

CNTRMONITOR

Perspektiven auf Dual Use



CNTRMONITOR 2024

Editorial	3
Fokus: Perspektiven auf Dual Use	4
Trends	15
Künstliche Intelligenz	
Künstliche Intelligenz, Halbleiter und das Militär	16
Drohnen	
Technische, militärische und politische Entwicklungen im Bereich Drohnen	22
Additive Fertigung	
Additive Fertigung in der Kriegsführung	30
Künstliche Intelligenz, Biologie	
Technologische Implikationen von KI für biologische Risiken	38
Biotechnologie	
Auswirkungen von technologischem Fortschritt auf die Biosicherheit	46
Analysen	57
Neue Militärtechnologien in nationalen Sicherheitsstrategien – eine vergleichende Analyse	58
Dual-Use-Risiken bei der gentechnischen Veränderung von onkolytischen Viren	78
Anhang	87
Internationale Verträge im Zusammenhang mit der Abrüstung und Nichtverbreitung biologischer Waffen	88
Andere Instrumente zur Unterstützung der Abrüstung und Nichtverbreitung biologischer und chemischer Waffen	89
Ausgewählte Instrumente zur Verbesserung der Biosicherheit, zur Minderung von Dual-Use-Risiken und zur Förderung sicherer und ethisch verantwortungsbewusster biologischer Forschung	91
Internationale Initiativen und Kernprinzipien für den sicheren Umgang mit KI	93
Glossar	96
Stichwortverzeichnis	100

Editorial

Kriege und Konflikte haben in den letzten Jahren weltweit zugenommen. Die Zahl der Todesopfer steigt stark an, insbesondere in der Ukraine und im Nahen Osten. In diesen Kriegen zeigt sich der zunehmende militärische Einsatz neuer und neuester Technologien. Tatsächlich hat Technologie das Potenzial, die konventionelle Art und Weise Kriege zu führen, fundamental zu verändern. Gleichzeitig bleibt die bekannte Bedrohung durch unkonventionelle Massenvernichtungswaffen bestehen und nimmt in einigen Regionen sogar zu.

Um die Auswirkungen von Technologie auf Krieg und Frieden umfassend zu verstehen, müssen Forschung und Erkenntnisse aus den Natur- und Ingenieurwissenschaften und den Sozialwissenschaften integriert werden. Das ist die Aufgabe des neu geschaffenen Clusters für Natur- und Technikwissenschaftliche Rüstungskontrollforschung (CNTR), das am Leibniz-Institut für Friedens- und Konfliktforschung (PRIF, Peace Research Institute Frankfurt), der Technischen Universität Darmstadt und der Justus-Liebig-Universität Gießen angesiedelt ist. Hier arbeiten Politikwissenschaftler*innen Hand in Hand mit Forschenden aus der Biologie, Chemie, Physik, den Ingenieurwissenschaften und der Informatik. Dank der großzügigen Unterstützung durch das Auswärtige Amt freuen wir uns, zum ersten Mal den *CNTR Monitor – Technologie und Rüstungskontrolle* als das Aushängeschild des Projekts zu präsentieren.

Der Monitor ist eine jährlich erscheinende Publikation, die nicht nur die Risiken abschätzt, die von einzelnen Technologien und F&E-Aktivitäten für die internationale Sicherheit ausgehen, sondern auch die Möglichkeiten ihrer Regulierung und Kontrolle thematisiert. Darüber hinaus werden aber auch die Chancen evaluiert, die neue Technologien für die Friedens- und Sicherheitspolitik bieten, beispielsweise bei der Überwachung der Einhaltung von Rüstungskontrollvereinbarungen.

Der Fokus des Monitors liegt in diesem Jahr auf dem Thema *Dual Use*. Technologien, die später im militärischen Bereich eingesetzt werden, werden häufig zunächst im zivilen Bereich entwickelt. In frühen Phasen der F&E oder der Grundlagenforschung sind mögliche disruptive militärische Anwendungen in der Regel schwer vorhersehbar und ergeben sich oft als unbeabsichtigte Folge. Der CNTR Monitor beleuchtet diese Zusammenhänge, indem er eine Reihe von aktuellen technologischen Trends aufzeigt und diese einer vertieften Analyse unterzieht.

In Bezug auf moderne Dual-Use-Technologien in der Kriegsführung beleuchten wir künstliche Intelligenz, Drohnen und additive Fertigung, untersuchen ihre Auswirkungen auf die Sicherheit und diskutieren ihren Einsatz in aktuellen Kriegen, insbesondere in der Ukraine und im Nahen Osten. Im Bereich der akademischen Forschung finden die bemerkenswertesten Debatten über Dual Use in den Biowissenschaften statt, die daher ebenfalls im Mittelpunkt dieses Berichts stehen.

Wir sind zuversichtlich, dass unser CNTR Monitor wichtige Hintergrundinformationen für Entscheidungsträger und Entscheidungsträgerinnen aus Politik und Fachpraxis, für Forschende und die interessierte Öffentlichkeit gleichermaßen liefern wird. Wir wünschen Ihnen eine informative Lektüre und hoffen, dass der Monitor den Dialog zwischen allen Stakeholdern belebt, um in diesen schwierigen Zeiten zur Stärkung von Frieden und Sicherheit beizutragen.



Prof. Dr. Malte Göttsche



Prof. Dr. Christopher Daase

Fokus: Perspektiven auf Dual Use

Das Konzept des Dual Use – die Tatsache, dass viele Güter sowohl für zivile als auch für militärische Zwecke verwendet werden können – ist nicht neu. Mit dem wissenschaftlichen und technologischen Fortschritt wird jedoch die Regulierung von Hard- und Software, die dieser Beschreibung entspricht, immer komplexer und stellt zunehmend eine Herausforderung für Frieden und Sicherheit dar. Die Kapitel dieser Ausgabe des CNTR Monitors betrachten einige aktuelle Entwicklungen in den Bereichen Künstliche Intelligenz, Additive Fertigung, Biologie und Drohnen, einschließlich solcher mit Dual-Use-Potenzial. Dieses Fokuskapitel liefert die konzeptionelle Grundlage, indem es den Begriff „Dual Use“ in seinen vielen Facetten beleuchtet.

Im Bereich der klassischen militärischen nationalen Sicherheit werden Güter in der Regel dann als Dual-Use-Güter verstanden, wenn es für sie – gegebenenfalls in angepasster Form – sowohl eine legitime zivile als auch eine militärische Verwendung gibt.¹ Dieselbe Definition gilt auch für internationale Sicherheit und Frieden im weiteren Sinne.² Der Begriff „Güter“ umfasst sowohl physische Artefakte als auch Software oder grundlegende Technologien. Während viele Güter oder Technologien grundsätzlich unter diese Definition fallen, muss es sich bei dem Gut präziser um ein „Haupt- oder Schlüsselement für die inländische Entwicklung, Herstellung, Nutzung oder Verbesserung der militärischen Fähigkeiten“³ handeln. Der Einsatz solcher Güter oder Technologien kann legitime militärische Anwendungen umfassen, aber auch unrechtmäßige, wenn die Güter oder Technologien in einer Weise eingesetzt werden, die nicht mit internationalen rechtlichen Verpflichtungen, einschließlich des humanitären Völkerrechts, vereinbar ist. Über die klassische Dichotomie von ziviler und militärischer Nutzung hinaus kann der Begriff „Dual Use“ auch verwendet werden, wenn legitime, mit guten Absichten betriebene Forschung nicht per se militärische Anwendungen hat, aber dennoch für bösartige Zwecke wie illegale Waffenprogramme oder kriminelle oder terroristische Handlungen missbraucht werden könnte.

Während sich Dual-Use-Anwendungen bei bereits vorhandenen oder genutzten Technologien sowie bei der angewandten Forschung und Entwicklung von Technologien in fortgeschrittenen Stadien (z. B. Prototypen) leichter identifizieren lassen, sind sie typischerweise in früheren Entwicklungsstadien und in der Grundlagenforschung schwieriger vorhersehbar. Hier muss die Verantwortung der einzelnen Forschenden betont werden, mögliche unbeabsichtigte Folgen kritisch zu prüfen. Unbeabsichtigte Folgen können die illegitime Nutzung von Wissen und Technologie betreffen, aber auch die rechtlich zulässige militärische Nutzung, wenn sich Forschende oder einschlägige Einrichtungen zur rein zivilen Forschung verpflichtet haben. So wichtig die Verantwortung des Einzelnen auch ist, müssen für neue Technologien, die schwerwiegende Auswirkungen auf die Sicherheit haben könnten, möglicherweise neue institutionelle Formen der Regulierung entwickelt werden. Vor diesem Hintergrund haben führende Forschende im Bereich der Künstlichen Intelligenz beispielsweise kürzlich die Gründung einer inter-

nationalen Organisation gefordert, die die Entwicklung dieser Schlüsseltechnologie des 21. Jahrhunderts überwachen soll.⁴

Dieses Kapitel gibt zunächst einen allgemeinen Überblick über die Dual-Use-Regulierung und juristische Hintergründe. Danach wird näher auf die Forschungs- und Technologiebereiche eingegangen, die im Mittelpunkt dieser Publikation stehen: Forschung und Entwicklung mit Relevanz für konventionelle Waffen einerseits und potenzielle Risiken der biologischen Forschung andererseits.

Für einen Überblick über internationale Initiativen zur Regulierung von KI, siehe S. 93.

Dual-Use-Regulierung

Während die ersten juristischen Debatten über die Regulierung von Dual-Use-Gütern im Zusammenhang mit (strategischen) Export-/Handelskontrollen geführt wurden,⁵ hat sich das Dual-Use-Problem zunehmend auf andere Bereiche des Völkerrechts ausgewirkt, die für den internationalen Frieden und die Sicherheit relevant sind.

Strategische Handelskontrollen, wie z. B. nationale Ausfuhrkontrollvorschriften, waren traditionell das Instrument der Wahl für die Regulierung von Dual-Use-Gütern. Solche Verordnungen wurden weitgehend als politisches Instrument wahrgenommen, das die Festlegung einseitiger (oder allenfalls koordinierter) strategischer Prioritäten ermöglichte, anstatt einer breiteren Rüstungskontrollagenda zu folgen. Mit einem strengen verwaltungsrechtlichen Rahmen für die Erteilung von Ausfuhrgenehmigungen, der sich weitgehend an den Modellen der Waffenexportregulierung orientierte, verfügten die nationalen Behörden über einen großen Ermessensspielraum. Der öffentliche Diskurs konzentrierte sich häufig auf die Unwirksamkeit solcher Vorschriften und die politischen Prioritäten, die die Regierungen in diesem Zusammenhang verfolgten. Nationale Rechtsrahmen, die weitgehend während des Kalten Krieges entwickelt wurden, bestehen weiterhin. Es ist bemerkenswert, dass die Europäische Union (EU)⁶ einen ähnlichen Ansatz verfolgt hat, nachdem sie die Debatte darüber, ob strategische Exportkontrollgesetze in die Zuständigkeit der Mitgliedstaaten oder der Union fallen, hinter sich gelassen hatte. Im EU-Kontext fällt die Umsetzung der EU-Rechtsvorschriften weiterhin in die Zuständigkeit der Mitgliedstaaten, d. h. es gibt keine administrative Durchführung von Dual-Use-Kontrollen durch die Union selbst.

Die Internationalisierung der Ausfuhrkontrollvorschriften für Dual-Use-Güter⁷ erfolgte in der Regel durch Soft-Law-Instrumente. Rechtlich nicht bindende Kooperationsvereinbarungen wie das Wassenaar-Arrangement, die Gruppe nuklearer Lieferländer (Nuclear Suppliers Group), das Zangger-Komitee, das Missile Technology Control Regime und die Australische Gruppe wurden bevorzugt. Denn sie wahren den nationalen Ermessensspielraum hinsichtlich der Frage, welche Güter, Software und Technologie an wen weitergegeben werden dürfen. Oft standen Bündniserwägungen über Überlegungen zur Rüstungskontrolle.

Für bestimmte Waffensysteme gibt es jedoch Vorschriften, die über die Exportkontrolle hinausgehen. Insbesondere wurden alle Massenvernichtungswaffen durch rechtsverbindliche internationale Abkommen reguliert oder verboten. So verbietet der Vertrag über die Nichtverbreitung von Kernwaffen (NVV) von 1968 den Nichtkernwaffenstaaten den Erwerb von Kernwaffen. Biologische Waffen sind durch das Biowaffen-Übereinkommen (BWÜ) von 1972 umfassend verboten. Das 1993 zur Unterzeichnung aufgelegte Chemiewaffenübereinkommen (CWÜ) verbietet chemische Waffen. Alle drei Verträge verpflichten die Mitgliedstaaten, die Proliferation der fraglichen Waffen zu verhindern. Gleichzeitig können Nichtverbreitungs- und Rüstungskontrollabkommen Bestimmungen zum Transfer von Technologie und relevantem Wissen enthalten. Das CWÜ enthält

Für eine kurze Einführung zum BWÜ, siehe S. 88.

konkrete Bestimmungen über den internationalen Handel mit Chemikalien und deren Entwicklung (Artikel XI (2) (b) des CWÜ), und das BWÜ und das CWÜ verpflichten die Mitgliedstaaten ganz allgemein, die internationale Zusammenarbeit zu fördern und den technologischen Austausch im Bereich der Biologie bzw. der Chemie nicht zu behindern. Der NVV erlaubt nicht nur die zivile Nutzung der Kernenergie, sondern verpflichtet Staaten, die Kernenergie nutzen, Staaten, die noch nicht über diese Technologie verfügen, bei der Einführung der zivilen Nutzung zu unterstützen (Art. III NVV). Es besteht also ein inhärentes Spannungsverhältnis zwischen Nichtverbreitung und internationaler Zusammenarbeit. Das überträgt sich auch auf die Frage des Umgangs mit Dual-Use-Gütern und -Technologien.

Schließlich ist der Umgang mit Dual-Use-Forschung in inländischen Einrichtungen eine gesonderte Frage. Es findet derzeit eine lebhafte Debatte statt, die auch Diskussionen über geeignete Strategien und Maßnahmen zur Steuerung umfasst, insbesondere in Bezug auf die sogenannte „Dual-Use Research of Concern“ (DURC) – also Forschung, die zu Ergebnissen führen könnte, die ein unmittelbares Risiko des Missbrauchs mit potenziell schwerwiegenden Folgen bergen. Ursprünglich konzentrierte sich diese Debatte auf die Biowissenschaften, hat sich aber inzwischen auch auf die Regulierung der Dual-Use-Forschung in anderen wissenschaftlichen Disziplinen ausgeweitet.

In Deutschland hat die Regierung 2013 den Deutschen Ethikrat gebeten, sich mit dem Thema zu befassen. Im Jahr 2014 veröffentlichte der Rat seine Stellungnahme.⁸ Sie konzentrierte sich auf die Verantwortung von Forschenden in den Biowissenschaften und empfahl unter anderem, das Problembewusstsein zu schärfen, Verhaltenskodizes für verantwortungsvolle Forschung aufzustellen und einen rechtsverbindlichen Rahmen für DURC auszuarbeiten. Etwa zur gleichen Zeit veröffentlichten die Deutsche Forschungsgemeinschaft (DFG) und die Nationale Akademie der Wissenschaften Leopoldina ihre Empfehlungen. Diese konzentrieren sich ganz auf die Selbstregulierung und Selbstverwaltung der Wissenschaft und betonen die Freiheit der Forschung, die in Deutschland ein verfassungsmäßiges Grundrecht ist.⁹ Die 2022 aktualisierten DFG/Leopoldina-Empfehlungen gehen über die Biowissenschaften hinaus und richten sich an alle akademischen und wissenschaftlichen Disziplinen. Die Empfehlungen haben sich seit 2014 in der deutschen Wissenschaft durchgesetzt und sind derzeit der vorherrschende Ansatz im Umgang mit Dual-Use-Forschung in Deutschland.¹⁰

Rechtliche Überlegungen

Generell ist es wichtig zu betonen, dass das Dual-Use-Dilemma Formen der Regulierung notwendig macht, die über rein objektive Kriterien hinausgehen.¹¹ Um zwischen zivilen und militärischen Verwendungszwecken zu unterscheiden, müssen Gegenstand – also das betreffende Gut – und Zweck, genauer gesagt die beabsichtigte Verwendung und damit ein subjektives Element betrachtet werden. Bei Definitionen, die in erster Linie auf objektiven Kriterien beruhen, ist der Auslegungsspielraum begrenzt. Die Auslegung und Anwendung subjektiver Elemente wie Absichten und Zwecke hingegen ist mit viel mehr Unsicherheiten verbunden. Aus diesem Grund enthält die Regulierung von Dual-Use-Gütern häufig nicht nur Kriterien für die Auslegung solcher subjektiven Elemente, sondern auch einen institutionellen Rahmen. Dieser wirft die Frage auf, wer entscheidet – also wer auslegt und wer anwendet. Während die Auslegungskriterien und die institutionelle Ausgestaltung, die für eine Dual-Use-Regulierung notwendig sind, in der Regel auf nationaler Ebene (mit einem mehr oder weniger „geschlossenen“ Rechtssystem) realisiert werden können, ist die Regulierung von Dual Use auf internationaler Ebene mit zahlreichen Herausforderungen verbunden. Das liegt nicht zuletzt an fehlenden umfassenden institutionellen und administrativen Strukturen auf internationaler Ebene, aber

auch an der Unvollständigkeit und Offenheit des internationalen Rechtssystems. Die Staaten haben bisher unterschiedliche Wege beschritten, um diese Herausforderungen zu bewältigen.

Im BWÜ und im CWÜ wurden beispielsweise Gegenstand und Zweck von Materialien und Technologien in die Definition der verbotenen Waffen aufgenommen. Das führte zur Entstehung des sogenannten Allgemeinen Zweckkriteriums (*General Purpose Criterion*) (z. B. Artikel II (1) (a) CWÜ: „die für nach diesem Übereinkommen nicht verbotene Zwecke bestimmt sind“; Artikel I BWÜ, der das Verbot auf biologische Agenzien und Trägermittel bezieht, die zum Einsatz „für feindselige Zwecke oder in einem bewaffneten Konflikt“ bestimmt sind).¹² Es ist bemerkenswert, dass das BWÜ und das CWÜ nur deshalb zu umfassenden Rüstungskontrollverträgen werden konnten, weil sie diese subjektiven Elemente in die Definition der verbotenen Waffen aufgenommen haben. Die Herausforderung bestand darin, Bestimmungen zu entwickeln, die den Auslegungsspielraum des Allgemeinen Zweckkriteriums eingrenzen würden.¹³ Gleichzeitig ist im Falle des CWÜ zu bemerken, dass es zwar von einer der eindrucksvollsten internationalen Organisationen unterstützt wird, die zur Umsetzung eines internationalen Übereinkommens geschaffen wurde. Die Rolle der Organisation für das Verbot chemischer Waffen (OVCW) ist jedoch im Hinblick auf die Handhabung des Allgemeinen Zweckkriteriums begrenzt. Die Auslegung dieses Kriteriums liegt weiterhin weitgehend in den Händen der Vertragsstaaten, die jedoch die Möglichkeit haben, ihre Vorgehensweise und ihre Bemühungen zur Umsetzung der Vertragsbestimmungen auf internationaler Ebene zu koordinieren. Letzteres gilt auch für das BWÜ, das über keine internationale Organisation verfügt.

Die Einbeziehung subjektiver Elemente in die Definition von sensitiven Dual-Use-Materialien auf internationaler Ebene wurde bisher nicht durch internationale Verwaltungsverfahren, Entscheidungsbefugnisse oder die Einrichtung von Behörden unterstützt. Es besteht also ein konzeptionelles Ungleichgewicht bei der Behandlung von Dual-Use-Fragen auf internationaler Ebene. Der Sicherheitsrat der Vereinten Nationen (UNSC) hat mit der Verabschiedung der UNSC-Resolution 1540 (2004) versucht, einige der sich daraus ergebenden Unsicherheiten zu verringern. Aber die Bemühungen, sowohl die Regelungs- als auch die Entscheidungsbefugnisse in den Händen des Sicherheitsrats zu konzentrieren, waren nur von begrenztem Erfolg. Vielmehr muss die internationale Gemeinschaft bis auf weiteres mit diesem Ungleichgewicht zwischen (international vereinbarten) subjektiven Kriterien und (nationalen) Befugnissen zur (administrativen) Entscheidungsfindung leben. Der meistversprechende, wenn auch schwierige Weg, um Dual-Use-Probleme auf völkerrechtlicher Ebene zuverlässig zu lösen, wäre die Aufnahme von (objektiven) Kriterien, die den Interpretationsspielraum subjektiver Elemente einschränken, gleichzeitig aber den umfassenden Geltungsbereich der Verbote aufrechterhalten könnten. In Ermangelung einer internationalen Regelung haben die Staaten unterschiedliche Ansätze verfolgt, um die Dual-Use-Problematik im Bereich der konventionellen Waffen und im Bereich der Biologie zu bewältigen, wie in den folgenden Abschnitten dargelegt wird.

Für eine kurze Erläuterung der UNSC-Resolution 1540, siehe S. 90.

Dual Use und konventionelle Waffen

Aus der Sicht einzelner Länder ist Dual Use im Zusammenhang mit konventionellen Waffen zunächst nicht nachteilig, da die Produktion für den zivilen und militärischen Sektor Skaleneffekte in der Produktion ermöglichen kann (z. B. bei der Herstellung von CPUs oder Flugzeugtriebwerken). Somit können einzelne Güter für alle Verbraucher – zivile wie militärische – billiger produziert werden. Wie bei den traditionellen Rüstungsgütern liegt das Spannungsfeld im möglichen Export dieser Güter. Hier stehen die Skaleneffekte durch die Massenproduktion und damit das zivil zu rechtfertigende Geschäftsinter-

se den möglichen sicherheitspolitischen Risiken oder ethischen Problemen gegenüber. Diese entstehen, wenn Akteure, die von den Exporteuren als nicht vertrauenswürdig eingestuft werden, Zugang zu bestimmten Gütern oder Technologien erhalten, was zu regionalen oder globalen Instabilitäten, zum Einsatz gegen die Zivilbevölkerung oder zum Verlust des eigenen Technologievorsprungs führen kann.

Regelungen, die unter anderem die Ausfuhr von Dual-Use-Gütern beschränken und regulieren, wie zum Beispiel das Wassenaar-Arrangement, zielen ausdrücklich darauf ab

„einen Beitrag zur regionalen und internationalen Sicherheit und Stabilität zu leisten, indem **Transparenz und ein verantwortungsvolleres Handeln** [sic!] **bei Exporten** von konventionellen Rüstungsgütern und Dual-Use-Gütern (Waren, Software und Technologie) gefördert und auf diese Weise **destabilisierende Waffenanhäufungen verhindert** werden. Die Teilnehmerstaaten versuchen, über ihre nationale Politik zu verhindern, dass Exporte dieser Güter zur Entwicklung oder zum Ausbau militärischer Fähigkeiten beitragen, die diesen Zielsetzungen zuwiderlaufen, und zur Unterstützung derartiger Fähigkeiten umgeleitet werden. Ziel des Wassenaar Arrangement ist es auch, **den Erwerb dieser Güter durch Terroristen** zu verhindern.“¹⁴

Wie im Falle des Wassenaar-Arrangements und anderer Ausfuhrbeschränkungsregelungen sind die Mitglieder des Regimes in der Lage, die betreffende Technologie zu produzieren, und machen häufig davon Gebrauch. Während einige Regime, wie z. B. das Missile Technology Control Regime, sogar den Technologieaustausch zwischen den Mitgliedern einschränken (zumindest im Prinzip), erlauben andere Regime den Austausch von Technologie zwischen den Mitgliedern.

Die Frage, welche spezifische Technologie oder Ware einen Dual-Use-Charakter und somit eine relevante militärische Bedeutung hat, kann nicht abstrakt entschieden werden, sondern hängt von Zeit und Raum ab. Technologien, die im strengen Sinne eindeutig einen doppelten Verwendungszweck haben, aber auf den heutigen Schlachtfeldern oder bei militärischen Operationen im weiteren Sinne keine wichtige Rolle spielen, könnten weniger streng oder überhaupt nicht eingeschränkt werden. Computer-CPU's früherer Generationen, die während des Kalten Krieges Beschränkungen unterlagen, heute aber nur noch sehr eingeschränkt genutzt werden können, wären ein Beispiel dafür, wie einst regulierte Güter heute als unproblematisch angesehen werden. Gleichzeitig zielen die USA und andere westliche Akteure darauf ab, den Zugang Chinas und Russlands zu Chip-Herstellungstechnologien der neuesten Generation zu beschränken, um diese potenziellen Konkurrenten zumindest für eine Generation hinter sich zu lassen.

Dementsprechend führen Regime wie das Wassenaar-Arrangement umfassende und regelmäßig aktualisierte Listen, in denen ausdrücklich Güter und Technologien genannt werden, die Ausfuhrbeschränkungen unterliegen. Die Mitgliedsstaaten nehmen Anpassungen in zwei Richtungen vor: Zum einen geben sie Technologien frei, die veraltet oder irrelevant geworden sind. Zum anderen nehmen sie neue Technologien auf, denen eine besondere militärische Eignung zugeschrieben wird.

Das Dual-Use-Problem wird durch die Tatsache verstärkt, dass sich seit dem Ende des Kalten Krieges das Verhältnis von ziviler sowie militärischer Forschung und Entwicklung erheblich verändert hat. Obwohl es sicherlich Gegenbeispiele gibt, lässt sich allgemein sagen, dass die treibenden Kräfte hinter der Entwicklung von Hightech-Technologie während des Kalten Krieges sehr oft militärische Entwicklungen waren, die dann ihren Weg in zivile Anwendungen fanden.¹⁵ Dieses Verhältnis änderte sich nach den 1990er Jahren, insbesondere im Bereich der Mikroinformatik und der Telekommunikation. Die allgemeine Verfügbarkeit modernster Mikroelektronik und die Verbreitung von Wissen

in diesem Bereich haben die Beschränkung von Dual-Use-Technologien erschwert. Das derzeitige internationale Sicherheitsklima und die in Deutschland erneut aufgeflammete Debatte über das angemessene Verhältnis von ziviler und militärischer Forschung, die auch Forderungen nach einer verstärkten Erforschung von Dual-Use-Technologien und -Gütern zur Verbesserung der militärischen Fähigkeiten beinhaltet, kann zumindest im deutschen Kontext zusätzliche Herausforderungen für die Dual-Use-Governance mit sich bringen.

Dual Use und Biologie

Im Bereich der Biologie und Biotechnologie nimmt das Dual-Use-Problem einen anderen Charakter an, ist aber dennoch von großer Bedeutung. Wie oben dargelegt, sind biologische Waffen durch das BWÜ umfassend verboten, und das Verbot gilt vermutlich sogar über den Vertrag hinaus. Es gibt somit keine legitimen offensiven militärischen Anwendungen von Biologie und Biotechnologie, während Aktivitäten zu „prophylaktischen, Schutz- und anderen friedlichen Zwecken“, einschließlich der biologischen Verteidigung, nach dem BWÜ erlaubt bleiben.

Im Bereich der Biologie ist das Konzept des Dual Use von entscheidender Bedeutung, da es viele Überschneidungen zwischen biologischer Verteidigung und gesundheitsbezogener Forschung gibt. Zahlreiche Maßnahmen im Bereich der öffentlichen Gesundheit, z. B. zur Eindämmung des Ausbruchs von Infektionskrankheiten oder zur Abschwächung ihrer Auswirkungen, sind auch für die biologische Verteidigung wichtig, um Angriffe mit biologischen Waffen abzuschrecken und sich dagegen zu schützen. Schließlich ist eine Bevölkerung, die gut gegen den Ausbruch von Krankheiten geschützt ist, ein weniger attraktives Ziel für einen Angriff mit biologischen Waffen. Darüber hinaus gibt es bei der biologischen Verteidigung einen spezifischeren Dual-Use-Aspekt. Denn einige der Schritte, die zur Entwicklung von Offensiv- oder Schutzmaßnahmen im Zusammenhang mit biologischen Waffen erforderlich sind, können sehr ähnlich sein. Dies gilt beispielsweise für das Verständnis von Immunreaktionen auf potenzielle biologische Kampfstoffe, die entweder zur Stärkung der Immunreaktion (defensiv) oder zu ihrer Umgehung (offensiv) erforscht werden können. Ebenso können Impfstoffe gegen biologische Kampfstoffe entwickelt werden, um Truppen und Bevölkerungen vor einem biologischen Angriff zu schützen (defensiv) oder um Truppen zu schützen, die einen biologischen Angriff planen (offensiv). Die Bestimmung des offensiven oder defensiven Charakters staatlicher biologischer Aktivitäten kann daher in erheblichem Maße von Kontextfaktoren und den Absichten derjenigen abhängen, die die jeweiligen Aktivitäten durchführen. Dies stellt eine besondere Herausforderung für die Verifikation der Einhaltung des BWÜ, für die Untersuchung mutmaßlicher Verstöße sowie für die Kontrolle bestimmter Technologien und ihrer Weitergabe dar.

Eine weitere Dimension des Dual-Use-Problems im biologischen Bereich betrifft die Möglichkeit, dass legitime, nützliche Forschung unbeabsichtigte Risiken schafft. Diese können aus Laborunfällen oder aus dem vorsätzlichen Missbrauch von biologischen Materialien und Technologien für böswillige Zwecke resultieren, z. B. für kriminelle oder terroristische Handlungen mit biologischen Stoffen. Dual-Use-Forschung in diesem Sinne ist kein neues Phänomen – eines der ersten bekannt gewordenen Beispiele war das 2001 veröffentlichte „Mäusepocken-Experiment“, bei dem australische Forschende bei Mäusen versehentlich die Immunität gegen Mäusepocken aufhoben, als sie versuchten, durch Gentechnik Unfruchtbarkeit herbeizuführen, um Australiens übermäßige Mäusepopulation zu kontrollieren.¹⁶ Dies warf die Befürchtung auf, dass das Experiment dazu verwendet werden könnte, die Immunität gegen Pocken beim Menschen zu schwächen. Weitere bekannte Beispiele sind die chemische Synthese des Polio-Virus im Jahr 2002,¹⁷

die Rekonstruktion des verschwundenen Virus der Spanischen Grippe von 1918 im Jahr 2005¹⁸ oder die Veränderung des Hundestaupe-Virus im Jahr 2013, um es für den Menschen potenziell infektiös zu machen.¹⁹

Das prominenteste Beispiel für Forschung, die mit guten Absichten durchgeführt wurde, aber auch potenzielle neue Risiken birgt, sind die 2011/12 durchgeführten Experimente mit der H5N1-Variante der Vogelgrippe: Forschende in den USA und den Niederlanden hatten versucht, die Übertragbarkeit des Virus in Frettchen, deren Immunsystem ein gutes Modell für menschliche Immunprozesse ist, zu verbessern, um sein pandemisches Potenzial zu bewerten.²⁰ Eine Pandemie mit H5N1 beim Menschen könnte noch schwerer wiegende Folgen haben als die Covid-19-Pandemie, so dass die Verhinderung eines weltweiten Ausbruchs von höchstem Interesse für die öffentliche Gesundheit ist. Kritiker*innen des Experiments wiesen jedoch darauf hin, dass diese Art von Forschung dazu beitragen könnte, eben die Gefahr erst zu schaffen, gegen die sie gerichtet ist. Dies löste eine weltweite Kontroverse über sogenannte „Dual-Use Research of Concern“ (DURC) aus, also Dual-Use-Forschung mit besonders hohem Risikopotenzial. Die H5N1-Experimente stießen auch die Diskussion über den Umgang mit Dual-Use-Forschung in Deutschland an.

Für eine kurze Einführung zur Australischen Gruppe, siehe S. 90.

Wie auch in anderen Bereichen der Rüstungskontrolle gibt es keine global gültigen internationalen Weitergabe- oder sonstigen Vorschriften für biowaffenbezogene Dual-Use-Forschung oder -Güter. Die Australische Gruppe ist eine informelle Vereinigung, in der 43 Staaten und die EU ihre Ausfuhren koordinieren, die mit chemischen und biologischen Waffen in Zusammenhang stehen könnten; ihre Mitglieder haben Listen von Materialien, Ausrüstungen und Technologien erstellt, die als Dual-Use-Produkte gelten und von den Gruppenmitgliedern nationalen Ausfuhrkontrollen unterworfen werden sollen. Nach Artikel IV des BWÜ wird von allen BWÜ-Mitgliedsstaaten erwartet, dass sie nationale Exportkontrollen einführen, um die Verpflichtung des BWÜ zur Nichtverbreitung umzusetzen. Die genaue Ausgestaltung dieser Kontrollen bleibt jedoch dem Ermessen der einzelnen Staaten überlassen.

Auch für den Bereich der Biowissenschaften gibt es keine weltweit einheitlichen Definitionen, Konzepte oder Strategien für den Umgang mit Dual Use. Die Weltgesundheitsorganisation (WHO) hat 2022 einen „Globalen Orientierungsrahmen für die verantwortungsvolle Nutzung der Biowissenschaften“ veröffentlicht, der „Werte und Grundsätze, Instrumente und Mechanismen zur Unterstützung der Mitgliedstaaten und der wichtigsten Interessengruppen bei der Minderung und Vermeidung von Biorisiken und der Regelung der Dual-Use-Forschung“ bieten soll.²¹ Die Umsetzung dieses Rahmens erfolgt auf rein freiwilliger Basis, was dem im BWÜ verfolgten Ansatz entspricht, den Schwerpunkt auf freiwillige Maßnahmen und Selbstregulierung zu legen, wie z. B. die Sensibilisierung für das Dual-Use-Problem oder die Förderung von Verhaltenskodizes für Biowissenschaftler*innen, um die von Forschung mit Dual-Use-Potenzial ausgehenden Risiken einzudämmen. Dies erfordert eigentlich eine kontinuierliche Beobachtung der wissenschaftlichen und technologischen Entwicklungen. Derzeit ist dies ausschließlich den Staaten selbst überlassen, und die Kapazitäten dafür sind sehr unterschiedlich ausgeprägt. Im Rahmen des BWÜ wird aktuell über die Einrichtung eines wissenschaftlichen Beratungsmechanismus diskutiert, der auch dabei helfen könnte, Forschung mit Dual-Use-Potenzial zu erkennen. Die Regulierung solcher Forschung bleibt jedoch vorerst in den Händen der Staaten.

Fazit

Wenn es um die nationale und internationale Sicherheit geht, treten Dual-Use-Probleme in verschiedenen Formen auf und können durch unterschiedliche Governance-Ansätze angegangen werden. Erstens gibt es Ausfuhrkontrollmaßnahmen, die in der Regel nationalen strategischen Prioritäten folgen (und manchmal international koordiniert werden). Sie können Technologien betreffen, die für verbotene Waffensysteme relevant sind, aber auch Technologien für Waffen, die nach internationalem Recht legal sind. Häufig bedeuten solche Exportkontrollen, dass in einem Land verfügbare Technologien anderen Ländern aufgrund politischer Einschätzungen nicht zur Verfügung gestellt werden. Zweitens kann ein internationales Verbot von Waffen durch Abrüstungsabkommen wie das CWÜ oder das BWÜ erreicht werden. Diese Abkommen zielen auf ein weltweites Verbot der betreffenden Waffen ab, was bedeutet, dass die Staaten freiwillig auf militärische Optionen verzichten, die ihnen andernfalls zur Verfügung stehen würden. Atomwaffen sind nicht generell verboten, da die fünf Staaten, die rechtmäßig im Besitz von Atomwaffen sind, diese zwar behalten dürfen (obwohl auch sie verpflichtet sind, sie irgendwann abzuschaffen), aber dennoch bestimmten Beschränkungen unterworfen sind. Das Dual-Use-Dilemma in all diesen Fällen besteht in der Schwierigkeit zu unterscheiden, ob die Güter für verbotene militärische Zwecke oder für legitime Anwendungen bestimmt sind. Drittens kann sich die Regulierung auf Dual-Use-Forschung erstrecken. Dies umfasst auch, aber nicht ausschließlich, Forschung, deren Ergebnisse möglicherweise eine unmittelbare Gefahr des Missbrauchs mit potenziell schwerwiegenden Folgen darstellen. Hier spielen neben rechtlichen Erwägungen auch ethische Fragen eine Rolle. Zumindest in den westlichen Ländern wird dabei der Selbstkontrolle der Wissenschaft ein hoher Stellenwert beigemessen, da die Dual-Use-Problematik gegen die Forschungsfreiheit abgewogen werden muss (die in Deutschland im Grundgesetz verankert ist).

Dual-Use-Probleme treten in verschiedenen Formen auf und müssen daher durch unterschiedliche Governance-Ansätze angegangen werden: Maßnahmen zur Ausfuhrkontrolle, internationale Abrüstungsabkommen und Regulierung von Dual-Use-Forschung, wobei die Selbstkontrolle der Wissenschaft einen hohen Stellenwert hat.

In den folgenden Kapiteln werden all diese Aspekte aufgegriffen. Alle Kapitel über neu aufkommende disruptive Technologien im konventionellen Bereich (darunter künstliche Intelligenz und Halbleiter, Drohnen und additive Fertigung) befassen sich mit schwach regulierten Dual-Use-Technologien. In einigen Fällen, wie bei der additiven Fertigung, ist die Regulierung über die Ausfuhrkontrolle besonders schwierig, da die erforderliche Technologie weltweit verfügbar ist. In anderen Bereichen (z. B. Drohnen) gibt es zwar gewisse, aber schwache Maßnahmen zur Exportkontrolle. In vielen Fällen wäre eine Regulierung durch kollektive und kooperative Rüstungskontrollmaßnahmen unter dem Gesichtspunkt der internationalen Stabilität wünschenswert, ist aber zumindest kurzfristig unwahrscheinlich. Die Beiträge, die sich mit den Risiken und dem Nutzen wissenschaftlicher und technologischer Entwicklungen in der Biologie und Biotechnologie befassen, betonen die Verantwortung der einzelnen Wissenschaftler*innen. Sie beschreiben die zunehmende Konvergenz von künstlicher Intelligenz und Biologie, das Missbrauchspotenzial der gentechnischen Veränderung onkolytischer Viren und die Möglichkeiten zur Unterstützung der biologischen Abrüstung, die sich aus den Entwicklungen bei Nachweis- und Identifizierungstechnologien ergeben. Soweit möglich schlagen sie spezifische Ansätze für Forschende vor, um Dual-Use-Risiken zu mindern. Insgesamt zeigen alle Beiträge die Schwierigkeit auf, zivile und militärische Potenziale

hinter technologischen Entwicklungen zu bestimmen und Missbrauchspotenziale ansonsten nützlicher Forschung zu erkennen, zu bewerten und zu handhaben. Sie betonen die Rolle der Absicht in diesen Prozessen und weisen auf die damit verbundenen Herausforderungen für Regulierungsansätze hin. Sie zeigen auch, dass technologische Entwicklungen, selbst solche mit Dual-Use-Potenzial, in verschiedener Hinsicht Vorteile mit sich bringen können und dass das Bewusstsein für die Dual-Use-Dimension dazu beiträgt, ein Gleichgewicht zwischen der Minderung der Risiken und der Nutzung der Vorteile zu finden.

Prof. Dr. Christopher Daase

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

Prof. Dr. Malte Götsche

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

Dr. Una Jakob

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

Prof. Dr. Thilo Marauhn

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

Dr. Niklas Schörnig

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

- 1 Reppy, J. (2006, March 31). Managing Dual-Use Technology in an Age of Uncertainty. *The Forum*, 4(1). <https://doi.org/10.2202/1540-8884.1116>
- 2 Allerdings wird der Begriff im militärischen Bereich manchmal anders verwendet, z. B. für Waffensysteme, die sowohl konventionelle als auch nukleare Sprengköpfe tragen können, d. h. „dual-capable“ sind; diese Bedeutung soll hier aber nicht weiter verfolgt werden.
- 3 Wassenaar Arrangement. (2019). *Criteria for the selection of dual-use items*. https://www.wassenaar.org/app/uploads/2019/consolidated/Criteria_for_selection_du_sl_vsl.pdf; unsere Übersetzung.
- 4 Diese Forderung wurde auch von Staaten erhoben, beispielsweise in der Bletchley Declaration oder in den 11 AI-Prinzipien und dem Verhaltenskodex, die 2023 von den Staatsschefs der G7 vereinbart wurden. Weiterer Vorschläge beinhalten die Schaffung einer Welttechnologieorganisation oder die Einrichtung einer Organisation ähnlich der Internationalen Atomenergiebehörde (IAEO).
- 5 Joyner, D.H. (2022). Strategic trade controls. In E.P.J. Myjer, & T. Marauhn (Hrsg.), *Research Handbook on International Arms Control Law* (S. 121–130). Elgar.
- 6 Europäische Union. (2023, 20. Oktober). Compilation of national control lists under Article 9(4) of Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (C/2023/441). *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202300441
- 7 Joyner, D. (2004). Restructuring the multilateral export control regime system. *Journal of conflict and security law*, 9, 181–211. <https://doi.org/10.1093/jcsl/9.2.181>
- 8 Deutscher Ethikrat. (2024, 7. Mai). *Biosicherheit – Freiheit und Verantwortung in der Wissenschaft*. <https://www.ethikrat.org/publikationen/stellungnahmen/biosicherheit/>
- 9 Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung. (2022, 1. November). *Wissenschaftsfreiheit und Wissenschaftsverantwortung (2022): Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung*. Leopoldina und DFG. <https://www.sicherheitsrelevante-forschung.org/publikation-wissenschaftsfreiheit2022/>
- 10 Siehe Jakob, U., Kraemer, F., Kraus, F., Lengauer, T. (2024). Applying Ethics in the Handling of Dual Use Research: The Case of Germany, *Research Ethics*, online veröffentlicht am 10. Juni, 2024. <https://doi.org/10.1177/17470161241261044>.
- 11 Vgl., unter anderem: Marauhn, T. (2014). Global governance of dual-use trade: The contribution of international law. In O. Meier (Hrsg.), *Technology Transfers and Non-Proliferation: Between control and cooperation* (S. 45–75). Routledge.
- 12 Schweizer Eidgenossenschaft. (1976, 4. Mai). *Übereinkommen über das Verbot der Entwicklung, Herstellung und Lagerung bakteriologischer (biologischer) Waffen und von Toxinwaffen sowie über die Vernichtung solcher Waffen* (AS 1976 1438). Schweizer Eidgenossenschaft. https://www.fedlex.admin.ch/eli/cc/1976/1438_1439_1439/de
Schweizer Eidgenossenschaft. (1997, 29. April). *Übereinkommen über das Verbot der Entwicklung, Herstellung, Lagerung und des Einsatzes chemischer Waffen und über die Vernichtung solcher Waffen* (AS 1998 335). Schweizer Eidgenossenschaft. https://www.fedlex.admin.ch/eli/cc/1998/335_335_335/de

- Krutzsch, W., Trapp, R. (1994). *A Commentary on the Chemical Weapons Convention*, Dordrecht et al.: Martinus Nijhoff, 20-44; Pearson, G.S. (2000). The CWC general purpose criterion: how to implement?. *The CBW Conventions Bulletin*, 49, 1–7. https://projects.iq.harvard.edu/files/meselsonarchive/files/200049_cbwcb49.pdf
- 13 Ein Element zur Bewältigung dieser Herausforderung ist der Verweis auf die Arten und Mengen der Stoffe, siehe Artikel II (1) (a) CWÜ: „solange diese nach Art und Menge mit solchen Zwecken vereinbar sind“ und Artikel 1 (1) BWÜ „von Arten und in Mengen, die nicht durch Vorbeugungs-, Schutz- oder sonstige friedliche Zwecke gerechtfertigt sind“.
- 14 Wassenaar Arrangement. (2024). *Über uns*. <https://www.wassenaar.org/de/about-us/>; unsere Hervorhebung.
- 15 Molas, J., Walker, W. (1992). Military Innovation's Growing Reliance in Civil Technology: A New Source of Dynamism and Structural Change. In W.A. Smit, J. Grin, & L. Voronkov (Hrsg.), *Military Technology Innovation and Stability in a Changing World* (S.17). VU University Press.
- 16 Jackson, R.J., Ramsay, A.J., Christensen, C.D., Beaton, S., Hall, D.F., & Ramshaw, I.A. (2001). Expression of mouse interleukin-4 by a recombinant ectromelia virus suppresses cytolytic lymphocyte responses and overcomes genetic resistance to mousepox. *J Virol*, 75(3), 1205–1210. <https://doi.org/10.1128/jvi.75.3.1205-1210.2001>
- 17 Cello, J., Paul, A.V., & Wimmer, E. (2002, July 11). Chemical synthesis of poliovirus cDNA: generation of infectious virus in the absence of natural template. *Science*, 297(5583), 1016-1018. <https://doi.org/10.1126/science.1072266>.
- 18 Tumpey, T.M., Basler, C.F., Aguilar, P.V., Zeng, H., Solórzano, A., Swayne, D.E., Cox, N.J., Katz, J.M., Taubenberger, J.K., Palese, P., & García-Sastre, A. (2005, October 7). Characterization of the Reconstructed 1918 Spanish Influenza Pandemic Virus. *Science*, 310(5745), 277-80. <https://doi.org/10.1126/science.1119392>.
- 19 Bieringer, M., Han, J.W., Kendl, S., Khosravi, M., Plattet, P., Schneider-Schaulies, J. (2013, March 12). Experimental Adaptation of Wild-Type Canine Distemper Virus (CDV) to the Human Entry Receptor CD150. *PLOS ONE*, 8(3), e57488. <https://doi.org/10.1371/journal.pone.0057488>
- 20 Herfst, S., Schrauwen, E.J.A., Linster, M., Chutinimitkul, S., de Wit, E., Munster, V.J., Sorrell, E.M., Bestebroer, T.M., Burke, D.F., Smith, D.J., Rimmelzwaan, G.F., Osterhaus, A.D.M.E., & Fouchier, R.A.M. (2012, June 22). Airborne Transmission of Influenza A/H5N1 Virus Between Ferrets. *Science*, 336(6088), 1534–1541. <https://doi.org/10.1126/science.1213362>; Imai, M., Watanabe, T., Hatta, M., Das, S.C., Ozawa, M., Shinya, K., Zhong, G., Hanson, A., Katsura, H., Watanabe, S., Li, C., Kawakami, E., Yamada, S., Kiso, M., Suzuki, Y., Maher, E.A., Neumann, G., & Kawaoka, Y. (2012). Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5HA/H1N1 virus in ferrets. *Nature*, 486, 420–428. <https://doi.org/10.1038/nature10831>
- 21 World Health Organization. (2022, September 13). *Global guidance framework for the responsible use of the life sciences: mitigating biorisks and governing dual-use research*. <https://www.who.int/publications/i/item/9789240056107>; unsere Übersetzung.

TRENDS

Künstliche Intelligenz

Künstliche Intelligenz, Halbleiter und das Militär

Verfahren aus dem Bereich der Künstlichen Intelligenz (KI) haben in den vergangenen Jahren einen enormen Entwicklungsschub erfahren, der insbesondere durch globale Tech-Unternehmen und Forschungseinrichtungen vorangetrieben wird. Gleichzeitig demonstriert der Einsatz dieser Dual-Use-Technologie in der Gefechtsfeldsteuerung und Datenanalyse in der Ukraine oder zur großflächigen Auswahl militärisch relevanter Ziele in Gaza exemplarisch die Relevanz, die diese Technologie zunehmend auch für militärische Akteure entwickelt. Diese Anwendungen verdeutlichen jedoch auch die Herausforderungen dieser Technologie hinsichtlich der Grenzen menschlicher Kontrolle und der Nachvollziehbarkeit von automatischen Entscheidungen und unterstreichen die Notwendigkeit einer Regulierung. Parallel dazu entwickelt sich die Dominanz über KI- und Halbleitertechnologien sowie die Verfügbarkeit der zugrunde liegenden Produktionsketten zunehmend zu einem globalen Power-Play.

*Zur Vertiefung, siehe die
entsprechenden Einträge
im Glossar ab S. 96.*

Obgleich Künstliche Intelligenz und das darin enthaltene Teilgebiet des maschinellen Lernens (ML) eine große Bandbreite von Ansätzen abdeckt, basieren die aktuellen KI-Systeme nahezu ausschließlich auf dem Konzept der sogenannten künstlichen neuronalen Netzwerke (KNN). Bei diesem Ansatz, der auf Ideen aus den 1940er Jahren basiert, werden die Funktion und Vernetzung menschlicher Gehirnzellen nachempfunden. Obgleich in den 1980ern und 1990ern bereits umfangreich erforscht, haben erst aktuelle Halbleitertechnologien und die Herstellung hochgradig leistungsstarker, günstiger und kleiner Chips die Leistungsfähigkeit erreicht, die in Verbindung mit effizienteren Softwarearchitekturen moderne KI-Anwendungen ermöglichen. Weitere Ansätze wie symbolische KI, Entscheidungsbäume und evolutionäre Algorithmen spielen zwar in spezifischen Anwendungen eine Rolle, in öffentlichen Debatten bezieht sich der Begriff KI aber in aller Regel auf KNN.

*Zum Trainingsprozess
siehe auch den Eintrag
„Daten und Training (KI)“ im
Glossar, S. 96.*

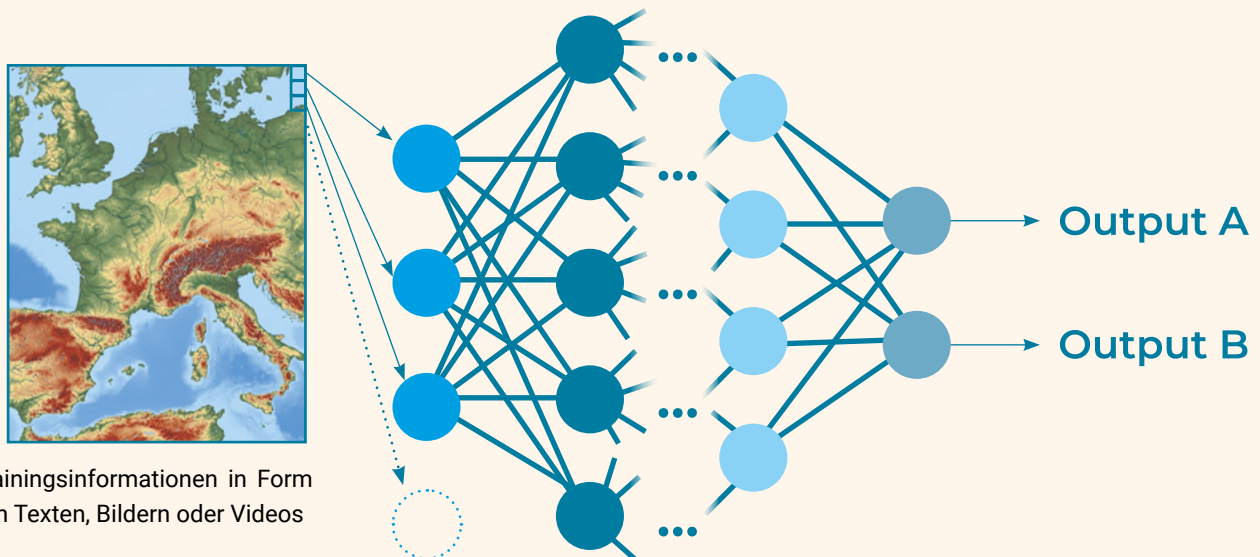
Kernstück einer KI-Anwendung ist das sogenannte Modell, eine Datenstruktur zum Speichern digitaler Informationen. Dieses wird mithilfe umfangreicher Daten, die auf die zu erzielende Problemlösungsfähigkeit zugeschnitten sind, in einem sogenannten Trainingsprozess aufgebaut. In der Regel handelt es sich hier um das sogenannte Deep Learning (DL). Modelle sind dabei entweder auf eine konkrete Aufgabe zugeschnitten oder in Form oft kommerziell vermarkteter Foundation-Modelle vortrainiert, die in weiteren Trainingsprozessen mit spezifischen Daten auf den eigentlichen Anwendungskontext optimiert werden. Die Qualität und Verfügbarkeit von Trainingsdaten ist dabei entscheidend für



die erzielbare Problemlösungsfähigkeit der KI, weshalb diese oft durch spezialisierte Unternehmen zusammengestellt, von Hand kuratiert und entsprechend am Markt als wirtschaftliches Gut angeboten werden. Aktuelle KI-Generationen unterscheiden sich hinsichtlich der Form der Daten, die im Training sowie während der Anwendung verarbeitet und für die Nutzerinteraktion eingesetzt werden können. Während sich diese Differenzierung jedoch zunehmend auflöst, arbeiten die weltweit führenden KI-Unternehmen wie OpenAI, Meta, Microsoft oder Anthropic an einer sogenannten „Künstlichen allgemeinen Intelligenz“ (AGI – Artificial General Intelligence). Diese soll menschenähnliche kognitive Fähigkeiten aufweisen und damit beispielsweise in der Lage sein, aus Erfahrungen zu lernen, Schlussfolgerungen selbstständig zu korrigieren oder mit anderen KI-Systemen zu interagieren. Wann und ob dieses ambitionierte Ziel überhaupt erreicht werden kann, ist aber in Expert*innen-Kreisen umstritten.¹

KI-Modelle lassen sich nach Fähigkeiten und Art der Trainingsdaten unterscheiden. Zur Erläuterung, siehe „LLM, LMM und AGI“ im Glossar, S. 97.

