning. In: *Journal of the South African Veterinary Association* 24(4), S. 215–217, https://doi.org/10.10520/AJA00382809_4792
- Tin, D. et al. (2021): Half-a-Century of Terrorist Attacks: Weapons Selection, Casualty Outcomes, and Implications for Counter-Terrorism Medicine. In: *Prehospital and Disaster Medicine* 36(5), S. 526–530, <https://doi.org/10.1017/S1049023X21000868>
- Tin, D. et al. (2022): Bioterrorism: An analysis of biological agents used in terrorist events. In: *The American Journal of Emergency Medicine* 54, S. 117–121, <https://doi.org/10.1016/j.ajem.2022.01.056>
- Tivey, A. et al. (2024): Mining nucleic acid „omics“ to boost liquid biopsy in cancer. In: *Cell Reports Medicine* 5(9), <https://doi.org/10.1016/j.xcrm.2024.101736>
- Tobias, A. V.; Wahab, A. (2025): Autonomous ‚self-driving‘ laboratories: a review of technology and policy implications. In: *Royal Society Open Science* 12(7), Art. 250646, <https://doi.org/10.1098/rsos.250646>
- Tom, G. et al. (2024): Self-Driving Laboratories for Chemistry and Materials Science. In: *Chemical Reviews* 124(16), S. 9633–9732, <https://doi.org/10.1021/acs.chemrev.4c00055>
- Török, T. J. et al. (1997): A large community outbreak of salmonellosis caused by intentional contamination of restaurant salad bars. In: *JAMA* 278(5), S. 389–395, <https://doi.org/10.1001/jama.1997.03550050051033>

- Tucker, J. B. (1999): Biological weapons in the former Soviet Union: an interview with Dr. Kenneth Alibek. *The Nonproliferation Review*, <https://www.nonproliferation.org/wp-content/uploads/npr/alibek63.pdf> (30.6.2026)
- Tumpey, T. M. et al. (2005): Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus. In: *Science* 310(5745), S. 77–80, <https://doi.org/10.1126/science.1119392>
- Turner, M. D. et al. (2025): The 1984 Rajneeshee Bioterrorism Attack: An Example of Biological Warfare by Violent Non-state Actors. In: *Cureus* 17(7), <https://doi.org/10.7759/cureus.88514>
- Turner, M. D.; Sapp, J. (2025): Lessons From Rhodesia’s Chemical and Biological Warfare Program. In: *Military Medicine* 191(3-4), Art. usaf301, <https://doi.org/10.1093/milmed/usaf301>
- UMD (o.J.): Violent Non-State Actor CBRN Event Database Search. University of Maryland, https://cbrn.umd.edu/event_database (17.10.2025)
- UN (2022): Final Document of the Ninth Review Conference. United Nations, o. O.
- UN (2025): Report on universalization activities. United Nations, o. O.
- UNICRI (2012): Security Implications of Synthetic Biology and Nanobiotechnology. United Nations Interregional Crime and Justice Research Institute, Turin
- UNIDIR (2026): Biological Weapons Convention National Implementation Measures Database. United Nations Institute for Disarmament Research, <https://bwcimplementation.org/> (16.1.2026)
- UNODA (o. J.a): Biological Weapons. United Nations Office for Disarmament Affairs, <https://disarmament.unoda.org/en/our-work/weapons-mass-destruction/biological-weapons> (17.9.2025)
- UNODA (o. J.b): Biological Weapons Convention. United Nations Office for Disarmament Affairs, <https://disarmament.unoda.org/en/our-work/weapons-mass-destruction/biological-weapons/biological-weapons-convention> (30.6.2026)
- UNODA (o. J.c): Confidence Building Measures. United Nations Office for Disarmament Affairs. <https://disarmament.unoda.org/en/our-work/weapons-mass-destruction/biological-weapons/confidence-building-measures> (30.6.2026)
- UNODA (o. J.d): Secretary-General’s Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons (UNSGM). United Nations Office for Disarmament Affairs, <https://disarmament.unoda.org/en/our-work/weapons-mass-destruction/secretary-generals-mechanism-investigation-alleged-use-chemical-and-biological-weapons-unsgm> (30.6.2026)
- U.S. Department of State (2025): Adherence to and Compliance with Arms Control, Nonproliferation, and Disarmament Agreements and Commitments. Washington, D.C.
- UVA (2025): The Chinese Communist Party’s Layered Artificial Intelligence Strategy. University of Virginia National Security Data and Policy Institute, Charlottesville
- Valentini, G. et al. (2023): The promises of large language models for protein design and modeling. In: *Frontiers in Bioinformatics* 3, Art. 1304099, <https://doi.org/10.3389/fbinf.2023.1304099>
- Valko, M. (2025): AI Safety is Dead: People Stripping Guardrails From Every Open-Source Model (And Why Governments Can’t Stop Them). <https://blog.namilink.com/open-weight-models-losing-their-guardrails-5d8e3652bb86> (6.11.2025)
- Vázquez Torres, S. et al. (2025): De novo designed proteins neutralize lethal snake venom toxins. In: *Nature* 639(8053), S. 225–231, <https://doi.org/10.1038/s41586-024-08393-x>
- Venkatesan, P. (2025): UK launch metagenomic pathogen surveillance programme. In: *The Lancet Microbe* 6(6), <https://doi.org/10.1016/j.lanmic.2025.101143>