Deep Learning in Künstlichen Neuronalen Netzen (KNN)



Die Interaktionen neuronaler Zellen werden in Form von KNN nachgestellt (vereinfachte Darstellung).

All diese KI-Systeme benötigen enorme Rechenleistungen, um trainiert und in einer fertigen Anwendung ausgeführt zu werden. Im Kontrast zu Cloud-Server-Zentren ist das nur mit sehr viel rechenstärkeren Chips möglich, die auch über längere Zeit unter Volllast betrieben werden können. Die neueste Generation von KI-Beschleunigern (die sogenannte GB200-Architektur) des Marktführers Nvidia, die einen KI-Chip (GPU) und weitere notwendige Hardware kombiniert, hat beispielsweise eine Leistungsaufnahme von rund 1500 Watt pro Geräteeinheit, bei einer dauerhaften Rechenleistung von $45 \cdot 10^{12}$ Billionen Operationen pro Sekunde.² Zum Vergleich: Ein iPhone 14 schafft in kurzen Lastspitzen ca. $1,4 \cdot 10^{12}$ Operationen pro Sekunde.³ KI-Rechenzentren, in denen Zehn- bis Hunderttausende dieser Geräte gemeinsam betrieben werden, erreichen so Gesamtleistungsaufnahmen von 100 Megawatt und mehr.⁴ Da solche Server-Systeme mit den notwendigen Netzwerk-Infrastrukturen für den internen Datenaustausch sowie für die Stromversorgung und die enorm aufwendige Kühlung der Anlagen ausgestattet werden müssen, sind die Herstellung dieser technischen Anlagen, deren Aufbau und Betrieb enorm kostspielig.⁵

Zur Vertiefung, siehe den Eintrag „GPU und KI-Chips“ im Glossar, S. 96.

Militärische KI-Anwendungen

Der Einsatz von KI im Kampf der Ukraine gegen Russland oder im Krieg Israels gegen die Hamas haben die Dynamiken der Einführung von neuen Technologien mit Dual-Use-



Soldaten benutzen ein Tablet während einer Übung, bei der die Möglichkeiten des KI-gestützten Advanced Battle Management System demonstriert werden. Foto: U.S. Air Force photo by Tech. Sgt. Joshua J. Garcia.

Potenzial in militärische Anwendungen verdeutlicht. Im ersten Fall sind KI-Anwendungen eher aus der Situation heraus entstanden und werden ad hoc in militärische Prozesse eingebettet und de facto im Feld getestet, angepasst und ausgebaut. Am Beispiel Israels wird dagegen die langfristige strategische Einbettung solcher Anwendungen in militärische Entscheidungsabläufe, verbunden mit dem notwendigen logistischen und technischen Struktur- aufbau, deutlich. Beiden Kriegen ist gemein, dass KI-Systeme darin überwiegend als Hilfsmittel in der taktischen Planung eingesetzt werden, um die Entscheidungsfindung durch die automatisierte Aggregation und Auswertung unterschiedlichster Datenquellen zu unterstützen und zu beschleunigen – sogenannter Decision-Support- bzw. Battlefield-Management-Systeme. Während in der Ukraine damit beispielsweise Truppenbewegungen vorhergesagt werden, sind im Zuge des Gaza-Krieges die israelischen Systeme „Lavender“⁶ und „Gospel“⁷ bekannt geworden, die eingesetzt werden, um physische Objekte aber auch Personen zu identifizieren und als potenziell relevante militärische Ziele zu markieren. Diese Anwendung von KI kann als

nächster Schritt nach dem als Big Data bekannten Ansatz verstanden werden, die umfangreichen Daten aus moderner militärischer Sensorik wie Bild- und Videodaten, aber auch Bewegungsprofile von Zielen zusammenzuführen und durch technische Unterstützung aufzubereiten.⁸ Diese, aus militärischer Perspektive als taktischer Vorteil verstandene, Verringerung der sogenannten Sensor-to-Shooter-Zeitspanne⁹ erhöht dabei die Geschwindigkeit der Kriegsführung weiter, während die Rolle der menschlichen Kontrolle und Eingriffsmöglichkeiten weiter zurückgedrängt und letztere zunehmend als Nadelöhr wahrgenommen werden.¹⁰

Auch der Trend zu Autonomisierung militärischer Waffensysteme befeuert die Entwicklung und den Einsatz von KI. Solche Systeme sollen zum einen entweder in unbekanntem Gebiet oder unter variablen Bedingungen operieren und benötigen im Gegensatz zu starren Anweisungen die Möglichkeit, flexibel auf Situationen zu reagieren. KI-Systeme ermöglichen diese Fähigkeiten, die beispielsweise darin bestehen können, autonom in einem Zielgebiet zu operieren und dabei Hindernisse zu berücksichtigen oder militärische Ziele auch bei verrauschten Datenquellen zu identifizieren. Zum anderen sind KI-Systeme in der Lage, im Trainingsprozess selbständig Muster zu erfassen oder Regeln aus Datenmaterial abzuleiten. Dadurch können KI-Systeme hochkomplexe Fähigkeiten wie die Steuerung und den Luftkampf von Kampfjets erlernen,¹¹ ohne dass diese explizit formuliert werden müssen. Technologisch kommt hierbei zum Tragen, dass unterschiedliche KI-Systeme auch gekoppelt betrieben werden können. So können beispielsweise die Auswertung von Radardaten, die Identifikation von potenziellen Zielen oder die Navigation eines Fahrzeuges durch einzelne KI-Systeme realisiert werden und deren Ausgaben dann in einer übergreifenden KI für die Gesamtsteuerung zusammengeführt werden.

Neben diesen komplexen Anwendungen von KI sind einige spezielle Fähigkeiten mittlerweile technologisch derart ausgereift – wie die Bildauswertung oder die Sprachanalyse,



die mittlerweile in jedem modernen Smartphone als Chips verbaut sind –, dass auch militärische Kleingeräte wie Quadrocopter damit massenhaft günstig versehen und entsprechend verbessert werden können. Dieses „Ausrollen in der Breite“ ermöglicht damit Anwendungen, wie sie beispielsweise im US-Programm „Replicator“¹² umgesetzt werden sollen, das den großflächigen, automatisierten und autonomisierten Einsatz von Drohenschwärmen vorsieht – eine Idee, die unlängst auch im Rahmen der NATO zur Grenzsicherung gegenüber Russland diskutiert worden ist.¹³

Auch im Cyberspace spielt KI eine zunehmende Rolle, beispielsweise bei der automatisierten Auswertung der Datentransfers, um ungewöhnliche Aktivitäten zu identifizieren, die auf Cyberattacken schließen lassen, um Schadsoftware zu entdecken oder auch um automatisiert Gegenmaßnahmen auszulösen.¹⁴ Gleichzeitig kann KI aber auch eingesetzt werden, um auf Grundlage verfügbarer Datenbanken von Sicherheitslücken neue Schadsoftware automatisiert zu erzeugen oder auf ausgewählte Ziele zuzuschneiden.¹⁵

Diese Fähigkeit von KI, neue Varianten eines digitalisierten Datensatzes auf Grundlage bestehender Informationen zu generieren, wird mit Blick auf die Herstellung neuer Bio- und Chemiewaffen als hochkritisch angesehen.

Für eine Diskussion dieses Aspekts, siehe den Beitrag von Kadri Reis ab S. 46.

Hinsichtlich der Analyse von Bild- und Sensordaten wird KI immer wieder auch im Rahmen der nuklearen Abschreckung und der dafür notwendigen Überwachungs- und Sensorinfrastrukturen diskutiert. Da insbesondere für diesen Einsatz die Reaktionsgeschwindigkeit bei einem hypothetischen nuklearen Angriff als entscheidend betrachtet wird, sollen KI-Systeme hier für die Erkennung nuklearer Angriffsvorbereitungen und Aktivitäten eingesetzt werden.¹⁶ Gleichzeitig verdeutlicht dieses Szenario die Gefahr der „Eskalation aus Versehen“ und die Unabwägbarkeiten beim Einsatz einer schwer kontrollierbaren oder nachvollziehbaren Technologie, selbst wenn diese „nur“ zur Filterung und Analyse von Daten dient.

Zusammengefasst wird KI seitens militärischer Akteure als „Enabling“-Technologie aufgefasst, die bestehende Anwendungen optimiert oder die operative Ausweitung in bestimmten Einsatzszenarien ermöglicht. Eine wesentliche Motivation besteht dabei darin, taktische Vorteile durch die Beschleunigung von Entscheidungsprozessen sowie Informationsvorteile zu erlangen. In Verbindung mit autonomen Waffensystemen spielen darüber hinaus auch Überlegungen eine Rolle, die Gefahr eigener menschlicher Verluste durch den Einsatz technischer Geräte zu verringern. KI wird darüber hinaus als Lösung angesehen für ein immanentes Problem der zunehmenden Technisierung der Streitkräfte, nämlich dass immer bessere Waffen- und Sensortechnik in aller Regel auch immer größere Datenmengen erzeugen, die kaum mehr durch menschliche Operateure handhabbar sind.

Zusammengefasst wird KI seitens militärischer Akteure als „Enabling“-Technologie aufgefasst, die bestehende Anwendungen optimiert oder die operative Ausweitung in bestimmten Einsatzszenarien ermöglicht.

Ausblick und Empfehlungen

Angesichts des rasanten Fortschritts von KI-Technologie debattieren Staaten gegenwärtig in unterschiedlichen Formaten und oft in enger Kooperation mit Vertreter*innen der KI-Tech-Unternehmen, wie ein verantwortungsvoller Umgang mit KI aussehen kann und welche Form der Regulation dafür notwendig wäre.¹⁷ Insbesondere für die militärische Anwendung sollten sich diese Debatten dabei unmittelbar an den Fragen orientieren, wie

Zur Vertiefung siehe den Eintrag „XAI – Explainable Artificial Intelligence“ im Glossar, S. 99.

sie bereits im Kontext autonomer Waffensysteme seit langem gestellt werden, etwa nach den Möglichkeiten menschlicher Kontrolle und Verantwortlichkeit sowie Vereinbarkeit solcher Systeme mit dem Völkerrecht, aber auch nach Gefahren für die militärische Stabilität zwischen möglichen Gegnern. Gleichzeitig darf dabei nicht außer Acht gelassen werden, dass selbst bei einer KI-gestützten Anwendung, deren finale Entscheidung durch einen menschlichen Operator getroffen wird, die KI selbst durch Filter- und Analyseprozesse unzählige Mikro-Entscheidungen getroffen hat, die weder im Trainingsprozess explizit und nachvollziehbar definiert worden sind noch dem Operator in der Situation der Entscheidung transparent sind.¹⁸ Auch wenn erste Ansätze der sogenannten „Erklärbaren KI“ (Explainable Artificial Intelligence – XAI)¹⁹ versuchen, diesen Black-Box-Charakter einer KI aufzulösen, so reichen diese bei weitem nicht an die benötigte Erklärbarkeit heran, wie sie menschliche Schlussfolgerungsprozesse bieten. Darüber hinaus führen diese Ansätze in aller Regel zu einer Reduktion der Leistungsfähigkeit und Reaktionsgeschwindigkeit einer KI, also den Hauptvorteilen dieser Technologie, und werden sich ohne verbindliche rechtliche Vorgaben kaum durchsetzen können.

Erste staatliche Vorstöße bei der Regulierung militärischer KI lassen aber auch Divergenzen hervortreten, insbesondere zwischen Staaten, die Teil der extrem zentralisierten KI-Produktionsketten sind, wie die USA, UK, die Niederlande und Taiwan, und Staaten, die daran aktuell nicht partizipieren, allen voran China. Angesichts der starken Zentralisierung und der globalen Abhängigkeit von Halbleiterfertigungsbetrieben in Taiwan wie TSMC (so genannte Foundries) verstärkt diese Entwicklung allerdings auch die Sorge vor zunehmenden internationalen Spannungen. Dies wird in besonderem Maße in Form der „Chip Wars“ deutlich, mit denen die USA einerseits versuchen, chinesische Hersteller vom Zugriff auf spezialisierte KI-Chips und das dafür benötigte Know-how, die Herstellungsgeräte, Materialien und Produktionsketten abzuhalten²⁰ und andererseits durch spezielle Mechanismen wie Kill-Switches in Chip-Herstellungsanlagen²¹ – die im Bedarfsfall die Geräte zerstören würden – ihren Verbündeten Taiwan vor dem chinesischen Hoheitsanspruch zu schützen.

Eine Übersicht von bisherigen Initiativen zur Regulierung von KI findet sich im Anhang ab S. 93.

Unabhängig von der individuellen Bewertung dieser Maßnahmen demonstrieren die USA aber auch, dass es durchaus Ansatzmöglichkeiten für die Regulierung von KI-Systemen gibt. So definiert die „Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence“ (Executive Order 14110 von 2023) technisch messbare Parameter, wie die für das Training oder die Ausführung eines KI-System benötigte Gesamtrechenleistung, als Grundlage für die US-Exportkontrolle solcher Geräte und fertiger KI-Produkte. Angesichts dieser Ansatzpunkte, verbunden mit dem Aspekt, dass es trotz des digitalen Charakters von KI-Anwendungen vor allem die spezialisierten Server- und Netzwerkgeräte sind, die leistungsfähige KI-Systeme ermöglichen, bestehen für die Rüstungskontrolle vielleicht noch Chancen. Dafür müssten auch andere Staaten diese Impulse aufgreifen, weiterentwickeln und unterstützen.

Dr. Thomas Reinhold

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

-
- 1 Fjelland, R. (2020). Why general artificial intelligence will not be realized. *Humanities and Social Sciences Communications*, 7(1), 10. <https://doi.org/10.1057/s41599-020-0494-4>
 - 2 Spille, C. (2024, 18. März). *Blackwell: Nvidia enthüllt seine nächste KI-Beschleuniger-Generation*. heise online. <https://www.heise.de/news/Nvidias-neue-KI-Chips-Blackwell-GB200-und-schnelles-NVLink-9658475.html>
 - 3 Owen, M. (2022, 26. September). *How iPhone speeds have grown in the last 5 years*. appleinsider. <https://appleinsider.com/articles/22/09/26/how-iphone-speeds-have-grown-in-the-last-5-years>



- 4 Patel, D., & Nishball, D. (2024, 17. Juni). *100k H100 Clusters: Power, Network Topology, Ethernet vs InfiniBand, Reliability, Failures, Checkpointing*. SemiAnalysis. <https://www.semianalysis.com/p/100000-h100-clusters-power-network>
- 5 Patel & Nishball, 2024.
- 6 Abraham, Y. (2024, 3. April). 'Lavender': The AI machine directing Israel's bombing spree in Gaza. 972 Magazine. <https://www.972mag.com/lavender-ai-israeli-army-gaza/>
- 7 Davies, H., McKernan, B., & Sabbagh, D. (2023, 1. Dezember). 'The Gospel': How Israel uses AI to select bombing targets in Gaza. The Guardian. <https://www.theguardian.com/world/2023/dec/01/the-gospel-how-israel-uses-ai-to-select-bombing-targets>
- 8 RAFAEL Advanced Defense Systems LTD. (2019). FIRE WEAVER - Tactical Networked Sensor-to-Shooter System. <https://www.rafael.co.il/system/fireweaver/>
- 9 Skove, S. (2024, 7. März). *Targeting time shrinks from minutes to seconds in Army experiment*. DefenseOne. <https://www.defenseone.com/threats/2024/03/targeting-time-shrinks-minutes-seconds-army-experiment/394758/>
- 10 Deutscher Ethikrat. (2023). *Mensch und Maschine – Herausforderungen durch Künstliche Intelligenz – Stellungnahme des Deutschen Ethikrates*. <https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/deutsch/stellungnahme-mensch-und-maschine.pdf>
- 11 Copp, T. (2024, 5. April). *An AI-controlled fighter jet took the Air Force leader for a historic ride. What that means for war*. Politico. <https://www.politico.com/news/2024/05/04/an-ai-controlled-fighter-jet-took-the-air-force-leader-for-a-historic-ride-what-that-means-for-war-00156147>
- 12 Katz, J. (2024, 20. Januar). *Replicator's 'PRIME' time: DIU seeks small USV interceptors ready for rapid production*. Breaking Defense. <https://breakingdefense.com/2024/01/replicators-prime-time-diu-seeks-small-usv-interceptors-ready-for-rapid-production/>
- 13 Milne, R. (2024). *Six Nato countries plan 'drone wall' to defend borders with Russia*. Financial Times. <https://www.ft.com/content/949db465-cd27-4c66-9908-c2faa80b602b>
- 14 Jun, J. (2024, 30. April). *How Will AI Change Cyber Operations?*. War on the Rocks. <https://warontherocks.com/2024/04/how-will-ai-change-cyber-operations>
- 15 Fang, R., Bindu, R., Gupta, A., Zhan, Q., & Kang, D. (2024, 2. Juni). *Teams of LLM Agents can Exploit Zero-Day Vulnerabilities* (arXiv:2406.01637). arXiv. <http://arxiv.org/abs/2406.01637>
- 16 Topychkanov, P. (2019, Mai). *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*. In *South Asian Perspectives* (Band 1). SIPRI. <https://www.sipri.org/publications/2019/research-reports/impact-artificial-intelligence-strategic-stability-and-nuclear-risk-volume-i-euro-atlantic>
- 17 Reinhold, T. (2024, 7. Mai). *Der militärische Einsatz künstlicher Intelligenz braucht Regeln: Nur welche, darüber besteht keine Einigkeit*. PRIF Blog. <https://blog.prif.org/2024/05/07/der-militaerische-einsatz-kuenstlicher-intelligenz-braucht-regeln-nur-welche-darueber-besteht-keine-einigkeit>
- 18 Heaven, W. D. (2024, 4. März). *Large language models can do jaw-dropping things. But nobody knows exactly why*. MIT Technology Review. <https://www.technologyreview.com/2024/03/04/1089403/large-language-models-amazing-but-nobody-knows-why/>
- 19 Barredo Arrieta, A., Díaz-Rodríguez, N., Del Ser, J., Bennetot, A., Tabik, S., Barbado, A., Garcia, S., Gil-Lopez, S., Molina, D., Benjamins, R., Chatila, R., & Herrera, F. (2020). *Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI*. *Information Fusion*, 58, 82–115. <https://doi.org/10.1016/j.inffus.2019.12.012>
- 20 Shepardson, D., & Nellis, S. (2024, 8. Mai). *Intel, Qualcomm say exports to China blocked as Beijing objects*. Reuters. <https://www.reuters.com/technology/intel-flags-revenue-hit-us-revokes-certain-export-licenses-chinese-customer-2024-05-08>
- 21 Bloomberg. (2024, 22. Mai). *ASML and TSMC can disable EUV machines*. Taipei Times. <https://www.taipeitimes.com/News/biz/archives/2024/05/22/2003818194>

Drohnen

Technische, militärische und politische Entwicklungen im Bereich Drohnen

Aktuelle Kriege zeichnen sich immer mehr dadurch aus, dass Drohnen in ihnen eine besondere Rolle zukommt. Der Konflikt um Bergkarabach 2020 und der Krieg in der Ukraine werden häufig als „Drohnenkriege“ apostrophiert. Dabei zeichnet sich erst langsam der komplette Einsatzumfang ab, der mit Drohnen der neuesten, aber vor allem auch zukünftiger Generationen möglich sein wird. Allerdings herrscht um den Begriff „Drohne“ einige Konfusion, da sehr viele unterschiedliche Arten unter ihm subsumiert werden. In diesem Kapitel werden zunächst verschiedene Drohnenarten technisch unterschieden, ehe die neuen militärischen Möglichkeiten und schließlich zukünftige Entwicklungen aufgezeigt werden.¹

Drohnen werden nach Größe, Zuladung, Flughöhe und Ausdauer unterschieden.

Die Europäische Union definiert Drohnen im Rahmen ihrer Drohnenregulierung für den zivilen Lufthbereich sehr breit als „all aircraft designed to fly without a pilot on board“.² Diese Definition schließt also klassische Flugzeuge, aber auch Helikopter (oder auch Quadcopter) ein. Im militärischen Bereich wird oft der Begriff UAV (für „Uncrewed Aerial Vehicles“) genutzt. Zentrales Kriterium ist also, dass eine Drohne ein *unbemanntes* Flugobjekt ist.

Beim Militär ist die Unterscheidung nach Größe, Zuladung, Flughöhe und Ausdauer („Stehzeit“ in der Luft) maßgeblich, wobei die Faktoren einander meist bedingen. Nano- und Minidrohnen sind nur für den Nahbereich vorgesehen, können eine Zuladung im Gramm- bzw. Kilogramm-Bereich aufnehmen und haben meist Flugzeiten von wenigen Minuten bis zu einer halben Stunde, selten mehr. Hierunter fallen die meisten kommerziell erhältlichen Drohnen, vor allem die Drohnen für Privatanwender und Hobbyisten. Entsprechend günstig sind diese Drohnen zu beschaffen: Die Kosten liegen hier meist bei Hunderten oder wenigen Tausend Euro. Obwohl ursprünglich aus dem zivilen Bereich kommend (und in der EU sehr detailliert reguliert³), haben Militärs und nichtstaatliche Gewaltakteure in jüngeren Konflikten das Dual-Use-Potenzial dieser Drohnenkategorie entdeckt.

Drohnen der *Medium Altitude, Long Endurance*-Klasse (MALE) zeichnen sich durch mittlere Flughöhen (unter 9000 Metern), eine Zuladung bis zu wenigen Tonnen und lange Stehzeit von mehreren Stunden bis zu 2-3 Tagen aus. Bekannt sind z. B. die amerikanischen MQ-1 Predator oder MQ-9 Reaper, die türkische Bayraktar TB2, die chinesische GJ-1 Wing Loong oder die israelische Heron. Diese Drohnen haben meist einen Turbopropeller-Antrieb und sind entsprechend langsam. Sie können direkt über Funk oder indirekt über Satellit gesteuert werden. Hier erreichen die Kosten, je nach Hersteller und Leistung, schnell ein- oder mehrstelligen Millionenbeträge pro Einheit. MALE-Drohnen besitzen neben einer

Vielzahl an Aufklärungssystemen nicht selten die Fähigkeit, Präzisionsbomben abwerfen oder Flugkörper, vulgo Raketen, abfeuern zu können. Durch ihre Bauart sind sie meist per Radar gut zu detektieren und durch klassische Flugabwehr leicht abzuwehren. MALE-Drohnen sind also primär für den nicht umkämpften Luftraum in einem asymmetrischen Konflikt konzipiert und dominierten deshalb die US-Operationen der späten 2000er und frühen 2010er Jahre sowie den Konflikt um Bergkarabach. Ihr Beitrag in einem symmetrischen staatlichen Konflikt ist aufgrund ihrer Verwundbarkeit gering – sofern eben beide Konfliktseiten eine umfassende und leistungsfähige Flugabwehr aufgebaut haben.⁴

Schließlich gibt es Drohnen, die sich durch hohe Flughöhen über 10.000 Meter und lange Stehzeiten auszeichnen: *High-Altitude, Long Endurance* (HALE). Bei diesen Drohnen steht die Aufklärung im Vordergrund. Sie sind nicht nur in der Lage, große Landstriche optisch zu überwachen, sondern können meist ein breites Spektrum an elektromagnetischen Wellen, z. B. Funk oder Handyfunk, erfassen und an die Basis zur Auswertung weiterleiten. Die auf der amerikanischen RQ-4 Hawk basierende Eurohawk-Drohne fällt in diese Kategorie.

Die eingangs genannte Definition verdeckt aber einen wesentlichen Unterschied, der aus militärischer Sicht große Relevanz hat – nämlich die Frage, ob die Drohne so konzipiert wurde, dass sie zu einer Basis bzw. dem Nutzer zurückkehren kann und somit wiederverwendbar ist (Aufklärungsdrohne oder Waffenträger), oder ob sie für einen einmaligen Gebrauch bestimmt ist („Kamikazedrohnen“ oder auch „Loitering Munition“). Diese Unterscheidung hat durchaus praktische bzw. politische Relevanz: So gab es zwischen Russland und den USA immer wieder Unstimmigkeiten über die Interpretation des – inzwischen außer Kraft befindlichen – Intermediate Nuclear Forces-Vertrages (INF). Während Russland argumentierte, US-Kampfdrohnen hätten einem Cruise-Missile vergleichbare Eigenschaften und würden entsprechend unter das Verbot des INF fallen, argumentierten die USA, Drohnen seien im Gegensatz zu Marschflugkörpern „two-way, reusable systems“ und würden entsprechend nicht vom Vertrag erfasst.⁵ Und auch die Bundesregierung selbst argumentiert heute: „Loitering Munition ist ... zum einmaligen Gebrauch (Verschuss) Unbemannte Systeme (UAS) sind hingegen grundsätzlich zum wiederholten Einsatz vorgesehen.“⁶ Dies zeigt nicht nur, wie wichtig es ist, die jeweilige „Drohnenart“ exakt zu spezifizieren, wenn es um Fragen von Rüstungs- und Exportkontrolle oder Einsatzbeschränkungen geht, sondern auch, dass technische Definitionen oft nicht ohne politische Hintergedanken gewählt werden.

Ein weiterer wesentlicher Unterschied ist, ob Drohnen zu einer Basis zurückkehren können oder für den einmaligen Gebrauch bestimmt sind.



US-amerikanische MQ-9 Reaper auf dem Flugfeld in Duke Field, Florida. Foto: U.S. Air Force photo/Ilka Cole.

Von der MALE-Drohne zur „steuerbaren Munition“

Aufgrund ihrer Bedeutung in den asymmetrischen Konflikten der 2000er und 2010er Jahre dominierten MALE-Drohnen lange die Vorstellung von Kampfdrohnen. In der Zwischenzeit haben sie durch die veränderten Konfliktlagen, konkret die Resymmetrisierung aktueller Konflikte, an Bedeutung verloren. Im Krieg Russlands gegen die Ukraine spielen MALE-Drohnen nach anfänglich erfolgreichen Einsätzen vor allem auf ukrainischer Seite praktisch keine Rolle mehr. Ihre Kosten stehen in keinem Verhältnis zu ihrer Überlebensfähigkeit und dem geringen Nutzen. Deshalb haben beide Seiten auf neue Techniken und Taktiken zurückgegriffen.

Drohnen als Cruise-Missile-Ersatz

Russland nutzt in großer Anzahl die relativ günstigen und technisch sehr einfachen iranischen Shahed-131-„Drohnen“ als GPS-geleitete Marschflugkörper, die in militärischer Infrastruktur oder auch in zivilen Zielen in Terrorabsicht zur Explosion gebracht werden sollten. Damit ähnelt diese „Drohne“ sowohl vom Einsatzzweck als auch technologisch (wenn auch erheblich fortgeschritten) im Kern der deutschen Fieseler Fi 103 aus dem Zweiten Weltkrieg – eher berüchtigt unter der Bezeichnung „Vergeltungswaffe 1“. Zwar ist auch hier eine Abwehr, z. B. durch Flugabwehrpanzer, Boden-Luft- und auch Luft-Luft-Raketen relativ leicht möglich – dies bewies die erfolgreiche Abwehr des iranischen Angriffs auf Israel, in dem mehr als 170 Drohnen, 120 ballistische Raketen und 30 Cruise-Missiles früh aufgeklärt und nach Angaben der israelischen Streitkräfte zu 99% abgewehrt werden konnten.⁷

Auf der anderen Seite zeigt der relativ erfolgreiche Einsatz Russlands gegen die Ukraine, dass es angesichts der Anzahl potenzieller Ziele bei einem großen Flächenstaat trotz umfangreicher und auch leistungsfähiger Flugabwehr extrem schwierig und teuer ist, ausreichend defensive Systeme zur Verfügung zu stellen. So verfügt die Ukraine z. B. aktuell nur über drei Patriot-Abwehrsysteme, geht aber von einem Minimum von sieben Systemen aus und strebt langfristig den Besitz von 25 Systemen an – während in ganz Europa außerhalb der Ukraine bislang nur 32 solcher Systeme beschafft sind.⁸

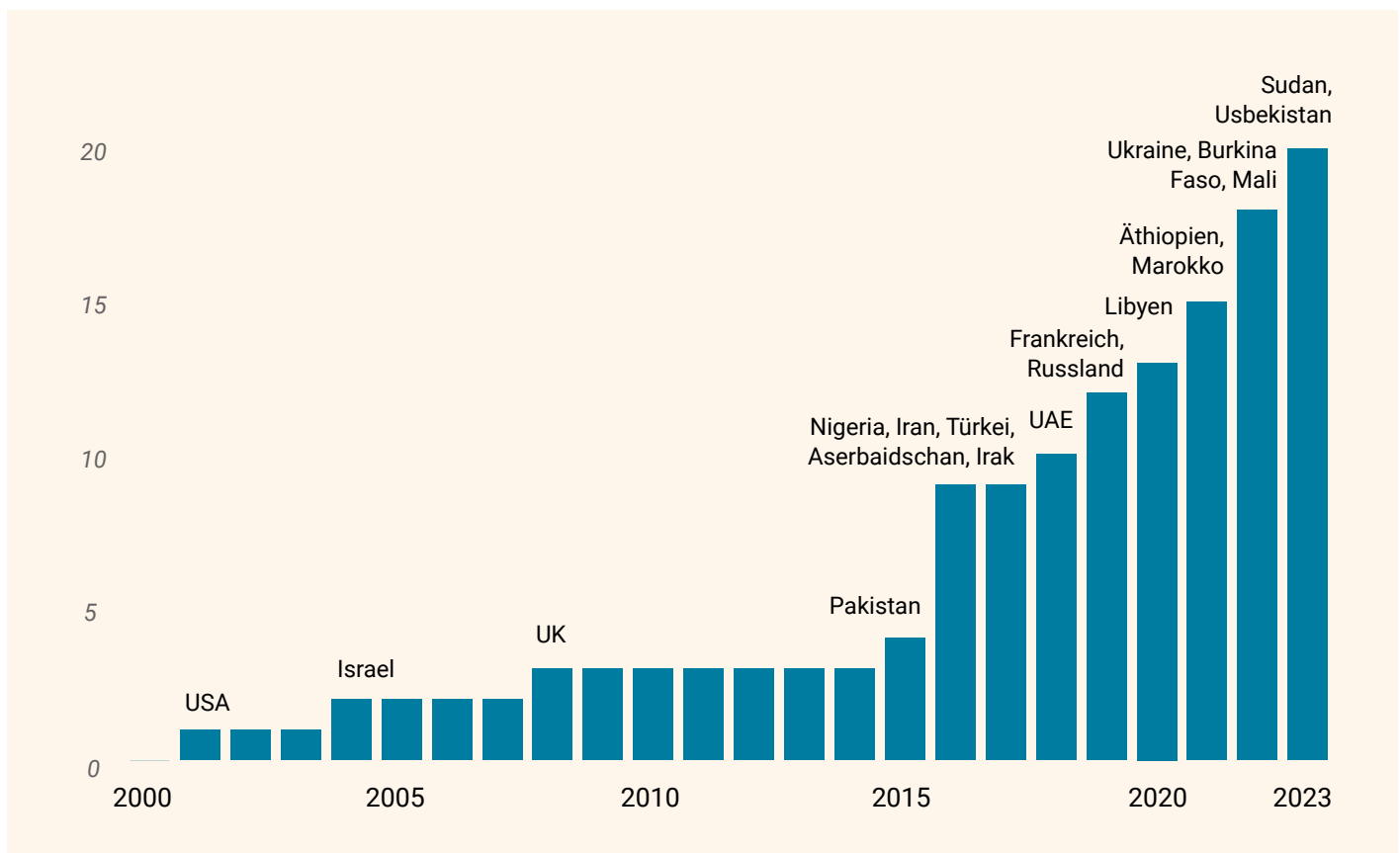


Abbildung: Staaten, die bewaffnete Drohnen bereits eingesetzt haben. Ausgewiesen sind jeweils die Länder, die im betreffenden Jahr zum ersten Mal Drohnen einsetzten. Nichtstaatliche Akteure wurden nicht berücksichtigt.

Gerade die geringen Herstellungskosten solcher Cruise-Missiles-Drohnen, bedingt durch die einfache verbaute Technologie, machen das – eigentlich technisch anspruchsvolle – System Cruise-Missile für viele Staaten erschwinglich und stellen ein großes Prolife-

rationsproblem und in Masse auch eine echte Gefahr für technologisch fortgeschrittene Staaten dar – vor allem vor dem Hintergrund, dass z. B. eine einzelne Patriot-Rakete mit über 5 Millionen US-Dollar zu Buche schlägt. Wie oben beschrieben wären solche Systeme bei der vom BMVg genutzten Drohnendefinition aber nicht erfasst und müssten in entsprechenden internationalen Verträgen zur Restriktion von Drohnen explizit mitbedacht werden.

Drohnen als Präzisionsmunition

Gleiches gilt, zumindest mit Einschränkungen, für die Klasse der Minidrohnern. Sie haben vor allem im Krieg gegen die Ukraine enorm an Bedeutung gewonnen. Solche leichten und erschwinglichen Drohnen mit Reichweiten um die 10 Kilometer und Schwebzeiten um eine halbe Stunde werden vielfach zur taktischen Echtzeitaufklärung eingesetzt. Die Aufklärungsdaten können dann händisch oder zunehmend auch automatisiert in Datenbanken eingetragen und z. B. an weitreichende Artillerie weitergegeben werden, so dass gegnerische Einheiten innerhalb eines Frontabschnitts mit minimaler Verzögerung bekämpft werden oder Fehlschüsse schnell korrigiert werden können. Die Kopplung von Drohne und Artillerie ist nicht neu und technisch unproblematisch. Aus politischen Gründen verzichten die meisten Staaten aber auf einen direkten Datenaustausch ohne menschliche Kontrolle.⁹ Solche Zurückhaltung findet auf den Schlachtfeldern in der Ukraine immer weniger statt.

Kleine Drohnen können aber auch mit einer frei fallenden Granate bestückt werden, die z. B. Stellungen, Geschütze oder Panzer vertikal, oft an der schwächsten Stelle angreift. Diese Einsatzoption ist ebenfalls nicht neu und wurde zuerst in den 2010er Jahren durch die Terrororganisation „Islamischer Staat“ (IS) im Irak sehr erfolgreich gegen US-Kräfte genutzt und wird so auch im Krieg zwischen Russland und Ukraine auf beiden Seiten angewendet.

Bei den meisten neuen Modellen steuern die Operatoren die Drohne nicht auf Sicht, sondern über eine Kamera aus der Ego-Perspektive – was diesen Modellen die Bezeichnung „FPV-Drohnen“ eingebracht hat und für „*First Person View*“ steht. Dies ermöglicht es auch bei Mikrodrohnen, jenseits der Sichtgrenze zu operieren, und man ist nur durch die Reichweite des eigenen Funks und die Akkuleistung des Antriebs begrenzt. Nutzt man zur Steuerung gar das Mobilfunknetz oder das Internet, könnten Mikrodrohnen wie auch MALE-Drohnen praktisch von jedem Ort der Welt aus gesteuert werden.

Speziell modifizierte zivile „Renndrohnen“, die sich durch sehr hohe Schnelligkeit, Beschleunigung und Wendigkeit auszeichnen, werden – inzwischen sogar oft mithilfe einer Virtual-Reality-Brille (VR-Brille) – im Tiefflug hochpräzise in ein mögliches Ziel gelenkt und dort zur Explosion gebracht. – So können sie inzwischen sogar Kampfpanzern gefährlich werden. Auch hier werden Drohnen also eher als hochpräzise Munition denn als Plattform genutzt, so dass man, wenn man die Position des BMVg zugrunde legt, nicht mehr von Drohnen, sondern von „steuerbarer Munition“ sprechen müsste – obwohl die zugrunde liegende Technologie identisch ist und unter Umständen sogar das gleiche Modell für Aufklärung und Selbstzerstörungsangriff genutzt werden kann.

Allerdings zeigen aktuelle Entwicklungen auch, dass gerade im Mikro-Bereich Drohnen immer stärker auf bestimmte Einsatzzwecke hin konzipiert und optimiert werden. Gerade auf Seiten der Ukraine gibt es inzwischen eine Vielzahl an Start-ups, die mit immer neuen Drohnendesigns experimentieren – was allerdings Nachteile bei Logistik und Wartung erzeugt. Immer öfter werden Drohnen oder zumindest Ersatzteile auch mittels 3D-Druck erstellt, was die Proliferation solcher kleiner Drohnenmodelle noch einmal erhöht. Wie bedeutsam Kleindrohnen inzwischen geworden sind, zeigt die Tatsache, dass 2023 auf beiden Seiten mehrere 10.000 dieser Drohnen zum Einsatz kamen. Inoffiziellen russischen

*Zum Thema 3D-Druck
siehe den Beitrag von Liska
Suckau ab S. 30.*

Quellen zufolge waren es gerade Kleinstdrohnen, die den russischen Vormarsch in der Ukraine stoppten. Dabei reichten im Schnitt sechs bis zehn Drohnen aus, um einen russischen Panzer zu zerstören.¹⁰ Anfang des Jahres verkündete die Ukraine dann, die Produktion 2024 auf eine Million(!) solcher FPV-Drohnen zu erhöhen,¹¹ während eine Gruppe europäischer Staaten zeitgleich versprach, der Ukraine im Jahr 2024 eine weitere Million Drohnen zu liefern.¹²

Das Wissen, wie man kleine Drohnen mit wenig Zuladung herstellt, ist inzwischen weit proliferiert, und praktisch jeder Luftfahrt-Lehrstuhl einer beliebigen Universität ist in der Lage, eigene Drohnen aus frei erhältlichen Komponenten in kürzester Zeit zusammenzubauen. Auch der zivile Markt boomt: Wurden 2022 weltweit noch geschätzte 8,8 Milliarden US-Dollar in diesem Segment umgesetzt, schätzt man die Umsätze 2030 auf fast 55 Milliarden.¹³ Entsprechend bedingen sich zivile und militärische Innovation im Bereich kleinerer Drohnen aktuell gegenseitig, aber vor allem das Militär profitiert enorm von der Dual-Use-Eigenschaft der Mikrodrohne.

Drohnenabwehr

Im Gegensatz zu den großen Modellen ist die Abwehr kleiner Drohnen aufgrund ihrer geringen Größe und damit verbundenen Wendigkeit schwierig. Für Soldatinnen und Soldaten bedeutet das eine konstante, extreme psychische Belastung, denn es ist oft nicht zu unterscheiden, ob das hohe Surren, das auf eine nahe Drohne und damit große Gefahr hindeutet, von einer feindlichen oder eigenen Drohne ausgeht. Zusätzlich zur physischen Abwehr, wo inzwischen neben Projektilen auch mit Netzen oder Lasern experimentiert wird, wird oft auch auf Störsender oder andere elektronische Kriegsführung zurückgegriffen, die die Kommunikation zwischen Piloten und Drohne unterbrechen soll. Solche Systeme kommen auch im zivilen Bereich zum Einsatz und waren während der Fußball-Europameisterschaft 2024 eines der zentralen Abwehrmittel der deutschen Polizei.¹⁴

Die Bedingung für den Erfolg solcher Abwehrmaßnahmen ist, dass die Drohnen immer noch von Menschen gesteuert werden – was noch für die meisten Modelle gilt. Es kommt aber auch die oben beschriebene „loitering munition“ zum Einsatz, also Drohnen, die über einem bestimmten Gebiet kreisen, nach Zielen, z. B. Radarstellungen, Ausschau halten und diese dann – entweder nach menschlicher Freigabe oder auch selbständig – angreifen und kaum noch auf menschliche Steuerung angewiesen sind. Da solche Systeme weniger anfällig für elektronische Störmaßnahmen sind, entsteht hier Druck zu einer immer stärkeren Automatisierung der Systeme, was wiederum den Druck zum Einsatz von menschenunabhängigen Abwehrsystemen erhöht – das klassische Katz-und-Maus-Spiel von Offensive und Defensive.

Aktuelle technische Entwicklungen

Autonome Funktionen

Gerade die aktuelle, zivil kommerziell erhältliche Drohnengeneration enthält schon umfangreiche Algorithmen, die durchaus als „KI“ verstanden werden können, auch wenn sie nicht auf Deep Learning basieren. Dank umfangreicher Hilfsfunktionen wie automatischer Stabilisierung und Ausrichtung im Raum ist die Steuerung moderner Kleinstdrohnen sehr einfach geworden und erlaubt es auch relativ unerfahrenen Pilotinnen und Piloten, diese Drohnen sicher zu steuern. Dies befeuert die mit diesen Systemen verbundene Verbreitungsgefahr.

Drohenschwärme

Agieren militärische Drohnen aktuell meist noch alleine, so ist schon jetzt absehbar, dass der vernetzte Einsatz als Schwarm¹⁵ gerade günstiger Drohnen zukünftig immer häufiger

Zum Thema Deep Learning, siehe die Diskussion im Beitrag von Thomas Reinhold ab S. 16.

werden wird – vor allem, wenn es dadurch gelingt, Verteidigungssysteme zu überlasten und so, wie es im Militärjargon heißt, „Wirkung zu erzielen“. Eher im Monats- als im Jahrestakt gibt es Meldungen zu neuen Rekorden, die im zivilen Bereich mit koordinierten Drohnenschwärmen aufgestellt wurden, und praktisch keine Großveranstaltung kommt ohne eine eindrucksvolle Drohnenshow aus. Zum Zeitpunkt des Schreibens dieses Textes stand der Weltrekord bei 5.293 Drohnen, die koordiniert dreidimensionale Figuren an den Nachthimmel zauberten¹⁶ – auch wenn die Steuerung meist noch zentral über einen Hauptrechner und nicht dezentral zwischen den Drohnen geschieht. Meist wechseln sich die USA und China als Rekordhalter ab.

Dass das Militär die Relevanz von Drohnenschwärmen erkannt hat, zeigt z. B. das Replicator-Projekt des US-Verteidigungsministeriums, das darauf zielt, bis 2025 „thousands of all-domain, attritable, autonomous swarming robots“ für einen möglichen Einsatz gegen China im pazifischen Raum zu beschaffen.¹⁷ Das entsprechende Budget sieht für 2024 und 2025 Gesamtausgaben in Höhe von ca. einer Milliarde US-Dollar vor. Aber auch Schwärme kleiner Drohnen, die in Masse z. B. Panzerkolonnen angreifen oder gegen Infanterie eingesetzt werden können, werden angestrebt. Auch hier spielt KI eine bedeutende Rolle, da es das Ziel ist, dass sich die Schwärme auch ohne externe Einflussnahme selbst organisieren, oder gar ohne GPS-Signal agieren können.

Aber Drohnenschwärme müssen nicht zwingend über hohe KI-Fähigkeiten verfügen, um auch leistungsfähige Akteure an den Rand der eigenen Verteidigungsfähigkeit zu führen, wenn sie diese, wie oben beschrieben, schlicht überlasten.

Drohnenträger und KI-Piloten

Welche Bedeutung Drohnen inzwischen einnehmen, zeigt sich daran, dass China mittlerweile dabei ist, den ersten dedizierten und entsprechend optimierten „Drohnenträger“ zu bauen. Das chinesische Schiff hat vermutlich etwa ein Drittel der Größe eines klassischen Flugzeugträgers und scheint geeignet, darauf Drohnen der MALE-Klasse, aber keine bemannten Flugzeuge operieren zu lassen.¹⁸ Damit sind China und der Iran, der ein ziviles Transportschiff angepasst hat, aktuell die einzigen Länder, die über eine solche maritime Einheit verfügen.

Nur China und der Iran verfügen aktuell über maritime Einheiten, die als „Drohnenträger“ dienen.

Diese Beispiele reiner Drohnenträger werden aber sicher Schule machen, zumal der gemischte Betrieb von Drohnen und bemannten Flugzeugen auf klassischen Flugzeugträgern nicht trivial ist und erheblichen Aufwand bedeutet.¹⁹ Inzwischen war aber eine Betankungsdrohne, die von Boeing entwickelte MQ-25 „Stingray“ über längere Zeit auf einem US-Flugzeugträger im Testbetrieb, der allerdings nicht ohne Probleme blieb und das Projekt verzögerte. Gleichwohl hält die Navy an dem Projekt fest.²⁰ Einer der Gründe wird sein, dass der Testbetrieb der Stingray wertvolle technische Daten lieferte – und in einem größeren Rahmen verstanden werden muss. Denn es ist schon heute möglich, klassische bemannte Jets durch den Einbau von zusätzlichen Computern weitgehend autonom fliegen zu lassen – inklusive Start und Landung. Aktuell arbeitet DARPA, die *Defense Advanced Research Projects Agency*, die hochriskante Forschungsprojekte finanziert, an Projekten, die KI-gestützten Luftkampf ermöglichen sollen. War es 2020 noch ein simulierter Luftkampf, den eine KI gegen einen menschlichen Elitepiloten 5:0 gewann und der für Aufsehen unter Expertinnen und Experten sorgte, waren es im September 2023 echte Jets, die von KI bzw. menschlich gesteuert in einem simulierten Dogfight gegeneinander antraten.²¹ Wer diesmal die Oberhand behielt, wollte DARPA nicht verraten²² – es zeigt aber, dass eine neue operable Drohnenklasse, der unbemannte Kampffjet, in nicht allzu ferner Zukunft ins Kampfgeschehen eingreifen könnte. Schon einige Monate zuvor war ein ähnlicher Kampf in China ausgetragen worden – hier hatte die KI dem menschlichen Piloten keine Chance gelassen. Kampfdrohnen auf Flugzeugträgern könnten so in der Zukunft Reichweite und Schlagkraft von klassischen Flugzeugträgern deutlich erhöhen.

Regulierung und Ausblick

Neue technische Entwicklungen haben in den letzten Jahren dazu geführt, dass der Einsatz von Drohnen nicht nur im zivilen Bereich rapide zugenommen hat. Gerade im militärischen Bereich haben Drohnen in inzwischen sehr unterschiedlichen Formen erheblich an Bedeutung gewonnen. Dabei spielt gerade der technische Austausch zwischen ziviler und militärischer Nutzung eine wichtige Rolle, und viele Innovationen in diesem Bereich kommen aus dem zivilen Umfeld. Im Bereich der großen Systeme scheint es nur eine Frage der Zeit, bis unbemannte Kampffjets zum Einsatz kommen werden – zu groß scheint der militärische Vorteil gegenüber bemannten Systemen. Allerdings ist der Bereich Drohnen international nur schwach reguliert und die konkreten Regelungen, die bestehen, beziehen sich im Wesentlichen auf asymmetrische Exportkontrollen. Trotz, oder vielleicht wegen der Allgegenwärtigkeit kleiner Drohnen im zivilen Bereich ist vielen Akteuren allerdings nicht bewusst, dass Drohnen schon länger als Dual-Use-Produkt kategorisiert werden und unter Exportkontrollrichtlinien fallen: So sieht z. B. das Wassenaar-Arrangement Restriktionen für Drohnen vor, wenn sie bestimmte Flugdauern überschreiten und auch bei Windstärke 6 oder mehr operieren können, sowie für Technologien, die es ermöglichen, ehemals bemannte Flugzeuge per Fernsteuerung zu fliegen.²³ Deutlich größere Drohnen mit über 500 kg Zuladung und Reichweiten über 300 km werden immer noch vom Missile Technology Control Regime (MTCR) erfasst und ihr Export wird durch eine „unconditional strong presumption of denial“ streng reglementiert. Allerdings sind die USA 2020 dazu übergegangen, Drohnen mit einer Geschwindigkeit unter 800 km/h nicht mehr dieser strengen Exportregulierung zu unterwerfen – eine Sichtweise, der sich die Regierung von Präsident Biden inzwischen angeschlossen hat.²⁴

Weitere Regulierungen militärischer Drohnen gibt es aktuell nicht, von einem Verbot ganz zu schweigen. Zwar gab es 2020 eine deutsche „Initiative zur Vereinbarung internationaler Rahmenprinzipien für die militärische Nutzung bewaffneter Drohnen“, die aber relativ schnell und lautlos beerdigt wurde. Hier hatte man den richtigen Zeitpunkt verpasst.

Ähnliches droht für den Bereich zunehmender Autonomie in Drohnen und anderen Waffensystemen. Denn, ob es international zu verbindlichen Regelungen oder gar Verboten von „autonomen Waffensystemen“ kommt, die dann z. B. auch unbemannte Kampffjets umfassen würden, wenn die Angriffe nicht durch Menschen gesteuert werden, erscheint angesichts der starken technischen Dynamiken fraglich.

Eines ist sicher: Kleine Drohnen sind die aktuelle „Weapon of Choice“ gerade ökonomisch schwächerer Akteure. In Masse schwer abzuwehren, leicht nachzuproduzieren und durch zivile Entwicklungen einer konstanten technischen Dynamik unterworfen, können Drohnen nicht nur regionale Machtgleichgewichte erheblich stören – sie stellen auch für technologisch fortgeschrittene und potente Akteure eine erhebliche Gefahr dar. Investition in ein breites Portfolio an Drohnenabwehrmaßnahmen ist also Pflicht.

Dr. Niklas Schörnig

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

1 Der Text basiert in Teilen auf Überlegungen, die schon im Friedensgutachten 2024 vorgestellt wurden, und übernimmt einige Abschnitte, siehe: BICC Bonn International Centre for Conflict Studies, IFSH Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg, INEF Institut für Entwicklung und Frieden, PRIF Leibniz-Institut für Friedens- und Konfliktforschung (Hrsg.). (2024). *Friedensgutachten 2024*. transcript Verlag. <https://doi.org/10.14361/9783839474211>

- 2 European Union. *Unmanned aircraft (drones)*.
https://transport.ec.europa.eu/transport-modes/air/aviation-safety/unmanned-aircraft-drones_en
- 3 European Union. *Easy Access Rules for Unmanned Aircraft Systems* (Regulations (EU) 2019/947 and 2019/945). European Union Aviation Safety Agency.
<https://www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-unmanned-aircraft-systems-regulations-eu>
- 4 Calcara, A., Gilli, A., Gilli, M., Zaccagnini, I. (2022, 31. Juli). Air Defense and the Limits of Drone Technology. *Lawfare Media*.
<https://www.lawfaremedia.org/article/air-defense-and-limits-drone-technology>
- 5 Vgl. das Zitat von Principal Deputy Under Secretary of Defense Brian McKeon, zitiert in
<https://crsreports.congress.gov/product/pdf/R/R43832>, S. 28
- 6 Bundesregierung. (2024). *Loitering Munition für die Bundeswehr. Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Gerold Otten und der Fraktion der AfD* (Drucksache 20/10266). Deutscher Bundestag.
<https://dserv.bundestag.de/btd/20/104/2010456.pdf>
- 7 Israel Defense Forces [IDF]. (2024, 14. April). *300+ launches. 99% interception rate. This is the breakdown of Iran's attack last night*: [Image attached] [Post]. X. <https://x.com/IDF/status/1779503384434819454>
- 8 Häslar, G., & Rüesch, A. (2024, 21. Juni). Die Ukraine erhält weitere Patriot-Abwehrsysteme und wird bei künftigen Lieferungen bevorzugt. *Neue Züricher Zeitung*.
<https://www.nzz.ch/international/ukraine-erhaelt-weitere-patriot-systeme-und-prioritaet-bei-lieferungen-id.1836207>
- 9 Persönliches Gespräch mit Angehörigen der Bundeswehr
- 10 Samuel Bendett [@sambendett]. (2023, 31. Dezember). *1/ THREAD on the impact of small quadcopters in the Ukraine war over the past year – based on my earlier* [Image attached] [Post]. X.
<https://x.com/sambendett/status/1741454000463941648?t=COXJ91RR3iQLVdKvsRYaxQ&s=19>
- 11 The Kyiv Independent news desk (2024, 25. Februar). *Fedorov: Ukraine to produce 1 million drones per year*. The Kyiv Independent.
<https://kyivindependent.com/fedorov-ukraine-to-produce-1-million-drones-per-year/>
- 12 Martin, T. (2024, 15. Februar). *European coalition bids to deliver 1 million drones to Ukraine*. Breaking Defense.
<https://breakingdefense.com/2024/02/european-coalition-bids-to-deliver-1-million-drones-to-ukraine/>
- 13 Fortune Business Insights. (2024, 12. August). *Commercial Drone Market Size, Industry Share & COVID-19 Impact Analysis (...)*.
<https://www.fortunebusinessinsights.com/commercial-drone-market-102171>
- 14 Kalus, T. (2024, 8. Juni). *Reul: Drohnen-Abwehr bei der Fußball-EM ist startklar*. WDR.
<https://www1.wdr.de/nachrichten/drohnenabwehr-stoersender-em-reul-100.html>
- 15 Verbruggen, M. (2019, Dezember). The Question of Swarm Control: Challenges to Ensuring Human Control over Military Swarms. *Non-Proliferation and Disarmament Papers*, (65).
- 16 Mackenzie, W. (2024, 13. Mai). *Largest Drone Swarm Display Sets New World Record*. Unmanned Systems Technology.
<https://www.unmannedsystemstechnology.com/2024/05/largest-drone-swarm-display-sets-new-world-record/>
- 17 Luckenbaugh, J. (2024, 4. Januar). Replicator Initiative Looks to Swarm Through 'Valley of Death'. *National Defense Magazine*.
<https://www.nationaldefensemagazine.org/articles/2024/1/4/replicator-initiative-looks-to-swarm-through-valley-of-death>
- 18 Sutton, H I. (2024, 15. Mai). *China Builds World's First Dedicated Drone Carrier*. Naval News.
<https://www.navalnews.com/naval-news/2024/05/china-builds-worlds-first-dedicated-drone-carrier>
- 19 Schwartz, S., Reuter, C. (2020). 90.000 Tonnen Diplomatie 2.0: Die Integration von unbemannten Systemen in den operativen Flugzeugträgerbetrieb am Beispiel der X-47B. *Zeitschrift für Außen- und Sicherheitspolitik*, 13(1). doi: 10.1007/s12399-020-00803-y
- 20 Tegler, J. (2024, 26. Januar). Despite Delays, Navy to Accelerate Delivery of Unmanned Tanker. *National Defense Magazine*.
<https://www.nationaldefensemagazine.org/articles/2024/1/26/despite-delays-navy-to-accelerate-delivery-of-unmanned-tanker>
- 21 Defense Advanced Research Project Agency. (2020, 26. August). *AlphaDogfight Trials Foreshadow Future of Human-Machine Symbiosis*. United States Department of Defense. <https://www.darpa.mil/news-events/2020-08-26>
- 22 Decker, A. (2024, 19. April). An AI took a human pilot in a DARPA-sponsored dogfight. *Defense One*.
<https://www.defenseone.com/technology/2024/04/man-vs-machine-ai-agents-take-human-pilot-dogfight/395930/>
- 23 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. (2023. 1. Dezember). 9.A.12.a and 9. A. 12. b.
<https://www.wassenaar.org/app/uploads/2023/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-2023-1.pdf>
- 24 Kimball, D. G. (2020, September). U.S. Reinterprets MTCR Rules. *Arms Control TODAY*, 50.
<https://www.armscontrol.org/act/2020-09/news/us-reinterprets-mtcr-rules>

Additive Fertigung

Additive Fertigung in der Kriegsführung

Im Folgenden wird ein kurzer Überblick über die Dynamik von Additiver Fertigung (AF) als militärische Fähigkeit und als Mittel zur (unkonventionellen) dezentralen Produktion von Rüstungsgütern und Ausrüstung gegeben. Vor allem letzteres hat sich sowohl im industriellen Umfeld als auch im Hobbybereich rasant entwickelt, was zu neuen Sicherheitsrisiken führt. Derzeit ist AF kaum reguliert, und es bedarf innovativer Ansätze, um die Herausforderungen der globalen Verbreitung von selbst hergestellten 3D-gedruckten Waffenkonstruktionen zu bewältigen. Darüber hinaus könnten Dual-Use-Regelungen die Verbreitung von Industriemaschinen, die sicherheitsrelevante Technologien herstellen können, kontrollieren.

Die Additive Fertigung (AF) – gemeinhin als 3D-Druck bezeichnet – ist vielseitig einsetzbar und hat das Interesse verschiedener Akteure geweckt. Diese reichen von Hobbybastler*innen über Ingenieur*innen aus verschiedenen Branchen bis hin zu böswilligen Akteuren, die die Technologie für kriminelle Absichten nutzen. Die Verwendung von AF für illegitime Zwecke ist daher ein Problem für die nationale und internationale Sicherheit geworden. AF umfasst eine Reihe von Grundlagentechnologien, die neben der Produktion von diversen zivilen Objekten, die Herstellung von Waffen oder anderen militärischen und sicherheitsrelevanten Ausrüstungsgegenständen verschiedenster Arten, einschließlich problematischer Objekte, ermöglichen. Das macht diese Technologien zu Dual-Use-Technologien.¹ Die größte Bedrohung ist aktuell die Fähigkeit nichtstaatlicher Akteure, Gegenstände selbst herzustellen, die die öffentliche Sicherheit gefährden, z. B. durch 3D-gedruckte Feuerwaffen oder andere sicherheitsrelevante Gegenstände, wie Teile für den Zusammenbau von improvisierten Sprengsätzen (*improvised explosive devices*, IEDs) oder andere waffenfähige Gegenstände. Während sich einige dieser Bedrohungen bereits verwirklicht haben, wie die ständig steigende Zahl der von der Polizei beschlagnahmten hochentwickelten 3D-gedruckten Schusswaffen zeigt,² sind die Auswirkungen von AF auf die internationale Sicherheit und Stabilität bisher weniger stark ausgeprägt.

An allen Kriegsschauplätzen lässt sich ein Zuwachs von 3D-gedruckten Gegenständen beobachten.

Angesichts des Zuflusses von 3D-gedruckten Gegenständen, der an aktuellen Kriegsschauplätzen wie der Ukraine und Myanmar zu verzeichnen ist, könnte sich dies jedoch ändern. Sowohl eine Top-down- als auch eine dezentralisierte Bottom-up-Entwicklung und -Verteilung von AF-gefertigten Gegenständen sind beobachtbar und prägen die materiellen Realitäten im Einsatzgebiet. Im Folgenden wird ein kurzer Überblick über die Dynamik von AF als militärische Fähigkeit zur Verbesserung der logistischen Widerstandsfähigkeit von Truppen und als Mittel zur (unkonventionellen) dezentralen Produktion von Rüstungsgütern und Ausrüstung gegeben. Schließlich werden die Implikationen für Rüstungskontrolle und -regulierung im Hinblick auf das technologische Umfeld von AF in der Kriegsführung

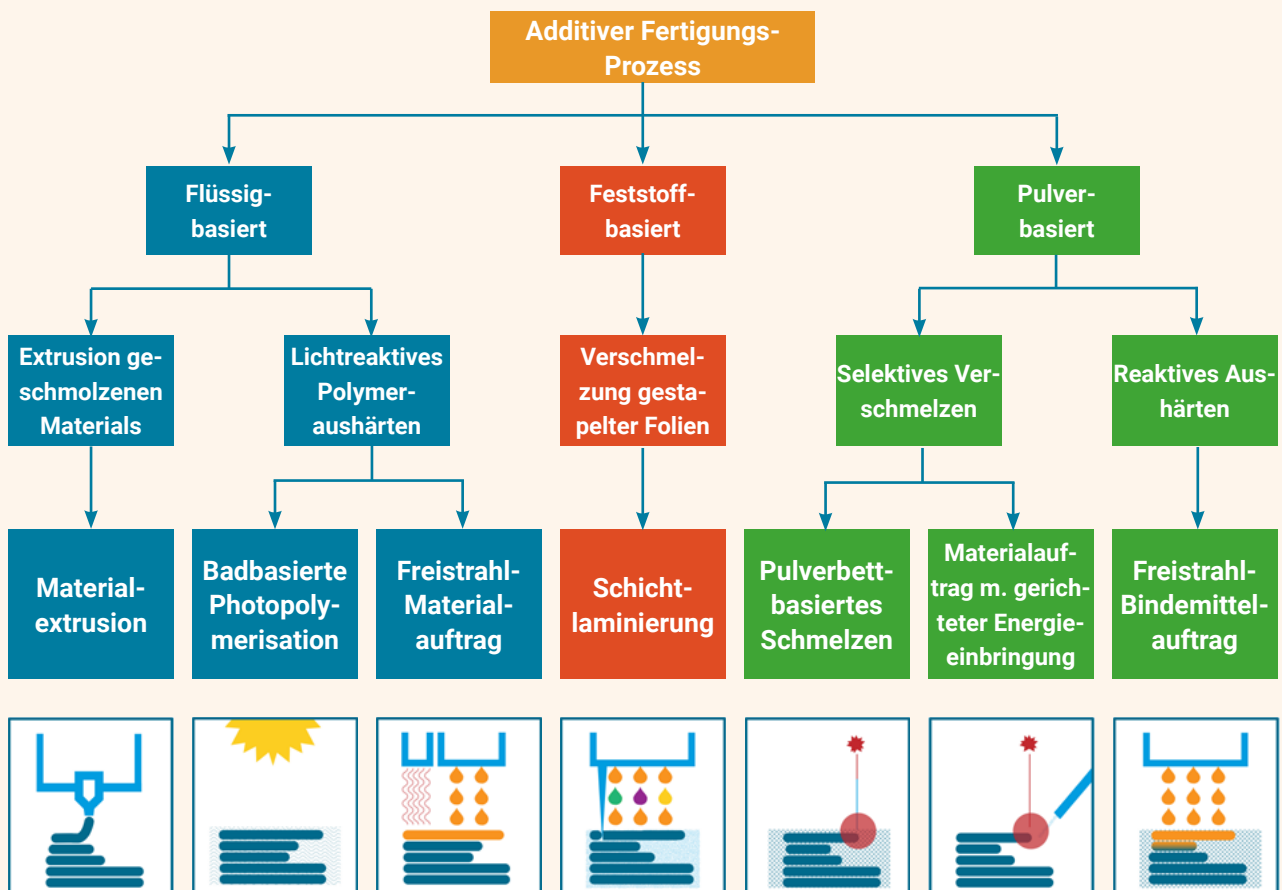


ung untersucht, das durch eine schrumpfende Distanz zwischen aktiven Kämpfer*innen und der zivilen Sphäre gekennzeichnet ist.

Technischer Hintergrund

Der grundlegende technologische Prozess hinter AF ist die schichtweise Herstellung von Gegenständen nach einem digitalen 3D-Modell oder -Design. Im Gegensatz zu konventionellen Fertigungsverfahren wie Umformen und Schneiden oder Fräsen wird nur das für das Endvolumen benötigte Material verwendet, was zu einer Verringerung des Materialabfalls führt. Der Zusammenhalt zwischen den Schichten wird durch das Schmelzen von Grenz-

AF-Prozesskategorien



Es gibt verschiedene Möglichkeiten, die Prozesse der AF zu kategorisieren. Die hier abgebildete Möglichkeit geht vom Zustand des Ausgangsmaterials bei der Herstellung der Schichten aus und ordnet dann die weiteren Prozesse nach dem Grundprinzip zur Herstellung der Schichten und des Materialzusammenhalts. Dies erlaubt eine übersichtliche Darstellung der Unterschiede der laut DIN EN ISO/ASTM 52900 bestimmten Prozesskategorien.

schichten oder durch chemische Prozesse gewährleistet. Die internationale Norm (DIN EN ISO/ASTM 52900) unterscheidet sieben verschiedene AF-Prozesskategorien, die sich wiederum in diverse Unterkategorien aufteilen.³ Wie bei den meisten Fertigungsverfahren hängt es stark vom jeweiligen Anwendungsfall ab, welches Material und welches Verfah-

Wire Arc Additive Manufacturing kombiniert die Technologie des Gas-Metall-Lichtbogenschweißens mit dem Verfahren der additiven Fertigung. Vereinfacht ausgedrückt werden Metallschichten von einem Roboter übereinander geschweißt, um das gewünschte Design zu realisieren.

ren zur Herstellung eines Gegenstandes verwendet wird. Eine breite Palette verschiedener Materialien kann verarbeitet werden, von Kunststoff über Metall bis hin zu Zellen und sogar Beton. Je nach Material kommen spezialisierte AF-Maschinen zum Einsatz: Das Spektrum reicht von relativ leicht zugänglichen und erschwinglichen Desktop-Druckern für zu Hause über technisch komplexe und teure Industriedrucker, in denen Schichten von Metallpulver mit einem Laser geschmolzen werden, um komplizierte Gegenstände zu drucken, bis hin zu großen Maschinen, die die Herstellung von Schiffsschrauben mit Wire Arc AF als Produktionstechnik ermöglichen. In den meisten Fällen ist eine zusätzliche Nachbearbeitung erforderlich, um den Materialzusammenhalt, die Haltbarkeit und die Oberflächenqualität sicherzustellen. All dies zeigt die Vielfalt von AF und motiviert zu weiterer intensiver Forschung, Erprobung und Standardisierung, um neue Optionen für die Produktion zu ermöglichen. Zu den Branchen, die bei der Integration voraussichtlich führend sein werden, gehören die Luft- und Raumfahrt, die Medizintechnik und der Werkzeugbau.⁴

AF an derzeit aktiven Kriegsschauplätzen

Es gibt Belege über eine zunehmende Vielfalt der Einsatzmöglichkeiten von AF in bewaffneten Konflikten. Die meisten Informationen über diese technologischen Entwicklungen stammen aus Berichten in sozialen Medien und Posts von Kämpfer*innen oder aus journalistischen Artikeln, in denen entweder über selbst hergestellte Waffen und Ausrüstungen oder über neue, von der Waffenindustrie entwickelte Anwendungsfälle berichtet wird. Aus solchen Berichten lässt sich eine Dichotomie der Nutzung von AF auf den Kriegsschauplätzen ableiten: Auf der einen Seite gibt es konventionelle militärische und industrielle Akteure, die AF als militärische Fähigkeit entwickeln, um die Einsatzbereitschaft und Reaktionsfähigkeit der Streitkräfte zu verbessern. Auf der anderen Seite stehen dezentralisierte Bottom-up-Anstrengungen verschiedener, oft global vernetzter nichtstaatlicher Akteure, die technische Militärausrüstung entwerfen und – in vielen Fällen kostenlos – produzieren und sie direkt an Kombattant*innen verteilen. Unabhängig von der Herkunft des Angebots besteht das allgemeine Ziel darin, kosteneffiziente Produktionsverfahren zu entwickeln, Lücken in der Lieferkette zu schließen oder den Zugang zu Gütern zu ermöglichen, die sonst nicht zugänglich sind.

AF als militärische Fähigkeit: Konventionelle staatlich geförderte Versorgung und Verteilung für mehr Widerstandsfähigkeit

Im Rahmen der Militärhilfe haben die Vereinigten Staaten den ukrainischen Streitkräften (*Ukrainian Armed Forces*, UAF) nicht näher spezifizierte 3D-Drucker zur Verfügung gestellt, mit denen die Truppen sich in Frontnähe mit Zündstiften für die Haubitzen M777 und anderen Gegenstände neu ausstatten können.⁵ Viele Plattformen, wie z. B. die Panzerhaubitze, sind ohne spezielle Fachkenntnisse schwer zu reparieren und zu warten. Daher haben die USA ein Programm entwickelt, um den ukrainischen Streitkräften diese Fachkenntnisse aus der Ferne zur Verfügung zu stellen, damit die Plattformen schnell wieder an die Front zurückkehren können.⁶ Dies ist ein Beispiel dafür, wie AF in der Anfangsphase eines Zermübungskrieges eingesetzt werden kann, in der konventionelle Versorgungslinien noch nicht etabliert sind. Daran zeigt sich auch der Stand der Technik von AF als militärische Fähigkeit, die bereits in kurzer Zeit eingesetzt werden kann. Die Verbesserung dieser Fähigkeit zielt darauf ab, die Reaktionsfähigkeit, die Einsatzbereitschaft und die Autonomie im Einsatzgebiet zu erhöhen, auch in späteren Phasen der Kampfhandlungen.⁷ Diese Vorteile sind nicht auf ein aktives Kampfgebiet beschränkt, sondern gelten allgemein für die Materialverwaltung und Logistik in den Streitkräften. Da die Systeme oft mehrere Jahrzehnte im Einsatz sind, stellen die Originalausstatter (*Original Equipment Manufacturer*, OEM) manchmal die Produktion von Ersatzteilen ein. AF kann zur Herstellung solcher Altteile verwendet werden und verlängert somit die Lebensdauer der entsprechenden Systeme. Die Professionalisierung der Fähigkeit, Teile an Ort und Stelle herzustellen, soll auch die Effizienz



in Militärlagern und -stützpunkten erhöhen, indem sie die Abhängigkeit von pünktlichen Ersatzteillieferungen aus dem Herkunftsland⁸ verringert und letztlich die Kosten senkt, die sich aus der materiellen Abhängigkeit von den OEM ergeben.⁹ Eine ähnliche Dynamik gilt für die Seestreitkräfte, da diese während der Einsätze von der Versorgung abgeschnitten sind und nur Zugang zu Werkzeugen und Teilen an Bord haben.¹⁰ Zusammenfassend lässt sich sagen, dass AF in der Kriegsführung das Potenzial hat, eine schnelle, zeitnahe und bedarfsgerechte Produktion von Teilen zu ermöglichen. Ein breites Spektrum von Anwendungen ist möglich, von vorübergehenden Ersatzteilen über normale Abnutzung bis hin zur Wartung von Altsystemen. AF-Technologien ermöglichen eine größere Materialunabhängigkeit vor Ort, den Druck von Teilen in geringen Stückzahlen und die schnelle Anfertigung maßgeschneiderter Teile für medizinische Anwendungen. All diese Anwendungen zusammen genommen zielen darauf ab, die *Widerstandsfähigkeit* der Streitkräfte zu erhöhen.

Additive Fertigung ermöglicht u. a. die schnelle und bedarfsgerechte Produktion von Ersatzteilen und Wartung von Altsystemen vor Ort. Damit kann sie die Widerstandsfähigkeit der Streitkräfte erhöhen.

Neben dem Einsatz bei der Integration in aktive Kriegsschauplätze ist die Rüstungsindustrie generell an der Nutzung von AF interessiert. Neue Entwicklungen und AF-Technologien versprechen die Konstruktion neuer, leichter Produkte und Senkung der Produktionskosten – alles im Einklang mit dem allgemeinen Ziel, die militärische Logistik zu verbessern und die Produktionseffizienz zu steigern.¹¹

AF in der Primärproduktion von Rüstungsgütern und Ausrüstung: eine wachsende Rolle nichtstaatlicher Akteure

Neben der Top-down-Integration in das Militär wird AF zunehmend von nichtstaatlichen Akteuren genutzt, um Militärtechnologie und -ausrüstung zu produzieren, die teilweise oder größtenteils 3D-gedruckt sind. Diese Entwicklung verläuft parallel zur konventionellen Entwicklung und Integration von AF in der Rüstungsindustrie und der Bereitstellung von Rüstungsgütern durch den Staat und etabliert dezentralisierte nichtstaatliche Akteure als Entwickler und unabhängige Bottom-up-Lieferanten von Rüstungsgütern. Ein berühmtes Beispiel sind die bereits erwähnten 3D-gedruckten Feuerwaffen und andere Geräte, die als Waffe verwendet oder umgerüstet werden können. Solche Gegenstände werden auf den Kriegsschauplätzen in der Ukraine und in Myanmar eingesetzt, kamen aber auch bei mehreren Vorfällen rechtsextremistischer Waffengewalt zum Einsatz. Vor allem rund um 3D-gedruckte Waffen hat sich eine ständig wachsende Online-Community gebildet, die Designs, bewährte Verfahren und detaillierte Informationen über den Waffenbau austauscht. Angefangen mit einem Modell namens „Liberator“, einem eher rudimentären Entwurf, der nur einen Schuss zulässt, haben sich diese Bemühungen zu halbautomatischen Pistolenkaliber-Karabinern wie dem 9-mm-Karabiner „FGC-9“ weiterentwickelt, der zu 80-90 % aus 3D-gedruckten Polymerteilen besteht. Um die Materialeigenschaften zu erreichen, die 3D-gedruckte Feuerwaffen funktionsfähig und damit gefährlich machen, ist ein beträchtliches Maß an Experimentieren mit verschiedenen Parametern erforderlich, z. B. mit dem Rohmaterial, der Prozesstemperatur und der Fließgeschwindigkeit. Untersuchungen nationaler Behörden haben gezeigt, dass solche Waffen der Leistungsfähigkeit konventioneller Waffen nahe kommen und als solche in Myanmar von den gegen die Militärjunta kämpfenden Rebell*innen eingesetzt werden.¹² Aufgrund der Zugänglichkeit und Erschwinglichkeit von 3D-Desktopdruckern beschränkt sich die Innovation von Polymerteilen nicht nur auf Feuerwaffen, sondern erstreckt sich auch auf neue Gegenstände wie kleine Drohnen, Munition und Bombenhülsen, medizinische Hilfsmittel wie Aderpressen usw.

3D-gedruckte Waffen, wie sie zunehmen von nichtstaatlichen Akteuren genutzt werden, können der Leistungsfähigkeit konventioneller Waffen nahe kommen.

Innovation nahe den Frontlinien

Sowohl in der Ukraine als auch in Myanmar entstand diese Innovation spontan aus den dezentralen und vielfältigen Bemühungen von Familienmitgliedern, Freiwilligen, Verbänden und Online-Gemeinschaften zur Unterstützung der Soldat*innen an der Front. Mit dem anhaltenden Konflikt werden diese Innovations-, Herstellungs- und Vertriebsnetze zunehmend professionalisiert. In der Ukraine hat die Regierung eine Innovationsstruktur mit der Bezeichnung Brave1 geschaffen, um die Effizienz des Entwicklungs- und Inno-

vationsprozesses zu steigern und die Erprobung und rasche Einführung neuer Systeme zu erleichtern. In Verbindung mit der individuellen und kollektiven nichtstaatlichen Unterstützung hat dies in der Ukraine zu einem Umfeld geführt, in dem viele neue Akteure unter anderem 3D-gedruckte militärische Ausrüstung entwerfen und anbieten.¹³ Beispiele sind



Prototyp einer Polymer-Raketenbombenspitze, die mit Material extrusion gedruckt wurde. © Marina Grigorivna/ Shutterstock

3D-gedruckte Grabenperiskope, Heckflossen für Bomben, Drohnenbombengehäuse, Drohnenabschussplattformen, Drohnen Greiferklaue, Sturmgewehr-Magazinlader usw.¹⁴ Mit zunehmender Professionalisierung werden einige Akteure zu Zulieferern der UAF und damit zu einem Teil der Top-down-Lieferkette. Viele Akteure sind jedoch nicht als Unternehmen, sondern als Netzwerk organisiert, das die Soldat*innen direkt beliefert und so die Nachschubkette von oben nach unten umgeht. Das Ergebnis ist ein Zustrom von oft nicht standardisierten Produkten, die flexibel auf den Materialbedarf der lokalen Einheiten reagieren. Da die Versorgung und Verteilung häufig dezentral erfolgt, kann davon ausgegangen werden, dass der Zugang zu diesen Gegenständen entlang der Frontlinie unterschiedlich ist. Inwieweit sich eine solche ungleiche Verteilung auf die Kriegsführung auswirkt, ist unklar, allerdings wurden Pro-

dukttests und Prototyping während der Kämpfe in der Ukraine zunehmend normalisiert.¹⁵ Da 3D-gedruckte Gegenstände Teil einer solchen Entwicklung sind, ergeben sich zusätzliche Risiken wie die Normalisierung einer Trial-and-Error-Praxis, bei der die Last solcher Experimente nicht von dem Akteur getragen wird, der die Tests durchführt, sondern von dem Subjekt, an dem getestet wird.¹⁶ Es ist sicher, dass die Do-it-yourself-Herstellung und der Vertrieb von AF-gefertigten Gegenständen für und an der Frontlinie ein Trend ist, der die Kriegsschauplätze weltweit weiter beeinflussen und die Distanz zwischen dem Kriegsgeschehen, den Kämpfen, den Kämpfer*innen und allen anderen weiter verringern wird.¹⁷

Rüstungs- und Exportkontrolle von AF-Technologien

Ausgehend von der Prämisse, dass Rüstungskontrollregime ein deeskalierendes Instrument sind, liegt der Schwerpunkt in diesem Abschnitt auf der Bewertung des Risikos von AF-Technologien für Stabilität und Sicherheit. Die beiden genannten Trends in der Kriegsführung – verbesserte Widerstandsfähigkeit der logistischen Versorgungskette und Primärproduktion neuer Militärtechnologie – weisen unterschiedliche Dynamiken auf und müssen daher getrennt betrachtet werden. Einerseits sind vom ersten Trend, den Verbesserungen in der logistischen Versorgungskette für Rüstung und Ausrüstung, keine destabilisierenden Effekte zu erwarten, die eine nähere Betrachtung für Zwecke der Rüstungskontrolle rechtfertigen. Der zweite Trend allerdings, nämlich die Fähigkeit zur Selbstproduktion von Waffen in Form von 3D-gedruckten Schusswaffen oder anderen Ausrüstungsgegenständen wie Drohnenkomponenten oder Munition (ohne Sprengstoff), ist besorgniserregend.

Der Hauptgrund für diese Besorgnis ist der Aufbau neuer Akteure und Netzwerke, die an der Produktion von Militärtechnologie beteiligt sind. Vor allem in der Ukraine ist ein neuer Markt für kommerzielle Akteure entstanden, die neue Systeme entwickeln, die ursprünglich aus zivilen Anwendungen stammen und nun für militärische Zwecke umgerüstet werden.¹⁸ In Verbindung mit Akteuren, die mit nichtkommerziellen Interessen die Kriegsanstrengungen unterstützen, wächst die Gemeinschaft der Fachleute, die wissen, wie man für militärische Zwecke angepasste Dual-Use-Güter entwirft, baut und vertreibt. Diese Entwicklung stellt ein Proliferationsrisiko dar, da es schwierig ist, den Wissenstrans-



fer von immateriellen Gütern wie Designdateien für illegale Zwecke zu unterbinden.¹⁹ Die nationalen Strafverfolgungsbehörden sind durch die Verbreitung von nicht registrierten 3D-gedruckten Waffen bereits mit erheblichen Herausforderungen konfrontiert. Da Fachwissen online ausgetauscht wird, ist es nur eine Frage der Zeit, bis sich die Innovationen auf andere Gegenstände wie 3D-gedruckte Raketenwerfer ausweiten werden. Gleiches gilt für die zunehmende Fertigkeit des Baus kleiner Drohnen, was sich wahrscheinlich aus dem Kriegskontext in den zivilen Bereich ausbreiten wird.

Regulativer Rahmen und Nichtverbreitungsstrategien

Die Risiken für die internationale Sicherheit und Stabilität durch AF-Technologien, -Software und -Rohstoffe sind derzeit wenig ausgeprägt. Staatliche Akteure, die auf eine Störung der internationalen Stabilität hinarbeiten könnten, erlangen durch AF keinen entscheidenden Vorteil. Die Verbreitung der Technologie kann eine effizientere Produktion von Gegenständen erlauben und ermöglichen, jedoch gibt es keine Anzeichen dafür, dass diese Effizienzsteigerung einerseits den Zugang zu Wissen und Materialien erleichtert, die zur Herstellung von Massenvernichtungswaffen benötigt werden, oder andererseits Akteure in die Lage versetzt, strategische Waffen- und Verteidigungssysteme erheblich zu gefährden. Für die Schaffung solcher Systeme ist mehr erforderlich als der Besitz von Produktionsmitteln, es braucht auch Expertise und unterstützende Infrastruktur. Es liegt an dieser Stelle an der Bundesregierung zu entscheiden, inwieweit die Kontrolle von anspruchsvoller Fertigungstechnologie – in diesem Fall AF – und deren Endnutzer*innen politisch gewollt ist. Was die nationale Sicherheit betrifft, so gibt es in Deutschland Gesetze, die sowohl die Herstellung als auch den Besitz von Kriegswaffen, sonstigen Rüstungsgütern und den Einsatz von Drohnen regeln. Von selbst hergestellten Geräten könnte ein Sicherheitsrisiko ausgehen, wenn ihre schiere Masse die Durchsetzungsmöglichkeiten überfordert. Bei Desktop-3D-Druckern, mit denen hauptsächlich Polymerteile wie Handfeuerwaffen oder Stabilisierungsflossen gedruckt werden, ist eine Verbreitungskontrolle durch Ausfuhrbestimmungen nicht möglich, da diese Drucker technologisch recht einfach und weltweit verfügbar sind und nicht speziell für den Druck von Rüstungsgütern modifiziert werden müssen. Ansätze zur Abwehr von Gefahren, die von selbst gedruckten Waffen ausgehen, sind in der Entwicklung, wie z. B. die „Vergiftung“ von 3D-Designs, d. h. die Verbreitung von manipulierten Designs im Internet, die entweder den Drucker beschädigen oder den Druck unbrauchbar machen. Ein weiterer möglicher Weg zur Kontrolle wäre es, gegen den Verkauf von Bausätzen vorzugehen, die die nicht gedruckten Teile dieser Waffen, wie z. B. den Lauf, enthalten. Diese Sets enthalten eine Auswahl von Artikeln, die in Baumärkten frei erhältlich sind, und sind auf die Selbstherstellung von Handfeuerwaffen ausgerichtet. Es wurde auch vorgeschlagen, das Verhalten zu überwachen und Regeln für Transparenz und friedliche Nutzung aufzustellen.²⁰ Da die Entwicklung und die Verfügbarkeit von Entwürfen im Internet weiter voranschreiten, werden sich auch die Möglichkeiten der Hobbybastler*innen und nichtstaatlichen Akteure zum Selbstbau von Waffen ausweiten, wodurch die Bemühungen der Strafverfolgungsbehörden umgangen werden. Vor allem rechtsextremistische Terrorist*innen haben 3D-gedruckte Feuerwaffen als Symbol der Unabhängigkeit für ihre Terroranschläge verwendet.²¹

Das Aktionsprogramm der Vereinten Nationen über Kleinwaffen

Im Juni 2024 stand das Thema auf der Tagesordnung der Überprüfungskonferenz des *Programme of Action (PoA) to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons (SALW) in All Its Aspects* der Vereinten Nationen. Das mündlich überarbeitete Ergebnisdokument ermutigt die Staaten, bewährte Praktiken auszutauschen, um der Verbreitung von Kleinwaffen und ihren immateriellen Konstruktionsunterlagen entgegenzuwirken, und mit der AF-Industrie zusammenzuarbeiten, um diese Bemühungen zu unterstützen.²² Darüber hinaus wurde eine offene technische Expert*innengruppe eingerichtet, die systematisch neue Wege zur Herstellung von Kleinwaffen erörtern und Wissen darüber austauschen soll.

Dieses internationale Forum bietet die Möglichkeit zu bewerten, inwieweit die für Kleinwaffen entwickelten Strategien auch für andere 3D-gedruckte Gegenstände geeignet sind, die als Waffe oder Teil einer solchen verwendet werden können. Da die Mechanismen des Entwurfs und der Herstellung, d. h. die gemeinsame Nutzung immaterieller Entwürfe im Internet und die dezentrale Herstellung zu Hause, bei 3D-gedruckten Kleinwaffen ähnlich sind, könnten die aus dem Aktionsprogramm resultierenden Maßnahmen auch auf andere sicherheitsrelevante Gegenstände anwendbar sein, die mit AF-Technologien von Hobbybastler*innen hergestellt werden.

Dual-Use-Ausfuhrbestimmungen

Komplexere und technologisch anspruchsvollere AF-Maschinen sind in den Dual-Use-Regulierungen nur spärlich geregelt.²³ Eine Ausnahme innerhalb der Europäischen Union ist der nationale Rechtsrahmen Spaniens, der sich speziell mit AF-Maschinen befasst, wie im jüngsten EU-Dokument zur Koordinierung der Ausfuhrkontrollen von Gütern mit doppeltem Verwendungszweck (C/2023/441) zu sehen ist.²⁴ In der spanischen Verordnung werden Maschinen mit der Fähigkeit zum Druck von Sprengstoffen herausgegriffen. Da die Erprobung solcher Anwendungen auch in Deutschland im Gange, aber noch nicht ausgereift ist, könnte ein Rechtsrahmen, der solche Anwendungen berücksichtigt, die Verbreitung dieser Technologie aus Deutschland und anderen europäischen Staaten und Partnerländern verhindern, bevor sie vollständig entwickelt ist.²⁵

Die verschwimmende Grenze zwischen ziviler und militärischer Forschung

Die Grenze zwischen der zivilen und der militärischen Nutzung von AF verschwimmt immer mehr, auf der nichtstaatlichen Seite vor allem durch Online-Communities und dezentralisierte Hersteller. Diese Entwicklung birgt Sicherheitsrisiken, von denen einige bereits bekannt sind und andere sich erst noch entwickeln werden. Maßnahmen, die die zivil-militärische Forschung fördern, wie z. B. die Bemühungen des deutschen Bundesministeriums für Bildung und Forschung, die strikte Trennung zwischen militärischer und ziviler Forschung in aufzuweichen,²⁶ müssen sich mit dem Potenzial einer sensiblen Wissensverbreitung außerhalb der ausgewiesenen Forschungsinstitute, Unternehmen und Universitäten befassen. Da die deutsche Forschungsethik für Dual-Use-Forschung stark auf die Verantwortung der Einzelperson abstellt,²⁷ ist es eine politische Überlegung, inwieweit ein ordnungspolitischer Rahmen die Regeln für die friedliche Nutzung durchsetzt oder aber lockert, um die Entwicklung neuer kommerzieller Militärtechnologieakteure zu fördern.

Liska Suckau

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

-
- 1 Forge, J. (2010). A Note on the Definition of "Dual Use". *Science and Engineering Ethics*, 16(1), 111–118. <https://doi.org/10.1007/s11948-009-9159-9>
 - 2 Schroeder, M., Florquin, N., Fabre, A. & Varisco, A. *Privately Made Firearms in the European Union*. Flemish Peace Institute. https://gunviolence.eu/wp-content/uploads/2023/11/Project_INSIGHT_Emerging-Threats_DEF.pdf
 - 3 DIN Media. *Additive Fertigung*. <https://www.dinmedia.de/de/themenseiten/additive-fertigungsverfahren>
 - 4 Gebler, M., Schoot Uiterkamp, A. J. M., & Visser, C. (2014). A global sustainability perspective on 3D printing technologies. *Energy Policy*, 74, 158–167. <https://doi.org/10.1016/j.enpol.2014.08.033>; Altıparmak, S. C., & Xiao, B. (2021). A market assessment of additive manufacturing potential for the aerospace industry. *Journal of Manufacturing Processes*, 68, 728–738. <https://doi.org/10.1016/j.jmapro.2021.05.072>
 - 5 Harper, J. (2023, 15. September). *Pentagon arms Ukraine with 'industrial-size' 3D printers*. Defensescoop. <https://defensescoop.com/2023/09/15/pentagon-arms-ukraine-with-industrial-size-3d-printers/>
 - 6 TOC. (2024, 24. Februar). *Ukraine's self-repair: M777 howitzer video sparks DIY weapon fix*. Bulgarianmilitary. <https://bulgarianmilitary.com/2024/02/15/ukraines-self-repair-m777-howitzer-video-sparks-diy-weapon-fix/>



- 7 Boer, J. D., Lambrechts, W., & Krikke, H. (2020). Additive manufacturing in military and humanitarian missions: Advantages and challenges in the spare parts supply chain. *Journal of Cleaner Production*, 257, 120301. <https://doi.org/10.1016/j.jclepro.2020.120301>
- 8 Westerweel, B., Basten, R., denBoer, J., & vanHoutum, G. (2021). Printing Spare Parts at Remote Locations: Fulfilling the Promise of Additive Manufacturing. *Production and Operations Management*, 30(6), 1615–1632. <https://doi.org/10.1111/poms.13298>; siehe S. 1628
- 9 Tegler, E. (2024, 7. Mai). Navy Pays \$100K To Replace Each F/A-18 Tire, 3D Printed Repairs Cuts Cost To \$300. The Warzone. <https://www.twz.com/sea/navy-pays-100k-to-replace-each-f-a-18-tire-3d-printed-repairs-cuts-cost-to-300>
- 10 Hartig, S. (2023). *Integrationslogik Additiver Fertigungsverfahren zur Unterstützung zeitweise autarker Systeme* [Dissertation, Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg]. <https://doi.org/10.24405/15016>
- 11 Santos González, D., & González Álvarez, A. (2018). *Additive Manufacturing Feasibility Study & Technology Demonstration—EDA AM State of the Art & Strategic Report*. European Defence Agency. https://eda.europa.eu/docs/default-source/projects/eda-am-study-and-strategic-report_v6.pdf
- 12 Molitch-Hou, M. (2023, 1. August). *Myanmar Rebels Rely on 3D Printed Guns to Fight Military Junta*. 3D Print. <https://3dprint.com/302100/myanmar-rebels-rely-on-3d-printed-guns-to-fight-military-junta/>
- 13 Gosselin-Malo, E. (2024, 22. Februar). *How Ukraine's defense companies have adapted to two years of war*. Defense News. <https://www.defensenews.com/global/europe/2024/02/22/how-ukraines-defense-companies-have-adapted-to-two-years-or-war/>
- 14 Hambling, D. (2024, 7. Juni). *Volunteers Worldwide With 3D Printers Are Aiding Ukraine's War Effort*. Forbes. <https://www.forbes.com/sites/davidhambling/2024/06/07/how-volunteers-worldwide-are-helping-ukraines-war-with-3d-printers/>
- 15 Siehe 14.
- 16 Hoijtink, M. (2022). 'Prototype warfare': Innovation, optimisation, and the experimental way of warfare. *European Journal of International Security*, 7(3), 322–336. <https://doi.org/10.1017/eis.2022.12>
- 17 Ford, M. C., & Hoskins, A. (2022). *Radical war: Data, attention and control in the twenty-first century*. Hurst & Company.
- 18 Bergengruen, E. (2024, 8. Februar). *Tech Companies Turned Ukraine Into an AI War Lab*. TIME. <https://time.com/6691662/ai-ukraine-war-palantir/?linkId=315027696>;
Volpicelli, G., Melkozerova, V., & Kayali, L. (2024, 16. Mai). 'Our Oppenheimer moment'—In Ukraine, the robot wars have already begun. POLITICO. <https://www.politico.eu/article/robots-coming-ukraine-testing-ground-ai-artificial-intelligence-powered-combat-war-russia/>
- 19 Kunertova, D. (2023). Drones have boots: Learning from Russia's war in Ukraine. *Contemporary Security Policy*, 44(4), 576–591. <https://doi.org/10.1080/13523260.2023.2262792>
- 20 Favaro, M. (2024). The Impact of Emerging Technologies. In J. A. Larsen & S. Smith (Hrsg.), *Arms control at a crossroads: Renewal or demise?* Lynne Rienner Publishers, Inc. 199.
- 21 Veilleux-Lepage, Y. (2021). *CTRL, HATE, PRINT- Terrorists and the Appeal of 3D-Printed Weapons* [Policy Brief]. International Centre for Counter-Terrorism - ICCT. <https://www.icct.nl/publication/ctrl-hate-print-terrorists-and-appeal-3d-printed-weapons>
- 22 United Nations Office of Disarmament Affairs. (2024, 28. Juni). *Fourth United Nations Conference to Review Progress Made in the Implementation of the Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons in All Its Aspects and the International Tracing Instrument: Draft Outcome Document*. A/CONF.192/2024/RC/CRP.1.Rev3. United Nations General Assembly. [https://docs-library.unoda.org/Programme_of_Action_on_Small_Arms_and_Light_Weapons_-Review_Conference_\(2024\)/CRP.1.Rev3_RevCon4_Draft_Outcome_Document_Orally_Revised_CLEAN_0.pdf](https://docs-library.unoda.org/Programme_of_Action_on_Small_Arms_and_Light_Weapons_-Review_Conference_(2024)/CRP.1.Rev3_RevCon4_Draft_Outcome_Document_Orally_Revised_CLEAN_0.pdf)
- 23 AF wird in der EU-Dual-Use-Verordnung nur in einem Abschnitt als zusätzliches Merkmal einer Maschine erwähnt, (EU) 2021/821 in Abschnitt 2B001, Anmerkung 4: „A machine tool having an additive manufacturing capability **in addition to** a turning, milling or grinding capability must be evaluated against each applicable entry 2B001.a.,b. or.c“.
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02021R0821-20231216&qid=1718280529662>
- 24 Europäische Union. (2023, 20. Oktober). Compilation of national control lists under Article 9(4) of Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (C/2023/441). *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202300441
- 25 Zhang, J., He, K., Zhang, D., Dong, J., Li, B., Liu, Y., Gao, G., & Jiang, Z. (2022). Three-dimensional printing of energetic materials: A review. *Energetic Materials Frontiers*, 3(2), 97–108. <https://doi.org/10.1016/j.enmf.2022.04.00>;
Muravyev, N. V., Monogarov, K. A., Schaller, U., Fomenkov, I. V., & Pivkina, A. N. (2019). Progress in Additive Manufacturing of Energetic Materials: Creating the Reactive Microstructures with High Potential of Applications. *Propellants, Explosives, Pyrotechnics*, 44(8), 941–969. <https://doi.org/10.1002/prep.201900060>
- 26 Bundesministerium für Bildung und Forschung. (2024). *Positionspapier des Bundesministeriums für Bildung und Forschung zur Forschungssicherheit im Lichte der Zeitenwende*. Bundesministerium für Bildung und Forschung. https://www.bmbf.de/SharedDocs/Downloads/de/2024/positionspapier-forschungssicherheit.pdf?__blob=publicationFile&v=1
- 27 Jakob, U., Kraemer, F., Kraus, F., & Lengauer, T. (2024). Applying Ethics in the Handling of Dual Use Research: The Case of Germany. *Research Ethics*, 0(0). <https://doi.org/10.1177/17470161241261044>

Künstliche Intelligenz & Biologie

Technologische Implikationen von KI für biologische Risiken

KI wird zunehmend auch in Verbindung mit den Bereichen konventionelle Rüstungskontrolle, Gefechtsfeldmanagement und Datenanalyse diskutiert, wie beispielsweise im Kontext der Ukraine und in Gaza zu sehen ist. Gleichzeitig unterstreicht der wachsende Einfluss von KI in verschiedenen Bereichen die Notwendigkeit, auch über Politik und Governance zu diskutieren. In diesem Kapitel sollen die möglichen Auswirkungen der Konvergenz zwischen Biowissenschaften und KI untersucht werden. Zunächst werden die zahlreichen Vorteile betrachtet, die sich an dieser Schnittstelle ergeben können (mit Beispielen aus den Bereichen Bioabwehr und Biowaffen/Attribution von gentechnischen Veränderungen), um dann die damit verbundenen Risiken zu analysieren und Vorschläge zu ihrer Eindämmung zu entwickeln. Obwohl einige dieser Risiken für die Biologie und die Chemie verallgemeinert werden können, z. B. die Verwendung von KI für das Design von Molekülen/Sequenzen, konzentriert sich dieses Kapitel weitgehend auf biologische Risiken.

Vorteile der Konvergenz von KI und Biowissenschaften

Die jüngsten Fortschritte auf dem Gebiet der Künstlichen Intelligenz (KI) bieten den modernen Biowissenschaften und dem Bioengineering enorme Vorteile. KI kann die rasche Entwicklung von Impfstoffen und Therapeutika unterstützen, einen Beitrag zur Materialwissenschaft leisten, die Wirtschaft ankurbeln und zur Bekämpfung des Klimawandels beitragen.¹

KI in der Pandemievorsorge

Die Verbesserung der Pandemievorsorge und -reaktion erfordert auch den Einsatz fortschrittlicher Technologien wie KI, um die Meldung und Analyse von Ausbrüchen zu optimieren.² Durch die effiziente Verarbeitung von Daten aus Ausbruchsmeldungen und die Analyse von Informationen über zurückkehrende Reisende können KI-Werkzeuge die Häufigkeit der Einschleppung von Infektionskrankheiten modellieren und deren Ursprung zurückverfolgen. Das Europäische Zentrum für die Prävention und die Kontrolle von Krankheiten stellt beispielsweise Werkzeuge für die Analyse von Überwachungsdaten zu Infektionskrankheiten bereit.³ Routinemäßige Überwachungsdaten werden einer statisti-



schen Analyse unterzogen, um Schwankungen in der Krankheitsinzidenz zu erkennen, so dass potenzielle Ausbrüche frühzeitig erkannt und untersucht werden können. In Kombination mit der Genomsequenzierung wird dieser Ansatz entscheidend sein, um Ausbrüche festzustellen und persistente Erregerreservoirs aufzudecken.

Darüber hinaus spielt die KI eine Schlüsselrolle bei der Vorhersage des Risikos, das von (neuen) Erregerstämmen ausgeht.⁴ Schnelle DNA-Analysen, die durch KI-Tools erleichtert werden, ermöglichen es Wissenschaftler*innen, potenzielle Pandemieerreger und Hochrisikovarianten zu identifizieren, bevor sie sich zu weit verbreiteten Ausbrüchen entwickeln.

KI in der Überwachung von Krankheitserregern

Metagenomische Überwachung, wie z. B. die Überwachung von Abwässern, kann Krankheitserreger identifizieren, die in Gemeinschaften zirkulieren.⁵ Angesichts der enormen Datenmengen, die erzeugt werden, können KI-Werkzeuge wie die Erkennung von Anomalien helfen, (neue) Bedrohungen zu identifizieren.⁶ Nukleinsäurepanels bieten eine kostengünstige Alternative zur DNA-Sequenzierung für die kontinuierliche Überwachung von Infektionskrankheiten.⁷ Die Entwicklung von Panels, die zahlreiche Krankheitserreger nachweisen können, kann komplex sein, aber KI-Optimierungstechniken können diesen Prozess vereinfachen.

KI in der Gentechnik-Attribution

Jüngste Fortschritte zeigen, dass KI-Werkzeuge gentechnisch veränderte Organismen effektiv identifizieren und ihrem Ursprungslabor zuordnen können. Die Designentscheidungen eines Bioingenieurs – z. B. die Wahl des Promotors (Transkriptionsstartpunkt einer DNA-Sequenz), die Optimierung des Codes, die Auswahl funktioneller Gene und die Wahl der Klonierungsmethode – bilden zusammen die „Signatur“ dieses Designers.⁸ Mehrere neue Techniken wurden entwickelt, um diese Signaturen zu erfassen. Ihre Analyse erfordert eine komplexe Datenanalyse, die durch maschinelles Lernen und KI-Werkzeuge verbessert werden könnte. Diese Werkzeuge sind zwar vielversprechend bei der Identifizierung von Akteuren, die biologische Gefahrenstoffe entwickeln, ihre Wirksamkeit bei der Attribution kann jedoch beeinträchtigt werden, wenn die Akteure Designentscheidungen manipulieren können, um der Entdeckung zu entgehen.

KI in der Synthetischen Biologie

Die Synthetische Biologie bietet ein großes Potenzial zur Bewältigung wichtiger gesellschaftlicher Herausforderungen. Ein Haupthindernis ist jedoch, dass biologische Systeme derzeit nicht so genau vorhergesagt werden können wie physikalische oder chemische Systeme, die auch simuliert werden können. Diese Einschränkung hat sowohl praktische als auch grundlegende Konsequenzen. In der Praxis können biologische Systeme (z. B. Proteine, Stoffwechselwege, Zellen) nicht nach bestimmten Anforderungen (z. B. Bindungsaffinität, Produktionsraten) entworfen werden. Grundsätzlich fehlt ein tiefes Verständnis der Mechanismen, die beobachtbare Merkmale oder Eigenschaften von Organismen hervorbringen. KI und maschinelles Lernen (ML) sind vielversprechende Methoden, um die in der Synthetischen Biologie benötigte Vorhersagekraft zu verbessern, und können während des gesamten Prozesses der Synthetischen Biologie eingesetzt werden.

In den letzten zwei Jahrzehnten wurden beispielsweise verschiedene Werkzeuge für maschinelles Lernen entwickelt, die das Enzym-Engineering unterstützen, indem sie Ansätze vereinfachen und den erforderlichen Screening-Aufwand verringern. ML kann Informationen über Enzymsequenzen und -eigenschaften verarbeiten und daraus neue Informationen ableiten, die diese Eigenschaften wahrscheinlich verbessern oder verfeinern. Diese Algorithmen haben zahlreiche Anwendungen in der Synthetischen Biologie, einschließlich

Nukleinsäure-Panel: Diagnostischer Test, bei dem mehrere Nukleinsäuresequenzen (DNA oder RNA) gleichzeitig untersucht werden, um verschiedene Organismen oder genetische Marker in einer einzigen Probe nachzuweisen und zu identifizieren. Siehe auch den Eintrag im Glossar, S. 98.

Für eine Diskussion dieses Aspekts, siehe S. 53.

der Optimierung von genetischen und metabolischen Netzwerken, der Steuerung der Enzymevolution, der Vorhersage der kinetischen Eigenschaften von nicht charakterisierten Enzymen und sogar das Neuerschaffen von ganzen Proteinen.

Risiken der KI-Bio-Konvergenz

Expert*innen, die die potenziellen Risiken von KI-Methoden für die Biowissenschaften analysieren, konzentrieren sich derzeit auf zwei Hauptfragen.⁹ Erstens: Verringern die Fortschritte bei den KI-Werkzeugen die Hürden für die Entwicklung von Krankheitserregern? Einige Expert*innen vermuten, dass dies der Fall ist.¹⁰ Zweitens: Welche KI-Modelle und -Werkzeuge bergen das größte Missbrauchsrisiko?

KI-Werkzeuge, die ein potenzielles Sicherheitsrisiko darstellen, lassen sich in drei Kategorien einteilen:¹¹ Large Language Models (LLMs), Biodesign-Tools (BDTs) und KI-gestützte Automatisierung in den Biowissenschaften. Obwohl diese Kategorien bei der Bewertung der jeweiligen potenziellen Biosicherheitsrisiken hilfreich sein können, verschwimmen die Grenzen zwischen diesen Fähigkeitstypen zunehmend.¹²

Large Language Models (LLMs)

Obwohl LLMs in natürlicher Sprache nicht speziell für die Förderung der Biowissenschaften entwickelt wurden, werden sie die biowissenschaftliche Forschung erheblich beeinflussen, indem sie Ausbildung, Grundlagenforschung und Laborkapazitäten unterstützen. LLMs sind in der Lage, Informationen aus einer Vielzahl von Quellen schnell zusammenzuführen und in verständlicher Sprache darzustellen. Im Grunde stellt dies bereits ein Dual-Use-Problem dar, da LLMs Wissen für die legitime Wissenschaft bereitstellen, aber auch für illegitime Zwecke genutzt werden können.¹³ Gegenwärtig scheinen diese Modelle vor allem für Nutzer*innen mit einem gewissen Grundwissen von Vorteil zu sein. Aber mehrere Expert*innen sind der Ansicht, dass sie auch Personen, die mit einem Thema gänzlich unvertraut sind, schnell zu einem Verständnis verhelfen können, das mit dem von Studierenden oder sogar Promovierenden vergleichbar ist. Laut einem Bericht der NTI (Nuclear Threat Initiative)¹⁴ teilen einige Expert*innen die Einschätzung, dass es den Instrumenten an Präzision und Genauigkeit mangelt, wenn es um technisch komplexere Fragen geht. Sie sind der Ansicht, dass die derzeitigen LLMs wahrscheinlich keine wesentlichen neuen Erkenntnisse über biologische Systeme liefern werden. Einige LLMs sind speziell auf wissenschaftliche Literatur ausgerichtet und könnten für Studierende und andere Personen, die sich mit technischen Themen vertraut machen wollen, nützlicher sein.

Es wurden Versuche unternommen, die damit verbundenen Risiken zu bewerten.¹⁵ Diese deuten darauf hin, dass die derzeitigen LLMs das biologische Risiko nicht signifikant erhöhen. Allerdings gab es auch erhebliche Kritik am Studiendesign und den verwendeten statistischen Methoden.¹⁶ So wurde unter anderem darauf hingewiesen, dass diese Berichte unter einer asymmetrischen Risikobewertung leiden könnten, bei der nur negative Ergebnisse veröffentlicht werden (da positive Ergebnisse, die zeigen, welchen potenziellen Schaden diese Modelle anrichten könnten, als gefährlich angesehen werden könnten). Diese Diskrepanz könnte möglicherweise die Wahrnehmung des tatsächlichen Risikos verzerren.

LLMs könnten potenziell dabei helfen, auf der Grundlage veröffentlichter Informationen molekularbiologische Experimente zu planen und Fehler darin zu suchen sowie Roboterplattformen zur Durchführung von Experimenten zu programmieren. Diese Fähigkeiten können es weniger notwendig machen, dass Einzelpersonen die technischen Fähigkeiten entwickeln, die für die Durchführung der Experimente selbst erforderlich

Siehe dazu auch die Erläuterung zu Large Language Models im Glossar, S. 97.



sind. Während die derzeitigen LLMs in der Regel auf textbasierte Informationen beschränkt sind, können einige Modelle auch Informationen aus Bildern und Videos einbeziehen, wodurch sie möglicherweise in der Lage sind, effektiveres Feedback und Vorschläge zur Fehlerbehebung bei Labortechniken in Echtzeit zu liefern. Diese KI-gestützten Laborassistenten könnten viele nützliche Anwendungen zur Unterstützung von Forschenden bieten, insbesondere solchen, die am Anfang ihrer Karriere stehen. Dieselben KI-gestützten Assistenten könnten jedoch auch die Laborarbeit zu unlaute- ren Zwecken unterstützen.