- Venter, J. C. et al. (2001): The Sequence of the Human Genome. In: *Science* 291(5507), S. 1304–1351, <https://doi.org/10.1126/science.1058040>
- Vieira, L. C. et al. (2026): Intrinsic dataset features drive mutational effect prediction by protein language models. <https://doi.org/10.64898/2026.03.08.710389>
- Villani, S. (2022): Regional Perspective: CBRN Terrorism-Related Obligations under European Union Law. In: *International Law and Chemical, Biological, Radio-Nuclear (CBRN) Events*, S. 156–175, https://doi.org/10.1163/9789004507999_011
- Vogel, K. (2006): Bioweapons Proliferation: Where Science Studies and Public Policy Collide. In: *Social Studies of Science* 36(5), S. 659–690, <https://doi.org/10.1177/0306312706059460>
- Vogel, K. M. (2012): Phantom menace or looming danger? A new framework for assessing bio-weapons threats. <https://doi.org/10.1353/book.72084>
- Volk, M. J. et al. (2023): Metabolic Engineering: Methodologies and Applications. In: *Chemical Reviews* 123(9), S. 5521–5570, <https://doi.org/10.1021/acs.chemrev.2c00403>
- de Vries, B. (2024a): The Biological Weapons Amendment to the ICC Statute and National Provisions: Mutually Reinforcing Evidence for Customary Criminalization? In: *Journal of International Criminal Justice* 22(3–4), S. 565–583, <https://doi.org/10.1093/jicj/mqae033>
- de Vries, B. (2024b): Biological and chemical weapons legislation in the EU: A need for harmonisation? In: *New Journal of European Criminal Law* 15(4), S. 462–480, <https://doi.org/10.1177/20322844241274165>
- Wachter, M. (2026): Biosecurity Catching Up to the Modern Era: A Look Into S.3741. *Health Law & Policy Brief*. <https://www.healthlawpolicy.org/2026/03/29/biosecurity-catching-up-to-the-modern-era-a-look-into-s-3741/> (15.4.2026)
- Wahome, N. (2025): Building a global AI platform for pandemic preparedness. CEPI, <https://cepi.net/building-global-ai-platform-pandemic-preparedness> (17.3.2026)
- Wainberg, M. et al. (2018): Deep learning in biomedicine. In: *Nature Biotechnology* 36(9), S. 829–838, <https://doi.org/10.1038/nbt.4233>
- Walls, A. C. et al. (2020): Elicitation of Potent Neutralizing Antibody Responses by Designed Protein Nanoparticle Vaccines for SARS-CoV-2. In: *Cell* 183(5), S. 1367–1382.e17, <https://doi.org/10.1016/j.cell.2020.10.043>
- Wan, J. C. M. et al. (2025): Promises and pitfalls of multi-cancer early detection using liquid biopsy tests. In: *Nature Reviews Clinical Oncology* 22(8), S. 566–580, <https://doi.org/10.1038/s41571-025-01033-x>
- Wang, D. et al. (2018): Comprehensive functional genomic resource and integrative model for the human brain. In: *Science* 362(6420), Art. eaat8464, <https://doi.org/10.1126/science.aat8464>
- Wang, D. et al. (2025a): Gene therapy then and now: A look back at changes in the field over the past 25 years. In: *Molecular Therapy* 33(5), S. 1889–1902, <https://doi.org/10.1016/j.ymthe.2025.02.040>
- Wang, J. Y.; Doudna, J. A. (2023): CRISPR technology: A decade of genome editing is only the beginning. In: *Science* 379(6629), Art. eadd8643, <https://doi.org/10.1126/science.add8643>
- Wang, J.-H. et al. (2024): Adeno-associated virus as a delivery vector for gene therapy of human diseases. In: *Signal Transduction and Targeted Therapy* 9, Art. 78, <https://doi.org/10.1038/s41392-024-01780-w>
- Wang, M. et al. (2025b): A call for built-in biosecurity safeguards for generative AI tools. In: *Nature Biotechnology* 43(6), S. 845–847, <https://doi.org/10.1038/s41587-025-02650-8>