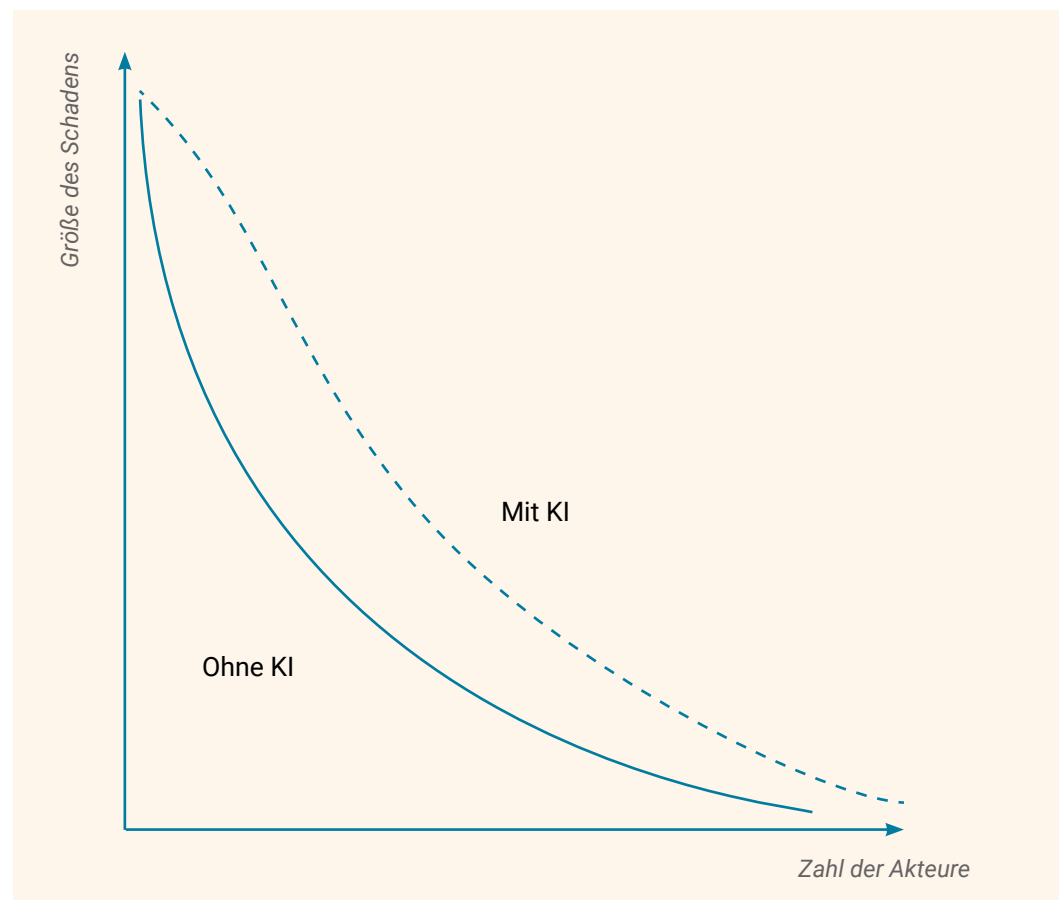
Biologische Design-Tools (BDTs)

Die zweite Kategorie von KI-Tools mit einem potenziellen Missbrauchsrisiko umfasst biologische Design-Tools (BDTs). Es wird angenommen, dass Large Language Models (LLMs), die auf biologischen Daten basieren, die effektivsten BDTs sein könnten. LLMs können mit DNA- und RNA-Sequenzierungsmustern trainiert werden, um Modifikationen und Regulierungsmechanismen innerhalb dieser Sequenzen vorherzusagen. Darüber hinaus können LLMs, die auf Proteindaten trainiert wurden, für verschiedene Anwendungen eingesetzt werden, z. B. zur Vorhersage von Proteinstrukturen, zur Generierung neuer Proteine, zur Annotation von Proteinfunktionen und zur Vorhersage von Proteininteraktionen. Derzeit werden BDTs häufig der Öffentlichkeit zugänglich gemacht, unabhängig davon, ob sie von der Wissenschaft (z. B. RFDiffusion) oder der Industrie (z. B. ProGen2) entwickelt wurden. Während die heutigen BDTs auf die Erzeugung von Proteinen mit relativ einfachen Einzelfunktionen beschränkt sind, dürften künftige Iterationen in der Lage sein, Proteine¹⁷ und Enzyme mit mehreren Funktionen zu optimieren. Neben Werkzeugen für das Design von Proteinen oder Organismen gibt es auch andere maschinelle Lernwerkzeuge mit doppeltem Verwendungszweck, darunter solche, die Eigenschaften wie die Immunabwehr vorhersagen oder das funktionelle Verständnis des menschlichen Genoms fördern. Deep-Learning-Architekturen wie Enformer verbessern die Genauigkeit von Vorhersagen der Genexpression aus DNA-Sequenzen erheblich.¹⁸

Mehrere Expert*innen befürchten, dass KI-Werkzeuge für das Proteindesign es den DNA-Anbietern erschweren könnten, die bestellte DNA umfassend zu überwachen. Da die derzeitigen DNA-Screening-Methoden auf einem Vergleich der in Auftrag gegebenen DNA mit der DNA eines

Zur Unterscheidung verschiedener Typen von KI-Modellen, siehe „LLM, LMM und AGI“ im Glossar, S. 97.

Zur Vertiefung siehe den Eintrag zu BDTs im Glossar, S. 96.



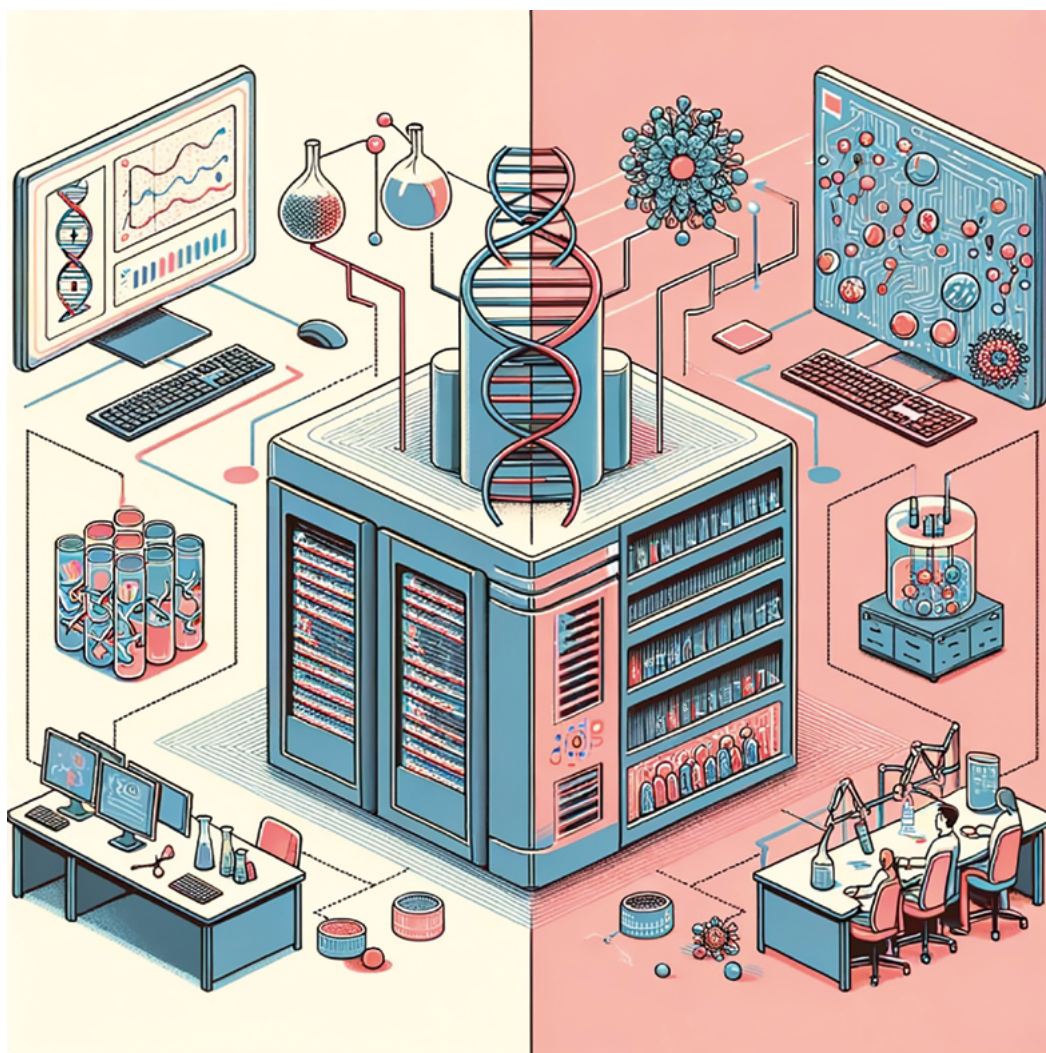
LLMs und KI-Biodesign-Tools werden wahrscheinlich die Risikolandschaft eines versehentlichen oder vorsätzlichen Missbrauchs der Biologie verändern. LLMs können mehr Akteure in die Lage versetzen, Schaden anzurichten, während künftige Biodesign-Werkzeuge die Obergrenze der Schäden, die durch einen biologischen Wirkstoff verursacht werden können, erhöhen können. Quelle: Abbildung angepasst mit Erlaubnis, nach J. Sandbrink, 2023, siehe Endnote 10.

Krankheitserregers beruhen, könnten sich die neu entworfenen Proteine dieser Kontrolle entziehen. Diese Werkzeuge könnten so die Schaffung neuer Bedrohungen unterstützen (um Toxin- oder Krankheitserregersdesigns zu erzeugen, die in der Natur nicht vorkommen) und sich dem DNA-Sequenzierungsscreening entziehen.¹⁹

KI-gestützte Automatisierung der Biowissenschaften

Vereinfacht ausgedrückt wird unter KI-gestützter automatisierter Wissenschaft die Übertragung eines, mehrerer oder aller Schritte des wissenschaftlichen Prozesses auf KI verstanden. Dem NTI-Bericht zufolge gab es zum Zeitpunkt seiner Erstellung mehrere

Beispiele für Forschungsprojekte, bei denen mindestens ein Schritt des wissenschaftlichen Prozesses automatisiert wurde. Zu diesen Schritten gehören die anfängliche wissenschaftliche Literaturrecherche, die Entwicklung von Hypothesen, die Planung und Durchführung von Experimenten mithilfe von Robotern, die Analyse der Ergebnisse und die Anpassung der Hypothese. Jede dieser Fertigkeiten könnte den wissenschaftlichen Prozess erheblich beschleunigen, indem sie Möglichkeiten zur Skalierung bietet, die Zahl der erforderlichen Experimente verringert und von Menschen verursachte Verzögerungen und Fehler reduziert. Die Möglichkeit einer vollständigen Automatisierung biologischer Experimente wird noch diskutiert.



Wie KI zur Automatisierung der Biowissenschaften eingesetzt werden könnte: von der Literaturrecherche über die Entwicklung von Hypothesen, bis hin zur Planung und Durchführung von Experimenten mittels Robotik und der anschließenden Auswertung. KI-generierte Abbildung: Shutterstock AI Generator.

Ein KI-Agent ist ein Softwareprogramm, das in der Lage ist, mit seiner Umgebung zu interagieren, Daten zu sammeln und diese zu nutzen, um Aufgaben zu erfüllen, die auf bestimmte Ziele ausgerichtet sind. Siehe Glossar, S. 97.

KI-Werkzeugen (z. B. LLMs) interagieren können, um komplexe Aufgaben zu koordinieren und auszuführen. Ein Beispiel aus der Chemie ist ChemCrow,²⁰ ein LLM-basierter Agent, der entwickelt wurde, um Aufgaben in den Bereichen organische Synthese, Arzneimittelforschung und Materialdesign auszuführen. Diese Art von Werkzeugen kann verwendet werden, um das Internet nach relevanten Informationen zu durchsuchen, sich über Anwendungsprogrammierschnittstellen (APIs) mit der Robotik zu verbinden und sich sogar mit anderen LLMs zu verbinden, um Aufgaben zu delegieren, wie das Ibuprofen-Syntheseprojekt²¹ gezeigt hat.

Ein neuerer Ansatz zur Automatisierung der Wissenschaft besteht in der Entwicklung autonomer KI-Agenten, die mit mehreren



KI in der Arzneimittelentwicklung

Derzeit besteht die Notwendigkeit, die Kosten und den Zeitaufwand für die Entdeckung von Arzneimitteln zu senken. Dies wird die Entwicklung von Behandlungsmöglichkeiten für Krankheiten erleichtern, für die weniger Forschungsmittel zur Verfügung stehen, wie z. B. Tropenkrankheiten und vernachlässigte Krankheiten, und die Verfügbarkeit neuer Arzneimittel insgesamt erhöhen. Wissenschaftler*innen machen Fortschritte mit Wissensrobotern wie Eve,²² einem System, das die Entdeckung von Arzneimitteln in einem frühen Stadium automatisiert, um neue Behandlungen für vernachlässigte tropische Krankheiten zu finden. In den letzten Jahren wurde auch zunehmend diskutiert, wie KI-Technologien für die Arzneimittelentdeckung möglicherweise missbraucht werden könnten.²³

Risikominderung und Governance

Expert*innen haben mehrere Methoden vorgeschlagen, um die Risiken von LLMs und BDTs anzugehen. Eine davon ist die Bewertung der Modelle vor ihrer Freigabe. Die Charakterisierung von Risiken und die Bewertung der Wirksamkeit von Schutzmaßnahmen vor der Freigabe würde für Entwickler*innen einen Anreiz darstellen, schädliches Modellverhalten während der gesamten Trainings- und Nutzungsphase zu bereinigen.

Eine andere Methode, die Kompromisse in Betracht zieht, ist die Abwägung zwischen der Notwendigkeit eines uneingeschränkten Zugangs und Sicherheitsbedenken. Verschiedene Interessengruppen müssen Beweise sammeln und Werkzeuge entwickeln, um zu beurteilen, wann die Vorteile der Freigabe eines Modells durch die Risiken aufgewogen werden und dabei vielleicht auch Schritte zur Benutzerauthentifizierung für leistungsfähigere Modelle in Betracht ziehen.

Expert*innen empfehlen außerdem, die Biosicherheitsmaßnahmen an der Schnittstelle zwischen digitaler und physischer Welt zu verstärken. Da der Zugang zu synthetischer DNA für die Umwandlung biologischer Designs in physische Wirkstoffe von entscheidender Bedeutung ist, haben führende Unternehmen der Branche freiwillig damit begonnen, Gensyntheseaufträge zu überprüfen (indem sie die Identität der Kunden verifizieren und die Bestellungen überwachen, um sicherzustellen, dass Sequenzen, die Schaden anrichten könnten, nicht unangemessen freigegeben werden). Sie setzen sich außerdem für eine gesetzliche Grundlage ein. Die in den USA vom Weißen Haus im Oktober 2023 erlassene KI-Durchführungsverordnung (Executive Order 14110) war ein Schritt in diese Richtung, da sie die Verwendung von kontrollierter DNA in der staatlich finanzierten Forschung vorschreibt. Die EU hat jedoch noch keine Regelungen zu diesem Thema erlassen. Im Jahr 2024 wurde eine globale Grundlage für das Screening von Nukleinsäuresynthese vorgeschlagen, der sogenannte „Common Mechanism for DNA Synthesis Screening“.²⁴ Dieses Instrument wurde in Zusammenarbeit mit einem technischen Konsortium von Expert*innen aus den Bereichen DNA-Synthese, synthetische Biologie, Biosicherheit und Politik entwickelt, um bestehende Hindernisse zu überwinden. Die Common-Mechanism-Software verwendet mehrere Methoden, um bedenkliche Sequenzen zu identifizieren, sie taxonomisch mit regulierten Krankheitserregern abzugleichen und gutartige Gene für die Synthese freizugeben.

Die Charakterisierung von Risiken und die Bewertung der Wirksamkeit von Schutzmaßnahmen vor der Freigabe würde für Entwickler*innen einen Anreiz darstellen, schädliches Modellverhalten während der gesamten Trainings- und Nutzungsphase zu bereinigen.

Red Teaming (im KI-Kontext): ein interaktives Verfahren zum Testen von KI-Modellen, das schädliches Verhalten wie die Preisgabe sensibler Daten und die Erzeugung toxischer, voreingenommener oder sachlich falscher Inhalte verhindern soll.

Ende 2023 wurden in den USA mehrere neue Anforderungen an leistungsstarke KI-Bio-Modelle eingeführt. Die Executive Order schreibt umfassende Maßnahmen vor, um die von KI-Systemen ausgehenden nationalen Sicherheitsrisiken zu mindern. Unternehmen, die „Dual-Use-Basismodelle“ entwickeln, müssen regelmäßig über ihre Modellentwicklungspläne und Risikomanagementstrategien berichten, einschließlich der Absicherung von Modellgewichten und der Durchführung von Red-Team-Tests zur Identifizierung gefährlicher Fähigkeiten. Für KI-Modelle, die mit biologischen Sequenzdaten trainiert werden, gelten neue Berichts- und Compliance-Anforderungen.

Dr. Kadri Reis

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

- 1 Carter, S. R., Wheeler, N., Chwalek, S., Isaac, C., & Yassif, J. M. (2023). *The Convergence of Artificial Intelligence and the Life Sciences: Safeguarding Technology, Rethinking Governance, and Preventing Catastrophe*. Nuclear Threat Initiative. <https://www.nti.org/analysis/articles/the-convergence-of-artificial-intelligence-and-the-life-sciences/>
- 2 Syrowatka, A., Kuznetsova, M., Alsubai, A., Beckman, A. L., Bain, P. A., Craig, K. J. T., Hu, J., Jackson, G. P., Rhee, K., & Bates, D. W. (2021, 10. Juni). Leveraging artificial intelligence for pandemic preparedness and response: A scoping review to identify key use cases. *Npj Digital Medicine*, 4(1), 96. <https://doi.org/10.1038/s41746-021-00459-8>
- 3 European Centre for Disease Prevention and Control. (2018, 17. Dezember). *New tools for public health experts: Outbreak detection and epidemiological reports*. Europäische Union, European Centre for Disease Prevention and Control (ECDC). <https://www.ecdc.europa.eu/en/news-events/new-tools-public-health-experts-outbreak-detection-and-epidemiological-reports>
- 4 Njage, P. M. K., Henri, C., Leekitcharoenphon, P., Mistou, M., Hendriksen, R. S., & Hald, T. (2018). Machine Learning Methods as a Tool for Predicting Risk of Illness Applying Next-Generation Sequencing Data. *Risk Analysis*, 39(6), 1397–1413. <https://doi.org/10.1111/risa.13239>
Zhao, A. P., Li, S., Cao, Z., Hu, P. J.-H., Wang, J., Xiang, Y., Xie, D., & Lu, X. (2024, 2. Juni). AI for science: Predicting infectious diseases. *Journal of Safety Science and Resilience*, 5(2), 130–146. <https://doi.org/10.1016/j.jnlssr.2024.02.002>
- 5 Ahmed, W., Angel, N., Edson, J., Bibby, K., Bivins, A., O'Brien, J. W., Choi, P. M., Kitajima, M., Simpson, S. L., Li, J., Tschärke, B., Verhagen, R., Smith, W. J. M., Zaugg, J., Dierens, L., Hugenholtz, P., Thomas, K. V., & Mueller, J. F. (2020, 1. August). First confirmed detection of SARS-CoV-2 in untreated wastewater in Australia: A proof of concept for the wastewater surveillance of COVID-19 in the community. *Science of The Total Environment*, 728, 138764. <https://doi.org/10.1016/j.scitotenv.2020.138764>
- 6 Eze, P. U., Geard, N., Mueller, I., & Chades, I. (2023). Anomaly Detection in Endemic Disease Surveillance Data Using Machine Learning Techniques. *Healthcare*, 11(13), 1896. <https://doi.org/10.3390/healthcare11131896>
Ren, H., Li, Y., & Huang, T. (2023). Anomaly Detection Models for SARS-CoV-2 Surveillance Based on Genome k-mers. *Microorganisms*, 11(11), 2773. <https://doi.org/10.3390/microorganisms11112773>
- 7 Metsky, H. C., Welch, N. L., Pillai, P. P., Haradhvala, N. J., Rumker, L., Mantena, S., Zhang, Y. B., Yang, D. K., Ackerman, C. M., Weller, J., Blainey, P. C., Myhrvold, C., Mitzenmacher, M., & Sabeti, P. C. (2022, 3. März). Designing sensitive viral diagnostics with machine learning. *Nature Biotechnology*, 40(7), 1123–1131. <https://doi.org/10.1038/s41587-022-01213-5>
- 8 Alley, E. C., Turpin, M., Liu, A. B., Kulp-McDowall, T., Swett, J., Edison, R., Von Stetina, S. E., Church, G. M., & Esvelt, K. M. (2020, 8. Dezember). A machine learning toolkit for genetic engineering attribution to facilitate biosecurity. *Nature Communications*, 11(1), 6293. <https://doi.org/10.1038/s41467-020-19612-0>
- 9 Carter et al., 2023.
- 10 Sandbrink, J. B. (2023). *Artificial intelligence and biological misuse: Differentiating risks of language models and biological design tools* (Version 8). arXiv. <https://doi.org/10.48550/ARXIV.2306.13952>
- 11 Rose, S., & Nelson, C. (2023, 18. Oktober). *Understanding AI-Facilitated Biological Weapon Development*. The Centre for Long-Term Resilience. <https://www.longtermresilience.org/post/report-launch-examining-risks-at-the-intersection-of-ai-and-bio>
- 12 Toews, R. (2023, 16. Juli). The Next Frontier For Large Language Models Is Biology. *Forbes*. <https://www.forbes.com/sites/robtoews/2023/07/16/the-next-frontier-for-large-language-models-is-biology/>
- 13 Sandbrink, 2023.
- 14 Carter et al., 2023.



- 15 Rose et al., 2023;
Mouton, C., Lucas, C., & Guest, E. (2024, 25. Januar). *The Operational Risks of AI in Large-Scale Biological Attacks: Results of a Red-Team Study*. (RAND).
- 16 Marcus, G. (2024, 4. Februar). When looked at carefully, OpenAI's new study on GPT-4 and bioweapons is deeply worrisome. *Marcus on AI*. <https://garymarcus.substack.com/p/when-looked-at-carefully-openais>
- 17 Spotlight on protein structure design. (2024, 15. Februar). *Nature Biotechnology*, 42(2), 157–157. <https://doi.org/10.1038/s41587-024-02150-1>
- 18 Avsec, Ž., Agarwal, V., Visentin, D., Ledsam, J. R., Grabska-Barwinska, A., Taylor, K. R., Assael, Y., Jumper, J., Kohli, P., & Kelley, D. R. (2021). *Effective gene expression prediction from sequence by integrating long-range interactions*. <https://doi.org/10.1101/2021.04.07.438649>
- 19 Carter et al., 2023.
- 20 Bran, A. M., Cox, S., Schilter, O., Baldassari, C., White, A. D., & Schwaller, P. (2024, 8. Mai). Augmenting large language models with chemistry tools. *Nature Machine Intelligence*, 6(5), 525–535. <https://doi.org/10.1038/s42256-024-00832-8>
- 21 Boiko, D. A., MacKnight, R., & Gomes, G. (2023, 11. April). *Emergent autonomous scientific research capabilities of large language models* (Version 1). arXiv. <https://doi.org/10.48550/ARXIV.2304.05332>
- 22 Williams, K., Bilsland, E., Sparkes, A., Aubrey, W., Young, M., Soldatova, L. N., De Grave, K., Ramon, J., De Clare, M., Sirawaraporn, W., Oliver, S. G., & King, R. D. (2015, 6. März). Cheaper faster drug development validated by the repositioning of drugs against neglected tropical diseases. *Journal of The Royal Society Interface*, 12(104), 20141289. <https://doi.org/10.1098/rsif.2014.1289>
- 23 Urbina, F., Lentzos, F., Invernizzi, C., & Ekins, S. (2022, 7. März). Dual use of artificial-intelligence-powered drug discovery. *Nature Machine Intelligence*, 4(3), 189–191. <https://doi.org/10.1038/s42256-022-00465-9>
- 24 Wheeler, N. E., Carter, S. R., Alexanian, T., Isaac, C., Yassif, J., & Millet, P. (2024, 20. Juni). Developing a Common Global Baseline for Nucleic Acid Synthesis Screening. *Applied Biosafety*, 29(2), 71–78. <https://doi.org/10.1089/apb.2023.0034>

Biotechnologie

Auswirkungen von technologischem Fortschritt auf die Biosicherheit

Dieses Kapitel befasst sich mit Strategien zum Schutz vor biologischen Gefahren. Es untersucht zunächst eine Auswahl von Methoden zur Identifizierung von Krankheitserregern und gibt einen Überblick über ihre technischen Möglichkeiten, Mängel und zugrunde liegenden Prinzipien. Der zweite Teil taucht in eine breitere Analyse biologischer Angriffe ein und diskutiert dabei die mikrobielle Forensik und das Potenzial der gentechnischen Attribution.

Kulturenbasierte mikrobielle Techniken: Kultivierung mikrobieller Organismen durch Vermehrung in einem vordefinierten Nährmedium unter kontrollierten Laborbedingungen. Nicht alle Mikroorganismen wachsen unter diesen Bedingungen.

Polymerase-Kettenreaktion (PCR): eine Labortechnik zur Herstellung (oder Vervielfältigung) von Millionen bis Milliarden von Kopien eines bestimmten DNA-Abschnitts, der dann genauer untersucht werden kann. Siehe auch den Eintrag im Glossar, S. 98.

Ein zentrales Ziel der biologischen Abwehr (*Biodefense*) ist die Entwicklung schneller, empfindlicher und automatisierter Technologien, die in der Lage sind, biologische Kampfstoffe mit hoher Selektivität, Empfindlichkeit und Genauigkeit aufzuspüren und zu bestimmen. Der ideale Biomarker für den Nachweis von Krankheitserregern wäre einer, der für jeden biologischen Gefahrenstoff einzigartig und quantifizierbar ist. Die meisten Systeme zum Nachweis von Erregern verwenden Nukleinsäuren (z. B. DNA), Lipide und Proteine als primäre Elemente für die Erkennung. Gängige mikrobielle Stoffwechselprodukte wie flüchtige organische Verbindungen (VOCs) haben sich ebenfalls als vielversprechend für die Pathogenidentifizierung gezeigt.¹

Die Detektionstechnologien konzentrieren sich auf eine Vielzahl von Methoden, die Oberflächenmerkmale, genomische Marker (DNA-Sequenz mit bekannter physischer Position auf einem Chromosom), Proteomanalysen usw. umfassen. Während kulturenbasierte Methoden wie die Genomsequenzierung aufgrund ihrer hohen Sensitivität als guter Maßstab für den Nachweis von Krankheitserregern gelten, sind sie arbeitsintensiv, kostspielig und langsam, weshalb sich diese Methoden weniger an die Erfordernisse schneller Reaktionen anpassen lassen. Im Gegensatz dazu bieten molekulare Methoden wie die Polymerase-Kettenreaktion (PCR) oder der Enzym-Immunoassay (ELISA) eine vergleichbare Sensitivität, Schnelligkeit und Genauigkeit. Allerdings erfordern molekulare Verfahren wie diese in der Regel hoch qualifiziertes Personal. Überdies ist zu beachten, dass Toxine mit diesen molekularen Strategien nicht identifiziert werden können, da sie keine DNA enthalten.

Molekulare Nachweismethoden

Pandemieviren und Schädlinge besitzen wie alle lebenden Organismen Genome, die aus Nukleinsäuren bestehen. Molekulare Nachweismethoden hängen von den unterschiedlichen Nukleinsäuremarkern ab, die für jeden biologischen Erreger spezifisch sind.



PCR (Polymerase-Kettenreaktion)

- Nach wie vor die bekannteste und meistgenutzte Technik
- Hauptvorteil ist ihre Spezifität, die sich aus der Einzigartigkeit des Genoms lebender Organismen ergibt.
- Höhere Sensitivität im Vergleich zu antikörperbasierten Methoden
- Ein erheblicher Nachteil ist die Unfähigkeit zur Unterscheidung lebender und toter Erreger.
- Um den Datendurchsatz zu erhöhen, müssten mehrere DNA-Zielsequenzen gleichzeitig nachgewiesen werden, indem mehrere Sätze von Primern in einer Reaktion kombiniert werden (sog. Multiplexing²).

Real-Time PCR (Echtzeit-PCR)

- Eine quantitative Methode, die den gleichzeitigen Nachweis und die Quantifizierung der Nukleinsäure in jeder Probe ermöglicht³

Wirksame Überwachungssysteme sollten unabhängig von spezifischen Phänotypen, Symptomprofilen oder Sequenzen funktionieren, die bei künftigen natürlichen Ausbrüchen oder Biowaffen erwartet werden. Angesichts der begrenzten Anzahl der bisher sequenzierten Viren kann es die Erkennungssysteme insensitiv für neue Pandemieerreger machen, wenn man sich auf bestehende Sequenzdatenbanken verlässt. Die oben genannten Methoden können eine Informationslücke bezüglich der genetischen Zusammensetzung eines Organismus offenlassen – ein kritischer Faktor für bioforensische Lösungen.

Genomik: Untersuchung der Gesamtheit aller Gene im Erbgut einer Zelle. Während sich die Genetik mit einzelnen Genen befasst, untersucht die Genomik das gesamte Genom (alle Gene eines Organismus) und wie es durch die Umwelt beeinflusst wird.

Sequenzbasierte Methoden

Next-Generation-Sequenzierung (NGS)

Mehrere Expert*innen sind der Ansicht, dass „Amerithrax“ (ein Wortgebilde aus „America“ und „Anthrax“, nach dem Namen des FBI-Falls⁴) eines der entscheidenden Ereignisse war, die zu einem erheblichen Anstieg der Forschungsmitteln für (Next-Generation-)Sequen-

Bioüberwachung

Aktive Sammlung von Daten der Biosphäre mit der Absicht, Frühwarnung vor gesundheitlichen Bedrohungen für Menschen und Tiere zu erhalten

- Entdeckung
- Mitigation
- Tracking

Bioforensik

Analyse biologischer Beweismittel im Zusammenhang mit Bioterrorismus, Biokriminalität oder der ungewollten Freisetzung eines ätiologischen Wirkstoffs, mit dem Zweck der Attribution

- Attribution
- Intention
- Mitigation

Klinische Anwendung

Analyse von klinischen Proben mit dem Ziel, die den Beschwerden eines Patienten zugrunde liegende Krankheit zu bestimmen

- Diagnose
- Behandlung
- Mitigation

Drei der wichtigsten Anwendungen von NGS bei biologischen Gefahren: Bioüberwachung (blau), Bioforensik (grün), klinischer Einsatz oder Diagnostik (lila) (Minogue et al., 2019).⁶

Next Generation Sequencing (NGS): Methode zur Analyse von genetischem Material, die eine schnelle Sequenzierung großer Mengen von DNA oder RNA ermöglicht. Siehe auch den Eintrag im Glossar, S. 98.

NGS-Bibliothek: Sammlung von DNA-Fragmenten, die mit einer bestimmten Sequenzierungsplattform kompatible Adaptersequenzen und Indizierungs-Barcodes zur Identifizierung einzelner Proben enthält.

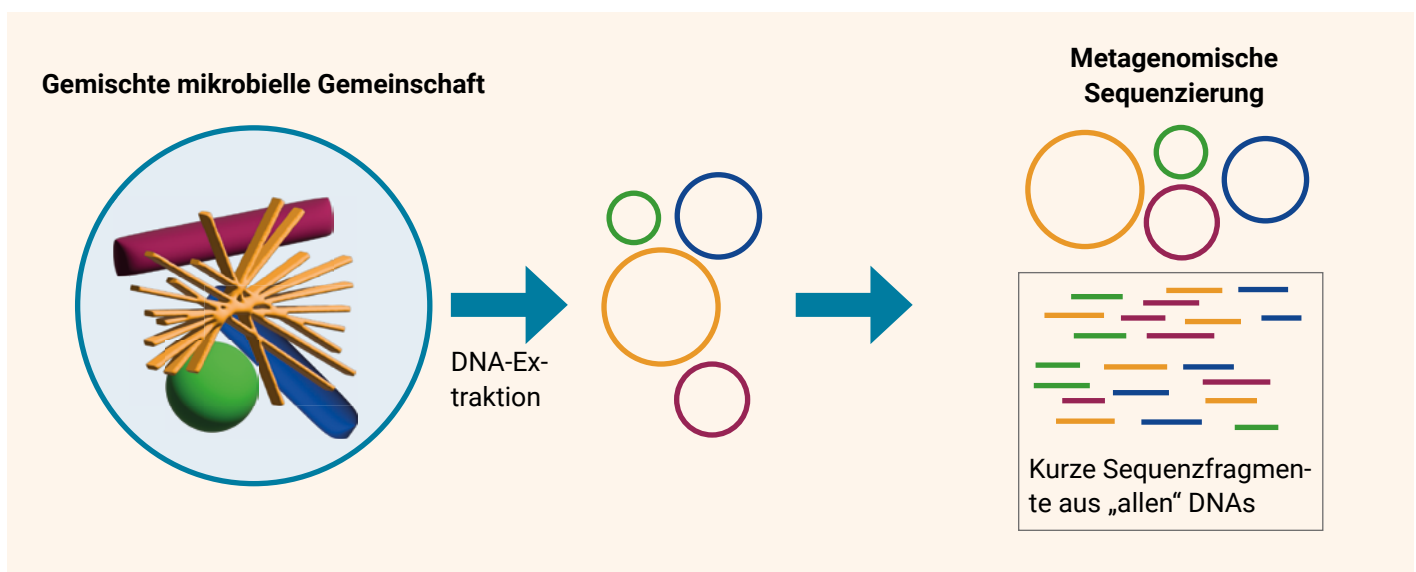
Shotgun-Sequenzierung: Methode, bei der DNA-Sequenzen nach dem Zufallsprinzip in viele kleine Teile zerlegt werden, die dann einzeln sequenziert und anschließend wieder zusammengesetzt werden, indem nach Überlappungsbereichen gesucht wird.

zierungsanwendungen führten.⁵ Bei „Amerithrax“ handelte es sich um die biologischen Anschläge nach dem 11. September 2001, bei denen Briefe mit Milzbrandsporen an mehrere Medienbüros und Regierungsangestellte verschickt wurden. In den Untersuchungen wurde die Next-Generation-Sequenzierung (NGS) zwar nicht direkt eingesetzt, aber die Forscher*innen verwendeten hochauflösende Ganzgenomsequenzierung (WGS) und vergleichende Genomik, um genetische Merkmale des *Bacillus anthracis*-Stammes aus den Briefen zu identifizieren. Durch die Möglichkeit, alle Nukleinsäuren in einer Probe für den Erregernachweis zu sequenzieren, sind keine Vorkenntnisse über den Erreger nötig, wie sie normalerweise für gezielte molekulare Tests (wie Echtzeit-PCR) erforderlich sind. Der Prozess beginnt mit der Extraktion der Genom-DNA aus der Probe. Diese DNA wird dann in eine NGS-Bibliothek umgewandelt, die anschließend sequenziert wird. Die sich daraus ergebenden Sequenzdaten werden mit bekannten Referenzsequenzen von Mikroorganismen verglichen, von denen angenommen wird, dass sie in der Probe vorkommen.

- Next-Generation-Sequenzierung (Next Generation Sequencing, NGS) umfasst mehrere Technologien, die zur Sequenzierung der Nukleotide in vollständigen Genomen oder in bestimmten DNA- oder RNA-Regionen eingesetzt werden.
- Die NGS-Plattformen bieten eine massiv parallele Sequenzierung, entweder von klonal amplifizierten oder einzelnen DNA-Molekülen.
- NGS sequenziert DNA durch wiederholte Zyklen von polymerasegesteuerten Nukleotidverlängerungen, wobei in einem einzigen Durchlauf Hunderte von Megabasen bis hin zu Gigabasen an Sequenzdaten erzeugt werden.
- Bei NGS-Experimenten werden riesige Datenmengen erzeugt, die eine Herausforderung für die Datenverarbeitung, -speicherung und vor allem für die Analyse darstellen.
- NGS hat die Erforschung der mikrobiellen Vielfalt sowohl in der Umwelt als auch in klinischen Umgebungen revolutioniert.

Metagenomische Sequenzierung

Bei der metagenomischen Sequenzierung werden *alle* mikrobiellen und Wirtsnukleinsäuren in einer Probe ohne vorherige Selektion (kulturunabhängig) sequenziert. Dies geschieht in der Regel mit der sogenannten Shotgun-Sequenzierungsmethode.⁷ Das Endziel der Metagenomik besteht darin, die mikrobielle Überwachung zu revolutionieren und Initiativen im Bereich der öffentlichen Gesundheit durch proaktives Screening auf Bedrohungen zu stärken.





Nach mehreren Runden der Fragmentierung und Sequenzierung ergeben sich mehrere überlappende Reads für die Ziel-DNA. Die überlappenden Enden der verschiedenen Reads werden verwendet, um sie zu einer kontinuierlichen Sequenz zusammenzusetzen.

- Das metagenomische NGS ist unvoreingenommen und daher erregernunabhängig. Es werden keine spezifischen Primer oder Sonden verwendet, so dass jeder Erreger nachgewiesen werden kann.
- Die überwiegende Mehrheit der sequenzierten Reads stammt aus dem menschlichen Wirt, was das Verfahren rechnerisch komplexer macht. Die Identifizierung von Krankheitserregern in diesen metagenomischen Bibliotheken wird zu einer schwierigen Aufgabe.

Sequenzierung von Abwässern

DNA- und RNA-Fragmente von Krankheitserregern (und anderen lebenden Organismen) werden immer wieder in Gewässern auf der ganzen Welt entdeckt. Neue Techniken ermöglichen es, sie zu identifizieren.⁹ So wurde beispielsweise SARS-CoV-2 einige Tage vor der Meldung der ersten klinischen Fälle im Abwasser nahegelegener Gemeinden nachgewiesen.¹⁰ Anhand der Abwassersequenzierung konnten auch Varianten des Virus nachgewiesen und identifiziert werden.¹¹

Dabei werden Proben vor der Abwasseraufbereitung entnommen und in Labors analysiert, um die Art und die Menge an Krankheitserregern in einer Gemeinde zu ermitteln. Next-Generation-Sequenzierung kann auch für diese Analyse eingesetzt werden und bietet Angeestellten im öffentlichen Gesundheitswesen eine schnelle und umfassende Methode, um Infektionen großflächig zu überwachen. Die Überwachung von Krankheitserregern ist eine regelmäßige Praxis im öffentlichen Gesundheitswesen, die in verschiedenen Einrichtungen wie Krankenhäusern, Wasseraufbereitungsanlagen und landwirtschaftlichen Betrieben durchgeführt wird, wobei der Schwerpunkt auf Umgebungen liegt, die als anfällig für potenzielle Krankheitsausbrüche erachtet werden. Der Hauptvorteil der Abwassersequenzierung zum Nachweis von Humanpathogenen besteht darin, dass die Privatsphäre gewahrt wird.¹² Zudem ermöglicht sie es, bekannte und neu auftretende Krankheitserreger zu beobachten sowie frühzeitig Risikominderungsstrategien für den Gesundheitsschutz von Menschen und Tieren anzuwenden.

Proteomik- und Lipidomik-Methoden

Die Proteomik hat das Verständnis der Virulenz, der Struktur und der Pathogenese von Krankheitserregern verbessert, was bei der Diagnose von Krankheiten und der Entwicklung von Impfstoffen hilft. Die Proteomik wurde eingesetzt, um bakterielle und virale Proteine zu untersuchen, die für die Übertragung von Krankheiten bei Menschen und Tieren verantwortlich sind – Membranproteine, Oberflächenproteine und sekretierte Proteine sind der Schlüssel zur Pathogenität. Diese Proteine, die verschiedene kritische Funktionen erfüllen, z. B. als Enzyme, Transporter und Rezeptoren, sind für den Ausbruch und das Fortschreiten von Krankheiten von entscheidender Bedeutung.

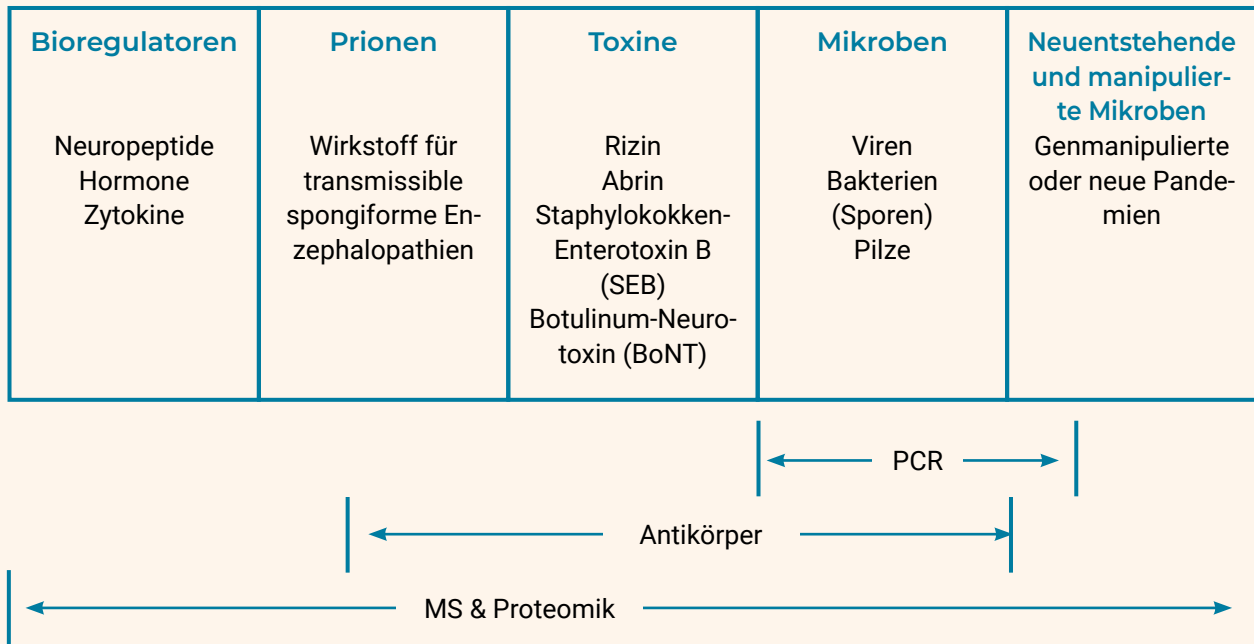
Die Analyse proteomischer Variationen in der Pathogenese von Bakterien und Viren ermöglicht es, verschiedene Stämmen hinsichtlich der Schwere der Infektion, der Auswirkungen auf die Umwelt und der Folgen genetischer Veränderungen zu vergleichen.

Die Massenspektrometrie (MS) ist der umfassendste Ansatz zur quantitativen Profilerkennung von Proteinen, ihren Wechselwirkungen und Veränderungen. Die Verfügbarkeit verschiedener Massenspektrometrie-Plattformen in Verbindung mit mikrobiellen Genomdatenbanken eröffnet neue Möglichkeiten.¹⁴ Die Fähigkeit der Massenspektrometrie, mehrere Analyten wie Luft, Wasser, Nährmedien, Körperflüssigkeiten und Lebensmittel

Proteomik: Untersuchung aller von der Zelle produzierten Proteine und ihrer Lage. Auf diese Weise kann eine 3D-Proteinkarte der Zelle erstellt werden, die Aufschluss über die Proteinregulation liefert.

Lipidomik: Untersuchung der Lipidzusammensetzung biologischer Proben. Siehe auch den Eintrag im Glossar, S. 97.

Massenspektrometrie (MS): ein analytisches Instrument zur Messung des Masse-Ladungs-Verhältnisses (das Verhältnis der Masse eines Ions zu seiner Ladung) eines oder mehrerer Moleküle in einer Probe. Siehe auch den Eintrag im Glossar, S. 98.



Klassen potenzieller biologischer Kampfstoffe (mit zunehmender Masse und Komplexität) und die wichtigsten Sensortypen für deren Nachweis und Identifizierung (Demirev & Fenselau, 2008).¹³

gleichzeitig in komplexen Matrizen zu analysieren, verschafft einen wesentlichen Vorteil dabei, biologische Bedrohungen zu erkennen und zu bekämpfen. MS-Technologien werden in Verbindung mit anderen Methoden auch häufig in der chemischen Forensik zu Ermittlungszwecken eingesetzt.

- MS ist sowohl schnell als auch sensitiv – ein typisches Experiment, einschließlich Probenentnahme und -vorbereitung, kann innerhalb von Minuten durchgeführt werden, während herkömmliche mikrobiologische oder toxikologische Tests Tage in Anspruch nehmen.
- Was die Sensitivität betrifft, so kann MS biologische Gefahren in Proben nachweisen, die eine geringe Menge intakter Organismen oder eines Toxins enthalten.

Beispiele für MS-Methoden zur Identifizierung von Mikroorganismen

1. Plattformen wie die Matrix-Assistierte Laser-Desorptions-Ionisations-Flugzeit-Massenspektrometrie (MALDI-TOF-MS) und die Flüssigchromatographie-Tandem-Massenspektrometrie (LC-MS/MS) werden zunehmend in der mikrobiologischen Forschung, insbesondere zu diagnostischen Zwecken, eingesetzt. Sie basieren auf Techniken des Massen-Fingerprintings oder der Peptidsequenzierung.¹⁵ Die U.S. Food and Drug Administration hat auch MALDI-TOF-MS-basierte Plattformen wie den MALDI Biotyper (MBT) zugelassen.¹⁶ Aufgrund der schnellen Analysezeit und der geringen Kosten für die Probenverarbeitung ist der MBT eine zuverlässige Option für die Identifizierung von Mikroorganismen. Indem es den einzigartigen proteomischen Fingerabdruck eines Organismus bestimmt, vergleicht MALDI-TOF MS diesen mit einer umfassenden und ständig aktualisierten Referenzbibliothek, um die Identität des Organismus genau zu bestimmen.
2. In einigen Fällen sollte eine mikrobielle Charakterisierung auf der Grundlage anderer Biomarker wie Lipide in Betracht gezogen werden.¹⁷ In diesem Zusammenhang eröffnen die Fortschritte bei einer anderen MS-Technologie – der Umgebungsionisations-Massenspektrometrie (AIMS) – neue Perspektiven für den schnellen und präzi-

Peptid-Massen-Fingerprinting (PMF)/Protein-Fingerprinting: ein analytisches Verfahren zur Bestimmung von Proteinen. Das Protein wird zunächst in kleinere Peptide gespalten, deren absolute Massen dann mit einem Massenspektrometer wie MALDI-TOF gemessen werden.



sen Echtzeitnachweis von Spuren neu auftkommender pathogener Mikroorganismen und Toxine. Diese Methode erfordert wenig oder keine Vorbereitung der Probe, was einen großen Vorteil darstellt.¹⁸ Die „Umgebungsionisierung“ ist eine Ionisierungsmethode, bei der Ionen in der Gasphase direkt in Freiluft erzeugt werden, wodurch eine chromatografische Trennung überflüssig wird und die vorherige Probenvorbereitung erheblich verringert wird.¹⁹ Dies ermöglicht eine nahezu sofortige Charakterisierung mikrobieller Spezies.

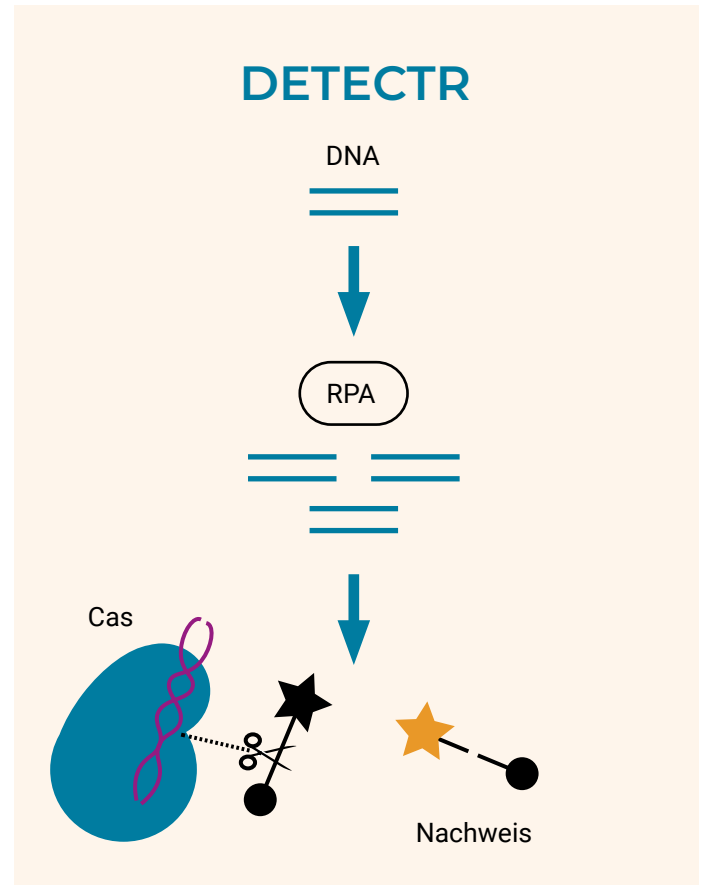
3. Unternehmen, die sich auf die biologische Abwehr und den Nachweis von Krankheitserregern spezialisiert haben, wie BioFlyte,²⁰ stellen tragbare Massenspektrometer für den Nachweis von Aerosolen her. Diese MS-Geräte können Substanzen in Aerosolen nachweisen, darunter Viren, Bakterien, Sporen, Opioiden und andere Stoffe. Zu den neusten Entwicklungen gehören Systeme zum Nachweis von Atemwegserregern in Innenräumen.

CRISPR-Cas-Systeme für die Diagnostik und den Nachweis von Krankheitserregern

Neben hochspezifischen Veränderungen menschlicher Gene können CRISPR-Systeme auch einen schnelleren und genaueren Nachweis von viralen und bakteriellen Nukleinsäuren bieten. Zwei analoge Diagnosesysteme, bekannt als DETECTR und SHERLOCK, wurden entwickelt, um RNA- bzw. DNA-Sequenzen nachzuweisen.²¹ Virale oder bakterielle RNA oder DNA wird amplifiziert und dann mit einem CRISPR/Cas-System gemischt, das die gewünschte Sequenz identifiziert und schneidet. Nach der Spaltung der Zielsequenzen beginnt das Cas-Protein, alle anderen DNAs oder RNAs in der Lösung zu spalten. Wenn also eine Reportersequenz eingeführt wird, deren Fluoreszenzsignal durch ein anderes Molekül unterdrückt wird, spaltet Cas auch diesen Komplex und erzeugt ein Fluoreszenzsignal, das gemessen werden kann.

Beispielsweise entwickelt Mammoth Biosciences²² Diagnostika, Therapeutika und Proteinforschung auf der Grundlage der CRISPR-Technologie, die hohe Genauigkeit, Vielseitigkeit (Pathogen-Agnostizismus) und einfache Anwendung verspricht.²³ CRISPR-Cas-Proteine gelten aufgrund ihrer Schnelligkeit und Genauigkeit als ideale Werkzeuge für den Nachweis von Nukleinsäuren, da sie eine Leit-RNA (gRNA) verwenden, um DNA- oder RNA-Sequenzen auf natürliche Weise zu adressieren. Gewünschte Genome können durch einfache Veränderung der gRNA-Zielregion anvisiert werden, wie die schnelle Anpassung der CRISPR-basierten Diagnostik während der COVID-19-Pandemie gezeigt hat.²⁴

Zur Erläuterung von CRISPR, siehe den Eintrag im Glossar, S. 96.



DETECTR – DNA Endonuclease Targeted CRISPR Trans Reporter. Abbildung übernommen aus Cecchetelli, 2020.²⁵

Mikrobielle Forensik und Attribution von Gentechnik

Motivation für mikrobielle Forensik

Obwohl Mikroben schon seit Jahrhunderten als Waffen eingesetzt werden, lösten die Milzbrandanschläge in den USA im Jahr 2001 in der Öffentlichkeit große Angst aus.²⁶ Diese Ereignisse machten deutlich, dass eine Infrastruktur von Analyseinstrumenten und Wissensgrundlagen benötigt wird, die zügig Hinweise für die Ermittlungen liefert, die Identifizierung von Verantwortlichen (Attribution) unterstützt, Aufschluss über die Quelle des Erregers gibt und Details darüber aufdeckt, wie und wo die Waffe hergestellt wurde. Die mikrobielle Forensik hatte sich zwar bereits vor den 2000er Jahren als wissenschaftliches Gebiet entwickelt, erfuhr jedoch durch die Amerithrax-Ereignisse einen enormen Aufschwung. Dieser Zweig der forensischen Wissenschaft befasst sich mit der Untersuchung von Beweismaterial, das aus bioterroristischen Anschlägen, biologischen Verbrechen oder der unbeabsichtigten Freisetzung von Mikroorganismen oder Giftstoffen stammt, um deren Ursprung zu ermitteln. Der Schwerpunkt dabei liegt darauf, die Herkunft von Krankheitserregern zurückzuverfolgen, um die Strafverfolgung der für ihre Verbreitung verantwortlichen Personen zu unterstützen. Ziel ist es, eine Probe unklarer Herkunft mit größtmöglicher wissenschaftlicher Gewissheit einer oder mehreren bekannten Quellen genau zuzuordnen und gleichzeitig andere Quellen auszuschließen. Die globale COVID-19-Pandemie und die Ungewissheit über die Herkunft des Virus unterstreichen sowohl die Dringlichkeit als auch die potenziellen geopolitischen Auswirkungen dieser Technologien. Biologische Ereignisse zu untersuchen und einer Quelle zuzuordnen stellt eine Herausforderung dar, und selbst vier Jahre nach der COVID-19-Pandemie sind sich die US-Geheimdienste über den Ursprung des Virus nicht einig.

Gentechnische Attribution

Das Risiko, dass die Biologie missbraucht wird und weitreichende Schäden verursacht, steigt mit dem rasanten technologischen Fortschritt. Dies wiederum erschwert die Herausforderung der Attribution – der Feststellung, ob der verursachende Organismus gentechnisch verändert wurde, und falls ja, der Identifizierung der Verantwortlichen. Die Attribution kann drei wesentliche Vorteile für die Sicherheit bringen. Erstens hilft die Kenntnis der verantwortlichen Personen, ihrer Motive und Fähigkeiten, die Reaktionsmaßnahmen zu justieren. Zweitens ermöglicht Attribution, die verantwortlichen Parteien zu identifizieren, so dass angemessene zivil-, strafrechtliche oder diplomatische Sanktionen angewendet werden können. Drittens wirkt eine wirksame Attribution in Verbindung mit entschlossenen Maßnahmen, um die Verantwortlichen zur Rechenschaft zu ziehen, als Abschreckung gegen rücksichtsloses oder schädliches Verhalten.²⁷ Das Risiko erhöht sich für diejenigen, die an illegalen Biowaffen-, Bioterrorismus- oder Bioproliferationsaktivitäten beteiligt sind, wenn sie gefasst und zur Rechenschaft gezogen werden oder wenn die realistische Aussicht darauf besteht.

Einzelnukleotid-Polymorphismus (Single nucleotide polymorphism, SNP): Eine Variation auf einer einzelnen Nukleotidposition in einer DNA-Sequenz, die zwischen verschiedenen Organismen auftritt.

In der mikrobiellen Forensik wird, wann immer dies möglich ist, eine detaillierte Identifizierung des mikrobiellen Erregers bis auf Substammbene (ein Stamm, der von dem charakterisierten Stamm abstammt, sich aber von ihm unterscheidet) angestrebt. Im Labor vorgenommene Veränderungen an Mikroorganismen, wie Klonierung und gentechnische Veränderung, hinterlassen nachweisbare Spuren in ihren Genomen.²⁸ Diese genetischen Marker dienen zusammen mit beobachtbaren Merkmalen als Beweis dafür, dass gefährliche Erreger absichtlich erzeugt und verbreitet wurden, um Schäden anzurichten. Ein Merkmal in mikrobieller DNA, das für die Analyse der molekularen Phylogenie nützlich ist, sind Einzelnukleotid-Polymorphismen (SNPs). SNPs sind als



genetische Marker sehr stabil und informativ für Stammbaumstudien, obwohl sie für die Identifizierung einzelner Isolate nur eine geringe Aussagekraft haben.

In einem Genom können sich verräterische Spuren gentechnischer Veränderung auf verschiedene Weise manifestieren. Der Entscheidungsprozess des Genforschers wird von verschiedenen Faktoren beeinflusst, wie z. B. der Ausbildung, früheren Erfahrungen, etablierten Praktiken und der Verfügbarkeit von Ressourcen. Diese gesammelten Entscheidungen bilden eine unverwechselbare „methodische Signatur“, die es ermöglicht, die Design-Entscheidungen auf den wahrscheinlichen Designer zurückzuführen. Dies kann das Vorhandensein fremden genetischen Materials in einer bestimmten Sequenz ebenso einschließen wie das unerwartete Auftauchen etwa von Verdopplungen, Einfügungen (Insertionen) oder Streichungen (Deletionen) von Basen. Darüber hinaus können Sequenzen, die für Antibiotikaresistenzen kodieren, und kurze Abschnitte, die als „Narben“ bekannt sind und auf Veränderungen der DNA-Sequenz hinweisen, als Hinweise für die Entdeckung von Manipulationen dienen. Obwohl es keine endgültige Liste aller „Engineering-Sequenzen“ gibt, bieten Plattformen wie Addgene²⁹ umfangreiche Datenbanken mit molekularen Werkzeugen, die für DNA-Manipulationen im Labor genutzt werden. Der Addgene-Datensatz, ein umfassendes und sorgfältig kuratiertes Repositorium von Plasmidsequenzen zusammen mit Informationen zu den Autor*innen, dient als vereinfachte Darstellung der Gentechnik-Attribution (*Genetic Engineering Attribution*, GEA). Während dieser Datensatz für die Weiterentwicklung der GEA-Methoden unverzichtbar war, müssen praktische Attributionsmodelle letztlich über diesen ursprünglichen Rahmen hinausgehen und ein breiteres Spektrum von Szenarien abdecken.

Design-Entscheidungen bilden eine „methodische Signatur“, mit der sich Aussagen darüber treffen lassen, wer wahrscheinlich für eine gentechnische Veränderung verantwortlich ist.

Einige Expert*innen haben die Befürchtung geäußert, dass das Wissen über die gentechnische Attribution die politische Komplexität erhöhen könnte, da ein böswilliger Akteur absichtlich gentechnische Merkmale auswählen könnte, um ein anderes Labor oder ein anderes Land fälschlich zu belasten. Darüber hinaus könnte der Grad an Vertrauen, der erforderlich ist, um ein bestimmtes Labor als Täter zu benennen, komplexe diplomatische Entscheidungen beinhalten.

Auch wenn die GEA-Methoden noch in den Kinderschuhen stecken und die Attribution eine komplexe Aufgabe bleibt, könnten sie dennoch eine wissenschaftliche Grundlage für die BWÜ-Diskussionen zu Verifikation und Compliance bieten.

Dr. Kadri Reis

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

- 1 Filipiak, W., Ager, C., & Troppmair, J. (2017). Predicting the future from the past: Volatile markers for respiratory infections. *European Respiratory Journal*, 49(5), 1700264. <https://doi.org/10.1183/13993003.00264-2017>
- 2 Kreitmann, L., Miglietta, L., Xu, K., Malpartida-Cardenas, K., D'Souza, G., Kaforou, M., Brengel-Pesce, K., Drazek, L., Holmes, A., & Rodriguez-Manzano, J. (2023). Next-generation molecular diagnostics: Leveraging digital technologies to enhance multiplexing in real-time PCR. *TrAC Trends in Analytical Chemistry*, 160, 116963. <https://doi.org/10.1016/j.trac.2023.116963>
- 3 Dung, T. T. N., Phat, V. V., Vinh, C., Lan, N. P. H., Phuong, N. L. N., Ngan, L. T. Q., Thwaites, G., Thwaites, L., Rabaa, M., Nguyen, A. T. K., & Duy, P. T. (2024, 7. Februar). Development and validation of multiplex real-time PCR for simultaneous detection of six bacterial pathogens causing lower respiratory tract infections and antimicrobial resistance genes. *BMC Infectious Diseases*, 24(1), 164. <https://doi.org/10.1186/s12879-024-09028-2>
- 4 The United States Department of Justice. (2010, 19. Februar). *Amerithrax Investigative Summary*. The United States Department of Justice. <https://www.justice.gov/archive/amerithrax/docs/amx-investigative-summary.pdf>
- 5 Rasko, D. A., Worsham, P. L., Abshire, T. G., Stanley, S. T., Bannan, J. D., Wilson, M. R., Langham, R. J., Decker, R. S., Jiang, L., Read, T. D., Phillippy, A. M., Salzberg, S. L., Pop, M., Van Ert, M. N., Kenefic, L. J., Keim, P. S., Fraser-Liggett, C. M., & Ravel, J. (2011, 7.

- März). *Bacillus anthracis* comparative genome analysis in support of the Amerithrax investigation. *Proceedings of the National Academy of Sciences*, 108(12), 5027–5032. <https://doi.org/10.1073/pnas.1016657108>
- 6 Minogue, T. D., Koehler, J. W., Stefan, C. P., & Conrad, T. A. (2019, 1. März). Next-Generation Sequencing for Biodefense: Biothreat Detection, Forensics, and the Clinic. *Clinical Chemistry*, 65(3), 383–392. <https://doi.org/10.1373/clinchem.2016.266536>
 - 7 Quince, C., Walker, A. W., Simpson, J. T., Loman, N. J., & Segata, N. (2017, 12. September). Shotgun metagenomics, from sampling to analysis. *Nature Biotechnology*, 35(9), 833–844. <https://doi.org/10.1038/nbt.3935>
 - 8 Lee, M. (2019, 29. September). Happy Belly Bioinformatics: An open-source resource dedicated to helping biologists utilize bioinformatics. *Journal of Open Source Education*, 2(19), 53. <https://doi.org/10.21105/jose.000539>
 - 9 The Nucleic Acid Observatory Consortium. (2021). *A Global Nucleic Acid Observatory for Biodefense and Planetary Health (arXiv:2108.02678)*. arXiv. <https://doi.org/10.48550/ARXIV.2108.02678>
 - 10 Peccia, J., Zulli, A., Brackney, D. E., Grubaugh, N. D., Kaplan, E. H., Casanovas-Massana, A., Ko, A. I., Malik, A. A., Wang, D., Wang, M., Warren, J. L., Weinberger, D. M., Arnold, W., & Omer, S. B. (2020, 18. September). Measurement of SARS-CoV-2 RNA in wastewater tracks community infection dynamics. *Nature Biotechnology*, 38(10), 1164–1167. <https://doi.org/10.1038/s41587-020-0684-z>
 - 11 Crits-Christoph, A., Kantor, R. S., Olm, M. R., Whitney, O. N., Al-Shayeb, B., Lou, Y. C., Flamholz, A., Kennedy, L. C., Greenwald, H., Hinkle, A., Hetzel, J., Spitzer, S., Koble, J., Tan, A., Hyde, F., Schroth, G., Kuersten, S., Banfield, J. F., & Nelson, K. L. (2021, 19. Januar). Genome Sequencing of Sewage Detects Regionally Prevalent SARS-CoV-2 Variants. *mBio*, 12(1), e02703-20. <https://doi.org/10.1128/mBio.02703-20>
Pérez-Cataluña, A., Chiner-Oms, Á., Cuevas-Ferrando, E., Díaz-Reolid, A., Falcó, I., Randazzo, W., Girón-Guzmán, I., Allende, A., Bracho, M. A., Comas, I., & Sánchez, G. (2021, 10. Februar). *Detection Of Genomic Variants Of SARS-CoV-2 Circulating In Wastewater By High-Throughput Sequencing*. medRxiv. <https://doi.org/10.1101/2021.02.08.21251355>
 - 12 The Nucleic Acid Observatory Consortium, 2021.
 - 13 Demirev, P. A., & Fenselau, C. (2008). Mass spectrometry in biodefense. *Journal of Mass Spectrometry*, 43(11), 1441–1457. <https://doi.org/10.1002/jms.1474>
 - 14 Drake, R. R., Deng, Y., Schwegler, E. E., & Gravenstein, S. (2005). Proteomics for biodefense applications: Progress and opportunities. *Expert Review of Proteomics*, 2(2), 203–213. <https://doi.org/10.1586/14789450.2.2.203>
 - 15 Rajoria, S., Sabna, S., Babel, P., Kumar, R. B., Kamboj, D. V., Kumar, S., & Alam, S. I. (2020, 10. Februar). Elucidation of protein biomarkers for verification of selected biological warfare agents using tandem mass spectrometry. *Scientific Reports*, 10(1), 2205. <https://doi.org/10.1038/s41598-020-59156-3>
 - 16 Bruker. (2024). *MALDI Biotyper (MBT)*. <https://www.bruker.com/en/products-and-solutions/microbiology-and-diagnostics/microbial-identification.html>
 - 17 Su, H., Jiang, Z.-H., Chiou, S.-F., Shiea, J., Wu, D.-C., Tseng, S.-P., Jain, S.-H., Chang, C.-Y., & Lu, P.-L. (2022, 26. April). Rapid Characterization of Bacterial Lipids with Ambient Ionization Mass Spectrometry for Species Differentiation. *Molecules*, 27(9), 2772. <https://doi.org/10.3390/molecules27092772>
 - 18 Ferreira, C. R., Yannell, K. E., Jarmusch, A. K., Pirro, V., Ouyang, Z., & Cooks, R. G. (2016, 1. Januar). Ambient Ionization Mass Spectrometry for Point-of-Care Diagnostics and Other Clinical Measurements. *Clinical Chemistry*, 62(1), 99–110. <https://doi.org/10.1373/clinchem.2014.237164>
 - 19 Venter, A., Neffliu, M., & Graham Cooks, R. (2008). Ambient desorption ionization mass spectrometry. *TrAC Trends in Analytical Chemistry*, 27(4), 284–290. <https://doi.org/10.1016/j.trac.2008.01.010>
 - 20 Bioflyte. (2024). *BioFlyte – Biosecurity at Scale*. <https://www.bioflyte.com/>
 - 21 Für eine Zusammenfassung siehe: Kocak, D. D. & Gersbach, C. A. (2018). From CRISPR scissors to virus sensors. *Nature*, 557, 168–169. <https://doi.org/10.1038/d41586-018-04975-8>
 - 22 Mammoth Biosciences. (2024). *Mammoth Biosciences*. <https://mammoth.bio/>
 - 23 Verosloff, M. S., Shapiro, S. J., Hawkins, E. M., Alpay, E., Verma, D., Stanfield, E. G., Kreindler, L., Jain, S., McKay, B., Hubbell, S. A., Hendriks, C. G., Blizard, B. A., Broughton, J. P., & Chen, J. S. (2022). CRISPR-Cas enzymes: The toolkit revolutionizing diagnostics. *Biotechnology Journal*, 17(7), 2100304. <https://doi.org/10.1002/biot.202100304>
 - 24 Broughton, J. P., Deng, X., Yu, G., Fasching, C. L., Servellita, V., Singh, J., Miao, X., Streithorst, J. A., Granados, A., Sotomayor-Gonzalez, A., Zorn, K., Gopez, A., Hsu, E., Gu, W., Miller, S., Pan, C.-Y., Guevara, H., Wadford, D. A., Chen, J. S., & Chiu, C. Y. (2020, 16. April). CRISPR-Cas12-based detection of SARS-CoV-2. *Nature Biotechnology*, 38(7), 870–874. <https://doi.org/10.1038/s41587-020-0513-4>
 - 25 Cecchetelli, A. (2020, 16. April). Finding nucleic acids with SHERLOCK and DETECTR. *Addgene*. <https://blog.addgene.org/finding-nucleic-acids-with-sherlock-and-detectr>
 - 26 Centers for Disease Control and Prevention Animal and Plant Health Inspection Service. (2020, 10. September). *Bioterrorism: A Brief History*. <https://www.selectagents.gov/overview/history.htm>



- 27 Lewis, G., Jordan, J. L., Relman, D. A., Koblenz, G. D., Leung, J., Dafoe, A., Nelson, C., Epstein, G. L., Katz, R., Montague, M., Alley, E. C., Filone, C. M., Luby, S., Church, G. M., Millett, P., Esvelt, K. M., Cameron, E. E., & Inglesby, T. V. (2020, 8. Dezember). The biosecurity benefits of genetic engineering attribution. *Nature Communications*, 11(1), 6294. <https://doi.org/10.1038/s41467-020-19149-2>
- 28 Alley, E. C., Turpin, M., Liu, A. B., Kulp-McDowall, T., Swett, J., Edison, R., Von Stetina, S. E., Church, G. M., & Esvelt, K. M. (2020). A machine learning toolkit for genetic engineering attribution to facilitate biosecurity. *Nature Communications*, 11(1), 6293. <https://doi.org/10.1038/s41467-020-19612-0>
- 29 Kamens, J. (2015, 28. Januar). The Addgene repository: An international nonprofit plasmid and data resource. *Nucleic Acids Research*, 43(D1), D1152–D1157. <https://doi.org/10.1093/nar/gku893>

ANALYSEN

Emerging Disruptive Technologies

Neue Militärtechnologien in nationalen Sicherheitsstrategien – eine vergleichende Analyse

Wie betrachten Staaten Technologie im sicherheitspolitischen Kontext? Ein Vergleich der Analysen nationaler Sicherheitsstrategien (NSS) von zwölf Staaten zwischen 2017 und 2023 zeigt, dass unterschiedliche Ansätze bestehen, wie Sicherheit und Technologie wahrgenommen werden. Es gibt sowohl Konsens als auch Unterschiede bei relevanten Technologien, und es existieren Gruppen „gleichgesinnter“ Staaten. NSS neigen dazu, Sicherheit umfassend zu betrachten, weshalb Dual-Use-Technologien, insbesondere im Cyberbereich, KI oder Netzwerktechnologien, im Fokus stehen – entweder als militärische Ressourcen oder als Bedrohungen. Dies stellt die Rüstungskontrolle vor erhebliche Herausforderungen.

Die Diskussion über den Einfluss und die Bedeutung neuer Militärtechnologien für die (künftige) Kriegsführung und die globale Stabilität hat in den letzten zehn Jahren erheblich an Dynamik gewonnen, gerade im Zusammenhang mit den laufenden Kriegen gegen die Ukraine und im Gaza-Streifen. Insbesondere KI-gestützte Systeme für die Entscheidungsfindung und unbemannte Fahrzeuge werden in allen militärischen Bereichen getestet und in vielen Fällen in Operationen auf aktuellen Kriegsschauplätzen integriert. Dabei konzentrieren sich die Diskussionen dazu auf die Frage nach dem Potenzial dieser Technologien, nationale und internationale Sicherheit erheblich zu beeinflussen: Gleichzeitig gilt es, künftige, möglicherweise bahnbrechende Entwicklungen nicht zu verpassen und einen entsprechend breiten Blick einzunehmen. Diese Notwendigkeit und Dringlichkeit ergibt sich aus der janusköpfigen Natur bestimmter moderner Technologien, die sowohl als Chance als auch als Bedrohung wahrgenommen werden können – und die Reaktionen auf beide Aspekte werden als zeitkritisch empfunden. Einerseits bieten die neuen Technologien die Chance, durch rasche Innovation eine führende Rolle im globalen Wettbewerb einzunehmen und dadurch mehr strategische Autonomie, technologische Unabhängigkeit und militärische Macht zu erlangen – ganz zu schweigen von den zivilen Geschäftsmöglichkeiten. Andererseits sind neue Technologien oft mit sicherheitspolitischen Bedrohungswahrnehmungen verbunden, deren Relevanz und Bedeutung ex ante nur schwer einzuschätzen ist und auf die man im Zweifel vorbereitet sein muss.

In der polnischen Nationalen Sicherheitsstrategie wird zum Beispiel argumentiert:

„Die Entwicklung von Lösungen, die auf Festnetz- und mobilem Breitband (5G und nachfolgende Generationen), dem Internet der Dinge, Cloud Computing, Quantentechnologien, der Automatisierung von Dienstleistungen, maschinellem Lernen, Na-

notechnologie und künstlicher Intelligenz basieren, schafft **neue Entwicklungsmöglichkeiten** für Polen, **bringt aber auch bisher unbekannte Bedrohungen mit sich.**^{“1}

In diesem Zusammenhang ist bedeutsam, dass viele der Technologien, die derzeit als besonders wichtig für die nationale Sicherheit angesehen werden, im Kern *Dual-Use-Technologien* sind und damit sowohl für militärische als auch für zivile Zwecke genutzt werden können. Darüber hinaus sind, wie das obige Zitat zeigt, viele Technologien zuallererst zivile Technologien, die im zivilen Sektor entwickelt oder weiterentwickelt wurden. Dies ist ein wesentlicher Unterschied zwischen der Gegenwart und der Zeit des Kalten Krieges, als die Verteidigungsindustrie wesentlich innovativer war und der weit häufigere Fall war, dass Militärtechnologie in den zivilen Sektor übergang.

Einzelne Länder haben unterschiedliche Vorstellungen davon, welche Technologien in naher oder ferner Zukunft für die Lösung ihrer Sicherheitsprobleme von Bedeutung sein könnten. Im Folgenden erörtern wir die Ergebnisse einer ersten qualitativen Inhaltsanalyse von 19 nationalen Sicherheitsstrategien aus zwölf Ländern, die zwischen 2016 und 2023 veröffentlicht wurden, und zeigen auf, wo Konsens besteht und wo sich die Staaten unterscheiden – sowohl in ihrem Verständnis von Sicherheit als auch in den Technologien, die sie als wichtig erachten. Dies wird nicht nur Staaten dabei helfen, „gleichgesinnte“ Staaten zu finden, mit denen sie zusammenarbeiten können, sondern auch neue Militärtechnologien und technologische Entwicklungen aufzeigen, die noch nicht auf dem Radar oder im blinden Fleck einiger der untersuchten Staaten sind. Schließlich gibt die Analyse Aufschluss darüber, wo technologische Dynamiken angesiedelt sind. Während einige Entwicklungen genuin militärisch sind, beziehen sich andere auf Dual-Use-Technologien. Gerade die Regulierung von Dual-Use-Gütern wirft besondere und meist komplexe Probleme auf, weil es zivilen Druck zur Nutzung und zum Export gibt. Immerhin ist eine Beschränkung über Rüstungskontrollabkommen bzw. Exportkontrollabkommen zumindest prinzipiell möglich.

Die Relevanz neuer Militärtechnologien

Es ist umstritten, ob neue Militärtechnologien tatsächlich einen signifikanten Einfluss auf das Kampfgeschehen von heute und morgen haben und in welchem Umfang sie die nationale Sicherheit verbessern oder gefährden. Technologieenthusiasten verweisen in der Regel auf die aktuellen Entwicklungen auf den Kriegsschauplätzen in der Ukraine oder im Gazastreifen und argumentieren beispielsweise, dass bestimmte Arten von Drohnen die aktuelle Kriegsführung entscheidend verändert haben. Kritische Stimmen dagegen weisen darauf hin, dass Technologie allein noch nie ein entscheidender Faktor war und dass andere relevante Faktoren wie Strategie, Taktik, militärische Institutionen, Ausbildung oder Kultur – um nur einige zu nennen – die Relevanz der Auswirkungen von Technologie beeinflussen. Darüber hinaus haben einige Staaten eine sehr weit gefasste Definition von nationaler Sicherheit und betrachten auch Technologien, die zumindest auf dem Schlachtfeld nur eine begrenzte militärische Relevanz haben, während andere ein engeres Konzept sowohl in ihrem Verständnis von nationaler Sicherheit als auch im Hinblick auf relevante Technologien haben.

In aktuellen Debatten hat der Begriff „*emerging disruptive technologies*“ (EDTs), also neu auftretende und disruptive Technologien, in Bezug auf die nationale Sicherheit eine gewisse Zugkraft gewonnen – insbesondere bei militärischen und politischen Entscheidungsträger*innen. Das Konzept ist jedoch nicht unproblematisch, da noch immer unklar ist, welche Technologien im militärischen Bereich als „neu“ verstanden werden können, und es hierfür an Konsens mangelt. Die Europäische Verteidigungsagentur (EDA) zum Beispiel nennt sechs,² die NATO neun.^{3,4}

Für eine weiterführende Diskussion siehe das Kapitel von Niklas Schörnig ab S. 22.

Europäische Verteidigungsagentur (EDA)	NATO
Künstliche Intelligenz (KI)	Künstliche Intelligenz (KI)
Big Data	Autonome Systeme
Robotik und autonome Systeme	Quantentechnologien
Weltraum- und Hyperschallsysteme	Biotechnologie und <i>Human enhancement technology</i>
Neue fortschrittliche Materialien (<i>new advanced materials</i>)	Weltraum-Technologie
Quantentechnologien	Hyperschallsysteme
	Neue Materialien und Fertigungsenergie und Antrieb
	Kommunikationsnetze der nächsten Generation

Allen diesen Technologien ist jedoch gemeinsam, dass sie von vielen als „*disruptiv*“ angesehen werden, da ihnen ein großer Einfluss auf militärische Ereignisse zugeschrieben wird „die Kriegsführung potenziell zu revolutionieren“⁵ oder, wie die EDA es ausdrückt, „die Regeln oder die Art der Kriegsführung innerhalb von ein oder zwei Generationen erheblich [zu verändern]“.⁶ Das impliziert, dass diese Technologien das Potenzial hätten, die bestehenden Machtverhältnisse sowohl regional als auch global dramatisch zu verändern – sofern die Einsatzdoktrinen entsprechend angepasst werden und andere relevante Faktoren stabil bleiben. Umgekehrt ist die Ungewissheit, ob und inwieweit sich ein solcher Einfluss tatsächlich einstellen wird, ein wesentlicher Faktor für die Disruptivität von Technologien. Als „neu“ und „disruptiv“ werden daher oft Technologien angesehen, die weniger in militärische Operationen integriert sind, die neu und noch nicht ausgereift sind und/oder noch nie in einem Konflikt eingesetzt oder getestet wurden. Über deren faktische Auswirkungen auf die künftige Praxis der Kriegsführung kann in vielen Fällen nur spekuliert werden. Die bloße Befürchtung, dass sich eine Technologie auf dem Schlachtfeld als disruptiv erweisen könnte, kann in einigen Fällen eine massive Triebkraft sein, während in anderen Fällen ein Mangel an Vorstellungskraft und technischem Weitblick die Entwicklungsmöglichkeiten beeinträchtigt oder gänzlich verhindert.

Andererseits wird nicht jede Technologie, in die ein Staat militärisch investieren möchte, als eine dieser EDTs betrachtet. In manchen Fällen streben Staaten nach der Weiterentwicklung bestehender Technologien, z. B. nach Kampfflugzeugen der nächsten Generation, um die Luftüberlegenheit zu wahren, oder modernisierten Versionen von Kampfpanzern mit größerer Reichweite, mehr Durchschlagskraft oder besserem Schutz. Gründe dafür könnten entweder sein, dass gradueller technologische Fortschritt das Potenzial hat, bestehende militärische Fähigkeiten zu verbessern und zu erhalten, oder dass die Fusion von Technologien – z. B. die Einbindung von KI in bestehende Systeme – die militärische Macht erhöht. Entwicklung und Besitz moderner Militärtechnologien erfüllen daher mehrere wichtige Funktionen: die eigenen militärischen Fähigkeiten zu verbessern und Stärke in der internationalen Politik zu signalisieren, die eigenen Soldat*innen besonders effektiv zu schützen – oder sogar auf Status und Prestige abzu zielen,⁷ performative Funktionen zu erfüllen, die mit der Erwartung der besagten unklaren, aber potenziell großen zukünftigen Bedeutung verbunden sind. Letztlich gibt es auch wirtschaftliche Auswirkungen, insbesondere wenn es sich bei der betreffenden Technologie um eine Dual-Use-Technologie mit signifikanten zivilen Anwendungen handelt.

Einige Worte zur Methodik

Mit der Inhaltsanalyse von Nationalen Sicherheitsstrategien (NSS) wollen wir einen Überblick über Technologien gewinnen, die für Regierungen relevant sind, um ihre jeweilige nationale Sicherheit zu fördern und aufrechtzuerhalten. Auch wenn sich Sicherheitskonzepte von Staat zu Staat unterscheiden, hilft die Analyse nicht nur, unterschiedliche technologische Präferenzen zwischen Staaten zu beschreiben, sondern auch die Entwicklung der Position eines bestimmten Staates gegenüber bestimmten Technologien im Laufe der Zeit sicht-

bar zu machen. In diesem Text beschränken wir die Analyse jedoch auf eine Querschnittsstudie. Mit einer Langzeituntersuchung werden wir uns in zukünftigen Studien detaillierter befassen. Daher präsentieren die folgenden Abschnitte die Ergebnisse einer ersten Analyse der zwischen 2016 und 2023 veröffentlichten NSS von zwölf ausgewählten Ländern, um die folgenden Fragen zu beantworten: Welche spezifischen Technologien werden als strategisch relevant erachtet, um zur Sicherheit, entsprechend dem nationalen Sicherheitsverständnis, beizutragen? Die untersuchten Länder waren: Belgien, Frankreich, Deutschland, Japan, die Niederlande, Pakistan, Polen, Russland, Spanien, Südkorea, Großbritannien und die Vereinigten Staaten.⁸ Insgesamt wurden 19 Dokumente analysiert. Die Auswahl erfolgte mit dem Ziel, eine möglichst vielfältige Stichprobe zu erhalten, gleichzeitig mussten die untersuchten Dokumente aber auch auf Englisch (oder einer vom Team kodierbaren Sprache) verfügbar sein, weshalb beispielsweise China nicht berücksichtigt wurde.

Die Analyse basiert auf einem detaillierten Kodierschema, das zunächst deduktiv erstellt und dann während mehrerer Runden der Testkodierung induktiv erweitert wurde. Daraus ergaben sich 18 übergeordnete Technologiekategorien mit insgesamt 159 Unterkategorien, die die Breite der Innovation und Forschung erfassen. Diese 18 Kategorien decken offensichtlich mehr ab als die oben aufgeführten sechs bzw. neun Kategorien, und einige der Kategorien stellen eher evolutionäre Entwicklungen bestehender Technologien als neu aufkommende disruptive Technologien dar. Wir haben diese evolutionären Technologien jedoch einbezogen, um ein besseres Bild der technologischen Präferenzen der Länder zu erhalten.

Verschiedene Länder, verschiedene technologische Präferenzen

Dieser Abschnitt enthält eine kurze Analyse für die ausgewählten Länder, welche Technologien als strategisch relevant betrachtet werden und wie die einzelnen Staaten diese Technologien im Rahmen ihrer nationalen Sicherheitsstrategien priorisieren.

Eindrücke aus Belgien

Die erste und bisher einzige nationale Sicherheitsstrategie Belgiens, veröffentlicht 2021, positioniert das Land im Herzen der EU, als eine demokratische Gesellschaft, die eine breite internationale Zusammenarbeit anstrebt, um Sicherheit zu gewährleisten. Die Strategie stützt sich auf Werte und Grundsätze, deren Schutz die belgische Regierung als Teil des Sicherheitsverständnisses des Landes darstellt und die gleichzeitig die Maßnahmen zur Erreichung dieser Sicherheit bestimmen. Ausgehend von einer Analyse der globalen politischen Trends und Entwicklungen zeigt die belgische NSS zehn Bedrohungen für ihre nationale Sicherheitsstrategie auf. Diese Bedrohungen betreffen die Wirtschaft, ihre Prosperität und ihre Bedeutung für die Demokratie, angesichts von zunehmendem Extremismus und Radikalisierung sowie neuen Verwundbarkeiten aufgrund der Abhängigkeiten von lebenswichtigen Infrastrukturen. Die Strategie weist ferner auf eine Krise hin, die sich aus einem Rückgang der internationalen Zusammenarbeit und des normativen Zusammenhalts ergibt, die die Bedrohungen und negativen Auswirkungen von globalen Gesundheitsereignissen, Naturkatastrophen und Klimawandel verstärkt. Was die „harte Sicherheit“ betrifft, so ist sich der belgische Staat der Zunahme hybrider und konventioneller Konflikte in der Nähe der europäischen Grenzen, aber auch in Südost- und Ostasien, und der Folgen für die NATO und die EU sehr bewusst. Bedrohungen durch chemische, biologische, radiologische und nukleare Substanzen (CBRN) und im Cyberspace – auch und besonders durch nichtstaatliche Akteure – sind Teil der NSS-Bedrohungsanalyse, die eng mit den fortschreitenden technologischen Entwicklungen verknüpft ist. Kommunikationstechnologien spielen in der Strategie eine wichtige Rolle und werden als Systeme betrachtet, die Schwachstellen, Abhängigkeiten, aber auch Chancen mit sich bringen. In diesem Zusammenhang werden insbesondere weltraumbasierte

Systeme genannt, aber auch Technologien wie 5G. Daneben betont die belgische Regierung die Bedeutung von offensiven Cyber-Instrumenten – die am häufigsten genannte Unterkategorie – als Bedrohung, aber auch als Fähigkeit. Konventionelle Rüstungsgüter werden nicht breit diskutiert, was zeigt, dass der Fokus dieser ersten NSS auf eher hybride und immaterielle Gefahren und deren weitreichende Bedrohung für Gesellschaft und Frieden liegt.

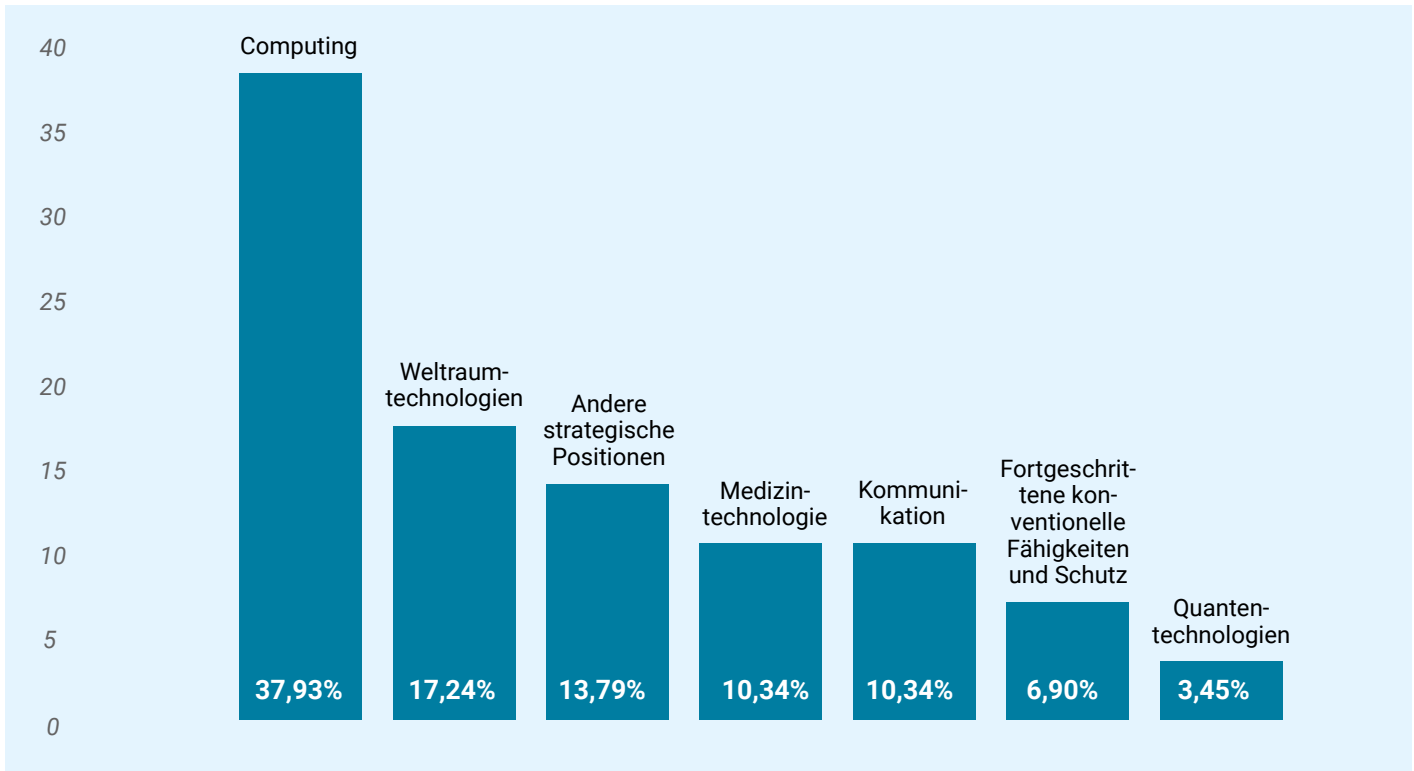


Abbildung 1: Verteilung kodierter Technologiegruppen – Belgische Nationale Sicherheitsstrategie 2021

Eindrücke aus Frankreich

In der nationalen strategischen Überprüfung von 2022, die auf der Version von 2017 und einer Aktualisierung von 2021 aufbaut, setzt Frankreich seine Ziele unter dem Eindruck einer „Welt neuer Spannungen“ und den Übergang „vom strategischen Wettbewerb zur strategischen Konfrontation“. ⁹ Auf dieser Grundlage ruht Frankreichs nationale Sicherheit auf drei Säulen: (1) strategische Autonomie als Nation, aber auch als Führungsmacht innerhalb der Europäischen Union, (2) Widerstandsfähigkeit der Industrie und der Gesellschaft insgesamt und (3) starke Streitkräfte, die „eine robuste und glaubwürdige atomare Abschreckung bei[...] behalten“. ¹⁰ Neben der Fähigkeit der „Force de Frappe“, der französischen Nuklearstreitkräfte, zur atomaren Abschreckung haben Frankreichs koloniale Vergangenheit und sein Streben nach einer aktiven Rolle auf der internationalen Bühne zu dem Balanceakt geführt, dass die konventionellen Fähigkeiten der französischen Streitkräfte das gesamte Spektrum von der globalen Intervention bis zur Landes- und Bündnisverteidigung abdecken müssen. In diesem Zusammenhang betont Frankreich die Idee, eine „Rahmennation“ ¹¹ zu sein, was bedeutet, dass Frankreich – zumindest im Prinzip – volle Autonomie über seine Beschaffungs- und Technologieentscheidungen hat und eine industrielle Basis anstrebt, die dies ermöglicht, auch, um eine führende Rolle bei der Organisation und Koordination multinationaler Streitkräfte übernehmen zu können.

Neue und disruptive Technologien für das Militär werden in den NSS nur teilweise als Mittel zur Erreichung dieses Ziels gesehen, aber in erster Linie als potenzielle Herausforderungen, die es zu bewältigen gilt, wie die Fähigkeit zu einer „herausragenden Cyber-Resilienz“ und Maßnahmen, um „Handlungen unserer Konkurrenten im gesamten Spektrum der Hybridität

entgegenzuwirken“ als „wesentlicher Bestandteil des Ausdrucks von Macht“. ¹² Was die eigenen militärischen Investitionen angeht, so geht aus Frankreichs Strategiepapieren hervor, dass die traditionellen Luft-, Boden- und Seesysteme technologisch aufgerüstet werden sollen, um optimal gegen alte und neue Bedrohungen zu schützen. Darüber hinaus soll in Bereiche investiert werden, die ein umfassendes und klares Bild der Lage ermöglichen und neue Bedrohungen identifizieren, bevor diese zu einer Gefahr werden. Der Fokus liegt hier primär auf Cyber- und Weltraumtechnik, aber auch auf herkömmlichen Aufklärungsmethoden wie Radar. Frankreich ist jedoch auch an offensiven Optionen interessiert, insbesondere im Bereich Cyber oder über Stealth-Optionen. Etwas überraschend ist, dass künstliche Intelligenz eine vergleichsweise geringe Rolle bei den militärischen Zielen der NSS spielt. Über diese militärischen Ziele hinaus, verbindet Frankreich die nationale Sicherheit mit der Fähigkeit, Bedrohungen zu begegnen, die sich „aus den Folgen des Klimawandels und der Verschlechterung der Biodiversität ergeben: Nahrungsmittel als Waffe, Macht und Selbstversorgung, [einschließlich] chemischer, biologischer, radiologischer und nuklearer Gefahren (CBRN)“. ¹³

Eindrücke aus Deutschland

Die erste nationale Sicherheitsstrategie Deutschlands aus dem Jahr 2023 hat ein sehr breites Verständnis von Sicherheit und deckt ein breites Spektrum ab, von konventionellen militärischen Bedrohungen, der Sicherheit der Energieversorgung (als Antwort auf die Abhängigkeit von russischer Energie) und die sichere Versorgung mit Medikamenten bis hin zum Klimawandel und dem Schutz der internationalen Ordnung. In Folge konzentriert sich das Dokument wenig auf spezifische (militärische) Technologien. Stattdessen befasst es sich mit den übergreifenden strategischen Zielen, wie integrierte Sicherheit und Resilienz, und den Herausforderungen, die sich aus diesen Zielen ergeben. Eine der zentralen Herausforderungen sind Cyber-Bedrohungen durch verschiedene Akteure und die Anfälligkeit kritischer Systeme, wie in den in den letzten Jahren in mehreren Situationen schmerzlich erfahren wurde, sowie die Erfahrung von Abhängigkeiten im IT- und Halbleitersektor während der Covid-19-Pandemie oder die Diskussion um die Sicherheitsimplikationen der von chinesischen Unternehmen dominierten 5G-Mobilfunknetze. Basierend auf dieser Einschätzung sind Computer- und Kommunikationstechnologien einer der wenigen technologischen Bereiche, die ausdrücklich erwähnt werden. Dabei sind die wichtigsten Prioritäten künstliche Intelligenz und die damit verbundene Verfügbarkeit der notwendigen IT-Infrastrukturen, Cybersicherheit und die Entwicklung von Netzwerkinfrastrukturen und -technologien. Einen weiteren Schwerpunkt bilden Quantencomputing und quantensichere Kommunikation. Als übergreifendes nationales Ziel verfolgt die NSS Deutschlands die Erreichung und Erhaltung der gesamtgesellschaftlichen Resilienz. Vor diesem Hintergrund sollen die genannten Technologien auch unter ökonomischen Perspektiven ihren Teil beitragen, insbesondere in Zusammenarbeit mit europäischen Partnern.

KI und Cybersicherheit zählen zu den Prioritäten Deutschlands.

Eindrücke aus Japan

Die nationale Sicherheitsstrategie Japans von 2022 unterstreicht, dass die internationale Ordnung vor fundamentalen Herausforderungen steht, und konzentriert sich zunächst auf die militärischen Aufrüstungen in der Region. Sie erweitert das Verständnis von nationaler Sicherheit auch auf nicht-militärische Aspekte, insbesondere die Wirtschaft, und stellt hierbei aber eine klare Verbindung zwischen militärischer und wirtschaftlicher Macht her. China, Nordkorea und Russland werden explizit als die Staaten genannt, deren umfangreiche Aufrüstung als Bedrohung gekennzeichnet wird. Weiterhin wird von Russland und China angenommen, dass sie ein Interesse an territorialer Expansion und dem Umsturz der bestehenden Weltordnung hegen, während Nordkorea vor allem wegen seines Raketen- und Atomprogramm als eine unmittelbare Bedrohung gesehen wird.

In der NSS wird erläutert, wie und warum Japan vor diesem Hintergrund seine eigenen nationalen Interessen verfolgen sollte. Um das zu erreichen, werden unter anderem Computertechnologien, einschließlich Cybersicherheit, künstliche Intelligenz und Data Science als

Japan misst ballistischer Raketentechnologie und Hyperschallwaffen Bedeutung zu.

unabdingbar für die Sicherheit angesehen. Weitere Bedeutung wird Raketentechnologien zugewiesen, insbesondere fortgeschrittenen ballistischen Raketentechnologien, Hyperschalltechnologien und Waffen, die davon Gebrauch machen können. In diesem Zusammenhang wird stets auf die Wichtigkeit der entsprechenden Raketen- und Flugabwehr verwiesen. Technologien im Hinblick auf fortgeschrittene konventionelle Fähigkeiten und Schutz haben für Japan höchste Priorität. Nachrichtendienstliche Fähigkeiten und informationelle Informationskriegsführung machen hierbei einen großen Teil aus, während der Schutz vor CBRN-Waffen und die konventionellen Fähigkeiten der japanischen Selbstverteidigungskräfte ebenfalls hervorgehoben werden. Die in der NSS erwähnten Technologien werden häufig im Zusammenhang mit regionalen Akteuren wie China und Nordkorea kontextualisiert, was die Bedeutung von Forschung und Entwicklung für Japan in den jeweiligen Bereichen zusätzlich zum Ausdruck bringt.

Eindrücke aus der Republik Korea

Die nationale Sicherheitsstrategie der Republik Korea wurde im Jahr 2023 veröffentlicht und bildet einen umfassenden Ansatz zur Lösung globaler Probleme, während Nordkoreas kontinuierliche Weiterentwicklung seiner (taktischen) nuklearen Fähigkeiten und anderer Massenvernichtungswaffen als die größte Bedrohung in der Region angesehen wird. Die Nation nimmt eine Verschiebung in der Weltpolitik zur Kenntnis und unterstreicht die Bedeutung des sich verschärfenden Wettbewerbs zwischen den Vereinigten Staaten und der Volksrepublik China, der zu einer Militarisierung von Industrien und Ressourcen sowie zur Fragmentierung globaler Lieferketten geführt hat. Zusätzlich werden aktuelle Sicherheitsbedrohungen, z. B. Infektionskrankheiten, Klimawandel und Cyberangriffe, als wichtige Aspekte angesehen, die angegangen werden müssen.

Dafür ist es unumgänglich, so deutet die NSS an, ein schlagkräftiges Militär mit einem soliden technologischen Rückgrat zu entwickeln. Dem kommt aufgrund der Auswirkungen

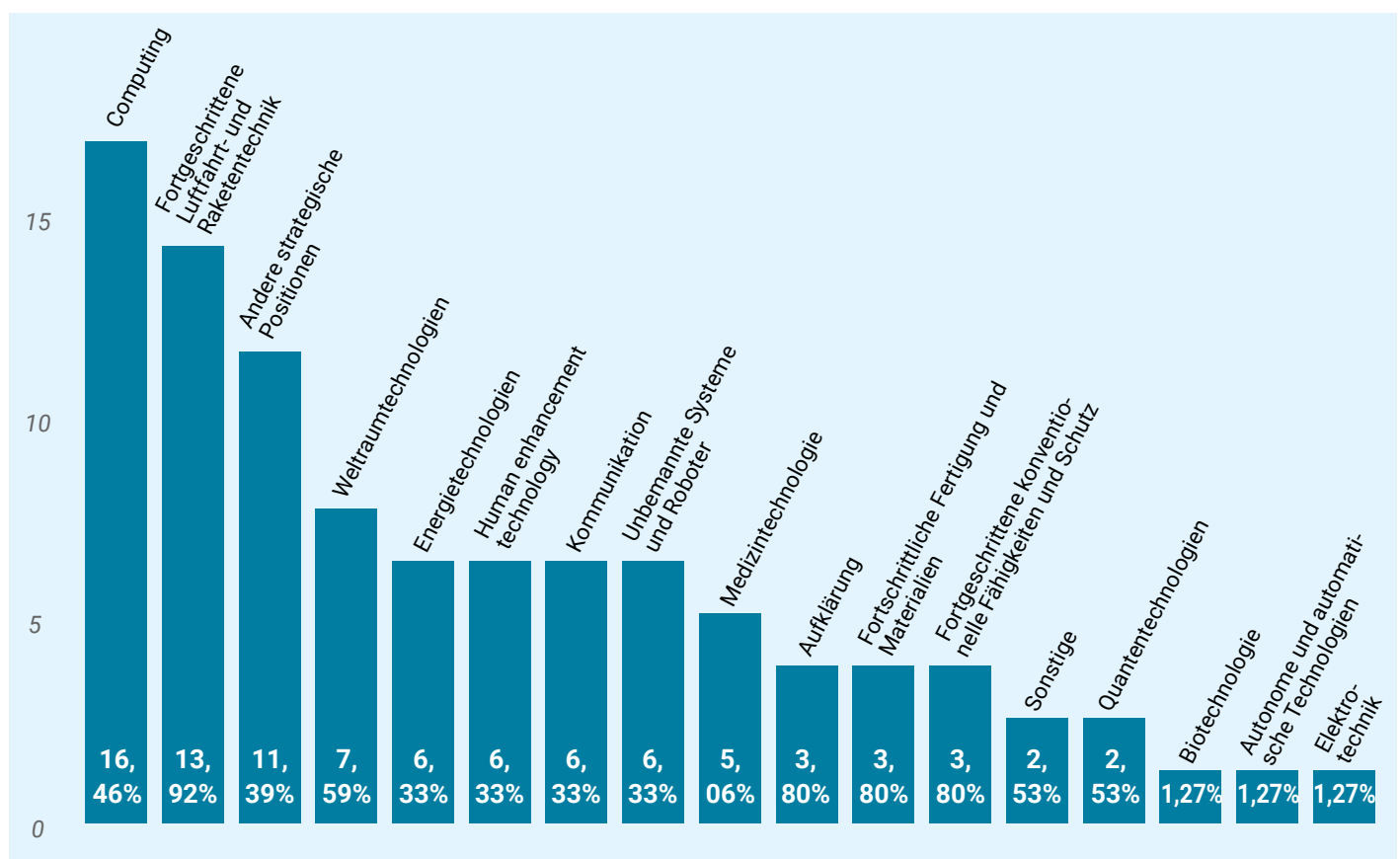


Abbildung 2: Verteilung kodierter Technologiegruppen – Republik Korea, Nationale Sicherheitsstrategie 2023

auf die nationale Sicherheit Südkoreas höchste Priorität zu. Insbesondere Computertechnologien spielen dabei eine wichtige Rolle. In diesem Zusammenhang gehen verschiedene Anwendungen, die auf künstlicher Intelligenz und Data Science beruhen, Hand in Hand mit offensiven und defensiven Aspekten im Cyber-Bereich. Die NSS nennt auch Technologien, die für Umweltlösungen und die Landwirtschaft benötigt werden, und konstatiert die Bedeutung der Nukleartechnologie im Allgemeinen. Ein weiterer Schwerpunkt ist die fortgeschrittene Luftfahrt- und Raketentechnologie. Hinsichtlich Nordkoreas Fähigkeiten und Entwicklungen, einschließlich Hyperschallwaffen, konzentriert sich die NSS auf die Entwicklung und den weiteren Ausbau kompetenter Raketen- und Flugabwehr, fortgeschrittener ballistischer und anderer Raketentechnologien, um potenziellen Angriffen entgegenzuwirken und sie abzuwehren.

Eindrücke aus den Niederlanden

Wie die Bemühungen der niederländischen Diplomatie in internationalen Gremien zeigen, spiegeln die drei nationalen und internationalen Sicherheitsstrategien von 2018, 2019 und 2023 eine sich wandelnde Welt wider, in der sich die Gesellschaft und die Bedrohungen für die nationale und internationale Sicherheit verändern und das internationale Umfeld umgestalten. Neue, sich ständig wandelnde und potenziell disruptive Umstände in verschiedenen Bereichen können, so wird festgestellt, die nationale Sicherheit beeinflussen und dazu führen, dass das Königreich der Niederlande seine Sicherheitsstrategie anpassen muss. Allen drei NSS gemeinsam ist der Schwerpunkt auf digitale Bedrohungen und Cybersicherheit, wobei Cybersicherheit nicht nur mit nationaler Sicherheit, sondern auch mit gesellschaftlichem Frieden, demokratischer Kontinuität und wirtschaftlichem Wohlstand in Verbindung gebracht wird. Auch wenn die Strategien nur wenige Technologien als Lösung für Sicherheitsbedrohungen nennen, beschreiben sie verschiedene politische Programme wie die Überwachung und die Prüfung neuer Technologien, um potenziellen Bedrohungen zu begegnen. Die Entwicklung und der Ausbau inländischer technologischer Anstrengungen werden als unumgänglich für die nationalen Sicherheitsinteressen der Niederlande angesehen. Darüber hinaus ist das Königreich besonders besorgt über offensive Cyberangriffe, die sich gegen die Bevölkerung und die Wirtschaft richten und zu massiven Zusammenbrüchen führen könnten. In ähnlicher Weise hebt die NSS die Risiken von Falsch- und Desinformationen hervor, die die Gesellschaft zunehmend beeinflussen und im Informationskrieg zu mehr hybriden Konflikten führen könnten, ohne klare Grenze, aber mit weitreichenden Sicherheitsauswirkungen. Eine zusätzliche Sorge der niederländischen Strategie ist die internationale Verbreitung und Rolle von Massenvernichtungswaffen, woran sich ihr Interesse an Abrüstung und internationaler Stabilität zeigt. Wie andere Staaten sind auch die Niederlande sensibilisiert für die Folgen des Klimawandels und die Rolle des technologischen Fortschritts bei der Bewältigung seiner Folgen.

Eindrücke aus Pakistan

Die nationale Sicherheitsstrategie Pakistans ist das erste offizielle Dokument seiner Art und wurde im Jahr 2022 veröffentlicht. Sie konzentriert sich auf verschiedene Aspekte der Sicherheit, von Geopolitik bis hin zu eher innenpolitischen Themen wie Wirtschaft, Technologie und Wohlergehen der Bevölkerung. Pakistan stellt wirtschaftliche Sicherheit in den Mittelpunkt seines nationalen Sicherheitsverständnisses und betont, dass dies notwendig sei, um Bedrohungen der nationalen Sicherheit und anderen Sicherheitsherausforderungen begegnen zu können. Diese Bedrohungen reichen von wirtschaftlichen Disruptionen, Defiziten im öffentlichen Sektor bis hin zu natürlichen und gesundheitlichen Gefahren. Im Sinne eines traditionellen Sicherheitsverständnisses adressiert Pakistan die vom Terrorismus und der Aufrüstung von konventionellen Kräften in der Region ausgehende Gefahr, die territoriale Souveränität des Landes verletzen zu können; wobei letzteres im Verlauf der NSS mehrfach betont wird. Es ist keine Überraschung, dass Pakistan als Atommacht die nukleare Abschreckung als unverzichtbares Mittel für seine nationale Sicherheit betrachtet. Allerdings werden in der NSS von Pakistan verschiedenste Bedrohungen thema-

tisiert, wobei es im Allgemeinen für notwendig gehalten wird, die eigenen konventionellen Fähigkeiten zu erweitern, um Herausforderungen begegnen und seine nationale Sicherheit verteidigen zu können. An dieser Stelle ist es auch wichtig zu erwähnen, dass an unterschiedlichen Stellen Indien zur Diskussion gestellt wird. Hierbei werden hegemoniale Ansprüche und der gleichzeitige Auf- und Ausbau der Armee durch fortschrittliche Technologien Indiens thematisiert und kritisiert. Somit wird erneut deutlich, wie wichtig es für Pakistan ist, technologische Lücken zu schließen, insbesondere in Bezug auf Indien.