- Warrick, J.; Ley Jarrett (2024): Satellite images show major expansion at Russian site with secret bioweapons past. The Washington Post, <https://www.washingtonpost.com/national-security/interactive/2024/russia-biological-chemical-weapons-laboratory-expansion/> (8.12.2025)
- Washington, M. A. et al. (2024): Barriers to Biological Weapons Development: Potential Implications for Pathway Disruption. In: *Countering WMD Journal* 28, S. 19–27
- Waters, K. (2024): NIAID Modeling Host Responses to Understand Severe Human Virus Infections, Multi-Omic Viral Dataset Catalog Collection. DataHub, <https://data.pnnl.gov/group/nodes/project/13299>
- Watson, J. L. et al. (2023): De novo design of protein structure and function with RFdiffusion. In: *Nature* 620(7976), S. 1089–1100, <https://doi.org/10.1038/s41586-023-06415-8>
- WD (2021): Zu Entwicklungen in der Biosicherheitspolitik seit 2014. Initiativen in der Wissenschaft und auf internationaler Ebene. Deutscher Bundestag, Wissenschaftliche Dienste, WD 8 - 3000 - 073/21, Berlin
- Webster, S. A. et al. (2026): Examining the Landscape and Limitations of the Federal Push to Override State AI Regulation. Ropes & Gray LLP, <https://www.ropesgray.com/en/insights/alerts/2026/03/examining-the-landscape-and-limitations-of-the-federal-push-to-override-state-ai-regulation> (16.3.2026)
- Webster, T. et al. (2025): Global Risk Index for AI-enabled Biological Tools. Summary Assessment & Methods Report. The Centre for Long-Term Resilience & RAND Europe, o. O.
- Wei, B. et al. (2025): Best Practices for Biorisk Evaluations on Open-Weight Bio-Foundation Models. arXiv, <https://doi.org/10.48550/arXiv.2510.27629>
- Weissenow, K. et al. (2022): Protein language-model embeddings for fast, accurate, and alignment-free protein structure prediction. In: *Structure* 30(8), S. 1169–1177, <https://doi.org/10.1016/j.str.2022.05.001>
- Wells, G. (2026): OpenAI Employees Raised Alarms About Canada Shooting Suspect Months Ago. Feb. 21, 2026. Wall Street Journal, <https://www.wsj.com/us-news/law/openai-employees-raised-alarms-about-canada-shooting-suspect-months-ago-b585df62> (26.2.2026)
- Wen, S. et al. (2025): Generative artificial intelligence for enzyme design: Recent advances in models and applications. In: *Current Opinion in Green and Sustainable Chemistry* 52, Art. 101010, <https://doi.org/10.1016/j.cogsc.2025.101010>
- Wheelis, M. (2002): Biological Warfare at the 1346 Siege of Caffa. In: *Emerging Infectious Diseases* 8(9), S. 971–975, <https://doi.org/10.3201/eid0809.010536>
- White & Case (2024): AI Watch: Global regulatory tracker – Council of Europe. <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-council-europe> (21.1.2026)
- White & Case (2025a): AI Watch: Global regulatory tracker – China. <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china> (19.1.2026)
- White & Case (2025b): AI Watch: Global regulatory tracker – European Union. <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-european-union> (20.1.2026)
- White & Case (2025c): AI Watch: Global regulatory tracker – United Nations. <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-nations> (21.1.2026)
- White & Case (2025d): AI Watch: Global regulatory tracker – United States. <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states> (19.1.2026)