Auf den ersten Blick scheint es einen Unterschied zwischen militärischen Mitteln wie der Modernisierung konventioneller militärischer Fähigkeiten sowie der elektronischen Kriegsführung einerseits und Technologien für zivile Zwecke andererseits zu geben, die nicht nur für die Sicherheit, sondern für die gesamte Entwicklung Pakistans benötigt werden. Zu diesen Technologien zählen Computertechnologien, darunter auch Anwendungen, die auf künstlicher Intelligenz und Data Science aufbauen und sichere sowie effiziente Kommunikationsfähigkeiten über alle Bereiche hinweg umschließen. Sie sind für Pakistan von höchster Priorität. Im Zusammenhang mit den genannten Technologien konzentriert sich die NSS auch auf unterschiedliche Aspekte der Cybersicherheit und -verteidigung. Aus der NSS geht hervor, dass Pakistan einen Technologieansatz anstrebt, der der gesamtwirtschaftlichen Entwicklung zugutekommen soll. Gleichzeitig sollen hieraus entstehende Nutzen und Fortschritte in die Verteidigungskapazitäten einfließen, um sich wandelnden Bedrohungen für die nationale Sicherheit begegnen zu können.

Eindrücke aus Polen

Polens nationale Sicherheitsstrategie von 2020 beruht auf einer klaren Vision nationaler Interessen sowie der Analyse interner und externer Probleme und Chancen durch technologische Entwicklungen, sowohl ziviler als auch militärischer Art. Die NSS betont die wachsende Rivalität zwischen den USA, China und Russland und benennt deren Auswirkungen auf die internationalen Beziehungen. Während die USA als Partner bezeichnet werden und die Volksrepublik China nur einmal erwähnt wird, kommt Russland in Polens NSS eine besondere Rolle zu. Es ist bemerkenswert, dass Polen bereits im Jahr 2020 von den Risiken spricht, die von Russlands „neoimperialer Politik“ ausgehen. Darauf aufbauend wird Russland als die „größte Bedrohung“ für die nationale Sicherheit Polens wie auch für die Sicherheit des internationalen Systems im Allgemeinen angesehen. Russlands „intensive Entwicklung“ seiner militärischen Fähigkeiten wird als eine weitere Bedrohung betrachtet, mit der Polen und seine internationalen Partner in Europa konfrontiert sind.¹⁴

Infolgedessen werden die Entwicklung und Förderung „neuer Technologien“¹⁵ mit militärischem Fokus als Notwendigkeit für Polens nationale Sicherheit gesehen. Zunächst wird in der NSS angesichts der russischen Aggression in der Nachbarschaft eine proaktive Teilnahme an einer Politik der nuklearen Abschreckung unter dem Dach der NATO akzentuiert. Darüber hinaus weist sie auf die Bedeutung des technologischen Fortschritts bei ballistischen Raketen und anderer Raketentechnik und deren entsprechenden Gegenmaßnahmen hin, z. B. Flug- und Raketenabwehr. Trotz eines breiten Blicks auf neu aufkommende und disruptive Technologien liegt der Schwerpunkt der NSS auf technologischen Bereichen wie Computing und Kommunikation. Es wird darauf hingewiesen, dass Netzwerk- und elektromagnetische Technologien, zusammen mit fortgeschrittenem „Command and Control“,¹⁶ die auf neuen Wegen der Verschlüsselung und Netzsicherheit aufbauen, einen enormen Einfluss auf die Wettbewerbsfähigkeit Polens auf internationaler Ebene haben werden. Innerhalb der Computertechnologien werden die Implementierung von künstlicher Intelligenz sowie Cybersicherheit und offensive Cyber-Instrumente als wichtig für Polens nationale Interessen genannt.

Der Schwerpunkt der polnischen Sicherheitsstrategie liegt auf Computing und Kommunikation.

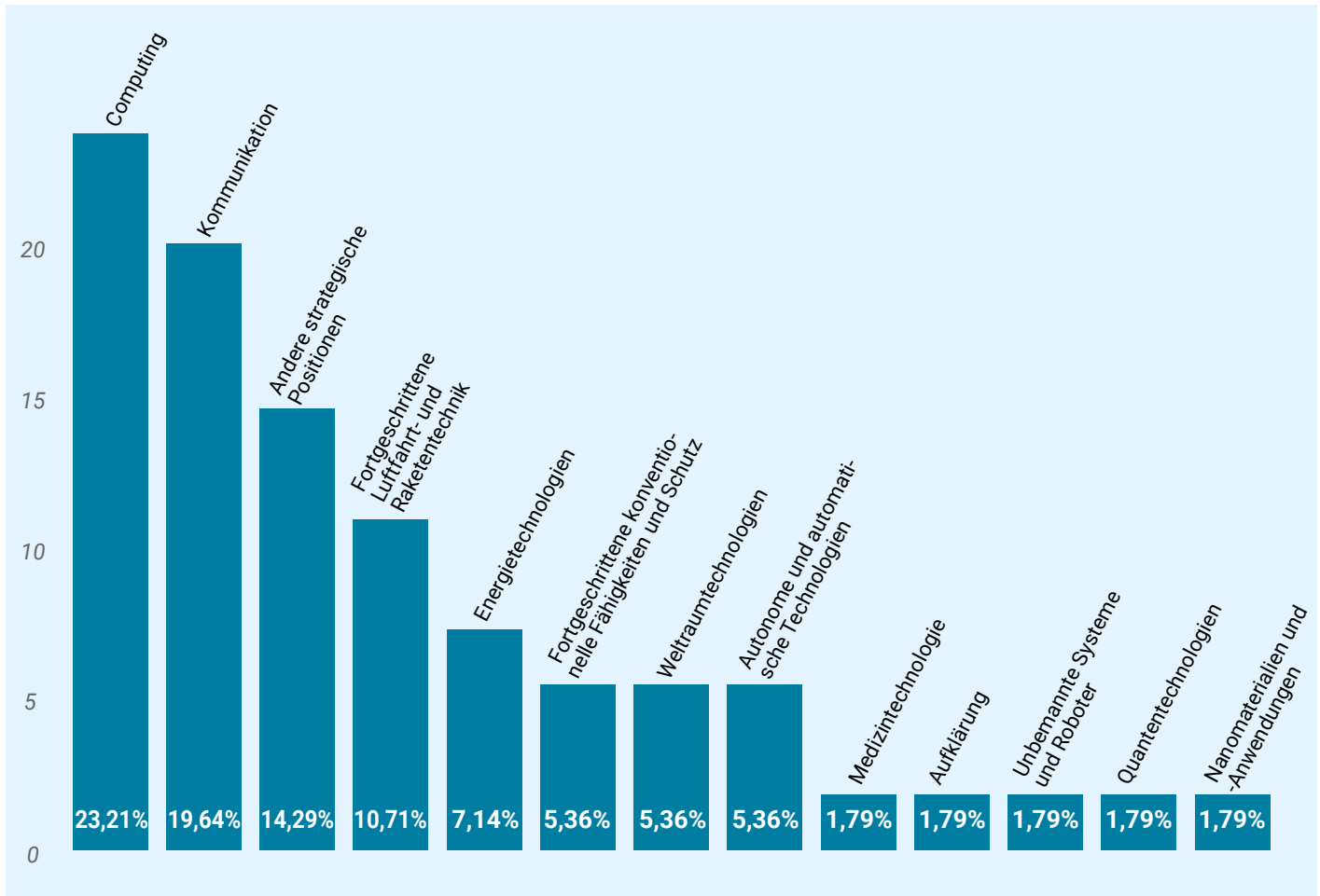


Abbildung 3: Verteilung kodierter Technologiegruppen – Nationale Sicherheitsstrategie Polens 2020

Eindrücke aus Russland

Im Allgemeinen betont die nationale Sicherheitsstrategie Russlands von 2021 die Wahrung und den Schutz der Rechte und Freiheiten russischer Bürger*innen und zielt darauf ab, Bedrohungen von außen und innen abzuwenden, die sich negativ darauf auswirken. Vor dem Hintergrund dieser Prioritäten identifiziert die Strategie Bedrohungen mit Auswirkungen auf die Gesundheit, Lebenserwartung und Sterblichkeit der Bürger oder die destabilisierende Wirkung von Internetkommunikation und – aus russischer Sicht – Falschinformationen und deren Auswirkungen auf die soziale und politische Lage. In Bezug auf militärische Gewalt betont die nationale Sicherheitsstrategie, dass diese von den Akteuren in den internationalen Beziehungen zunehmend eingesetzt wird, um ihre geopolitischen Ziele zu erreichen. Als eine besondere Bedrohung für strategische Stabilität und internationale Sicherheit wird die Stationierung von Mittel- und Kurzstreckenraketen in Europa und im asiatisch-pazifischen Raum sowie die Eskalation der Spannungen in Regionen im und um den postsowjetischen Raum, in Afghanistan, auf der koreanischen Halbinsel und im Nahen Osten benannt. Um diesen so wahrgenommenen Bedrohungen zu begegnen, verfolgt Russland den Ansatz, eine technologische Unabhängigkeit aufrechtzuerhalten, indem es seinen Rüstungsindustriekomplex unterstützt, Innovationen fördert und weiterhin neue Modelle, Komplexe und Systeme für zivile und militärische Mittel schafft. Wissenschaftlicher und technologischer Fortschritt wird daher als unverzichtbar für internationale Wettbewerbsfähigkeit und nationale Sicherheit angesehen. Innerhalb der NSS liegt der Schwerpunkt auf fortschrittlichen Fertigungsmethoden und Werkstoffen, wie z. B. additiver Fertigung, Nukleartechnologie zur Energieerzeugung sowie Lösungen für Umweltfragen. Wenig überraschend wird die Fähigkeit der atomaren Abschreckung als bedeutsam für das nationale

Interesse betrachtet. Computing-Technologien, die eine Kombination aus künstlicher Intelligenz, Hochleistungscomputern, Data Science und Aspekte der Cybersicherheit, aber auch Maßnahmen zum Schutz der Bürger vor Fehlinformationen und zur Erlangung von „Informationssicherheit“ beinhalten, sind weitere instrumentelle Fähigkeiten für Russland.

Eindrücke aus Spanien

Die nationalen Sicherheitsstrategien Spaniens für 2017 und 2021 befassen sich ausführlich mit globalen Transformationsprozessen sicherheitspolitischer, wirtschaftlicher wie ökonomischer und ökologischer Natur. Sie diskutieren detailliert die Risiken, Gefahren und den Anpassungsbedarf, den diese für Spanien mit sich bringen. Die NSS betonen auch die Rivalität zwischen den USA und China, insbesondere im technologischen Bereich. Darüber hinaus wird Chinas Fortschritt bei „kritischen und Dual-Use-Technologien“¹⁷ als ein Aspekt gesehen, der internationale Konflikte weiter verschärfen kann. Indien, Iran, Russland und die Türkei werden als regionale Akteure genannt, die eine stärkere internationale Position anstreben. Spaniens Antwort auf ein sich veränderndes internationales Umfeld basiert auf einem ganzheitlichen Ansatz und stellt sogar ein Modell zur Krisenprävention vor, das in den Rahmen des nationalen Sicherheitssystems gestellt werden sollte. Die wichtigsten technologischen Säulen dieses Systems sind Computer- und Energietechnologien. Angesichts der geopolitischen Rolle Spaniens als Erzeuger von Solarenergie, aber auch für den Transfer erneuerbarer Energie von Afrika nach Europa, werden Energietransport- und -übertragungstechnologien, Energiespeichersysteme und -infrastrukturen sowie neue Energiematerialien stark hervorgehoben. Neben diesem Schwerpunkt offenbart die breite Analyse der Strategie und ihrer gesamtgesellschaftlichen Perspektive die Berücksichtigung vieler verschiedener weiterer Technologien und Technologiebereiche als EDTs. Computing-Technologien wie künstliche Intelligenz und Cybersicherheit haben höchste Priorität. Darüber hinaus spielen weltraumbezogene Themen wie Mikrosatelliten für Kommunikation, Navigation und Überwachung sowie eine umfassendere Sicherheitsvision für den Weltraum eine wichtige Rolle. Eine weitere wichtige Erkenntnis aus den NSS Spaniens ist die Betonung der Verflechtung von Technologie, Wirtschaft und geopolitischer Konfrontation, was die Bedeutung des technologischen Fortschritts für die nationale Sicherheit Spaniens unterstreicht.

Spanien betont die Verflechtung von Technologie, Wirtschaft und geopolitischer Konfrontation.

Eindrücke aus dem Vereinigten Königreich von Großbritannien und Nordirland

Die beiden Strategien des Vereinigten Königreichs, die 2021 bzw. 2023 veröffentlicht wurden, spiegeln das sich verändernde internationale Umfeld gut wider. Das Papier von 2021 beschreibt eine fragmentierte internationale Gemeinschaft und Herausforderungen für die innere Sicherheit, den Wohlstand und die Souveränität, verstärkt durch Klimawandel, Gesundheitskrisen und Bedrohungen für die liberale Demokratie. „Refresh“, das Papier von 2023, ist wesentlich expliziter. Hier findet sich ein deutlich stärkerer Fokus auf traditionelle Sicherheitsbedrohungen und die geopolitischen Veränderungen und Sicherheitsherausforderungen, insbesondere im Verhältnis zu Russland und China. Der technologische Wandel wird als eine der wichtigsten Triebkräfte für die Gestaltung des internationalen Umfelds verstanden. Es überrascht entsprechend nicht, dass beide Papiere viele Errungenschaften des Vereinigten Königreichs benennen und neben den derzeitigen wirtschaftlichen, militärischen und diplomatischen Fähigkeiten explizit auch die technologischen Fähigkeiten des Vereinigten Königreichs erwähnt werden.

Nach dem Brexit unterstreicht das Land die Bedeutung internationaler Allianzen und neuer Partner, die ähnliche Interessen verfolgen. Was die vorrangigen Technologien anbelangt, so nennt das Vereinigte Königreich als Atommacht seine Fähigkeiten und Nuklearstrategie in den NSS am häufigsten. Neben den sicherheits- und stabilitätsrelevanten Atomwaffen, betont das Vereinigte Königreich die Bedeutung konventioneller Plattformen, die zur Sicherung seiner militärischen Fähigkeiten benötigt werden. Darin spiegelt sich einer der Schwerpunkte der Strategien, der darauf liegt, auf die Verteidigung der inneren Si-

cherheit vorbereitet zu sein. Interessanterweise sind digitale Technologien weniger stark vertreten, d. h. sie wurden weniger detailliert beschrieben als Technologien, die mit dem britischen nuklearen und konventionellen Arsenal in Verbindung stehen. Allerdings bedeutet das nicht, dass digitale Technologien für das Vereinigte Königreich keine Priorität haben, denn es ist anzunehmen, dass sie als neu aufkommende Technologien verstanden werden, die das Land tatsächlich mehrfach als zentralen Faktor im globalen Wettbewerb nennt. Nur einmal werden hier auch Beispiele genannt, nämlich KI, Quantentechnologien und synthetische Biologie. Da das Vereinigte Königreich über eine lange etablierte strategische Kultur verfügt, gibt es zusätzliche sicherheits- und verteidigungsbezogene Strategien, die sich sehr detailliert mit militärischer Wissenschaft, Technologie und Innovation im digitalen und konventionellen Bereich auseinandersetzen.

Eindrücke aus den Vereinigten Staaten von Amerika

Die beiden analysierten NSS der USA aus den Jahren 2017 und 2022 sind jeweils durch eine eigene Risikoanalyse und ein eigenes Verständnis von Sicherheit geprägt – was angesichts der beiden herausgebenden Administrationen auch nicht überrascht –, unterscheiden sich aber dennoch nicht in der breiteren strategischen Bedrohungswahrnehmung in Bezug auf den Großmachtwettbewerb mit China und Russland. Beide Strategien erklären die beiden Staaten zu Herausforderern in einem globalen Wettbewerb um Macht und Hegemonie. Während die Strategie von 2017 andere Bedrohungen der nationalen Sicherheit berücksichtigt, indem sie die nationale von der internationalen Sphäre abgrenzt, beinhaltet die Strategie von 2022 mehr transnationale Bedrohungen, wie Klimawandel und (nach Corona wenig überraschend) Pandemien, und verbindet internationale Bemühungen mit der nationalen Sicherheit. Die Bedeutung von militärischer Macht und Atomwaffen ist ein roter Faden, entweder um Stärke zu zeigen und das als Vorteil zu nutzen und/oder um solche militärischen Fähigkeiten zur Abschreckung und für die eigene Sicherheit zu nutzen.

Die USA sehen technologische Innovation in erster Linie als Instrument, um ihren Wettbewerbsvorteil aufrechtzuerhalten, denn Technologie wird als zentral im Großmachtwettbewerb verstanden und ist daher entscheidend für die nationale Sicherheit. Die NSS zeigen, dass die USA beabsichtigen, ihren technologischen Vorsprung zu halten, indem sie weiter in Forschung und Entwicklung neuer disruptiver Technologien investieren – ein Thema, das die USA bereits spätestens seit den 1990er Jahren unter dem Label „*keeping the technological edge*“¹⁸ verfolgen.

Die USA verstehen Technologie als zentral im Großmachtwettbewerb.

Computing-Technologien wie (zuverlässige/vertrauenswürdige) künstliche Intelligenz, Data Science und die Anwendung höchstleistungsfähiger Computer in Kombination mit Cybersicherheit und -verteidigung stehen im Mittelpunkt. Darüber hinaus weisen die USA sowohl auf die Bedeutung des CBRN-Schutzes als auch auf Technologien für (defensive) nachrichtendienstliche Fähigkeiten und Informationskriegsführung hin. Außerdem betonen die USA die Bedeutung von Weltraumtechnologien, insbesondere Technologien, die weitere Fähigkeiten zur Kommunikation und Überwachung ermöglichen sollen. Energietechnologien, womit erneuerbare Energien, Energieunabhängigkeit sowie deren Management, Speicherung und effiziente Nutzung abgedeckt werden sollen, spielen ebenfalls eine wichtige Rolle. Außerdem wird Energie als ein Bereich angesehen, in dem die USA ihre Dominanz behaupten und ihren Wettbewerbsvorteil weiter ausbauen können. Letzteres ist die wichtigste Erkenntnis aus den NSS der USA. Beide Strategien legen einen klaren Schwerpunkt auf den weiteren Ausbau und den Erhalt des technologischen Vorsprungs, insbesondere angesichts der Machtkonkurrenz mit Staaten wie Russland und China.

Die Staaten im Vergleich – Schwerpunkte und blinde Flecken

Vergleicht man die Daten länderübergreifend, ergeben sich interessante Beobachtungen, von denen hier nur einige exemplarisch aufgegriffen werden.

Zunächst ist es wichtig festzustellen, dass eine nationale Sicherheitsstrategie das entscheidendste und richtungsweisendste Dokument für die nationale Sicherheitspolitik ist. Wenn auf dieser Ebene einzelne neue Militärtechnologien als relevant, erstrebenswert oder bedrohlich erachtet werden, ist dies sehr bedeutsam. Je mehr dieser Technologien erwähnt werden, desto wahrscheinlicher ist es, dass ein Staat bestrebt ist, sein Militär entsprechend technologisch auszurüsten und notwendige Organisationsstrukturen aufzubauen oder anzupassen. Im Gesamten betrachtet ist die Bandbreite der Erwähnungen von Technologien in den NSS sehr groß. Während die deutsche NSS gerade einmal fünf von 18 Technologiekategorien erwähnt (gefolgt von Belgien mit sieben), sind es in der koreanischen NSS 17. Während es nicht überraschend ist, dass die amerikanische und britische NSS ebenfalls viele Technologiekategorien erwähnen (14 bzw. 15), überrascht dagegen die spanische NSS mit 15 Erwähnungen. Russland nennt wie Polen jeweils 13 Kategorien als wichtig, Frankreich elf.

	BEL	DEU	ESP	FRA	GBR	JPN	KOR	NLD	PAK	POL	RUS	USA	
Fortgeschrittene Luftfahrt- und Raketentechnik	0	0	1	1	1	1	1	1	0	1	1	1	9
Fortgeschrittene konventionelle Fähigkeiten und Schutz	1	1	1	1	1	1	1	1	1	1	1	1	12
Fortschrittliche Fertigung und Materialien	0	0	1	1	1	1	1	0	0	0	1	1	7
Andere strategische Positionen	1	0	1	0	1	1	1	1	1	1	1	1	10
Autonome und automatische Technologien	0	0	1	1	1	1	1	1	1	1	0	1	9
Biotechnologie	0	0	1	0	1	0	1	1	0	0	1	1	6
Kommunikation	1	1	1	1	1	1	1	1	1	1	1	1	12
Computing	1	1	1	1	1	1	1	1	1	1	1	1	12
Elektrotechnik	0	0	1	0	1	1	1	0	0	0	0	1	5
Energietechnologien	0	0	1	0	1	1	1	0	0	1	1	1	7
Human enhancement technology	0	0	0	0	0	0	1	0	0	0	0	0	1
Medizintechnologie	1	1	1	0	1	0	1	1	0	1	1	1	9
Nanomaterialien und -Anwendungen	0	0	0	1	0	0	0	0	0	1	1	1	4
sonstige	0	0	1	0	0	0	1	0	0	0	0	0	2
Quantentechnologien	1	1	1	1	1	0	1	1	1	1	1	1	11
Aufklärung	0	0	0	1	1	0	1	0	1	1	0	0	5
Weltraumtechnologien	1	0	1	1	1	1	1	0	1	1	1	1	10
Unbemannte Systeme und Roboter	0	0	1	1	1	0	1	1	0	1	1	0	7
1 = Treffer	7	5	15	11	15	10	17	10	8	13	13	14	
0 = Kein Treffer													

Tabelle: Überblick darüber, welche Länder welche und wie viele Technologien nennen

Welche Länder weisen Ähnlichkeiten in Bezug auf die Nennung von Technologien auf? Die USA haben ähnliche Prioritäten wie Großbritannien, Russland und – überraschenderweise – Spanien und unterscheiden sich am meisten von Deutschland. Deutschland wiederum setzt ähnliche Technologieprioritäten wie Belgien, gefolgt von Korea und Pakistan. Generell unterscheiden sich die deutschen Prioritäten erheblich von denen seiner größeren EU- und NATO-Partner, z. B. Spanien, Großbritannien oder die USA. Diese drei Staaten bilden eine recht ähnliche Gruppe. Russland kommt jedoch nahe heran und setzt ähnliche Technologieprioritäten wie die USA oder Großbritannien.

Schwerpunkte: Sicherheitsrelevante Technologien für die meisten Staaten

Trotz der großen Bandbreite an Nennungen stechen einige der genannten Technologien als besonders bedeutsam hervor und werden von besonders vielen Staaten erwähnt. Die folgende Grafik gibt einen Überblick darüber, wie viele der zwölf betrachteten Länder das jeweilige Technologiefeld in ihren NSS erwähnt haben.

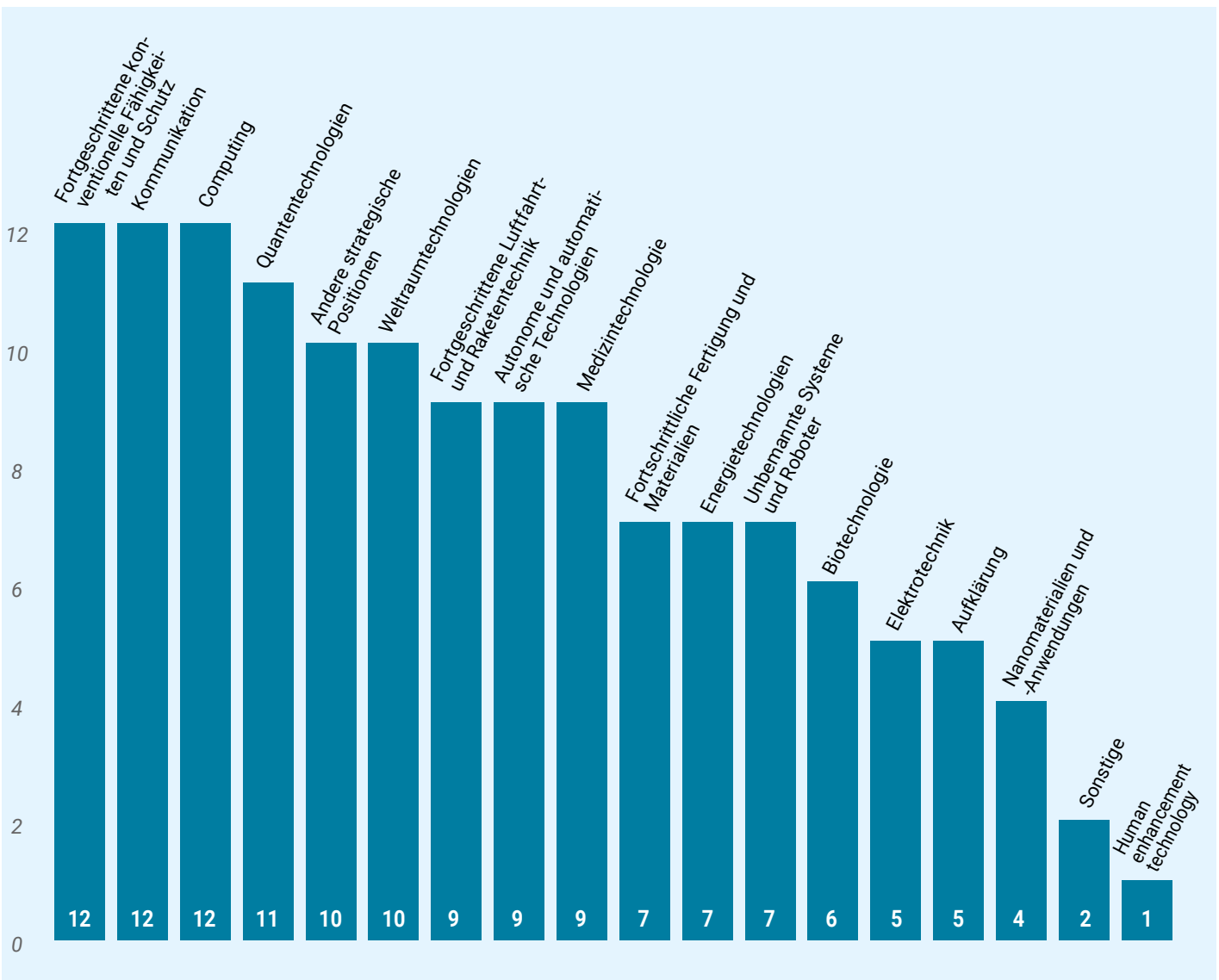


Abbildung 4: Nennung der Technologiekategorien durch die 12 betrachteten Staaten

Drei Technologiefelder werden von allen betrachteten Ländern als relevant erachtet: Kommunikation, Computing und „fortgeschrittene konventionelle Fähigkeiten und Schutz“, gefolgt von Quantentechnologie, die von elf von zwölf Ländern genannt wird.

Der hohe Wert von Computing ist hier keine große Überraschung, da die Kategorie die besonders intensiv diskutierten Bereiche Cyber und künstliche Intelligenz umfasst. Alle zwölf Länder diskutieren diese Themen, wobei oft digitale Herausforderungen und Reaktionen darauf diskutiert werden. Angesichts der Bedeutung von Cyberangriffen seit Anfang der 2000er Jahre ist dies keine Überraschung.

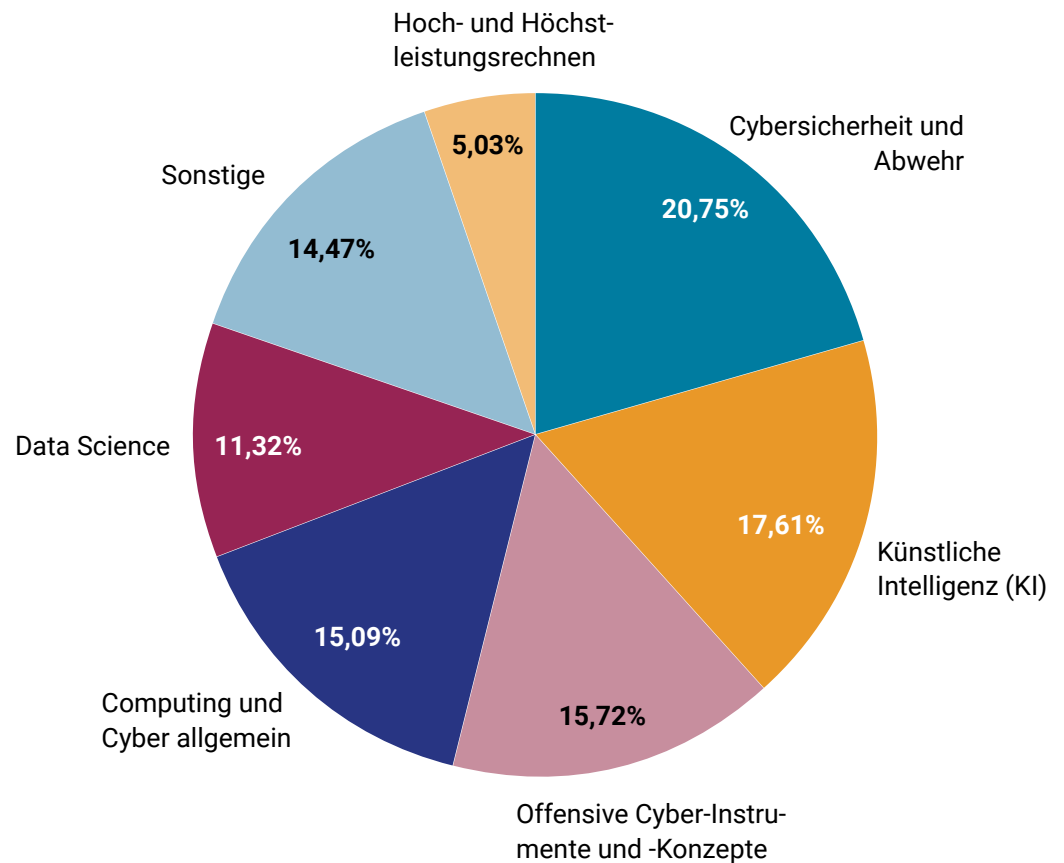


Abbildung 5: Technologie-Unterkategorien, die in der Kategorie „Computing“ genannt werden.

Vor diesem Hintergrund ist nachvollziehbar, dass Cybersicherheit und Abwehrmaßnahmen eine besonders wichtige Rolle spielen, wobei auch das Streben nach offensiven Cyberfähigkeiten immer wieder genannt wird. Dieses explizite Interesse an offensiven Cyberoperationen, das hier auf der Ebene der NSS zum Ausdruck kommt, ist insofern besorgniserregend, als es Ängste vor Überraschungsangriffen und einem „Cyber-Wett-rüsten“ schürt und die Gefahr von Rüstungsdynamiken erhöht. Im Zusammenhang mit Computing wird auch künstliche Intelligenz häufig als Schlagwort erwähnt, bleibt aber in Bezug auf konkrete Anwendungen, zumindest auf dieser Ebene, interessanterweise vage. Konkretere Themen, die erwähnt werden, sind insbesondere die Datenwissenschaft, also die Analyse von Mustern, die in großen Datenmengen, manchmal aus unterschiedlichen Quellen, von Interesse sind. Manchmal wird KI auch mit der Entwicklung autonomer Systeme in Verbindung gebracht. Es wird erwartet, dass KI bedeutende Teile der Gesellschaft verändern wird, daher gehen die meisten Militärs davon aus, dass die Auswirkungen auf die Kriegsführung und das Militär ebenfalls enorm sein werden. Interessant ist jedoch, dass gerade in diesem Bereich einige Länder militärisch stärker von der Dual-Use-Relevanz von KI zu profitieren scheinen als andere. Während es beispielsweise bei westlichen KI-Entwickler*innen eine gewisse Zurückhaltung zu geben scheint, ihre Produkte vom Militär verwenden zu lassen (die Weigerung der Google-Programmierer*innen, am Projekt „Maven“ teilzunehmen, ist das deutlichste Beispiel¹⁹), sind diese Vorbehalte in anderen

Ländern, beispielsweise in China, viel weniger ausgeprägt. Diese Dynamik könnte sich jedoch ändern, wenn man bedenkt, dass Silicon Valley und andere ehemalige zivile IT-Dienstleister in der Ukraine Produkte speziell für militärische Anwendungen entwickeln.²⁰

Die zweite Kategorie, auf die sich alle Staaten einigen können, ist der damit verbundene Bereich der Kommunikation mit einem besonderen Schwerpunkt auf Netzwerktechnologie, Verschlüsselung und Netzwerksicherheit – auch hier ein Beispiel, wo sich zivile und militärische Anwendung derselben Technologien überschneiden. Andere aufkommende Aspekte der Kommunikation mit stärkerem militärischem Schwerpunkt, wie neue Formen der Befehls- und Kontrollgewalt oder elektronische Kriegsführung, werden etwas weniger häufig benannt. Dies kann jedoch daran liegen, dass diese Aspekte für die nationalen Sicherheitsstrategien zu militärspezifisch sind, und es ist anzunehmen, dass diesen Technologien in nationalen Strategien, die stärker auf militärische Forschung und Entwicklung ausgerichtet sind, eine größere Bedeutung beigemessen wird.

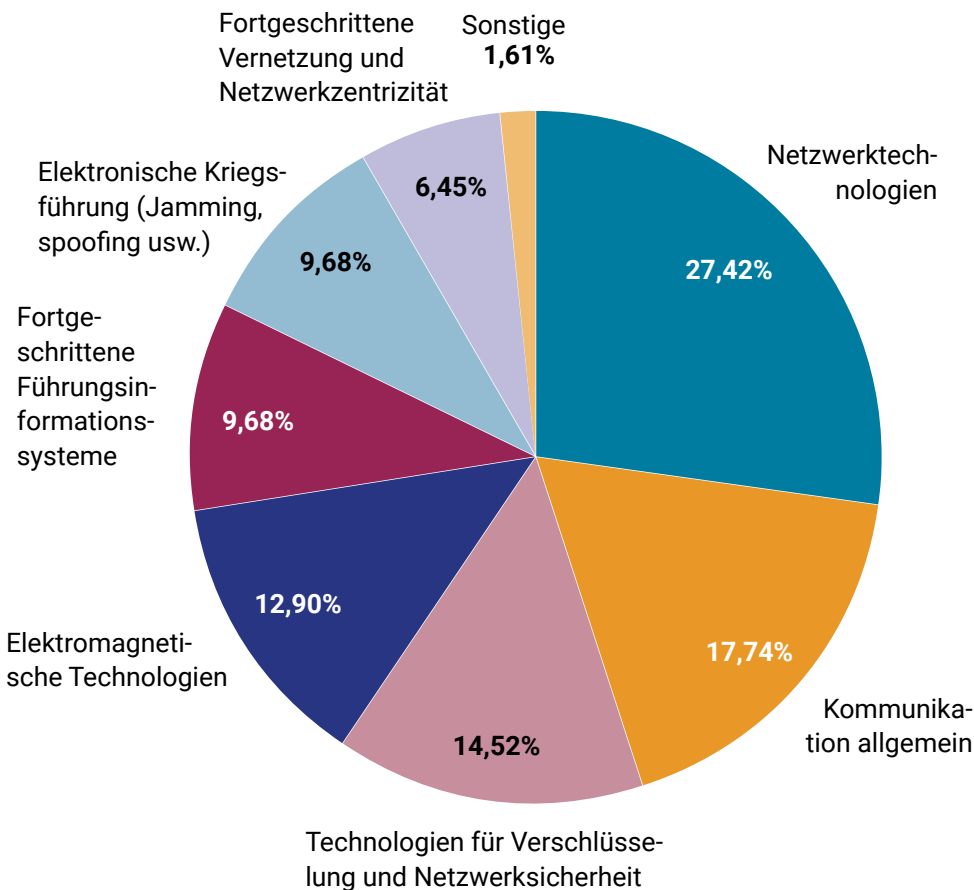


Abbildung 6: Technologie-Unterkategorien der Kategorie „Kommunikation“.

Der dritte Bereich, in dem alle Staaten technologischen Investitionsbedarf sehen, ist „fortgeschrittene konventionelle Fähigkeiten und Schutz“, wobei der Schwerpunkt hauptsächlich auf bereits vorhandenen Technologien liegt. Diese Kategorie umfasst Technologien, Prozesse, Materialien und Anwendungen, die darauf abzielen, konventionelle Bewaffnung und Schutzfähigkeiten zu verbessern, die von keiner anderen Kategorie abgedeckt werden. Der Schwerpunkt liegt daher eher auf der evolutionären Verbesserung bestehender Technologien, beispielsweise CBRN-Schutz, konventionellerer Schutz, nächste Generationen von Land-, See- oder Luftsystemen, Verbesserungen der Stealth-Technologie oder sogar fortschrittlicher Sprengstoffe oder Munition. Die Bedeutung der Verbesserung der

Geheimdienstfähigkeiten und der Absicherung der Infrastruktur gegen Informationskriege wird ebenfalls hervorgehoben.

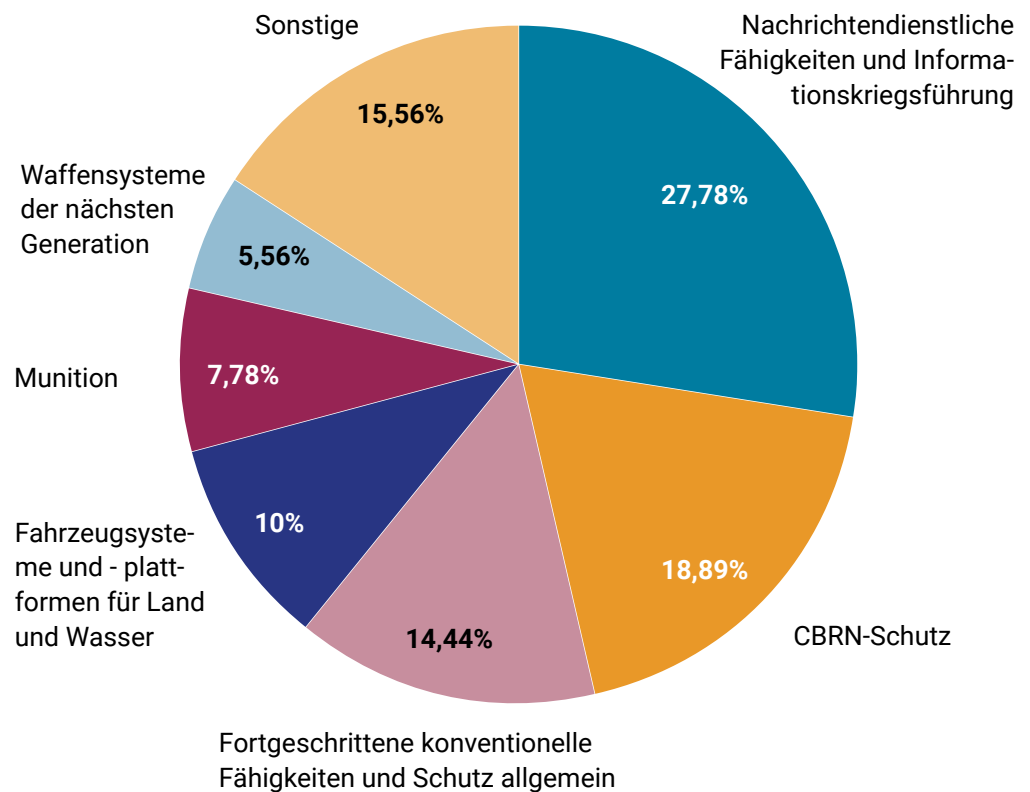


Abbildung 7: Technologie-Unterkategorien, die in der Kategorie „Fortgeschrittene konventionelle Fähigkeiten und Schutz“ genannt werden.

Die vierte Kategorie, die von elf von zwölf Staaten mit Ausnahme Japans genannt wird, ist die Quantentechnologie. Angesichts der Tatsache, dass Quantentechnologie im Vergleich zu vielen anderen hier diskutierten Technologien ein relativ neues Thema ist, überrascht dies. Obwohl seitens der Staaten Unsicherheit über die möglichen Anwendungen zu herrschen scheint, wird in den NSS oft der Eindruck geäußert, dass dieses Thema ein starkes Disruptionspotenzial haben kann, insbesondere durch Entschlüsselung und die Untergrabung aktueller Ansätze sicherer Kommunikation. Ähnlich wie bei KI sind jedoch Verweise auf konkrete Anwendungen über die allgemeine Erwähnung von „Quantentechnologie“ hinaus selten, wobei Quantencomputing dann am häufigsten vorkommt, gefolgt von Quantensensorik und -bildung sowie Quantenkommunikation (siehe Abbildung 8).

Für einen Überblick über sicherheitsrelevante Anwendungen von Quantentechnologie, siehe das CNTR Fact Sheet unter cntrarmscontrol.org/quantum

Blinde Flecken

Neben den Interessensschwerpunkten der Staaten ist in gleichem Maße aber auch interessant, welche Technologien, die in öffentlichen Debatten und an anderer Stelle oft als EDTs kategorisiert werden, fehlen. Human Enhancement, als auffälligstes Beispiel, wird nur von einem Land erwähnt – der Republik Korea. Human Enhancement ist ein weites Feld für sich und umfasst Themen von entfernbaren Gegenständen wie Nachtsichtbrillen oder Exoskeletten bis hin zu leistungssteigernden Medikamenten oder sogar Körpermodifikationen, einschließlich implantierter Chips oder künstlicher Gliedmaßen (meist als Prothesen). Viele dieser Technologien sind ziemlich neu und aktuell noch „Science Fiction“, aber zum Beispiel im Bereich der Mensch-Maschine-Interaktion wird viel geforscht, um die Schnitt-

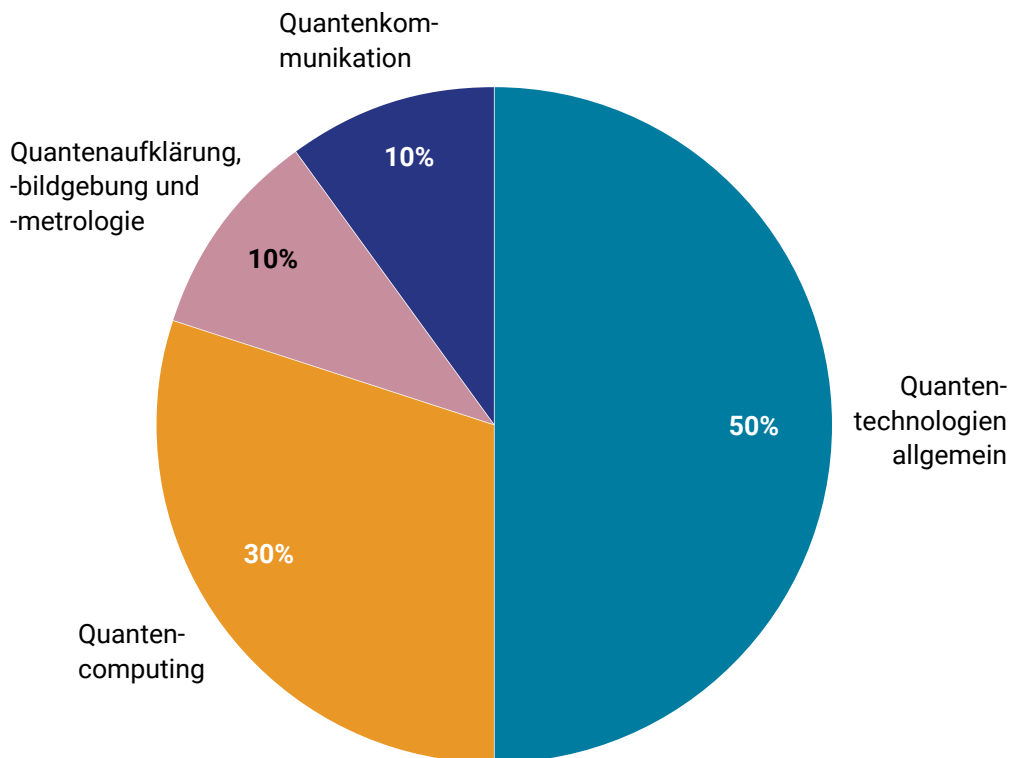


Abbildung 8: Technologie-Unterkategorien, die in der Kategorie „Quantentechnologie“ genannt werden.

stelle zwischen Computer und Mensch zu optimieren. Die Forschung in diesem Bereich steckt noch in den Kinderschuhen, aber angesichts des zivilen und militärischen Nutzens der Mensch-Maschine-Interaktion scheint es plausibel zu erwarten, dass das Momentum und die Erfolge im zivilen Bereich auch breites militärisches Interesse wecken werden. Dieser Bereich sollte daher im Auge behalten und genau beobachtet werden.

Andere „blinde Flecken“ relativ selten erwähnter Technologien fallen unter die Kategorien „Nanotechnologie“ (von vier Staaten genannt) und „Sensorik“ (von fünf Staaten genannt). Schließlich, auch wenn man nicht sagen kann, dass die Kategorie „unbemannte Systeme/Roboter“ im engeren Sinne selten erwähnt wird, da sieben von zwölf Staaten sie nennen, ist das Ergebnis aus unserer Sicht erstaunlich niedrig. Das erscheint merkwürdig, könnte aber daran liegen, dass die besondere Bedeutung von Drohnen in den Konflikten der Zukunft erst durch den Krieg Russlands gegen die Ukraine deutlich geworden ist und noch nicht in die NSS eingeflossen ist. Eine andere Erklärung könnte sein, dass ferngesteuerte Drohnen nicht mehr als „neu aufkommend“ angesehen werden, da mehrere (neun) Staaten automatisierte oder sogar autonome Systeme durchaus als relevant ansehen. Auf jeden Fall ist es wichtig, hier noch einmal genau hinzusehen, zumal die ehemals zivile Technologie der Mikro- oder Hobbydrohnen einen enormen Einfluss auf die Schlachtfelder der 2020er Jahre hat.

Für eine weiterführende Diskussion zu Drohnen, siehe das Kapitel von Niklas Schörnig ab S. 22.

Fazit

Die Analyse der nationalen Sicherheitsstrategien hat gezeigt, dass Staaten auf dieser Ebene nicht nur ein sehr unterschiedliches Verständnis von Sicherheit haben, sondern in der Folge auch sehr unterschiedliche Prioritäten in Bezug auf moderne neue Technologien für Sicherheit setzen. Während einige Staaten sehr zurückhaltend darin sind, ihr Interesse an neuen Technologien zu bekunden, sehen andere eine Notwendigkeit, ein breites Spektrum an neuen Technologien in ihr Militär einzuführen oder zumindest in diese Richtung zu justieren.

Interessanterweise traten „der Westen“ oder die untersuchten NATO-Staaten nicht als ein einheitlicher Block mit synchronisierten technologischen Präferenzen zutage. Vielmehr kann davon ausgegangen werden, dass Bedrohungswahrnehmungen, die eigene Stellung im internationalen System und historische Tendenzen zur Technikbegeisterung die individuellen Technologiepräferenzen bestimmen.

Die Analyse zeigt auch, dass bestimmte Technologien von praktisch allen Staaten als relevant angesehen werden, darunter der – inzwischen etablierte – Bereich der Cyber-Verteidigung und Cyber-Kriegsführung, modernste Kommunikation oder der Einsatz von KI, während andere Technologien noch nicht auf diesem hohen Niveau angekommen sind. Interessant ist auch, dass der Einsatz von „Quantentechnologie“ von fast allen Staaten als sicherheitsrelevant angesehen wird, obwohl in der Mehrheit der Fälle der Effekt und die Wirkweise von Quantenanwendungen für Militär und Sicherheit noch durch Machbarkeitsstudien erforscht werden und werden müssen. Zusammengefasst machen diese Entwicklungen deutlich, dass die Erkenntnis der Notwendigkeit einer umfassenden und breit angelegten Digitalisierung der Streitkräfte zumindest in der Rhetorik das höchste Niveau erreicht. Die Fokussierung auf das Digitale ist jedoch nicht ohne Gefahren, denn in einem militärischen Konflikt kann Cyber nicht „die Stellung halten“.

Interessant ist auch, wie die Diskussion um Dual-Use-Technologien ihren Weg in die nationalen Sicherheitsstrategien findet. Einerseits wird sie verwendet, um die Absicht eines Gegners zu beschreiben, Technologie in einer Weise zu nutzen, die zwischen zivilem und militärischem Einsatz austauschbar ist. Ein Beispiel ist die NSS der USA aus dem Jahr 2022, in der die Volksrepublik China als Akteur bezeichnet wird, der wissenschaftliche Erkenntnisse aus der zivilen Forschung umfunktioniert, um von Dual-Use-Aspekten für militärische Anwendungen zu profitieren. Ein genauerer Blick auf andere NSS zeigt, dass der Brückenschlag zwischen zivilen und militärischen Technologien keine Ausnahme ist. Zum Beispiel weisen die NSS von Japan, Pakistan, der Republik Korea und Russland darauf hin, dass der Transfer von privatem, wirtschaftlichem und zivilem Wissen an das Militär dazu beitragen könnte, militärische Technologien weiter zu verbessern.

In diesem Zusammenhang ist es wichtig darüber nachzudenken, wie nationale Positionen zur Technologie im Kontext der NSS in die Diskussionen über die Dual-Use-Problematik einfließen, insbesondere angesichts des zunehmenden globalen Wettbewerbes, in dem solche Technologien oft im Mittelpunkt stehen. Zum Beispiel gibt es trotz Zivilklauseln an vielen deutschen Universitäten auch eine lange Tradition der Abstimmung zwischen dem Bundesministerium für Bildung und Forschung (BMBF) und dem Verteidigungsministerium (BMVg).

Die Analyse zeigt aber auch, dass umfassendere Forschung notwendig und dass die NSS nicht die ganze Geschichte erzählen. Dies liegt daran, dass insbesondere die breit angelegten Sicherheitsstrategien nicht unterscheiden zwischen Technologien, die nur zivil genutzt werden, Dual-Use-Technologien, Verbesserungen, und wirklich neuen Technologien, die dem Militär völlig neue und potenziell disruptiven Fähigkeiten bieten. Viele Fragen bleiben daher an dieser Stelle unbeantwortet, die CNTR in zukünftiger Forschung angehen wird, denn wenn es um die Frage der Regulierung und sogar der Rüstungskontrolle geht, wird die Tatsache, dass viele der relevanten Technologien in der Tat Dual-Use-Technologien sind, es schwieriger machen, restriktive Lösungen zu finden, denen viele Akteure zustimmen. Das Chemiewaffenübereinkommen beweist, dass es nicht unmöglich ist, strenge Verifikationsmaßnahmen zu ergreifen, selbst in einem Bereich, in dem ein unrechtmäßiger Einsatz möglich ist. Allerdings spielen hier auch historisch gewachsene normative Vorbehalte eine Rolle, die auf viele neue Technologien nicht zutreffen. Internationale Bestrebungen sind derzeit im Gange, zum Beispiel die Diskussion im UN-Waffenübereinkommen über tödliche autonome Waffensysteme. Auch gibt es Ansätze zur Cyber-Rüstungskontrolle, auch wenn sie noch in den Anfängen steckt. Beispielsweise gibt es Strategien zur Regulierung der für

hohe Leistung benötigten Hardware, und mit der von den Niederlanden und der Republik Korea initiierten REAIM-Konferenz beginnt sich ein internationales Forum herauszubilden, das den verantwortungsvollen Einsatz militärischer KI diskutiert.