- White & Case (2026): AI Watch: Global regulatory tracker – India. <https://www.whitecase.com/in-sight-our-thinking/ai-watch-global-regulatory-tracker-india> (15.5.2026)
- White House (2023): FACT SHEET: Biden-Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI. <https://perma.cc/Q8QS-3AGS> (29.5.2026)
- White House (2025): America’s AI Action Plan. <https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf> (1.6.2026)
- Whitford, C. M. et al. (2021): The Design-Build-Test-Learn cycle for metabolic engineering of *Streptomyces*. In: *Essays in Biochemistry* 65(2), S.261–275, <https://doi.org/10.1042/EBC20200132>
- WHO (2004): Laboratory biosafety manual, 3rd edition. World Health Organization, o. O.
- WHO (2020): Laboratory biosafety manual, 4th edition. World Health Organization, o. O.
- WHO (2022a): Global guidance framework for the responsible use of the life sciences. World Health Organization, o. O.
- WHO (2022b): Towards a global guidance framework for the responsible use of life sciences: summary report of consultations on the principles, gaps and challenges of biorisk management, May 2022. World Health Organization, o. O.
- WHO (2024a): Laboratory biosecurity guidance. World Health Organization, o. O.
- WHO (2024b): WHO updates laboratory biosecurity guidance. World Health Organization, <https://www.who.int/news/item/04-07-2024-who-updates-laboratory-biosecurity-guidance> (7.1.2026)
- WHO (o. J.a): Safeguarding biosafety and biosecurity in laboratories. World Health Organization, <https://www.who.int/activities/safeguarding-biosafety-and-biosecurity-in-laboratories> (7.1.2026)
- WHO (o. J.b): Technical Advisory Group on Biosafety (TAG-B). World Health Organization, [https://www.who.int/groups/technical-advisory-group-on-biosafety-\(tag-b\)](https://www.who.int/groups/technical-advisory-group-on-biosafety-(tag-b)) (2.6.2026)
- Widman, A. J. et al. (2024): Ultrasensitive plasma-based monitoring of tumor burden using machine-learning-guided signal enrichment. In: *Nature Medicine* 30(6), S.1655–1666, <https://doi.org/10.1038/s41591-024-03040-4>
- Wilczok, D.; Zhavoronkov, A. (2025): Progress, Pitfalls, and Impact of AI-Driven Clinical Trials. In: *Clinical Pharmacology & Therapeutics* 117(4), S.887–890, <https://doi.org/10.1002/cpt.3542>
- Williams, B. et al. (2025): Forecasting LLM-enabled biorisk and the efficacy of safeguards. Forecasting Research Institute, o. O.
- Willis, E. A. (2003): Seascape with Monkeys and Guinea-Pigs: Britain’s Biological Weapons Research Programme, 1948-54. In: *Medicine, Conflict and Survival* 19(4), S.285–302
- Wilson, T. J. et al. (2016): Ribozymes and the mechanisms that underlie RNA catalysis. In: *Frontiers of Chemical Science and Engineering* 10(2), S.178–185, <https://doi.org/10.1007/s11705-016-1558-2>
- Wittmann, B. J. et al. (2025): Strengthening nucleic acid biosecurity screening against generative protein design tools. In: *Science* 390(6768), S.82–87, <https://doi.org/10.1126/science.adu8578>
- Wohlwend, J. et al. (2024): Boltz-1 Democratizing Biomolecular Interaction Modeling. *bioRxiv*, <https://doi.org/10.1101/2024.11.19.624167>