Abdullah Kasim Korkusuz

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

Dr. Thomas Reinhold

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

Dr. Niklas Schörnig

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

Liska Suckau

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

-
- 1 Republic of Poland (2020). *National Security Strategy of the Republic of Poland*. https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf; siehe S. 7, unsere Übersetzung und Hervorhebung. Englische Originalpassage:
„Development of solutions based on fixed line and mobile broadband (5G and subsequent generations), the Internet of Things, cloud computing, quantum technologies, automation of services, machine learning, nanotechnology and artificial intelligence create new development opportunities for Poland, while generating previously unknown threats“
Siehe auch: Federal Foreign Office (2023). *Robust. Resilient. Sustainable. Integrated Security for Germany* [Nationale Sicherheitsstrategie Deutschlands]. <https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf>; S. 24 und 54.
 - 2 Europäische Union. <https://eda.europa.eu/webzine/issue22/cover-story/driven-by-global-threats-shaped-by-civil-high-tech>
 - 3 NATO. https://www.nato.int/cps/en/natohq/topics_184303.html
 - 4 Aus dem Vergleich geht jedoch hervor, dass die EDA „Weltraum- und Hyperschallsysteme“ als eine technologische Kategorie versteht, während die NATO diese beiden Kategorien trennt.
 - 5 Clapp, S. (2022). *Emerging disruptive technologies in defence*. European Parliamentary Research Service. [https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733647/EPRS_ATA\(2022\)733647_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733647/EPRS_ATA(2022)733647_EN.pdf); siehe S. 1, unsere Übersetzung.
 - 6 Europäische Union. <https://eda.europa.eu/webzine/issue22/cover-story/driven-by-global-threats-shaped-by-civil-high-tech>
 - 7 Schörnig, N. (2014). Liberal Preferences as an Explanation for Technology Choices. The Case of Military Robots as a Solution to the West's Casualty Aversion. In M. Meyer, M. Carpes, R. Knoblich (Hrsg.). *The Global Politics of Science and Technology - Vol. 2* (S. 67-82). Springer;
Csernaton, R., & Martins, B. O. (2023). Disruptive Technologies for Security and Defence: Temporality, Performativity and Imagination. *Geopolitics*, 29(3), 849–872. <https://doi.org/10.1080/14650045.2023.2224235>
 - 8 Die Reihenfolge der Länder in diesem Text richtet sich nach der alphabetischen Sortierung im Englischen.
 - 9 République Française (2022). *Nationale strategische Überprüfung*. <https://www.sgdsn.gouv.fr/files/files/rns-de-20221202.pdf>; siehe S. 10.
 - 10 République Française, 2022; siehe S. 33.
 - 11 République Française, 2022; siehe S. 26, 29, 41, 45, 53.
 - 12 République Française, 2022; siehe S. 39; République Française; siehe S. 8.
 - 13 République Française; siehe S. 25.
 - 14 Republic of Poland, 2020; siehe S. 6, unsere Übersetzung.
 - 15 Republic of Poland, 2020; siehe S. 7, unsere Übersetzung.
 - 16 Republic of Poland, 2020; siehe S. 18, unsere Übersetzung.
 - 17 Kingdom of Spain (2021). *National Security Strategy 2021*. <https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021>; siehe S. 27, unsere Übersetzung.
 - 18 Carter, A. B. (2001). Keeping the Edge. Managing Defense for the Future. In A. B. Carter & J. P. White (Hrsg.), *Keeping the Edge. Managing Defense for the Future* (S. 1–25). MIT Press.
 - 19 Shane, S. & Wakabayashi, D. (2018, 4. April). 'The Business of War': Google Employees Protest Work for the Pentagon. *The New York Times*. <https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html>
 - 20 Bergengruen, V. (2024, 8. Februar). How Tech Giants Turned Ukraine Into an AI War Lab. *Time*. <https://time.com/6691662/ai-ukraine-war-palantir/>

Biotechnologie

Dual-Use-Risiken bei der gentechnischen Veränderung von onkolytischen Viren

Bestimmte Biotechnologien können die gentechnische Veränderung von Pathogenen erleichtern und damit das Risiko großflächiger biologischer Ereignisse wie z. B. Pandemien erhöhen. In diesem Artikel wird das Dual-Use-Potenzial der gentechnischen Veränderung von Viren am Beispiel von onkolytischen Viren betrachtet und bewertet. Außerdem werden mögliche Empfehlungen für den Umgang mit den Biosicherheitsrisiken gegeben, die mit dieser Forschung verbunden sind.¹

Trotz therapeutischer Fortschritte ist Krebs nach wie vor ein bedeutendes Gesundheitsproblem. Nach Angaben der WHO gab es im Jahr 2022 schätzungsweise 20 Millionen neue Krebsfälle und 9,7 Millionen Todesfälle.² Nach der letzten Schätzung wurde bei 53,5 Millionen lebenden Menschen in den letzten fünf Jahren Krebs diagnostiziert. Etwa jeder fünfte Mensch erkrankt im Laufe seines Lebens an Krebs, und etwa jeder neunte Mann und jede zwölfte Frau stirbt an der Krankheit. Neue Ansätze für Krebstherapien werden von Regierungen in erheblichem Umfang finanziert und finden auch in der Wirtschaft Beachtung.³ Ein Bereich der Krebstherapie, der in den letzten Jahren entstanden ist, ist der Einsatz von onkolytischen Viren. Dabei handelt es sich um eine Gruppe von sich replizierenden Viren, die bevorzugt Krebszellen infizieren und abtöten.⁴ Der Einsatz von onkolytischen Viren wurde in den letzten zehn Jahren rapide ausgeweitet, und sie gelten heute als wichtige Methode der Krebsimmuntherapie.⁵ Vor 2010 wurden nur 15 klinische Studien mit onkolytischen Viren auf ClinicalTrials.gov registriert. Bis März 2024 waren es dagegen 188 Studien.⁶

Diese Therapieform entstand aus der Beobachtung heraus, dass Tumore nach einer natürlichen Virusinfektion schrumpfen. Während Viren zwar in einigen Fällen eher Krebszellen infizieren und abtöten als das normale Gewebe, waren natürliche Viren als Therapeutika zunächst nur begrenzt wirksam.⁷ Dies hat zu einer raschen Ausweitung von Forschungen geführt, in denen onkolytische Viren genetisch modifiziert werden, um ihr Wirtsspektrum oder ihre Spezifität zu verändern, gegen Krebszellen gerichtete Immunreaktionen zu verstärken und ihr lytisches Potenzial zu erhöhen. So können beispielsweise onkolytische Adenoviren so verändert werden, dass sie Proteine exprimieren, die die Apoptose, eine Form des programmierten Zelltods, verstärken.⁸

Während die gentechnische Veränderung von Viren generell für die Entwicklung wirksamer Therapeutika sehr wichtig sein kann, birgt die verstärkte Forschung an der gentechnischen Veränderung von onkolytischen Viren auch Risiken. Forscher*innen haben bereits Bedenken geäußert, dass Fortschritte in der Virustechnologie auch die Entwicklung von

manipulierten Krankheitserregern für böswilligen Missbrauch ermöglichen könnten. So wurden Dual-Use-Risiken bei der Erforschung viraler Vektoren identifiziert, bei der Viren als Träger dafür verwendet werden, Substanzen in Zielzellen zu bringen.⁹ Wenn Wissenschaftler*innen in diese Richtung forschen, sollten sie ihre Entscheidungen daher auf eine fundierte Bewertung der Wirksamkeit, Sicherheit und des Dual-Use-Potenzials stützen. Dieser Text zielt darauf ab, die mit der gentechnischen Veränderung onkolytischer Viren verbundenen Dual-Use-Risiken sorgfältig zu untersuchen, um solche Abwägungen zu unterstützen. Er identifiziert zudem risikoreiche und risikoarme Ansätze und schließt mit Empfehlungen dazu, welche Strategien angesichts der identifizierten Risiken für die Entwicklung von Therapeutika mit onkolytischen Viren am angemessensten sind.

Auswahl des Virus für die onkolytische Virotherapie

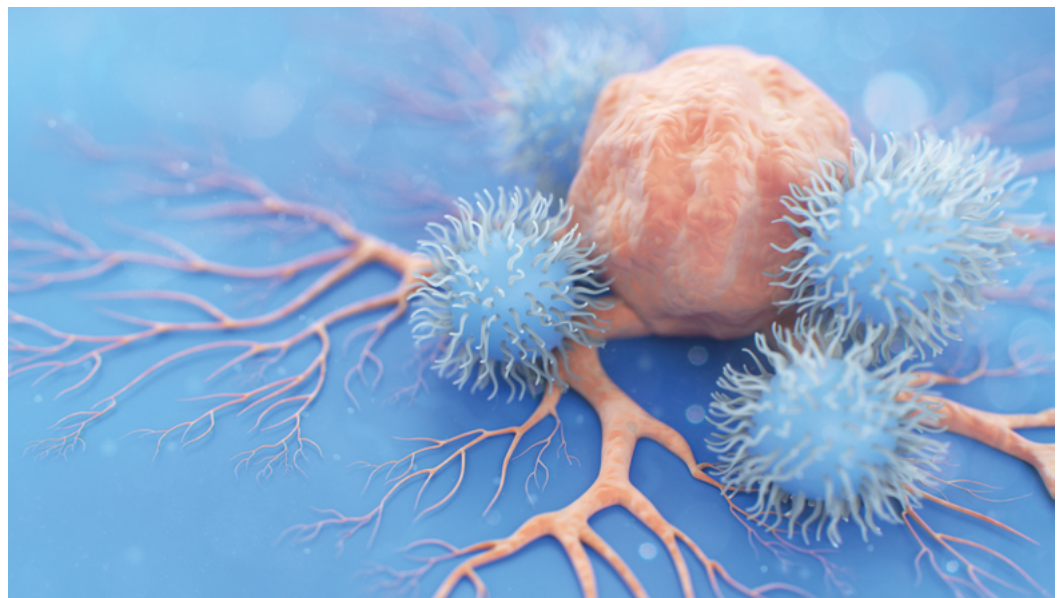
Wie groß das Dual-Use-Potenzial der Forschung an onkolytischen Viren ist, hängt davon ab, wie unmittelbar Erkenntnisse aus der viralen Genforschung auf die Krankheitserreger angewendet werden können. Daher bestimmt die Wahl der viralen Vektoren das Dual-Use-Risiko wesentlich mit. Im Gegensatz zu anderen therapeutischen Anwendungen von Viren, z. B. in der Gentherapie, ist es bei der Erforschung onkolytischer Viren besonders wahrscheinlich, dass mit Humanpathogenen verwandte Viren verwendet werden. Ein wirksames onkolytisches Virus kann sich im Menschen vermehren, krebszerstörend wirken und Immunreaktionen auslösen, die Bystander-Tumorzellen abtöten können. Zu den zehn Virusfamilien, die in klinischen Versuchen zur onkolytischen Virotherapie untersucht werden, gehören daher Hochrisikoviren wie das Influenzavirus, das Masernvirus und das Variola-Virus (siehe Tabelle 1). Influenza- und Masernviren sind beides humanpathogene Erreger, gegen die ein großer Teil der Bevölkerung geimpft ist. Erkenntnisse über die Verstärkung dieser Viren, insbesondere in Bezug auf die Eigenschaft, entscheidende Immunreaktionen zu umgehen, könnten erhebliche Risiken für die öffentliche Gesundheit mit sich bringen.

Ebenso werden mehrere Arten von Vaccinia-Viren verwendet, da sie bedeutende Vorteile aufweisen, wie z. B. die Möglichkeit der effizienten Verabreichung, intravenöse Stabilität, große Klonierungskapazität und die nachgewiesene Fähigkeit, effiziente Immunreaktionen auszulösen. Vaccinia-Viren

gehören zur Familie der Poxviridae und sind somit mit dem Variola-Virus, dem Erreger der Pocken, verwandt. Als 2018 eine Beschreibung der Synthese des Pferdepockenvirus veröffentlicht wurde, äußerten Biosicherheitsexpert*innen die Befürchtung, dass durch die Arbeit an Pockenviren wie dem Vaccinia- und dem Pferdepockenvirus auch die Fähigkeiten zur Rekonstruktion der Pocken verbreitet werden könnten. Die Arbeit an onkolytischen Viren, die auf dem Vaccinia-Virus basieren, könnte ebenfalls die Barrieren für einen Missbrauch senken.

Viraler Vektor: Modifiziertes Virus, das dazu bestimmt ist, genetisches Material in die Zellen einzuschleusen.

Bystander-Tumorzellen: Benachbarte Tumorzellen



Onkolytische Viren sind eine Gruppe von sich replizierenden Viren, die bevorzugt Krebszellen infizieren und abtöten. Bild: iStock, luismmolina.

Risikolevel des onkolytischen Virus	Eigenschaften	Beispiele
Hohes Risiko	Verwandt mit potenziell pandemischen Erregern	Orthomyxoviridae (Influenza ¹⁰), Paramyxoviridae (Masern ¹¹), NDV ¹² , Poxviridae (Vaccinia ¹³), Variola ¹⁴ , Retroviridae ¹⁵
Mittleres Risiko	Verwandt mit humanen oder tierischen Viren mit hoher Pathogenität	Picornaviridae (Polio ¹⁶), SVV ¹⁷ , Retroviridae ¹⁸ , Rhabdoviridae (VSV ¹⁹), Togaviridae ²⁰
Niedriges Risiko	Verwandt mit humanen oder tierischen Viren mit niedriger Pathogenität	Adenoviridae ²¹ , Herpesviridae (HSV-1 ²²), Parvoviridae ²³ , Reoviridae ²⁴
Niedrigstes Risiko	Nicht eigenständig von Mensch zu Mensch übertragbar	Adeno-assoziiertes Virus (AAV) ²⁵

Tabelle 1: Charakterisierung der derzeit in der Forschung mit onkolytischen Viren verwendeten Viren.

Zu den Viren mit mittlerem Risiko gehören Viren, die mit menschlichen oder tierischen Viren mit hoher Pathogenität verwandt sind, während Viren, die mit Erregern mit geringer Pathogenität verwandt sind, im Allgemeinen ein geringes Risiko aufweisen (Tabelle 1). Das geringste Risiko besteht bei Viren, die ohne Unterstützung nicht von Mensch zu Mensch übertragen werden können, wie z. B. Adeno-assoziierte Viren oder Vektorviren, die durch Bisse von Mücken, Zecken und Flöhen übertragen werden.

Risiken bei der Entwicklung übertragbarer Methoden zur Immunevasion

Virustiter: Virenkonzentration; Anzahl der Viruspartikel, die in eine Wirtszelle eindringen können.

Vorhandene neutralisierende Antikörper können den effektiven Virustiter eines onkolytischen Virus reduzieren und damit seine therapeutische Wirkung abschwächen. Um die unerwünschte Verringerung der therapeutischen Wirksamkeit zu umgehen, modifizieren Forschende Viren so, dass das Auslösen von Immunreaktionen des Wirts moduliert wird (d. h. Immunevasion). Es wurden mehrere Methoden entwickelt, um virale Oberflächenproteine mit polymeren Materialien zu maskieren, damit sie besser vor neutralisierenden Antikörpern geschützt sind und sich die Halbwertszeit der Viruszirkulation verlängert.

So werden beispielsweise Adenoviren und Herpes-simplex-Viren häufig entweder durch natürliche oder durch Impfung induzierte Immunität neutralisiert. Der Adenovirus-Serotyp 5 (Ad5) wird durch bereits vorhandene neutralisierende Antikörper erheblich eingeschränkt, was damit umgangen werden kann, dass die hypervariablen Regionen (HVRs) durch Versionen mit geringerer Immunität ersetzt werden.²⁶ Ein ähnlicher Ansatz könnte verwendet werden, um ein Adenovirus zu schaffen, das die natürliche oder impfstoffinduzierte Immunität umgehen kann.

Vererbte Ansätze, wie eine dauerhafte, an nachfolgende Virusgenerationen weitergegebene Veränderung des Virusgenoms hin zu Immunevasion, bergen erhebliche Dual-Use-Risiken, wenn sie auf Erreger mit pandemischem Potenzial übertragbar sind.

Virale Assemblierung: Während der Replikation des Virus lagern sich Proteine um die virale Nukleinsäure und bilden schließlich ein Kapsid.

Es werden außerdem zunehmend breit anwendbare Tools für die genetische Veränderung von Viren entwickelt, mit denen mehrere Viruseigenschaften gleichzeitig modifiziert werden können. Dadurch werden diese Fähigkeiten auch zunehmend für Personen ohne umfassende virologische Fachkenntnisse zugänglich. Universale Methoden der Genveränderung von Viren, die präzise Experimente ermöglichen, könnten die Hürde für die Entwicklung neuer pandemischer Erreger erheblich senken. Immer mehr Laboratorien nutzen computergestützte Methoden zur Vorhersage kritischer Loci, z. B. für die virale Assemblierung.²⁷

Ogden et al. haben beispielsweise Daten aus einer AAV(Adeno-assoziierte Viren)-Kapsid-Bibliothek verwendet, um Modelle für die gleichzeitige Optimierung mehrerer Eigenschaften zu trainieren, darunter die Virusproduktion, die Umgehung des Immunsystems, die Thermostabilität und die Verbreitung.²⁸

Um Immunreaktionen auf virale Vektoren und Transgenprodukte zu umgehen, werden diese Vektoren so verändert, dass durch Einfügen bestimmter genetischer Elemente das Auslösen von Immunreaktionen eines Wirts moduliert wird, wie an anderer Stelle beschrieben wurde.²⁹ Solche universellen Elemente für die Immunmodulation könnten besonders bedenklich sein, da sie auf jedes Virus mit ausreichender genomischer Flexibilität übertragbar sind.

(Virale) Kapsid-Bibliothek: Genomische Bibliothek, die zur Herstellung von Virus-kapsiden (den Proteinzellen der Viren) verwendet wird.

Transgenprodukt: Zelle oder Organismus, dessen Genom durch Einführung fremder DNA-Sequenz(en) verändert worden ist.

Dual-Use-Erkenntnisse aus der Erweiterung des viralen Tropismus und der Steigerung der Virulenz

Ein weiterer Forschungszweig mit Dual-Use-Bedenken ist die gentechnische Erweiterung des viralen Tropismus, d. h. die Erweiterung der Typen von Zellen, die ein bestimmtes Virus infizieren kann. Ein dichtes Tumorstroma kann die Ausbreitung, Replikation und Infektiosität von Viren einschränken. Daher arbeiten mehrere Forschungsgruppen an der Veränderung onkolytischer Viren, um ihre Fähigkeit zu optimieren, bestimmte Stroma-komponenten wie krebsassoziierte Fibroblasten (*Cancer Associated Fibroblasts*, CAFs) anzugreifen. CAFs tragen spezifische Zelloberflächenmarker, die Fibroblasten-Aktivierungsproteine (FAP),³⁰ die in vielen Tumoren hochreguliert sind, aber auch von normalen Fibroblasten verschiedener Bindegewebe exprimiert werden. Onkolytische Viren (z. B. Enadenotucirev, ein chimäres onkolytisches Adenovirus) werden so verändert, dass sie solche FAP-spezifischen Fusionsproteine tragen.³¹ Auch wenn keine böswillige Absicht vorliegt, können Viren, die auf diese Eigenschaften hin verändert wurden, Risiken bergen. So besteht die Möglichkeit einer genetischen Rekombination zwischen Impfstoffvektoren, die manipulierte Virulenzelemente tragen, und Wildtypviren,³² wie etwa zwischen onkolytischen Adenoviren und Wildtyp-Adenoviren. Diese kann zu einer unvorhergesehenen Verstärkung bestimmter Eigenschaften wie Virulenz und Immunevasion bei diesen Erregern führen.

Stroma: Teil eines Gewebes oder Organs mit einer strukturellen und/oder bindegewebigen Funktion, der aus Bindegewebe, Blutgefäßen, Lymphgefäßen und Nerven besteht.

Chimäre (Zellen): Zellen mit anderen Genen als der Rest eines Organs oder Gewebes.

Risiken bei der Entwicklung von „Plug-and-Play“-Ansätzen für das Engineering viraler Eigenschaften

In der Synthetischen Biologie wird auch an „programmierbaren“ onkolytischen Viren geforscht, d. h. an Viren, die leicht für bestimmte Zwecke entworfen und programmiert werden können.³³ Plattformen für die gezielte Evolution wurden entwickelt, um für bestimmte Zelloberflächenrezeptoren spezifische onkolytische Viren zu schaffen.³⁴

Für fast alle Virusfamilien sind Reverse-Genetik-Systeme, teilweise einschließlich öffentlich zugänglicher Schritt-für-Schritt-Protokolle, verfügbar.³⁵ Dies schafft die Voraussetzungen dafür, dass zukünftig synthetische oder natürlich vorkommende genetische Elemente und Funktionen bei einem Virus relativ einfach hinzugefügt oder entfernt werden können.³⁶ Auch versuchen Tools, die auf maschinellem Lernen basieren, die virale

Infektiosität in einem bestimmten Wirt vorherzusagen; diese Methoden könnten in hohem Maße auf andere Virusfamilien übertragbar sein.³⁷ Zwar stellen diese frühen Studien für sich genommen wahrscheinlich kein großes Risiko dar. Sie zeigen aber einen Trend zur Nutzung öffentlich verfügbarer Daten und übertragbarer Machine-Learning-Tools, um die Infektiosität von Viren mit großer Genauigkeit zu beeinflussen und vorherzusagen.

Entsprechend geht die Entwicklung allgemeiner Protokolle und Plattformen für die gentechnische Veränderung von Viren mit der Gewinnung von Erkenntnissen über virale Eigenschaften und deren Veränderung einher.³⁸ Detaillierte, öffentlich zugängliche Protokolle stellen unter bestimmten Umständen besondere Risiken dar³⁹ und „enable researchers from different research backgrounds to master the use of the reverse genetic system“.⁴⁰

Diskussion: Minderung der Dual-Use-Risiken

Aus neuen Forschungsgebieten der onkolytischen Virenthherapie ergeben sich also Dual-Use-Risiken. Den Fortschritten wohnt zwar ein erhebliches Potenzial für die Verbesserung der menschlichen Gesundheit inne, sie eröffnen aber auch Möglichkeiten für die Entwicklung biologischer Kampfstoffe. Die folgenden Erörterungen und Empfehlungen sind spekulativer Natur, da Krebsforscher*innen, die sich mit onkolytischen Viren befassen, über fundierte Kenntnisse auf diesem Gebiet verfügen und gute Gründe für ihre Entscheidungen haben. Nichtsdestotrotz sollten Forschende auf diesem Gebiet die Risiken sorgfältig abschätzen und Möglichkeiten zur Risikominderung erkunden.

Aus neuen Forschungsgebieten der onkolytischen Virenthherapie ergeben sich Dual-Use-Risiken. Forschende sollten die Risiken sorgfältig abschätzen und Möglichkeiten zur Risikominderung erkunden.

Die einfachste Möglichkeit, die Risiken der Forschung an Therapien mit onkolytischen Viren zu verringern, wäre die Arbeit mit Viren, die nicht mit potenziellen Pandemieerregern verwandt sind. Forschende, die onkolytische Viren erforschen, die durch bestehende Immunität gehemmt werden, könnten sich für nicht vererbare Methoden entscheiden, um eine Immunevasion auszulösen. So haben sich beispielsweise chemische Modifikationen von Adenoviren hierfür als nützlich erwiesen.⁴¹ Eine Alternative zu nicht vererbaren Verstärkungsmethoden ist die zunehmende Konzentration auf die medikamentöse Verabreichung immunmodulierender Stoffe, um es onkolytischen Viren zu ermöglichen, angeborene antivirale Immunreaktionen zu umgehen.⁴² Die Verwendung von Trägerzellen – Transportvehikel, die Viren vor Neutralisierung schützen – ist eine weitere risikoärmere Methode, wie onkolytische Viren effektiver in Gewebe verbracht werden können.⁴³

Wenn andere Krebstherapiestrategien ähnliche Vorteile ohne die oben beschriebenen Risiken aufweisen, könnten diese gegenüber onkolytischen Viren bevorzugt entwickelt werden. In ihrem jüngsten Jahresbericht nennt die American Society of Clinical Oncology (Amerikanische Gesellschaft für klinische Onkologie) Immun-Checkpoint-Inhibitoren und zelluläre Immuntherapien als die meistversprechenden Entwicklungen bei Immuntherapien, während die onkolytische Virotherapie nicht erwähnt wird.⁴⁴ Fortschritte bei der Erstellung von molekularen Profilen ermöglichen heute sehr gezielte, tumorspezifische Antikörpertherapien. Chimer Antigenrezeptor-T-Zelltherapien (CAR-T)⁴⁵ zeigen ebenfalls rasch Wirksamkeit und werden für verschiedene Formen von Lymphomen und anderen bösartigen Erkrankungen

zugelassen. Die bevorzugte Förderung dieser vielversprechenden Methoden könnte wirk-same Krebstherapien hervorbringen, die jedoch nicht das gleiche Dual-Use-Risiko bergen wie die Versuche, onkolytische Viren dafür zu entwickeln.

Dr. Kadri Reis

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

- 1 Danksagung: J. Sandbrink, PhD und J. Pannu, MD gaben wichtiges Feedback zu früheren Fassungen des Beitrags. Die endgültige Fassung wurde außerdem von Prof. Kathryn Nixdorff kommentiert.
- 2 WHO. (2024, 1. Februar). *Global cancer burden growing, amidst mounting need for services*. <https://www.who.int/news/item/01-02-2024-global-cancer-burden-growing-amidst-mounting-need-for-services>
- 3 The White House. (2022, 2. Februar). *Fact Sheet: President Biden Reignites Cancer Moonshot to End Cancer as We Know It* [Online post]. <https://www.whitehouse.gov/briefing-room/statements-releases/2022/02/02/fact-sheet-president-biden-reignites-cancer-moonshot-to-end-cancer-as-we-know-it/>
- 4 Patel, M. R., & Kratzke, R. A. (2013). Oncolytic virus therapy for cancer: The first wave of translational clinical trials. *Translational Research*, 161(4), 355–364. <https://doi.org/10.1016/j.trsl.2012.12.010>;
Russell, S. J., Peng, K.-W., & Bell, J. C. (2012). Oncolytic virotherapy. *Nature Biotechnology*, 30(7), 658–670. <https://doi.org/10.1038/nbt.2287>
- 5 Russell, S. J., Bell, J. C., Engeland, C. E., & McFadden, G. (2022). Advances in oncolytic virotherapy. *Communications Medicine*, 2(1), 33. <https://doi.org/10.1038/s43856-022-00098-4>
- 6 National Library of Medicine. (2024, 1. März). *ClinicalTrials.Gov*. <https://clinicaltrials.gov>
- 7 Asada, T. (1974). Treatment of human cancer with mumps virus. *Cancer*, 34(6), 1907–1928. [https://doi.org/10.1002/1097-0142\(197412\)34:6<1907::AID-CNCR2820340609>3.0.CO;2-4](https://doi.org/10.1002/1097-0142(197412)34:6<1907::AID-CNCR2820340609>3.0.CO;2-4);
Patel & Kratzke, 2013; Russell et al., 2012.
- 8 Yoon, A.-R., Hong, J., & Yun, C.-O. (2017). Adenovirus-mediated decorin expression induces cancer cell death through activation of p53 and mitochondrial apoptosis. *Oncotarget*, 8(44), 76666–76685. <https://doi.org/10.18632/oncotarget.20800>
- 9 Sandbrink, J. B., Alley, E. C., Watson, M. C., Koblentz, G. D., & Esvelt, K. M. (2022). Insidious Insights: Implications of viral vector engineering for pathogen enhancement. *Gene Therapy*. <https://doi.org/10.1038/s41434-021-00312-3>;
Sandbrink, J. B., & Koblentz, G. D. (2022). Biosecurity risks associated with vaccine platform technologies. *Vaccine*, 40(17), 2514–2523. <https://doi.org/10.1016/j.vaccine.2021.02.023>
- 10 Yang, H., Lei, G., Sun, F., Cheng, J., Yan, J., Zhang, S., & Yang, P. (2022). Oncolytic Activity of a Chimeric Influenza A Virus Carrying a Human CTLA4 Antibody in Hepatocellular Carcinoma. *Frontiers in Oncology*, 12, 875525. <https://doi.org/10.3389/fonc.2022.875525>
- 11 Msaouel, P., Opyrchal, M., Dispenzieri, A., Peng, K. W., Federspiel, M. J., Russell, S. J., & Galanis, E. (2018). Clinical Trials with Oncolytic Measles Virus: Current Status and Future Prospects. *Current Cancer Drug Targets*, 18(2), 177–187. <https://doi.org/10.2174/1568009617666170222125035>
- 12 Schulze, T., Kemmner, W., Weitz, J., Wernecke, K.-D., Schirrmacher, V., & Schlag, P. M. (2009). Efficiency of adjuvant active specific immunization with Newcastle disease virus modified tumor cells in colorectal cancer patients following resection of liver metastases: Results of a prospective randomized trial. *Cancer Immunology, Immunotherapy*, 58(1), 61–69. <https://doi.org/10.1007/s00262-008-0526-1>
- 13 Heo, J., Reid, T., Ruo, L., Breitbach, C. J., Rose, S., Bloomston, M., Cho, M., Lim, H. Y., Chung, H. C., Kim, C. W., Burke, J., Lencioni, R., Hickman, T., Moon, A., Lee, Y. S., Kim, M. K., Daneshmand, M., Dubois, K., Longpre, L., ... Kirn, D. H. (2013). Randomized dose-finding clinical trial of oncolytic immunotherapeutic vaccinia JX-594 in liver cancer. *Nature Medicine*, 19(3), 329–336. <https://doi.org/10.1038/nm.3089>
- 14 Ricordel, M., Foloppe, J., Pichon, C., Sfrontato, N., Antoine, D., Tosch, C., Cochlin, S., Cordier, P., Quemeneur, E., Camus-Bouclainville, C., Bertagnoli, S., & Erbs, P. (2017). Cowpox Virus: A New and Armed Oncolytic Poxvirus. *Molecular Therapy - Oncolytics*, 7, 1–11. <https://doi.org/10.1016/j.omto.2017.08.003>
- 15 Li, F., Guo, Y., Han, L., Duan, Y., Fang, F., Niu, S., Ba, Q., Zhu, H., Kong, F., Lin, C., & Wen, X. (2012). In vitro and in vivo growth inhibition of drug-resistant ovarian carcinoma cells using a combination of cisplatin and a TRAIL-encoding retrovirus. *Oncology Letters*, 4(6), 1254–1258. <https://doi.org/10.3892/ol.2012.926>

- 16 Toyoda, H., Ido, M., Hayashi, T., Gabazza, E. C., Suzuki, K., Kisenge, R. R., Kang, J., Hori, H., & Komada, Y. (2004). Experimental treatment of human neuroblastoma using live-attenuated poliovirus. *International Journal of Oncology*, 24(1), 49–58.
- 17 Reddy, P. S., Burroughs, K. D., Hales, L. M., Ganesh, S., Jones, B. H., Idamakanti, N., Hay, C., Li, S. S., Skele, K. L., Vasko, A.-J., Yang, J., Watkins, D. N., Rudin, C. M., & Hallenbeck, P. L. (2007). Seneca Valley Virus, a Systemically Deliverable Oncolytic Picornavirus, and the Treatment of Neuroendocrine Cancers. *JNCI: Journal of the National Cancer Institute*, 99(21), 1623–1633. <https://doi.org/10.1093/jnci/djm198>
- 18 Tai, C.-K. (2012). Replicating retroviral vectors for oncolytic virotherapy of experimental hepatocellular carcinoma. *Oncology Reports*. <https://doi.org/10.3892/or.2012.1789>
- 19 Muik, A., Dold, C., Geiß, Y., Volk, A., Werbizki, M., Dietrich, U., & von Laer, D. (2012). Semireplication-competent vesicular stomatitis virus as a novel platform for oncolytic virotherapy. *Journal of Molecular Medicine*, 90(8), 959–970. <https://doi.org/10.1007/s00109-012-0863-6>
- 20 Cai, J., & Yan, G. (2021). The Identification and Development of a Novel Oncolytic Virus: Alphavirus M1. *Human Gene Therapy*, 32(3–4), 138–149. <https://doi.org/10.1089/hum.2020.271>
- 21 Kirn, D. (2000). Replication-selective oncolytic adenoviruses: Virotherapy aimed at genetic targets in cancer. *Oncogene*, 19(56), 6660–6669. <https://doi.org/10.1038/sj.onc.1204094>; Zhao, Y., Liu, Z., Li, L., Wu, J., Zhang, H., Zhang, H., Lei, T., & Xu, B. (2021). Oncolytic Adenovirus: Prospects for Cancer Immunotherapy. *Frontiers in Microbiology*, 12, 707290. <https://doi.org/10.3389/fmicb.2021.707290>
- 22 Harrington, K. J., Puzanov, I., Hecht, J. R., Hodi, F. S., Szabo, Z., Murugappan, S., & Kaufman, H. L. (2015). Clinical development of talimogene laherparepvec (T-VEC): A modified herpes simplex virus type-1–derived oncolytic immunotherapy. *Expert Review of Anticancer Therapy*, 15(12), 1389–1403. <https://doi.org/10.1586/14737140.2015.1115725>; Masoud, S. J., Hu, J. B., Beasley, G. M., Stewart, J. H., & Mosca, P. J. (2019). Efficacy of Talimogene Laherparepvec (T-VEC) Therapy in Patients with In-Transit Melanoma Metastasis Decreases with Increasing Lesion Size. *Annals of Surgical Oncology*, 26(13), 4633–4641. <https://doi.org/10.1245/s10434-019-07691-3>
- 23 Marchini, A., Bonifati, S., Scott, E. M., Angelova, A. L., & Rommelaere, J. (2015). Oncolytic parvoviruses: From basic virology to clinical applications. *Virology Journal*, 12(1), 6. <https://doi.org/10.1186/s12985-014-0223-y>
- 24 Samson, A., Scott, K. J., Taggart, D., West, E. J., Wilson, E., Nuovo, G. J., Thomson, S., Corns, R., Mathew, R. K., Fuller, M. J., Kottke, T. J., Thompson, J. M., Ilett, E. J., Cockle, J. V., van Hille, P., Sivakumar, G., Polson, E. S., Turnbull, S. J., Appleton, E. S., ... Melcher, A. A. (2018). Intravenous delivery of oncolytic reovirus to brain tumor patients immunologically primes for subsequent check-point blockade. *Science Translational Medicine*, 10(422), eaam7577. <https://doi.org/10.1126/scitranslmed.aam7577>
- 25 Pan, J. G., Zhou, X., Zeng, G. W., & Han, R. F. (2012). Potent antitumour activity of the combination of HSV-TK and endostatin armed oncolytic adeno-associated virus for bladder cancer in vitro and in vivo. *Journal of Surgical Oncology*, 105(3), 249–257. <https://doi.org/10.1002/jso.22107>
- 26 Roberts, D. M., Nanda, A., Havenga, M. J. E., Abbink, P., Lynch, D. M., Ewald, B. A., Liu, J., Thorner, A. R., Swanson, P. E., Gorgone, D. A., Lifton, M. A., Lemckert, A. A. C., Holterman, L., Chen, B., Dilraj, A., Carville, A., Mansfield, K. G., Goudsmit, J., & Barouch, D. H. (2006). Hexon-chimaeric adenovirus serotype 5 vectors circumvent pre-existing anti-vector immunity. *Nature*, 441(7090), 239–243. <https://doi.org/10.1038/nature04721>
- 27 Marques, A. D., Kummer, M., Kondratov, O., Banerjee, A., Moskalenko, O., & Zolotukhin, S. (2021). Applying machine learning to predict viral assembly for adeno-associated virus capsid libraries. *Molecular Therapy - Methods & Clinical Development*, 20, 276–286. <https://doi.org/10.1016/j.omtm.2020.11.017>
- 28 Ogden, P. J., Kelsic, E. D., Sinai, S., & Church, G. M. (2019). Comprehensive AAV capsid fitness landscape reveals a viral gene and enables machine-guided design. *Science*, 366(6469), 1139–1143. <https://doi.org/10.1126/science.aaw2900>
- 29 Sandbrink, J. B., Alley, E. C., Watson, M. C., Koblenz, G. D., & Esvelt, K. M. (2022). Insidious Insights: Implications of viral vector engineering for pathogen enhancement. *Gene Therapy*. <https://doi.org/10.1038/s41434-021-00312-3>
- 30 Rettig, W. J., Chesa, P. G., Beresford, H. R., Feickert, H.-J., Jennings, M. T., Cohen, J., Oettgen, H. F., & Old, L. J. (1986). Differential expression of cell surface antigens and glial fibrillary acidic protein in human astrocytoma subsets. *Cancer Research*, 46(12 Part_1), 6406–6412.
- 31 Freedman, J. D., Duffy, M. R., Lei-Rossmann, J., Muntzer, A., Scott, E. M., Hagel, J., Campo, L., Bryant, R. J., Verrill, C., Lambert, A., Miller, P., Champion, B. R., Seymour, L. W., & Fisher, K. D. (2018). An Oncolytic Virus Expressing a T-cell Engager Simultaneously Targets Cancer and Immunosuppressive Stromal Cells. *Cancer Research*, 78(24), 6852–6865. <https://doi.org/10.1158/0008-5472.CAN-18-1750>
- 32 Baldo, A., Leunda, A., Willemarck, N., & Pauwels, K. (2021). Environmental Risk Assessment of Recombinant Viral Vector Vaccines against SARS-Cov-2. *Vaccines*, 9(5), 453. <https://doi.org/10.3390/vaccines9050453>
- 33 Monie, D. D., Bhandarkar, A. R., Parney, I. F., Correia, C., Sarkaria, J. N., Vile, R. G., & Li, H. (2021). Synthetic and systems biology principles in the design of programmable oncolytic virus immunotherapies for glioblastoma. *Neurosurgical Focus*, 50(2), E10. <https://doi.org/10.3171/2020.12.FOCUS20855>

- Twumasi-Boateng, K., Pettigrew, J. L., Kwok, Y. Y. E., Bell, J. C., & Nelson, B. H. (2018). Oncolytic viruses as engineering platforms for combination immunotherapy. *Nature Reviews Cancer*, 18(7), 419–432. <https://doi.org/10.1038/s41568-018-0009-4>
- 34 Dai, H.-S., Liu, Z., Jiang, W., & Kuhn, R. J. (2013). Directed Evolution of a Virus Exclusively Utilizing Human Epidermal Growth Factor Receptor as the Entry Receptor. *Journal of Virology*, 87(20), 11231–11243. <https://doi.org/10.1128/JVI.01054-13>
- 35 Pannu, J., Sandbrink, J. B., Watson, M., Palmer, M. J., & Relman, D. A. (2022). Protocols and risks: When less is more. *Nature Protocols*, 17(1), 1–2. <https://doi.org/10.1038/s41596-021-00655-6>; Xie, X., Lokugamage, K. G., Zhang, X., Vu, M. N., Muruato, A. E., Menachery, V. D., & Shi, P.-Y. (2021). Engineering SARS-CoV-2 using a reverse genetic system. *Nature Protocols*, 16(3), 1761–1784. <https://doi.org/10.1038/s41596-021-00491-8>
- 36 Maroun, J., Muñoz-Alía, M., Ammayappan, A., Schulze, A., Peng, K.-W., & Russell, S. (2017). Designing and building oncolytic viruses. *Future Virology*, 12(4), 193–213. <https://doi.org/10.2217/fvl-2016-0129>
- 37 Karabulut, O. C., Karpuzcu, B. A., Türk, E., Ibrahim, A. H., & Sözek, B. E. (2021). ML-AdVInfect: A Machine-Learning Based Adenoviral Infection Predictor. *Frontiers in Molecular Biosciences*, 8, 647424. <https://doi.org/10.3389/fmolb.2021.647424>
- 38 Sandbrink, J. B., & Koblenz, G. D. (2022). Biosecurity risks associated with vaccine platform technologies. *Vaccine*, 40(17), 2514–2523. <https://doi.org/10.1016/j.vaccine.2021.02.023>
- 39 Pannu, J., Sandbrink, J. B., Watson, M., Palmer, M. J., & Relman, D. A. (2022). Protocols and risks: When less is more. *Nature Protocols*, 17(1), 1–2. <https://doi.org/10.1038/s41596-021-00655-6>
- 40 Xie, X., Lokugamage, K. G., Zhang, X., Vu, M. N., Muruato, A. E., Menachery, V. D., & Shi, P.-Y. (2021). Engineering SARS-CoV-2 using a reverse genetic system. *Nature Protocols*, 16(3), 1761–1784. <https://doi.org/10.1038/s41596-021-00491-8>
- 41 Weaver, E. A., & Barry, M. A. (2008). Effects of Shielding Adenoviral Vectors with Polyethylene Glycol on Vector-Specific and Vaccine-Mediated Immune Responses. *Human Gene Therapy*, 19(12), 1369–1382. <https://doi.org/10.1089/hum.2008.091>
- 42 Arulanandam, R., Batenchuk, C., Varette, O., Zakaria, C., Garcia, V., Forbes, N. E., Davis, C., Krishnan, R., Karmacharya, R., Cox, J., Sinha, A., Babawy, A., Waite, K., Weinstein, E., Falls, T., Chen, A., Hamill, J., De Silva, N., Conrad, D. P., ... Diallo, J.-S. (2015). Microtubule disruption synergizes with oncolytic virotherapy by inhibiting interferon translation and potentiating bystander killing. *Nature Communications*, 6(1), 6410. <https://doi.org/10.1038/ncomms7410>; Diallo, J.-S., Boeuf, F. L., Lai, F., Cox, J., Vaha-Koskela, M., Abdelbary, H., MacTavish, H., Waite, K., Falls, T., Wang, J., Brown, R., Blanchard, J. E., Brown, E. D., Kirn, D. H., Hiscott, J., Atkins, H., Lichty, B. D., & Bell, J. C. (2010). A High-throughput Pharmacoviral Approach Identifies Novel Oncolytic Virus Sensitizers. *Molecular Therapy*, 18(6), 1123–1129. <https://doi.org/10.1038/mt.2010.67>; Dornan, M. H., Krishnan, R., Macklin, A. M., Selman, M., El Sayes, N., Son, H. H., Davis, C., Chen, A., Keillor, K., Le, P. J., Moi, C., Ou, P., Pardin, C., Canez, C. R., Le Boeuf, F., Bell, J. C., Smith, J. C., Diallo, J.-S., & Boddy, C. N. (2016). First-in-class small molecule potentiators of cancer virotherapy. *Scientific Reports*, 6(1), 26786. <https://doi.org/10.1038/srep26786>
- 43 Kim, J., Hall, R., Lesniak, M., & Ahmed, A. (2015). Stem Cell-Based Cell Carrier for Targeted Oncolytic Virotherapy: Translational Opportunity and Open Questions. *Viruses*, 7(12), 6200–6217. <https://doi.org/10.3390/v7122921>; Power, A. T., Wang, J., Falls, T. J., Paterson, J. M., Parato, K. A., Lichty, B. D., Stojdl, D. F., Forsyth, P. A. J., Atkins, H., & Bell, J. C. (2007). Carrier Cell-based Delivery of an Oncolytic Virus Circumvents Antiviral Immunity. *Molecular Therapy*, 15(1), 123–130. <https://doi.org/10.1038/sj.mt.6300039>
- 44 Smith, S. M., Wachter, K., III, H. A. B., Schilsky, R. L., George, D. J., Peterson, D. E., Johnson, M. L., Markham, M. J., Mileham, K. F., Beg, M. S., Bendell, J. C., Dreicer, R., Keedy, V. L., Kimple, R. J., Knoll, M. A., LoConte, N., MacKay, H., Meisel, J. L., Moynihan, T. J., ... Uzzo, R. (2021). Clinical Cancer Advances 2021: ASCO's Report on Progress Against Cancer. *Journal of Clinical Oncology*. <https://doi.org/10.1200/JCO.20.03420>
- 45 Sadelain, M., Brentjens, R., & Rivière, I. (2013). The Basic Principles of Chimeric Antigen Receptor Design. *Cancer Discovery*, 3(4), 388–398. <https://doi.org/10.1158/2159-8290.CD-12-0548>

ANHANG

Internationale Verträge im Zusammenhang mit der Abrüstung und Nichtverbreitung biologischer Waffen

Das Genfer Protokoll von 1925

Das „Protokoll über das Verbot der Verwendung von erstickenden, giftigen oder ähnlichen Gasen sowie von bakteriologischen Mitteln im Kriege“, üblicherweise als Genfer Protokoll von 1925¹ bezeichnet, verbietet den Einsatz chemischer und biologischer Waffen in Kriegen zwischen seinen Vertragsparteien. Im August 2024 hatte das Genfer Protokoll 146 Mitglieder. Mit der Unterzeichnung erklärten viele Vertragsparteien, dass sie sich gegenüber Staaten, die dessen Bestimmungen nicht einhalten, nicht mehr an das Protokoll gebunden fühlen würden, und behielten sich damit de facto das Recht vor, mit gleichen Mitteln Vergeltung zu üben. Das Verbot des Einsatzes von chemischen und biologischen Waffen hat sich jedoch zu einer völkergewohnheitsrechtlichen Norm entwickelt, d. h., es gilt heute universell für alle Staaten und in internationalen sowie innerstaatlichen Konflikten.²

Deutschland unterzeichnete das Protokoll am 17. Juni 1925 und ratifizierte es am 25. April 1929. Es hat seine Mitgliedschaft zu keinem Zeitpunkt mit Vorbehalten verbunden.

Biowaffen-Übereinkommen

Das „Übereinkommen über das Verbot der Entwicklung, Herstellung und Lagerung bakteriologischer (biologischer) Waffen und von Toxinwaffen sowie über die Vernichtung solcher Waffen“ (Biowaffen-Übereinkommen, BWÜ)³ ist der älteste internationale Abrüstungsvertrag, der eine ganze Waffenkategorie verbietet.⁴ Es wurde 1972 zur Unterschrift aufgelegt und trat 1975 in Kraft. Im August 2024 waren ihm 187 Staaten beigetreten. Das BWÜ verbietet uneingeschränkt die Entwicklung, die Herstellung, den Besitz, den Erwerb, das Zurückbehalten und die Weitergabe biologischer Waffen. Es verpflichtet seine Mitglieder außerdem, die Verbreitung von biologischen Waffenmaterialien zu verhindern, die internationale Zusammenarbeit bei der friedlichen Nutzung von Biologie und Biotechnologie zu fördern und die Vertragsbestimmungen in nationales Recht umzusetzen. Biologische Forschung wurde nicht in das BWÜ aufgenommen, vermutlich weil der Dual-Use-Charakter eines großen Teils der biologischen Forschung und der Biotechnologie sowie die enge Verflechtung mit Fragen der öffentlichen Gesundheit es unmöglich gemacht hätten, bestimmte Forschungen pauschal zu verbieten oder einzuschränken, da

dies auch legitime und nützliche Forschungsaktivitäten einschränken könnte.⁵

Als biologische Waffen bezeichnet man mikrobiologische oder andere biologische Agenzien oder Toxine „von Arten und in Mengen, die nicht durch Vorbeugungs-, Schutz- oder sonstige friedliche Zwecke gerechtfertigt sind“, sowie „Waffen, Ausrüstungen oder Einsatzmittel, die für die Verwendung solcher Agenzien oder Toxine die für feindselige Zwecke oder in einem bewaffneten Konflikt bestimmt sind“ (BWÜ Artikel I). Das Verbot ist also umfassend und nicht über bestimmte biologische Agenzien oder Arten von Trägersystemen, sondern über die Anwendungsabsicht für biologische Waffenzwecke definiert (Allgemeines Zweckkriterium). Dies bedeutet, dass auch neue wissenschaftliche und technologische Entwicklungen automatisch vom BWÜ abgedeckt werden.

Das BWÜ sieht keine Maßnahmen dafür vor, die Einhaltung seiner Bestimmungen zu überprüfen. Bemühungen, ein Verifikationssystem hinzuzufügen, schlugen 2001 fehl, und das Thema wurde erst vor kurzem wieder auf die offizielle BWÜ-Agenda gesetzt. Auf der 9. BWÜ-Überprüfungskonferenz im Jahr 2022 einigten sich die Vertragsstaaten darauf, eine neue Arbeitsgruppe einzurichten, deren Mandat es ist, konkrete und wirksame Maßnahmen, einschließlich möglicher rechtlich verbindlicher Maßnahmen, zu identifizieren und auszuarbeiten, um den Vertragsstaaten entsprechende Vorschläge zur Stärkung und Institutionalisierung des BWÜ zur weiteren Befassung vorzulegen.⁶ Neben Verifikation und Compliance behandelt die Arbeitsgruppe folgende Themen: internationale Zusammenarbeit und Unterstützung (*International Cooperation and Assistance*); nationale Implementierung (*National Implementation*); Unterstützung, Reaktion und Vorsorge (*Assistance, Response and Preparedness*); organisatorische, institutionelle und finanzielle Angelegenheiten (*Organizational, Institutional and Financial Matters*); Vertrauensbildung und Transparenz (*Confidence-Building and Transparency*) sowie wissenschaftliche und technologische Entwicklungen (*Scientific and Technological Development*).

Neue Entwicklungen in der Biologie und Biotechnologie bieten sowohl Chancen als auch Herausforderungen für das BWÜ und für die internationalen Bemühungen, es zu stärken. Einige Fortschritte in diesen und anderen einschlägigen wissenschaftlichen Disziplinen (wie etwa der KI) könnten dafür genutzt werden, den Schutz vor Biowaffen zu verbessern oder die Verifikation des BWÜ zu erleichtern. Einige Materialien und Technologien könnten jedoch auch für illegitime und feindselige Zwecke missbraucht werden oder die Hürden für die Entwicklung und den Erwerb biologischer Waffen senken. Die Bedeutung wissenschaftlicher Fortschritte wurde bereits bei der Aushandlung des BWÜ erkannt, und die Beobachtung relevanter

wissenschaftlicher und technologischer Entwicklungen wurde als Aufgabe für die BWÜ-Überprüfungskonferenz in Artikel XII des Übereinkommens festgeschrieben. Während diese Aufgabe bisher nie systematisch ausgeführt wurde, ist die BWÜ-Arbeitsgruppe nun damit befasst, den Vertragsstaaten Empfehlungen zur Einrichtung eines „Mechanismus zur Überprüfung und Bewertung wissenschaftlicher und technologischer Entwicklungen, die für das Übereinkommen relevant sind, und zur Bereitstellung relevanter Beratung für die Vertragsstaaten“ vorzulegen.⁷ Würde ein solcher Mechanismus eingerichtet, könnten damit wissenschaftliche und technologische Entwicklungen beobachtet, analysiert und bewertet werden. Dies könnte den Vertragsstaaten helfen, potenzielle Risiken zu erkennen und zu mindern, wie etwa Risiken, die sich aus der (besorgniserregenden) Dual-Use-Forschung ergeben. Der Mechanismus könnte auch dabei helfen, mögliche sich aus technologischen Entwicklungen ergebende Chancen für eine bessere Vorsorge für Krankheitsausbrüche jeglichen Ursprungs und für die Stärkung des BWÜ als Ganzes zu nutzen.

Zwar nimmt das BWÜ selbst weder Bezug auf Bioterrorismus noch auf Biosicherheit und Gesundheitsvorsorge, diese Themen sind aber in den letzten 20 Jahren in den BWÜ-Diskurs eingegangen und sind nun integraler Bestandteil der Diskussionen. Nicht alle damit verbundenen Definitionen und Auffassungen sind jedoch unter den BWÜ-Mitgliedern Konsens. Die diskursive Verschiebung hat das BWÜ dennoch in den Mittelpunkt eines größeren Maßnahmenpakets zur Minderung biologischer Risiken gerückt, wobei das Spektrum solcher Risiken von natürlichen Krankheitsausbrüchen über die versehentliche Freisetzung biologischer Agenzien und den vorsätzlichen Einsatz biologischer Stoffe für kriminelle oder terroristische Zwecke bis zum Einsatz biologischer Waffen durch Staaten reicht.

Deutschland unterzeichnete das BWÜ am 10. April 1972 und ratifizierte es am 7. April 1983.

Dr. Una Jakob

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

E. Myjers. (Hg.), *Research Handbook on Arms Control Law* (S. 258–277). Cheltenham: Edward Elgar.

- 5 „Dual Use“ bezeichnet hier die Möglichkeit, dass legitime biologische Forschung, Technologien, Materialien oder Geräte für unfriedliche Zwecke – u. a. für Waffenzwecke – missbraucht werden könnten. Dual-Use-Forschung meint Experimente, die zwar nützlichen Zwecken dienen, deren Ergebnisse aber missbraucht werden könnten. Besorgniserregende Dual-Use-Forschung (engl. *Dual Use Research of Concern*, DURC) bezieht sich gemeinhin auf Forschung, deren Missbrauchspotenzial besonders groß und unmittelbar gegeben ist.
- 6 Vereinte Nationen. (2022, 22. Dezember). *Final Document of the Ninth Review Conference* (BWC/CONF.IX/9). Vereinte Nationen. <https://undocs.org/BWC/CONF.IX/9>
- 7 Vereinte Nationen, 2022; S. 11.

Andere Instrumente zur Unterstützung der Abrüstung und Nichtverbreitung biologischer und chemischer Waffen

UN-Generalsekretärsmechanismus

1987 ermächtigte die UN-Generalversammlung den UN-Generalsekretär durch die Resolution 42/37C der Generalversammlung,¹ mutmaßliche Einsätze biologischer oder chemischer Waffen zu untersuchen. Damit wurde der „UN Secretary-General’s Mechanism for Investigation of Alleged Use of Chemical and Biological Weapons“ (UNSGM)² eingerichtet. Der UNSGM basiert rechtlich auf dem Genfer Protokoll von 1925 sowie einschlägigen völkergewohnheitsrechtlichen Regeln und ist derzeit der einzige internationale Mechanismus zur Untersuchung vermuteter Biowaffeneinsätze.

Wenn ein UN-Mitglied eine UNSGM-Untersuchung beantragt und der UN-Generalsekretär feststellt, dass genügend Beweise vorliegen, um eine solche Untersuchung zu rechtfertigen, kann er oder sie auf bestehende Listen mit von UN-Mitgliedsstaaten benannten Expert*innen und Labors zurückgreifen und kurzfristig ein Untersuchungsteam entsenden. Dieses hätte die Aufgabe festzustellen, ob tatsächlich chemische oder biologische Waffen eingesetzt wurden. Der Mechanismus ist politisch unabhängig und untersteht ausschließlich dem UN-Generalsekretär; der UN-Sicherheitsrat hat bei der Untersuchung keine formelle Rolle.

1 <https://treaties.unoda.org/t/1925>

2 Henckaerts, J. & Doswald-Beck, L. (2005). *Customary International Humanitarian Law, Volume I: Rules*. International Committee of the Red Cross (ICRC). Cambridge University Press. <https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf>

3 <https://treaties.unoda.org/t/bwc>

4 Für eine Analyse des BWÜ-Regimes s: Jakob, U. (2022). The Biological Weapons Convention. In T. Marauhn, &

Deutschland ist Mitglied der „Gruppe der Freunde des UNSGM“ und einer der aktivsten Unterstützer der Bemühungen zur Stärkung des Mechanismus.