- Wohlwend, J. et al. (2025): Deep learning enhances the prediction of HLA class I-presented CD8+ T cell epitopes in foreign pathogens. In: *Nature Machine Intelligence* 7(2), S. 232–243, <https://doi.org/10.1038/s42256-024-00971-y>
- Workman, K. (2024): Engineering AAVs with Evo and AlphaFold. LatchBio, <https://blog.latch.bio/p/engineering-aavs-with-evo-and-alphafold> (30.1.2026)
- Wouters, O. J. et al. (2020): Estimated Research and Development Investment Needed to Bring a New Medicine to Market, 2009-2018. In: *JAMA* 323(9), S. 844–853, <https://doi.org/10.1001/jama.2020.1166>
- wwPDB consortium (2019): Protein Data Bank: the single global archive for 3D macromolecular structure data. In: *Nucleic Acids Research* 47(D1), S. D520–D528, <https://doi.org/10.1093/nar/gky949>
- Yang, Z. et al. (2021): An in silico deep learning approach to multi-epitope vaccine design: a SARS-CoV-2 case study. In: *Scientific Reports* 11, Art. 3238, <https://doi.org/10.1038/s41598-021-81749-9>
- Yaremenko, A. V. et al. (2025): Clinical advances of mRNA vaccines for cancer immunotherapy. In: *Med* 6(1), Art. 100562, <https://doi.org/10.1016/j.medj.2024.11.015>
- Yassif, J. M. et al. (2023): Guarding Against Catastrophic Biological Risks: Preventing State Biological Weapon Development and Use by Shaping Intentions. In: *Health Security* 21(4), S. 258–265, <https://doi.org/10.1089/hs.2022.0145>
- Yeh, A. H.-W. et al. (2023): De novo design of luciferases using deep learning. In: *Nature* 614(7949), S. 774–780, <https://doi.org/10.1038/s41586-023-05696-3>
- Yim, H. et al. (2011): Metabolic engineering of *Escherichia coli* for direct production of 1,4-butanediol. In: *Nature Chemical Biology* 7(7), S. 445–452, <https://doi.org/10.1038/nchembio.580>
- Yoneda, M. et al. (2006): Establishment of a Nipah virus rescue system. In: *Proceedings of the National Academy of Sciences* 103(44), S. 16508–16513, <https://doi.org/10.1073/pnas.0606972103>
- Youssef, N. et al. (2025): Computationally designed proteins mimic antibody immune evasion in viral evolution. In: *Immunity* 58(6), S. 1411–1421, <https://doi.org/10.1016/j.immuni.2025.04.015>
- Zacchia, N. A.; Schmitt, K. (2019): Medical Spending for the 2001 Anthrax Letter Attacks. In: *Disaster Medicine and Public Health Preparedness* 13(3), S. 539–546, <https://doi.org/10.1017/dmp.2018.113>
- Zakaria, S. et al. (2026): Cost–benefit analysis for synthetic nucleic acid screening in the European Union. RAND Corporation, Santa Monica
- Zanders, J. P. (2022): Catapulting Cadavers. A Medieval Practice of Biological Warfare? The Trench, <https://www.the-trench.org/catapulting-cadavers> (16.10.2025)
- Zanders, J. P. (2025): The 1925 Geneva Protocol. The League of Nations' Only Arms Control Agreement. The Trench, <https://www.the-trench.org/1925-geneva-protocol-negotiation> (30.6.2026)
- Zárate, A. et al. (2025): VirDetect-AI: a residual and convolutional neural network–based metagenomic tool for eukaryotic viral protein identification. In: *Briefings in Bioinformatics* 26(1), Art. bbaf001, <https://doi.org/10.1093/bib/bbaf001>
- Zeng, T.; Li, Y. I. (2022): Predicting RNA splicing from DNA sequence using Pangolin. In: *Genome Biology* 23, Art. 103, <https://doi.org/10.1186/s13059-022-02664-4>
- Zerr, I. et al. (2024): Creutzfeldt–Jakob disease and other prion diseases. In: *Nature Reviews Disease Primers* 10, Art. 14, <https://doi.org/10.1038/s41572-024-00497-y>

- Zeymer, C.; Hilvert, D. (2018): Directed Evolution of Protein Catalysts. In: *Annual Review of Biochemistry* 87, S. 131–157, <https://doi.org/10.1146/annurev-biochem-062917-012034>
- Zhang, C. et al. (2025a): Jailbreaking Commercial Black-Box LLMs with Explicitly Harmful Prompts. *arXiv*, <https://doi.org/10.48550/arXiv.2508.10390>
- Zhang, C. B. C. et al. (2026): LLM Novice Uplift on Dual-Use, In Silico Biology Tasks. *arXiv*, <https://doi.org/10.48550/arXiv.2602.23329>
- Zhang, K. et al. (2025b): Artificial intelligence in drug development. In: *Nature Medicine* 31(1), S. 45–59, <https://doi.org/10.1038/s41591-024-03434-4>
- Zhang, P. et al. (2023a): Deep flanking sequence engineering for efficient promoter design using DeepSEED. In: *Nature Communications* 14, Art. 6309, <https://doi.org/10.1038/s41467-023-41899-y>
- Zhang, S. et al. (2025c): A Multimodal Biomedical Foundation Model Trained from Fifteen Million Image–Text Pairs. In: *NEJM AI* 2(1), Art. Aloa2400640, <https://doi.org/10.1056/Aloa2400640>
- Zhang, Y. et al. (2023b): Vaxign-DL: A Deep Learning-based Method for Vaccine Design and its Evaluation. *bioRxiv*, <https://doi.org/10.1101/2023.11.29.569096>
- Zhao, G. et al. (2025): ConoGPT: Fine-Tuning a Protein Language Model by Incorporating Disulfide Bond Information for Conotoxin Sequence Generation. In: *Toxins* 17(2), Art. 93, <https://doi.org/10.3390/toxins17020093>
- Zhou, J. et al. (2018): Deep learning sequence-based ab initio prediction of variant effects on expression and disease risk. In: *Nature Genetics* 50(8), S. 1171–1179, <https://doi.org/10.1038/s41588-018-0160-6>
- Zhou, J. et al. (2019): Whole-genome deep-learning analysis identifies contribution of noncoding mutations to autism risk. In: *Nature Genetics* 51(6), S. 973–980, <https://doi.org/10.1038/s41588-019-0420-0>
- Zilinskas, R. A. (2016): The Soviet Biological Weapons Program and Its Legacy in Today's Russia. Center for the Study of Weapons of Mass Destruction, National Defense University, CSWMD Occasional Papers, Washington, D.C.
- Zou, J. et al. (2019): A primer on deep learning in genomics. In: *Nature Genetics* 51(1), S. 12–18, <https://doi.org/10.1038/s41588-018-0295-5>

7 Anhang

7.1 Abbildungen

7.2 Tabellen

7.3 Kästen

7.4 Abkürzungen

7.5 Glossar



7 Anhang

7.1 Abbildungen

Abbildung 2.1	Zeitleiste mit Meilensteinen von der frühen Bioinformatik zur Entwicklung und Nutzung von KI	30
Abbildung 3.1	Biowaffen bestehen aus einem biologischen Agens und einem Ausbringungsmechanismus	49
Abbildung 3.2	Die Herstellung von Biowaffen erfordert typischerweise mehrere und komplexe Schritte	55
Abbildung 3.3	Autonome Labore durch die Kombination von KI-Modellen und automatisierten Laborplattformen („self-driving labs“/„lab in the loop“)	89

7.2 Tabellen

Tabelle 2.1	Beispiele für die Verwendung von KI-Modellen bzw. -Systemen in der Molekularbiologie oder Biotechnologie	32
Tabelle 3.1	Bekannt gewordene staatliche Biowaffenprogramme nach dem Zweiten Weltkrieg	60
Tabelle 3.2	Einsatz von Biowaffen in bewaffneten Konflikten und Terrorakten in der Neuzeit	62
Tabelle 3.3	Kurzdarstellung ausgewählter empirischer Untersuchungen zu Biosecurity-Risiken von LLMs	66

7.3 Kästen

Kasten 3.1	Biosicherheit – Biosafety und Biosecurity	47
Kasten 3.2	Biologische Waffen (Biowaffen)	49
Kasten 3.3	Staatliche und nicht staatliche Biowaffenprogramme bzw. Entwicklungsaktivitäten	58
Kasten 3.4	Einsatz von Biowaffen in bewaffneten Konflikten und Terrorakten in der Neuzeit	61
Kasten 3.5	Jailbreaking – Umgehen eingebauter Sicherheitsmechanismen	75
Kasten 3.6	Biosecurity-Screening von Bestellungen für Nukleinsäuresynthesen (DNA-Synthesescreening)	83

7.4 Abkürzungen

AAV	adenoassoziierte Viren
AI/KI	artificial intelligence/künstliche Intelligenz
BWC	Biological Weapons Convention/Biowaffenkonvention
CBRN	chemisch, biologisch, radiologisch und nuklear, z. B. im Zusammenhang mit Gefahren oder Waffen
CRISPR-Cas9	clustered regularly interspaced short palindromic repeats and CRISPR-associated protein 9
CWC	Chemical Weapons Convention/Chemiewaffenkonvention
DBTL-Zyklus	Design-Build-Test-Learn-Zyklus
DFG	Deutsche Forschungsgemeinschaft
DNA	deoxyribonucleic acid/Desoxyribonukleinsäure
GPAI	general purpose AI models/KI-Modelle mit allgemeinem Verwendungszweck
GPT	generative pre-trained transformer
iGEM	International Genetically Engineered Machine
IGSC	International Gene Synthesis Consortium
IBBIS	International Biosecurity and Biosafety Initiative for Science
KEFs	Kommissionen für Ethik sicherheitsrelevanter Forschung
KIxBio	Zusammenspiel von KI mit molekularer Biologie und Biotechnologie
LLM	large language model/großes Sprachmodell
MINT	Mathematik, Informatik, Naturwissenschaften und Technik
ML	machine learning/maschinelles Lernen
mRNA	messenger RNA
RNA	ribonucleic acid/Ribonukleinsäure
UNSGM	Secretary-General's Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons/Mechanismus des Generalsekretärs der Vereinten Nationen zur Untersuchung eines mutmaßlichen Einsatzes von chemischen und biologischen Waffen
VCT	Virology Capabilities Test
WHO	World Health Organization/Weltgesundheitsorganisation

7.5 Glossar

Benchmarks: Testverfahren, mit denen typischerweise automatisch Leistungskennzahlen zum Wissensstand bzw. den Fähigkeiten von KI-Modellen generiert werden.

Biofoundries: Stellen typischerweise zentralisierte, oft öffentlich finanzierte Einrichtungen dar und sollen Infrastrukturen zur Verfügung stellen, um Forschenden – oft auch von außerhalb der betreibenden Institutionen – das Design und die Herstellung biologischer Systeme vor Ort oder über die Nutzung von Serviceleistungen zu ermöglichen. Biofoundries zeigen Ähnlichkeiten zu Cloud Labs, fokussieren aber oft stärker auf spezifische (Teil-)Prozesse von Bioproduktionsansätzen.

Bioinformatik: Die Erforschung und Verwendung computergestützter Methoden zur Erfassung, Speicherung, Verbreitung und Analyse biologischer Daten oder Information.

- biologische Agenzien: Organismen wie Bakterien oder Pilze, Viren sowie Moleküle wie infektiöse Prionen oder Toxine.
- biologische KI-Modelle: KI-Modelle, die mit biologischen Daten (z. B. DNA- oder Proteinsequenzen, Molekülstrukturen oder -funktionen) trainiert werden und Vorhersagen bzw. Vorschläge für Sequenzen und Strukturen biologischer Moleküle oder zu deren Funktion liefern.
- biologische Kampfstoffe: Biologische Agenzien, die über bestimmte Prozesse verändert/modifiziert wurden, um sie für die Massenproduktion, Lagerung oder Ausbringung über entsprechende Mechanismen bzw. Systeme besser geeignet (waffenfähig) zu machen.
- biologische Waffe: Bestehen aus in der Regel zwei Teilen: einem in eine waffenfähige Form gebrachten biologischen Agens (z. B. einem krankheitsauslösenden Organismus oder Toxin) und einem Mechanismus zu dessen Ausbringung.
- Biosecurity: Umfasst Grundsätze, Technologien und Praktiken, die absichtlich herbeigeführte Schäden durch missbräuchliche Nutzungen von biologischen Agenzien und/oder von Ausrüstung, Fähigkeiten und Daten für solche Nutzungen verhindern sollen.
- Cloud Labs (Cloudlabore): Meist kommerzielle Labore, auf die Forschende ferngesteuert über Internetoberflächen zugreifen können. Forschende spezifizieren die Protokolle für ihre eigenen Experimente über Onlineportale der Einrichtungen, die dann in den Laboren automatisiert durchgeführt werden.
- Deep Learning (DL): Eine besonders leistungsfähige und flexible Art von maschinellem Lernen, auf der sehr viele aktuelle KI-Modelle beruhen. DL-Modelle basieren auf mehreren Schichten softwaresimulierter künstlicher Neuronen (tiefe neuronale Netze) und können verschiedene Architekturen haben, welche für unterschiedliche Aufgaben verwendet werden.
- Do-it-yourself-Biologie (DIY-Biologie): Bezeichnet eine heterogene Szene von Freizeitforschung, die im häuslichen Umfeld, in Vereinen mit kleinen privaten Laboren, oder öffentlich zugänglichen Laboren (Communitylaboren) von Personen mit unterschiedlichem Hintergrund – von Laien bis hin zu Personen mit akademischer biologischer Ausbildung – betrieben wird. Durch die konzeptionelle Nähe zur Computerhackerszene werden die Mitglieder der Szene vor allem im deutschsprachigen Raum oft auch als Biohacker bezeichnet.
- generative KI: Im Gegensatz zu prädiktiven KI-Modellen, die erkannte Muster in historischen Daten zur Vorhersage künftiger Ereignisse oder von Molekülfunktionen nutzen, verwenden generative Modelle erkannte Muster und Beziehungen in Daten, mit denen sie trainiert wurden, um neue Inhalte zu erstellen, die die Originaldaten (z. B. Text, Bilder oder auch DNA- oder Proteinsequenzen) nachahmen.
- Large language models (LLMs, große Sprachmodelle): KI-Modelle, die typischerweise auf DL-Methoden beruhen und ursprünglich darauf ausgelegt wurden, komplexe Texte, Fragen oder Anweisungen zu verarbeiten und kohärente Antworten und Texte zu generieren. Hierzu gehören Modelle wie ChatGPT bzw. GPT (OpenAI), Claude (Anthropic) oder Gemini (Google). Aktuelle Versionen solcher Modelle sind meist multimodal, sie können verschiedene Arten (Modalitäten) von Daten verarbeiten und integrieren, z. B. Text, Bilder, Ton oder Video.
- Omik (omics): Bezeichnet Forschungsbereiche, die sich mit der Untersuchung der Gesamtheit eines bestimmten Typs von biologischen Molekülen oder molekularer Prozesse innerhalb von Zellen oder Organismen befassen. Das Ziel ist Moleküle und molekulare Prozesse zu identifizieren, zu beschreiben und zu quantifizieren, die zur Form und Funktion von Zellen und Geweben beitragen.
- „patient zero“: Bezeichnet in der Epidemiologie die Person, die als erste mit einer Krankheit infiziert wurde und von der die Ausbreitung der Krankheit ausging.

Red-Teaming-Übungen: Bezeichnet Verfahren, bei denen meist Gruppen von Expert/innen eingesetzt werden, um Möglichkeiten bzw. Risiken auszutesten und Schwachstellen zu identifizieren. Teilweise werden Teams von Expert/innen auch eingesetzt, um herauszufinden, inwieweit KI-Modelle bei der Auswahl und Herstellung biologischer Agenzien bzw. Biowaffen oder der Planung und Durchführung eines Angriffs helfen könnten.

„self-driving labs“: Autonome automatisierte Laborplattformen, die typischerweise durch die Kombination von KI-Modellen (darunter LLMs oder biologische KI-Modelle) zur Hypothesenbildung und dem Design von beispielsweise Molekülen oder von Synthesewegen sowie zur Analyse von Versuchsergebnissen mit Robotiksystemen für Laboraufgaben entstehen.

Systemkarten („system cards“): Von den entwickelnden Unternehmen erstellte Dokumente zu KI-Modellen. Sie enthalten Informationen über das KI-Modell selbst, die verwendeten Trainingsdaten, seine Fähigkeiten, Einschränkungen, Nutzungen sowie zu Aspekten von Sicherheit und Ethik (etwa hinsichtlich Verzerrungen).

tazites Wissen: Wissen, das in der Regel nicht in schriftlicher Form weitergeben werden kann. Es erfordert eigene Erfahrung und/oder die praktische Anwendung instruiert durch oder zusammen durchgeführt mit Personen, die solches Wissen bzw. Fähigkeiten besitzen (zum Teil ohne sich dessen bewusst zu sein).

Toxine: Gifte aus Tieren, Pflanzen oder Mikroorganismen oder ähnliche synthetisch hergestellte Substanzen

Uplift-Studien: Untersuchungen, bei denen Testpersonen eingesetzt werden, um herauszufinden, inwieweit KI-Modelle (typischerweise im Vergleich zu konventioneller Internetsuche) Kenntnisse bzw. Fähigkeiten der Personen verbessern können.

Verwaffnung („weaponization“): Bezeichnet die Veränderung/Modifikation von biologischen Agenzien, um sie für die Massenproduktion, Lagerung oder Ausbringung über entsprechende Mechanismen bzw. Systeme besser geeignet („waffenfähig“) zu machen, sowie die Kombination der Agenzien mit geeigneten Ausbreitungssystemen zur Herstellung funktionseller und effektiver biologischer Waffen. Die Verwaffnung ist Teil des typischerweise mehrstufigen, komplexen Herstellungsprozesses von Biowaffen.

Herausgeber

Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag
Neue Schönhauser Straße 10
10178 Berlin

Telefon: +49 30 28491-0

E-Mail: buero@tab-beim-bundestag.de

www.tab-beim-bundestag.de

2026

Bildnachweis

KI-generierte Darstellung/TAB (S. 1)

ISSN: 2364-2602

DOI: 10.5445/IR/1000195981

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) berät das Parlament und seine Ausschüsse in Fragen des wissenschaftlich-technischen Wandels. Das TAB wird seit 1990 vom Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) des Karlsruher Instituts für Technologie (KIT) betrieben. Grundlage ist ein Vertrag mit dem Deutschen Bundestag. Hierbei kooperiert es seit September 2013 mit dem IZT – Institut für Zukunftsstudien und Technologiebewertung gGmbH sowie dem Institut für Innovation und Technik (iit) in der VDI/VDE Innovation + Technik GmbH und Technologiebewertung gGmbH sowie dem Institut für Innovation und Technik (iit) in der VDI/VDE Innovation + Technik GmbH.