UN-Sicherheitsresolution 1540 (2004)

Im Jahr 2004 verabschiedete der UN-Sicherheitsrat die Resolution 1540,³ die alle UN-Mitglieder verpflichtet, die erforderlichen Maßnahmen zu ergreifen, um die Verbreitung nuklearer, biologischer oder chemischer (ABC-)Waffen und ihrer Trägersysteme an nichtstaatliche Akteure zu verhindern und über ihre Umsetzung der Resolution zu berichten. Die Resolution wurde seitdem mehrmals verlängert, zuletzt 2022 für einen Zeitraum von zehn Jahren.⁴ Zu den von den UN-Mitgliedern zu ergreifenden Maßnahmen gehören die Verabschiedung und Durchsetzung nationaler Gesetze, um nichtstaatliche Akteure an der Entwicklung oder dem Erwerb von ABC-Waffen zu hindern, nationale physische Schutzmaßnahmen für relevante ABC-Materialien sowie wirksame Grenz- und Transferkontrollen. Um die Umsetzung der Resolution 1540 zu unterstützen, wurde eigens das sogenannte „1540 Committee“ eingerichtet; unter anderem verwaltet es die nationalen Berichte und bietet den UN-Mitgliedern Hilfestellung bei der Implementierung der Resolution.

Deutschland hat die Resolution 1540 umgesetzt und fünf Berichte vorgelegt, den letzten im Jahr 2020.⁵

Sanktionen und Exportkontrollen

Staaten können verschiedene nationale und internationale Maßnahmen ergreifen, um die Verbreitung von Materialien, Ausrüstung und Technologien, die zur Entwicklung und Herstellung biologischer oder chemischer Waffen verwendet werden könnten, an Staaten oder nichtstaatliche Akteure zu verhindern. Dazu zählen unter anderem Sanktionen sowie nationale und international koordinierte Exportkontrollen.

Nach Kapitel VII der UN-Charta⁶ kann der UN-Sicherheitsrat Sanktionen gegen Akteure verhängen, die den Weltfrieden und die internationale Sicherheit gefährden. Der UN-Sicherheitsrat hat wiederholt festgestellt,⁷ dass die Verbreitung von nuklearen, chemischen und biologischen Waffen eine solche Gefährdung darstellt. Derzeit gibt es ein Sanktionsregime des Sicherheitsrats, das sich auch auf biologische Waffen bezieht: das Sanktionsregime gegen Nordkorea.⁸ Die Umsetzung dieser Sanktionen ist für alle UN-Mitgliedstaaten verpflichtend. Darüber hinaus gibt es auch unilaterale Sanktionen im Zusammenhang mit biologischen und chemischen Waffen gegen andere Staaten. So haben etwa die USA⁹ Sanktionen gegen Russland¹⁰ sowie gegen den Iran, Nordkorea und Syrien¹¹ verhängt, und die EU¹² hat ein Sanktionsregime im Zusammenhang mit dem Einsatz und der Verbreitung chemischer Waffen eingerichtet.

Exportkontrollen sind eine wichtige Maßnahme zur Umsetzung der Nichtverbreitungsverpflichtungen, die sich aus Artikel IV des BWÜ und der Resolution 1540 ergeben. Es gibt kein globales Exportkontrollregime im Zusammenhang mit biologischen Waffen. Vielmehr liegt die Kontrolle der entsprechenden Ausfuhren in der Verantwortung der einzelnen Staaten. Die Australische Gruppe und das EU-Exportkontrollregime für Güter mit doppeltem Verwendungszweck sind jedoch zwei Beispiele für multilateral koordinierte Maßnahmenpakete zur Exportkontrolle.

Die Australische Gruppe (AG)¹³ ist eine informelle Vereinbarung, in der 42 Länder und die EU auf der Grundlage gemeinsamer Kontrolllisten zusammenarbeiten, um ihre Exportkontrollen für Substanzen, Materialien, Ausrüstung und Technologien zu harmonisieren, die zur Herstellung biologischer oder chemischer Waffen verwendet werden könnten. Die AG wurde 1985 gegründet, nachdem bekannt geworden war, dass der Irak seine chemischen Waffen, die er in den 1980er Jahren im Iran-Irak-Krieg gegen den Iran einsetzte, teilweise mithilfe legaler Chemieexporte gebaut hatte. Biowaffenbezogene Güter wurden 1991 in die Kontrolllisten¹⁴ der Gruppe aufgenommen. Sie umfassen Listen für „Ausrüstungen zur Handhabung von biologischem Material, zugehörige Technologie und Software“, „Human- und Tierpathogen und Toxine“ und „Pflanzenpathogene“. Die Mitgliedschaft in der AG ist grundsätzlich für weitere Staaten möglich, sofern sie eine Reihe von Kriterien erfüllen, die auf der Website der AG aufgeführt sind, und sofern alle derzeitigen AG-Mitglieder zustimmen. Die AG wird kontrovers diskutiert: Während ihre Mitglieder die Existenz der Gruppe mit Verweis auf die Nichtverbreitungsverpflichtungen aus dem BWÜ, dem Chemiewaffenübereinkommen (CWÜ) und der Resolution 1540 rechtfertigen, kritisieren andere Staaten, dass die Gruppe diskriminierend sei und die wirtschaftliche und technologische Entwicklung in anderen Ländern durch die Einschränkung legitimer Transfers behindere.

Die EU hat 2021 mit der Verordnung (EU) 2021/821 (zuletzt geändert 2023)¹⁵ ein Kontrollregime für den Transfer von Gütern mit doppeltem Verwendungszweck eingerichtet, zu denen auch biologische und biowaffenrelevante Güter gehören. Es bezieht sich ebenfalls ausdrücklich auf das BWÜ, das CWÜ und die Resolution 1540 und verpflichtet alle EU-Mitglieder, Transferkontrollen für Güter einzuführen, die als Güter mit doppeltem Verwendungszweck gelten und in Anhang I der Verordnung aufgeführt sind. „Dual Use“ wird in Kapitel 1, Artikel 2 Absatz 1 der Verordnung wie folgt definiert: „Güter, einschließlich Datenverarbeitungsprogramme (Software) und Technologie, die sowohl für zivile als auch für militärische Zwecke verwendet werden können; darin eingeschlossen sind Güter, die zur Konstruktion, Entwicklung, Herstellung oder zum Einsatz von nuklearen, chemischen oder biologischen Waffen oder deren Trägersystemen verwendet werden können, einschließlich aller Güter, die so-

wohl für nichtexplosive Zwecke als auch für jedwede Form der Unterstützung bei der Herstellung von Kernwaffen oder sonstigen Kernsprengkörpern verwendet werden können.“

Deutschland setzt die vom UN-Sicherheitsrat verhängten Sanktionen sowie die von der EU erlassenen Sanktionen und Dual-Use-Exportbestimmungen im Rahmen seiner Verpflichtungen als Mitglied der UN und der EU um. Darüber hinaus ist Deutschland Gründungsmitglied der Australischen Gruppe. Die für die Umsetzung der deutschen Exportkontrollpolitik zuständige Behörde ist das Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA).¹⁶

Dr. Una Jakob

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

- 1 <https://undocs.org/Home/Mobile?FinalSymbol=a%2Fres%2F42%2F37&Language=E&DeviceType=Desktop&LangRequested=False>
- 2 <https://disarmament.unoda.org/wmd/secretary-general-mechanism/>
- 3 [https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1540%2520\(2004\)&Language=E&DeviceType=Desktop&LangRequested=False](https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1540%2520(2004)&Language=E&DeviceType=Desktop&LangRequested=False)
- 4 Sicherheitsrat der Vereinten Nationen. (2022, 30. November). *Resolution 2663 (2022) (S/RES/2663)*. Vereinte Nationen.
- 5 <https://www.un.org/en/sc/1540/documents/Germany-Report20Mar2020.pdf>
- 6 <https://www.un.org/en/about-us/un-charter/chapter-7>
- 7 Sicherheitsrat der Vereinten Nationen. (2024, 28. April). *Resolution 1540 (2004)*. S/RES/1540 (2004). Vereinte Nationen. [https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1540%2520\(2004\)&Language=E&DeviceType=Desktop&LangRequested=False](https://undocs.org/Home/Mobile?FinalSymbol=S%2FRES%2F1540%2520(2004)&Language=E&DeviceType=Desktop&LangRequested=False)
- 8 Sicherheitsrat der Vereinten Nationen. (2006). *Security Council Committee established pursuant to resolution 1718 (2006)*. Vereinte Nationen. <https://main.un.org/securitycouncil/en/sanctions/1718>
- 9 Bureau of International Security and Nonproliferation. *Nonproliferation Sanctions*. U.S. Department of State. <https://www.state.gov/key-topics-bureau-of-international-security-and-nonproliferation/nonproliferation-sanctions/>
- 10 Bureau of International Security and Nonproliferation. (2023, 15. August). *Master Sanctions List*. U.S. Department of State. <https://www.state.gov/wp-content/uploads/2023/08/MASTER-Sanctions-chart-508-Updates-Aug-2023-1.pdf>
- 11 Bureau of International Security and Nonproliferation. *Iran, North Korea, and Syria Nonproliferation Act Sanctions (INKSNA)*. U.S. Department of State. <https://www.state.gov/iran-north-korea-and-syria-nonproliferation-act-sanctions-inksna/>

12 Europäische Kommission. (2024, 29. August). *EU Sanctions Map*. Europäische Union. <https://www.sanctions-map.eu/#/main?checked=46,20,18,32&search=%7B%22value%22:%22%22,%22searchType%22:%7B%7D%7D>

13 The Australia Group. *Fighting the spread of chemical and biological weapons*. Department of Foreign Affairs and Trade. Australian Government. <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/index.html>

14 The Australia Group. *Common Control Lists*. Department of Foreign Affairs and Trade. Australian Government. <https://www.dfat.gov.au/publications/minisite/theaustraliagroupnet/site/en/common-control-lists.html>

15 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0821>

16 https://www.bafa.de/DE/Home/home_node.html

Ausgewählte Instrumente zur Verbesserung der Biosicherheit, zur Minderung von Dual-Use-Risiken und zur Förderung sicherer und ethisch verantwortungsbewusster biologischer Forschung

Globaler Leitfaden der WHO für die verantwortungsvolle Anwendung der Lebenswissenschaften

Die Weltgesundheitsorganisation (WHO) hat 2022 ihren „*Global Guidance Framework for the Responsible Use of the Life Sciences*“ veröffentlicht. Es handelt sich um ein umfassendes und praxisorientiertes Referenzdokument, das Staaten bei der Entwicklung nationaler Strategien zum Risikomanagement im Bereich der Biologie und Lebenswissenschaften unterstützen soll und sich auf Biosicherheit, Laborsicherheit und den Umgang mit Dual-Use-Forschung konzentriert. Es bietet eine Bewertung der aktuellen Situation und einige Leitwerte und -prinzipien für die Steuerung von biologischen Risiken sowie konkrete Instrumente und Mechanismen, die auf bestimmte Zielgruppen zugeschnitten sind. Im Anhang bietet es außerdem sieben hypothetische Szenarien, in denen Elemente des *Global Guidance Framework* angewendet werden könnten, und drei illustrative Fallstudien zu Forschungen, die Risikominderungs- oder Risikomanagementstrategien erforderten. Der *Global Guidance Framework* ist als unterstützende Ressource für Staaten gedacht; die Umsetzung ist nicht obligatorisch.

Tianjin-Biosicherheitsrichtlinien für Verhaltenskodizes für Wissenschaftler*innen

Die *Tianjin Biosecurity Guidelines for Codes of Conduct for Scientists*¹ wurden gemeinsam von Vertretern der Tianjin-Universität in China, des Johns Hopkins Center for Health Security in den USA und der Interacademy Partnership (IAP) entwickelt. Sie sollen dazu beitragen, den Missbrauch der Biowissenschaften, auch für Waffenzwecke, zu verhindern, indem sie das Bewusstsein für das Dual-Use- und Missbrauchspotenzial biologischer Forschungen schärfen. Sie enthalten Prinzipien für den verantwortungsvollen Umgang mit den Biowissenschaften, die in nationale Biosicherheitsvorschriften und Verhaltenskodizes aufgenommen werden könnten. Diese Initiative geht auf einen Vorschlag für einen freiwilligen Verhaltenskodex für Forschende in den Biowissenschaften zurück, den China und Pakistan 2016 vorlegten.² Auf der BWÜ-Überprüfungskonferenz im Jahr 2022 brachten China, Pakistan sowie Brasilien als Co-Sponsor die *Tianjin Guidelines* zur Endosierung durch die BWÜ-Vertragsstaaten ein.³ Zwar wurden die *Guidelines* von der Überprüfungskonferenz nicht formal angenommen, sie fanden aber unter den BWÜ-Mitgliedern sehr breite Unterstützung.

Der Umgang mit sicherheitsrelevanter Forschung in Deutschland

Der Umgang mit sicherheitsrelevanter Forschung in Deutschland folgt einem Bottom-up-Ansatz und betont die Verantwortung einzelner Forschenden und Forschungseinrichtungen in Anerkennung des Grundrechts auf Forschungsfreiheit, wie es in Artikel 5 des deutschen Grundgesetzes⁴ verankert ist.

Nachdem im Jahr 2012 umstrittene sogenannte Gain-of-Function-Experimente mit einem Vogelgrippevirus (H5N1) veröffentlicht worden waren, entwickelten der Deutsche Ethikrat sowie die Deutsche Forschungsgemeinschaft (DFG) und die Nationale Akademie der Wissenschaften Leopoldina jeweils Empfehlungen zum Umgang mit Dual-Use-Forschung in den Lebenswissenschaften. Beide Dokumente betonten die Freiheit der Forschung und die Notwendigkeit, Forschende für potenzielle Dual-Use-Risiken in ihrer Arbeit zu sensibilisieren. Während der Ethikrat⁵ auch einen Top-down-Regulierungsansatz vorschlug, der allerdings nicht umgesetzt wurde, konzentrierten sich DFG und Leopoldina⁶ auf die Selbstverwaltung der Wissenschaft und die Verantwortung der einzelnen Forschenden und Forschungseinrichtungen im Umgang mit sicherheitsrelevanter Forschung.

Letzterer Ansatz wird von DFG und Leopoldina weiterhin aktiv gefördert. Unter anderem werden Forschungseinrichtungen ermutigt, lokale Kommissionen für Ethik sicherheitsrelevanter

ter Forschung (KEF) einzurichten. Diese sollen Forschenden, die potenzielle Sicherheitsrisiken in ihrer Forschung identifiziert haben, Orientierung und Beratung bieten. Über den Gemeinsamen Ausschuss zum Umgang mit sicherheitsrelevanter Forschung, der 2014 eingerichtet wurde, um die Umsetzung ihrer Empfehlungen zu unterstützen, unternehmen DFG und Leopoldina auch Aufklärungs- und Sensibilisierungsbemühungen⁷ in der deutschen Wissenschaft.

Dr. Una Jakob

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

- 1 <https://www.interacademies.org/sites/default/files/2021-07/Tianjin-Biosecurity-Guidelines-Codes-Conduct.pdf>
- 2 Delegation von China & Pakistan zur 8. BWC Review Conference. (2016, 15. November). *Proposal for the development of a model code of conduct for biological scientists under the Biological Weapons Convention* (BWC/CONF.VIII/WP.30.). Vereinte Nationen. <https://documents.un.org/doc/undoc/gen/g16/252/49/pdf/g1625249.pdf>
- 3 Preparatory Committee. (2022, 7. April). *The Tianjin Biosecurity Guidelines for Codes of Conduct for Scientists* (BWC/CONF.IX/PC/WP.10.). Office of Disarmament Affairs, Vereinte Nationen. <https://documents.un.org/doc/undoc/gen/g22/303/49/pdf/g2230349.pdf>
- 4 <https://www.gesetze-im-internet.de/gg/index.html>
- 5 Deutscher Ethikrat. (2014, 7. Mai). *Biosecurity – Freedom and Responsibility of Research*. <https://www.ethikrat.org/fileadmin/Publikationen/Stellungnahmen/englisch/opinion-biosecurity.pdf>
- 6 Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung. (2022, 1. November). *Wissenschaftsfreiheit und Wissenschaftsverantwortung* (2022): Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung. Leopoldina und DFG. <https://www.sicherheitsrelevante-forschung.org/publikation-wissenschaftsfreiheit2022/>
- 7 Gemeinsamer Ausschuss zum Umgang mit sicherheitsrelevanter Forschung. (2022, 1. November). 4. *Tätigkeitsbericht*. Leopoldina und DFG. <https://www.sicherheitsrelevante-forschung.org/publikation-taetigkeitsbericht2022/>

Internationale Initiativen und Kernprinzipien für den sicheren Umgang mit KI

Summit on Responsible Artificial Intelligence in the Military Domain 2023 (REAIM)

Im Zuge der REAIM-Konferenz¹ haben Regierungsvertreter von 57 Staaten² – darunter die USA, China und der Großteil der EU-Staaten – einen gemeinsamen Aktionsaufruf zur verantwortungsvollen Entwicklung, Einführung und Nutzung von künstlicher Intelligenz (KI) im militärischen Bereich³ verabschiedet. Auf der Grundlage, dass KI einen massiven Einfluss auf militärische Systeme haben wird, dieser Einfluss aktuell aber noch gar nicht vollständig verstanden wird, wurden folgende, politisch nicht bindende, Prinzipien formuliert:

- Der Mensch soll beim Einsatz von KI im militärischen Bereich verantwortlich sowie rechenschaftspflichtig bleiben und der Einsatz von KI-Systemen stets unter menschlicher Aufsicht erfolgen.
- Militärisches Personal soll ausreichend geschult sein, um die möglichen Einflüsse wie potenzielle Verzerrungen in den Daten (Data-Bias) und die Konsequenzen des Vertrauens in die Entscheidungen von KI-Systemen und deren Einsatz zu überblicken.
- Auf die verfrühte Umsetzung von KI ohne ausreichende Forschung, Prüfung und Sicherheit sollte zugunsten eines alle Stakeholder einbeziehenden Ansatzes verzichtet werden, um ungewollten Schaden zu vermeiden.
- Trainingsdaten von KI-Systemen sollen in einer Weise erhoben, genutzt, weitergegeben, und archiviert werden, die dem Völkerrecht sowie den einschlägigen Rechtsrahmen und Daten- und Sicherheitsstandards entsprechen.

Da ein Großteil der globalen KI-Forschung und Innovation im zivilen Bereich stattfindet, rufen die unterzeichnenden Staaten dazu auf, dies mit Blick auf die Verantwortung für die internationale Sicherheit und im Einklang mit dem Völkerrecht zu leisten. Allerdings fehlen in den Prinzipien Aussagen zur Selbstbeschränkung von Staaten beim Einsatz militärischer KI.

AI Safety Summit 2023 und „Bletchley Declaration“

Der im November 2023 durch die britische Regierung veranstaltete AI Safety Summit 2023⁴ griff die Impulse der REAIM-2023-Konferenz auf und hatte sich zum Ziel gesetzt, Menschen- und völkerrechtliche Risiken beim Einsatz von KI – nicht nur im militärischen Bereich – zu erörtern. In

Kooperation mit Tech-Unternehmen sollten international koordinierte Maßnahmen ausgelotet werden, um die Gefahren dieser Technologie abzumildern.

Die als „Bletchley Declaration“⁵ betitelte und von 29 Staaten – darunter China, die USA und Deutschland – unterzeichnete Abschlusserklärung unterstreicht, dass folgende Prinzipien bei der Entwicklung und dem Einsatz von KI oberste Priorität haben sollen:

- der Schutz der Menschenrechte
- die Transparenz und Erklärbarkeit der Ergebnisse
- die angemessene menschliche Aufsicht der verwendeten KI-Systeme
- Rechenschaftspflicht und Einsatz der KI auf Grundlage ethischer Prinzipien

Die Erklärung unterstreicht darüber hinaus eine Warnung, die bereits im Rahmen der REAIM-Konferenz geäußert wurde: Angesichts der enormen Entwicklungsgeschwindigkeit von KI und den Trends hin zu hochgradig fähigen und universell einsetzbaren KI-Modellen (sogenannten *general-purpose AI models*) sind die sich daraus ergebenden Risiken nicht vollständig verstanden. Vor diesem Hintergrund regt die Deklaration die Entwicklung nationaler – und im besten Fall international abgestimmter – Regelungen und Frameworks zur Risikobewertung und Risikominimierungsstrategien an.

Die Perspektiven Chinas und der USA auf den Umgang mit Künstlicher Intelligenz

Nahezu zeitgleich zu der Konferenz in Bletchley Park und im Abstand von wenigen Wochen haben sowohl die USA als auch China eigene Vorschläge für den Umgang mit KI vorgelegt. Der Vorstoß der USA, betitelt als „Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy“⁶, dem sich mittlerweile 52 Staaten⁷ angeschlossen haben, bezieht sich dabei ausschließlich auf den militärischen Einsatz dieser Technologie. Demgegenüber widmet sich Chinas „Global AI Governance Initiative“⁸ dem breiteren Einsatz von KI, geht aber auch auf die militärische Nutzung ein. Beide Deklarationen folgen im Kern den bereits genannten Prinzipien, insbesondere bei der Hervorhebung des Spannungsfelds zwischen Fortschritt und Bedrohung, dem Aufruf geltendes internationales Recht zu beachten und dem Anspruch auf vertrauenswürdige und nachvollziehbare KI-Produkte und Anwendungen. Hinsichtlich der militärischen Nutzung von KI verweist Chinas Vorschlag zwar darauf, dass „insbesondere die großen Länder, (...) eine umsichtige und verantwortungsvolle Haltung gegenüber der Forschung, Entwicklung und Anwendung von KI-Technologien im militärischen Bereich einnehmen“ sollten, geht darüber hinaus aber nicht auf weitere, spezifischere Prinzipien ein. Der US-amerikanische Vorschlag

wiederum stellt die Notwendigkeit einer menschlichen Aufsicht über den Einsatz militärischer KI-Systeme heraus, lässt dabei aber offen, in welchem Umfang diese Systeme auch vollkommen autonom agieren dürfen – was im Umkehrschluss auch den autonomen Einsatz von Waffengewalt nicht ausschließt.

Vor dem Hintergrund, dass der Zugriff auf die notwendigen High-Tech-Ressourcen bei der Entwicklung und Anwendung moderner KI-Systeme, wie beispielsweise spezialisierte Mikrochips, zunehmend Bestandteil des globalen Power-Plays zwischen Staaten wird, enthält Chinas Position einen weiteren Aspekt der klar darauf abzielt. Die Deklaration spricht sich nämlich dagegen aus „ideologische Grenzen zu ziehen oder exklusive Gruppen zu bilden, um andere Länder an der Entwicklung von KI zu hindern“ sowie „gegen die Schaffung von Barrieren und die Unterbrechung der globalen KI-Lieferkette durch technologische Monopole und einseitige Zwangsmaßnahmen“. Dieser Passus kann nur als klare Kritik an den US- und teilweise auch EU-Exportkontrollrestriktionen⁹ auf die, für KI-Anwendungen benötigten, hochspezialisierten Mikroprozessoren verstanden werden.

Resolutionen der EU und UN mit Fokus auf nicht-militärische Nutzung von KI

Im März 2024 hat nun auch die EU ihre seit 2021 in Arbeit befindlichen Vorgaben für die Regulation von KI und KI-Produkten veröffentlicht, die als weltweit erstes verbindliches Rahmenwerk angesehen werden. Der „EU AI Act“¹⁰ (AIA) bezieht sich dabei jedoch explizit nicht auf militärisch genutzte KI-Systeme, da Militär und Verteidigung „dem Völkerrecht unterliegen (...), das daher der geeignete Rechtsrahmen für die für die Regulierung von KI-Systemen im Zusammenhang mit der Anwendung von tödlicher Gewalt und anderen KI-Systemen im Zusammenhang mit militärischen und verteidigungspolitischen Aktivitäten“ ist. Stattdessen betont der AIA die Relevanz von KI für gesellschaftliche und wirtschaftliche Fortschritte innerhalb der EU, erkennt aber die Sicherheitsgefahren an, die von diesen Systemen ausgehen können. Um die Kritikalität von KI-Anwendungen zu bewerten, werden Kriterien definiert, die sowohl technische, ökonomische als auch menschenrechtliche Aspekte bei der Herstellung und dem Einsatz von KI beinhalten. Entlang dieser Kriterien werden Auflagen zur Sicherung, der Kontrolle und Rechtssicherheit für KI-Systeme definiert, die als verbindliche Grundsätze in nationale Gesetzgebung der EU-Staaten übergehen sollen.

Schlussendlich hat sich auch die UN in ihrer Vollversammlung am 11.3.2024 auf die Resolution „Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development“¹¹ verständigt, die

sich der Nutzung und den Chancen sicherer und vertrauenswürdiger KI-Systeme widmet. Die Resolution basiert auf einem Vorschlag der USA und wurde von mehr als 120 Ländern angenommen, bezieht sich jedoch ähnlich wie der AIA ausdrücklich nur auf den nicht-militärischen Gebrauch von KI und die Förderung sicherer und vertrauenswürdiger KI-Systeme für den Fortschritt in Bezug auf Menschenrechte, gemeinsame Entwicklungsziele und Nachhaltigkeit. Gleichwohl wird aber auch betont, dass dabei Menschen im Zentrum stehen sollen und KI in den falschen Händen eine erhebliche Gefährdung darstellt. Um diese gezielt zu bewerten, wird die Entwicklung und der Einsatz von Werkzeugen zur „international interoperablen Identifizierung, Klassifizierung, Bewertung und Prüfung, Vorbeugung und Abschwächung von Schwachstellen und Risiken während der Konzeption, Entwicklung und der Nutzung von KI-Systemen“ empfohlen.

Die US-Executive Order 14110 als Ansatz für Exportkontrolle von für KI

Mit der „Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence“¹² von 2023 haben die USA einen wertvollen Ansatz für die zukünftige Entwicklung von Exportkontroll- und Regulierungsmaßnahmen von KI geliefert. Mit der Anordnung werden für die Entwicklung und den Einsatz von KI innerhalb der USA die Gültigkeit von Bürgerrecht festgeschrieben sowie Sicherheitsstandards im Bereich der Cybersicherheit aber auch hinsichtlich Maßnahmen zur Vermeidung von Biases definiert. Ein entscheidender Vorstoß der Anordnung besteht darin, die Gültigkeit dieser Auflagen an die benötigte Gesamtrechenleistung, die für das Training oder die Ausführung eines KI-System benötigt wird zu knüpfen. Dafür wird festgesetzt, dass:

(...) *The Secretary shall require compliance with these reporting requirements for:*

- (i) *any model that was trained using a quantity of computing power greater than 10²⁶ integer or floating-point operations, or using primarily biological sequence data and using a quantity of computing power greater than 10²³ integer or floating-point operations; and*
- (ii) *any computing cluster that has a set of machines physically co-located in a single datacenter, transitively connected by data center networking of over 100 Gbit/s, and having a theoretical maximum computing capacity of 10²⁰ integer or floating-point operations per second for training AI.*

Insbesondere die Rechenleistung sowie Netzwerk-Kapazitäten gelten als entscheidende Faktoren für komplexe KI-Systeme und sind essenzieller Bestandteil bei Planungen zu deren Einsatz. Vor diesem Hintergrund definiert die Exe-

utive Order eine messbare Schwelle für die Regulierung von KI, die effektiv und sinnvoll vor deren Einsatz festgesetzt und für Regulierungsbehörden berücksichtigt werden kann. Gleichwohl müssen solche festen Werte einer kontinuierlichen Überprüfung und Anpassung unterliegen, um mit technischen Entwicklungen Schritt zu halten.

[presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/](https://www.whitehouse.gov/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/)

Dr. Thomas Reinhold

PRIF – Leibniz Institut für Friedens- und Konfliktforschung

- 1 Ministry of Foreign Affairs. (2023). *REAIM 2023*. Government of the Netherlands. <https://www.government.nl/ministries/ministry-of-foreign-affairs/activiteiten/ream>
- 2 Ministry of Foreign Affairs. (2023, 21. Februar). *REAIM 2023 Endorsing Countries and Territories*. Government of the Netherlands. <https://www.government.nl/documents/publications/2023/02/16/ream-2023-endorsing-countries>
- 3 Ministry of Foreign Affairs. (2023, 21. Februar). *REAIM 2023 Call to Action*. Government of the Netherlands. <https://www.government.nl/documents/publications/2023/02/16/ream-2023-call-to-action>
- 4 Government of the United Kingdom. *About the AI Safety Summit 2023*. Government of the United Kingdom. <https://www.gov.uk/government/topical-events/ai-safety-summit-2023/about>
- 5 <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>
- 6 <https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy-2/>
- 7 Bureau of Arms Control, Deterrence, and Stability. (2024). *Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy*. U.S. Department of State. <https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/>
- 8 Ministry of Foreign Affairs. *Global AI Governance Initiative*. The People's Republic of China. http://gd.china-embassy.gov.cn/eng/zxhd_1/202310/t20231024_11167412.htm
- 9 Allen, G. C. (2023, 3. Mai). *China's New Strategy for Waging the Microchip Tech War*. Center for Strategic & International Studies. <https://www.csis.org/analysis/chinas-new-strategy-waging-microchip-tech-war>
- 10 https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6473
- 11 <https://news.un.org/en/story/2024/03/1147831>
- 12 <https://www.whitehouse.gov/briefing-room/>

Application Programming Interface (API): eine Reihe von Funktionen und Protokollen, die es Software-Anwendungen ermöglichen, miteinander zu kommunizieren, um Daten, Eigenschaften und Funktionen auszutauschen.

Biologische Design-Tools (BDT): Anstatt auf natürlicher Sprache wird ein biospezifisches großes Sprachmodell mit Aminosäuresequenzen oder anderen biologischen Sequenzen trainiert, so dass es selbst biologische Sequenzen erzeugen kann. Diese Werkzeuge können die vorteilhaften Eigenschaften von Biomolekülen erlernen und vielversprechende Kandidaten für Labortests vorschlagen, wodurch sich die Anzahl der Tests verringert, die zur Ermittlung der gewünschten Eigenschaften erforderlich sind. UniRep beispielsweise unterstützt Forschende bei der Entwicklung von Proteinen auf der Grundlage ihrer Funktion, während ESMFold sich auf die Struktur konzentriert, was sowohl zur effizienteren Entwicklung besserer Therapien als auch zur Verbesserung der Proteinentwicklung für eine effizientere Bioproduktion beiträgt. Diese Instrumente werden mit biologischen Daten trainiert und unterstützen die Entwicklung neuer Proteine oder anderer biologischer Wirkstoffe. Beispiele hierfür sind RFDiffusion sowie Proteinsprachmodelle wie ProGen2. Sie haben das Potential, die Entwicklung und das Design von Proteinen voranzutreiben, um wichtige Probleme für die menschliche Gesundheit und die Umwelt zu lösen.

Bystander-Tumorzellen: Benachbarte Tumorzellen.

Chimäre (Zellen): Zellen mit anderen Genen als der Rest eines Organs oder Gewebes.

CRISPR (Clustered regularly interspaced palindromic repeats): Technologie, mit der Teile des Genoms durch Entfernen, Hinzufügen oder Verändern von Abschnitten der DNA-Sequenz bearbeitet werden können. Die Technologie umfasst zwei Kernkomponenten: eine Leit-RNA, die mit dem Zielgen übereinstimmt, und eine Endonuklease, in der Regel das CRISPR-assoziierte Protein 9 (Cas9) – ein Enzym, das das DNA-Rückgrat spaltet, was einen Doppelstrangbruch in der DNA verursacht und so Änderungen am Genom ermöglicht.

Daten und Training (KI): Eine current-generation KI wird mit Hilfe von Daten trainiert, die auf die zu erzielende Problemlösungsfähigkeit zugeschnitten sein müssen. Diese Daten können in Form von Texten, Bildern, Videos oder anderen Informationen vorliegen. Ein Teil dieser Daten wird dabei im sogenannten Trainingsprozess verwendet, bei dem die Daten sukzessive durch die KI verarbeitet werden, was zu einer Anpassung der Datenspeicher-Struktur der KI führt. Der restliche Teil der Daten wird abschließend verwendet, um die Ergebnisse des Trainingsprozess zu prüfen. Aufgrund der Bedeutung der Daten für die späte-

ren Ergebnisse der KI kommt der Qualität und der Verfügbarkeit von Trainingsdaten eine erhebliche Rolle zu, die oft durch spezialisierte Unternehmen zusammengestellt, von Hand kuratiert und entsprechend am Markt als wirtschaftliches Gut angeboten werden.

DNA-Polymerase: Enzym, das längere Ketten von DNA-Molekülen synthetisiert.

DNA-Primer (für PCR): Kurze DNA-Abschnitte, die so konstruiert sind, dass sie komplementär zum Anfang und Ende der Zielsequenz in der Probe sind.

Einzelnukleotid-Polymorphismus (Single nucleotide polymorphism, SNP): Eine Variation auf einer einzelnen Nukleotidposition in einer DNA-Sequenz, die zwischen verschiedenen Organismen auftritt.

Entscheidungsbäume: Entscheidungsbäume sind eine Variante von Datenstrukturen zum Speichern von Wissen, bei der eine Baum-Struktur als Modell verwendet wird, um Schlussfolgerungen aus den Beobachtungen zu ziehen, die im Trainingsdatensatz enthalten sind. Gelernte Regeln werden durch Knoten und Zweige des Baums repräsentiert und Schlussfolgerungen durch seine Blätter. Nach dem Training kann man das Modell auch dazu verwenden, explizit und graphisch die Regeln darzustellen, die zu einer Entscheidung führen.

Evolutionärer Algorithmus: Evolutionäre Algorithmen sind eine Variante der sogenannten genetischen Algorithmen, also Optimierungsverfahren, die auf den Prinzipien der natürlichen Evolution basieren. Mit ihrer Hilfe lassen sich Lösungen auf Basis stochastischer Verfahren optimieren, indem Mechanismen der natürlichen Evolution wie Selektion, Mutation, Kreuzung und „Survival of the fittest“ nachgebildet werden. Auch bei evolutionären Algorithmen wird eine Lösung für ein Problem aus dem System heraus gebildet und nicht deterministisch vorgegeben.

Ganzgenomsequenzierung (Whole Genome Sequencing, WGS): Verfahren zur Bestimmung (fast) der gesamten DNA-Sequenz des Genoms eines Organismus.

Genomik: Untersuchung der Gesamtheit aller Gene im Erbgut einer Zelle. Während sich die Genetik mit einzelnen Genen befasst, untersucht die Genomik das gesamte Genom (alle Gene eines Organismus) und wie es durch die Umwelt beeinflusst wird.

GPU und KI-Chips: Die GPU (Graphic Processing Unit – Grafikverarbeitungseinheit) ist ein spezialisierter Rechenchip, der ursprünglich zur Beschleunigung von Computergrafiken und Bildverarbeitung in PCs, Smartphones und Spielkonsolen entwickelt wurde. Aufgrund ihrer Fähigkeit

zur massiv parallelen Berechnung von Algorithmen eignen sich GPUs auch für nichtgrafische Anwendungen wie das Training neuronaler Netze und das Mining von Kryptowährungen. Im Gegensatz zur sogenannten CPU (Central Processing Unit), die als Schaltzentrale eines Computers verstanden werden kann, sind GPUs in aller Regel auf den dauerhaften Betrieb unter Volllast optimiert und erzeugen dabei entsprechende elektrische Leistung im Umfang von mehreren hundert Watt, mit dem entsprechenden Strom- und Kühlungsbedarf. Aufgrund des massiven Booms werden GPUs zunehmend auch spezifisch auf die Anwendungen für KI optimiert und als vollständige Geräteeinheiten produziert, die zu Hunderten oder Tausenden in spezialisierten Rechenzentren zusammengeschaltet werden können. Solche Geräteeinheiten können dauerhafte Leistungsaufnahmen von mehr als 1000 Watt erreichen, was die benötigte Stromversorgung und Kühlung der Rechenzentren erheblich beeinflusst.

KI-Agent: Softwareprogramm, das in der Lage ist, mit seiner Umgebung zu interagieren, Daten zu sammeln und diese zu nutzen, um Aufgaben zu erfüllen, die auf bestimmte Ziele ausgerichtet sind. Während der Mensch die Ziele festlegt, entscheidet die KI autonom über die zur Erreichung dieser Ziele erforderlichen Maßnahmen.

KI-Modell: Das fertige Ergebnis der Lernphase einer KI wird als Modell bezeichnet und enthält die aus den im Lernprozess verwendeten Informationen erlernten Zusammenhänge. Dieses Wissen liegt jedoch nicht in Form explizit deterministischer Wenn-Dann-Regeln vor, sondern ist implizit in der Datenstruktur der KI und deren inneren Verknüpfungen enthalten. Eine solche KI wird daher als Black-Box betrachtet, deren innere Datenverarbeitung nicht ohne erhebliche technische Zusatzaufwände nachvollziehbar ist (die sogenannte Explainability). Modelle sind entweder vollständig angelernt und für den produktiven Einsatz bereit oder in Form sogenannter „Foundation Modells“ zwar für bestimmte Fähigkeiten geübt, die aber noch durch weitere Lernphasen auf einen bestimmten Anwendungskontext hin optimiert werden müssen.

KI-Modellgewicht: das gespeicherte Wissen, das ein Modell erworben hat. Technisch gesehen sind diese Gewichte numerische Werte, die das Modell während der Berechnungen verwendet, um auf Anfragen zu antworten. Wichtiger ist jedoch, dass diese Gewichte alles, was das Modell gelernt hat, und alle Informationen, die es besitzt, zusammenfassen.

Kulturenbasierte mikrobielle Techniken: Kultivierung mikrobieller Organismen durch Vermehrung in einem vordefinierten Nährmedium unter kontrollierten Laborbedingungen. Nicht alle Mikroorganismen wachsen unter diesen Bedingungen.

Künstliche Intelligenz (KI) und Maschinelles Lernen (ML): Als künstliche Intelligenz werden Verfahren aus einem Teilbereich der Informatik bezeichnet, bei denen der Ansatz verfolgt wird, die menschliche Repräsentation von Wissen oder das menschliche Schlussfolgern auf Grundlage von bekannten Fakten in Computeralgorithmen und Berechnungen nachzubilden. Die bekannteste Form von Künstlicher Intelligenz ist das sogenannte Maschinelle Lernen (ML), bei der die Regeln einer Datenverarbeitung – also des Erzeugens einer Ausgabe eines Programms auf Grundlage einer Eingabe – nicht von Anfang an fest durch den Programm-Code vorgegeben sind, sondern durch einen schrittweise Prozess des Trainings durch den Computer selbst erlernt werden. Andere KI-Ansätze wie symbolische KI, Entscheidungsbäume und evolutionäre Algorithmen spielen vor allem in spezifischen Anwendungen eine Rolle. Eine KI besteht in aller Regel aus einem definierten Algorithmus, der als Lernverfahren vorgibt, wie Informationen zum Lernen verarbeitet werden, und einer Datenstruktur, in welcher das erlernte Wissen und die identifizierten Wissenszusammenhänge gespeichert werden.

Künstliche neuronale Netze (KNN) und Deep Learning (DL): Bei künstlichen neuronalen Netzen werden die Funktionsweisen menschlicher neuronaler Zellen und deren Interaktionen nachgestellt. Das technische Grundprinzip von KNN basiert, unabhängig vom eigentlichen Einsatzzweck, auf einer Datenstruktur zur Speicherung und Verarbeitung von Informationen, vergleichbar mit den Systemen, wie sie für das Cloud-Computing verwendet werden. Diese Datenstruktur wird mithilfe umfangreicher, auf die zu erzielende Problemlösungsfähigkeit zugeschnittener Daten in einem sogenannten Trainingsprozess angelernt. Das bekannteste und wichtigste Lernverfahren ist Deep Learning (DL). Dabei wird die Struktur sukzessiv verändert, bis hin zum sogenannten Modell, also der fertigen Struktur, die zu einer Eingabe jeweils die gewünschte Ausgabe erzeugt. Deren komplexe Verknüpfung ist in der Lage, umfangreiche Daten zu verarbeiten und komplexe Datenmuster und Wissenszusammenhänge zu erlernen. KNN und DL gehören aktuell zu den wichtigsten Formen von KI.

Lipidomik: Untersuchung der Lipidzusammensetzung biologischer Proben. Mikroben enthalten eine Reihe charakteristischer Lipide und Lipoproteine, was den schnellen Nachweis von Krankheitserregern mit massenspektrometrischen Systemen unterstützt.

LLM, LMM und AGI: Je nach Art der verwendeten Trainingsdaten und Form der möglichen Nutzerinteraktion einer KI unterscheidet man verschiedene Typen. Bei „Large Language Modells“ (LLM) werden Textdaten zum Training und für die Ausgaben verwendet; Nutzer*innen chatten

also mit der KI. Bei „Large Multimodal Modells“ (LMM) werden auch Bild-, Video-, und Audiodaten im Training sowie für die Interaktion zwischen KI und Nutzer*in verwendet; die KI ist also in der Lage, unterschiedliche Medien zu verarbeiten und ihrerseits herzustellen. Angesichts der Geschwindigkeit des technologischen Fortschritts sind diese Grenzen jedoch fließend, je nach Anforderung des Anwendungsgebietes. Der nächste große Schritt, an dem Tech-Unternehmen arbeiten, besteht in der Vision einer sogenannten „Artificial General Intelligence“ (AGI), die nicht mehr auf eine bestimmte Problemlösung optimiert ist, sondern ein hochgradig flexibles künstliches System sein soll, das in allen Bereichen menschlichen kognitiven Fähigkeiten gleichwertig oder überlegen ist. Eine AGI soll dabei in der Lage sein, sich auf Problemstellung einzustellen und Lösungen zu entwickeln, ohne für diese spezifisch trainiert worden zu sein.

Massenspektrometrie (MS): Ein analytisches Instrument zur Messung des Masse-Ladungs-Verhältnisses (das Verhältnis der Masse eines Ions zu seiner Ladung) eines oder mehrerer Moleküle in einer Probe. Dazu wird das Material in der Ionisierungsquelle ionisiert und das Masse-Ladungs-Verhältnis genutzt, um die entstandenen Ionen zu trennen. Sowohl für die Ionisierung als auch für die Ionenanalyse stehen unterschiedliche Technologien zur Verfügung, sodass es viele verschiedene Arten von Massenspektrometern mit unterschiedlichen Kombinationen dieser beiden Verfahren gibt.

Metagenomik: Metagenomische Sequenzierung beinhaltet die Sequenzierung aller mikrobiellen und Wirtsnukleinsäuren in einer Probe ohne vorherige Selektion.

Next Generation Sequencing (NGS): Methode zur Analyse von genetischem Material, die eine schnelle Sequenzierung großer Mengen von DNA oder RNA ermöglicht. Im Vergleich zu herkömmlichen Sequenzierungstechniken (z. B. Sanger-Sequenzierung) kann NGS Millionen kleiner DNA-Fragmente gleichzeitig sequenzieren.

NGS-Bibliothek: Sammlung von DNA-Fragmenten, die mit einer bestimmten Sequenzierungsplattform kompatible Adaptersequenzen und Indizierungs-Barcodes zur Identifizierung einzelner Proben enthält.

Nukleinsäuren: RNA oder DNA, ein längeres Molekül, das aus Nukleotiden besteht.

Nukleinsäure-Panel: Diagnostischer Test, bei dem mehrere Nukleinsäuresequenzen (DNA oder RNA) gleichzeitig untersucht werden, um verschiedene Organismen oder genetische Marker in einer einzigen Probe nachzuweisen und zu identifizieren. Diese Art von Test wird häufig in der medizinischen Diagnostik eingesetzt, um schnell das

Vorhandensein mehrerer Krankheitserreger wie Viren, Bakterien oder Pilze nachzuweisen oder um genetische Variationen im Zusammenhang mit bestimmten Krankheiten oder Zuständen zu bewerten. Nukleinsäure-Panels liefern umfassende Informationen, die bei der genauen Diagnose, der Behandlungsplanung und der Überwachung von Krankheiten helfen können. Im Gegensatz zur Metagenomanalyse sind Vorkenntnisse über den (mikrobiellen) Erreger erforderlich.

Nukleotid: Grundbaustein der Nukleinsäuren (ein Monomer).

Pathogen-Agnostizismus: eine Diagnose-, Sequenzierungs- oder Nachweismethode, mit der alle Krankheitserreger nachgewiesen werden können.

Peptid-Massen-Fingerprinting (PMF)/Protein-Fingerprinting: ein analytisches Verfahren zur Bestimmung von Proteinen. Das Protein wird zunächst in kleinere Peptide gespalten, deren absolute Massen dann mit einem Massenspektrometer wie MALDI-TOF gemessen werden.

Polymerase-Kettenreaktion (PCR): eine Labortechnik zur Herstellung (oder Vervielfältigung) von Millionen bis Milliarden von Kopien eines bestimmten DNA-Abschnitts, der dann genauer untersucht werden kann. Dazu werden PCR-Primer benötigt. Es handelt sich dabei um kurze, einzelsträngige DNA-Abschnitte, die so konstruiert sind, dass sie zum Anfang und zum Ende der zu vervielfältigenden Zielsequenz komplementär sind.

Proteomik: Untersuchung aller von der Zelle produzierten Proteine und ihrer Lage. Auf diese Weise kann eine 3D-Proteinkarte der Zelle erstellt werden, die Aufschluss über die Proteinregulation liefert.

Red Teaming (im KI-Kontext): ein interaktives Verfahren zum Testen von KI-Modellen, das schädliches Verhalten wie die Preisgabe sensibler Daten und die Erzeugung toxischer, voreingenommener oder sachlich falscher Inhalte verhindern soll.

Shotgun-Sequenzierung: Methode, bei der DNA-Sequenzen nach dem Zufallsprinzip in viele kleine Teile zerlegt werden, die dann einzeln sequenziert und anschließend wieder zusammengesetzt werden, indem nach Überlappungsbereichen gesucht wird.

Stroma: Teil eines Gewebes oder Organs mit einer strukturellen und/oder bindegewebigen Funktion, der aus Bindegewebe, Blutgefäßen, Lymphgefäßen und Nerven besteht.

Symbolische KI: Bei der Symbolischen KI spricht man von einem Ansatz aus der Top-down-Perspektive. Er kann ver-

wendet werden, wenn ein festes und vollständig bekanntes Regelwerk vorhanden ist. Mittels mathematischer Logik kann so aus den Vorgaben neues Wissen generiert werden. Deshalb wird sie auch als „Wissensbasierte KI“ bezeichnet. Die Symbolische KI stößt allerdings dort an ihre Grenzen, wo Menschen sie nicht mit korrektem und konsistentem Wissen füttern können. Außerdem können Symbolische KIs sehr große Zustandsräume, wie etwa beim Beispiel des Brettspiels Go, bei dem es etwa 10^{170} mögliche Konstellationen gibt, nicht verarbeiten und daher in solchen Fällen nicht verwendet werden.

Synthetische Biologie: Wissenschaftszweig, in dem Organismen oder die Biomoleküle von Organismen auf genetischer Ebene umgebaut werden, um ihnen neue Eigenschaften zu verleihen.

Transgenprodukt: Zelle oder Organismus, dessen Genom durch Einführung fremder DNA-Sequenz(en) verändert worden ist.

Virale Assemblierung: Während der Replikation des Virus lagern sich Proteine um die virale Nukleinsäure und bilden schließlich ein Kapsid.

(Virale) Kapsid-Bibliothek: Genomische Bibliothek, die zur Herstellung von Viruskapsiden (den Proteinzellen der Viren) verwendet wird.

Viraler Vektor: Modifiziertes Virus, das dazu bestimmt ist, genetisches Material in die Zellen einzuschleusen.

Virustiter: Virenkonzentration; Anzahl der Viruspartikel, die in eine Wirtszelle eindringen können.

Wire Arc Additive Manufacturing: Wire Arc Additive Manufacturing kombiniert die Technologie des Gas-Metall-Lichtbogenschweißens mit dem Verfahren der additiven Fertigung. Vereinfacht ausgedrückt werden Metallschichten von einem Roboter übereinander geschweißt, um das gewünschte Design zu realisieren.

XAI – Explainable Artificial Intelligence: Ansätze der Erklärbaren Künstlichen Intelligenz sollen der „Black Box“-Tendenz des maschinellen Lernens entgegenwirken, also dem Umstand, dass bei einer KI nicht ersichtlich ist, warum sie zu einer bestimmten Entscheidung gelangt ist. Obgleich man bei einer KI das Modell und dessen Verarbeitung von Anfragen einsehen kann, lassen sich daraus im Kontrast zu deterministischen Verfahren, bei denen ein Algorithmus eine feste Wenn-Dann-Verarbeitungsabfolge vorgibt, keine Rückschlüsse auf den eigentlichen Schlussfolgerungsprozess schließen. Eine Erklärbarkeit von Entscheidungen, die eine „Zur Eingabe (a) wurde das Ergebnis (b) erzeugt auf Grundlage der erlernten Fakten

(X) und (Y)“, wie sie bei menschlicher Kommunikation üblich ist, kann damit nicht erreicht werden. XAI-Ansätze sollen als Erweiterung eines KI-Modells diese Schlussfolgerungsketten sichtbar machen.

#

3D-Druck, siehe Additive Fertigung
5G 58, 62 f.

A

ABC-Waffen, siehe Massenvernichtungswaffen
Abschreckung 19, 52, 62, 66 f., 69
Abwassersequenzierung 49
Addgene 53
Additive Fertigung 11, 25, 30 ff., 67
Afghanistan 67
AGI 17, 98
American Society of Clinical Oncology 82
Amerithrax 52
Application Programming Interface (API) 42, 96
Arzneimittel 42 f.
Atomwaffen 11, 19, 61 ff., 90
Attribution 39, 47, 52 f.
Aufklärung 22 f., 25, 63 ff., 75
Australische Gruppe 5, 10, 90
Autonome Waffensysteme 18 f., 26 f., 28, 60, 72 f., 76, 94

B

Ballistische Raketen 24, 64 ff.
Battle-Management-Systeme 18, 38
Bergkarabach 22 f.
Biodefense 46 ff.
Bioforensik 47, 52 f.
Biologische Design-Tools 40 ff., 96
Biorisiken 10, 38 ff.
Biosicherheit 40, 43, 46 ff., 78 ff., 89, 91 f.
Biotechnologie 9, 11, 38 ff., 46 ff., 60 ff., 78 ff., 88
Bioüberwachung 47
Biowaffen 5, 9 f., 19, 38 ff., 52 f., 88 ff.

Biowaffen-Übereinkommen 5 ff., 53, 88 ff.
Biowissenschaften 6, 10, 38 ff., 92
Bletchley Declaration 12, 93
Brexit 68 f.,

C

Cas 51, 96
CBRN 61, 63 f., 69, 73 f.
ChemCrow 42
Chemiewaffenübereinkommen 5 ff., 76, 90
Chimäre Antigenrezeptor-T-Zelltherapien (CAR-T) 82
China 8, 20, 27, 61, 63 ff., 92 ff.
Cloud Computing 58
Common Mechanism for DNA Synthesis Screening 43
Computer-Chips, siehe Halbleiter
Computing 58, 62 f., 66 ff., 70 ff., 74, 94, 97
Corona-Virus, siehe SARS-CoV2
CRISPR 51, 96
Cruise-Missiles, siehe Marschflugkörper
Cyber 19, 58, 61 ff., 72, 76, 94

D

Data Science 64 ff., 68 f., 72
Deep Learning 16 f., 26, 41, 97
Defense Advanced Research Projects Agency (DARPA) 27
DETECTR 51
DIN EN ISO/ASTM 52900 31
DNA 39, 41, 43, 46, 48 f., 51 ff., 81, 96, 98 f.
Drohnen 22 ff.
 Abwehr von 22 ff.
 FPV-Drohnen 25 f.
 GJ-1 22
 HALE 23
 Hawk 23
 Heron 22

Kamikazedrohnen 23
Loitering Munition 23, 26
MALE 22 f., 25, 27
MQ-25 Stingray 27
Predator 22
Reaper 22 f.
Schwärme 18 f., 26 f.
TB2 22

Dual Use 4 ff., 16 ff., 22, 26, 28, 30, 34, 36, 40, 44, 58 ff., 68, 72, 76, 78 ff., 88 ff., 91 f.

E

Emerging Disruptive Technologies 58 ff.
Energie 6, 31, 60, 63 f., 67 ff., 70 f.
Erregernachweis 39, 46 ff., 97 f.
Europäische Verteidigungsagentur 59 f.
EU AI Act 94
Eve 43
Executive Order 14110 20, 43, 94
Explainable AI (XAI) 19 f., 99
Exportkontrollen 5, 8, 10 ff., 20, 23, 28, 34 ff., 90 f., 94

F

FGC-9 33
Flugabwehr, siehe Luftverteidigung
Flugzeugträger 27
Führungsinformationssysteme, siehe Battle-Management-Systeme

G

Gaza 18, 38, 58 f.
Geheimdienste, siehe Nachrichtendienste
Genfer Protokoll 88 f.
Gentechnik 9, 11, 39, 46, 52 f., 78 ff.
Global AI Governance Initiative 93
GPS 24, 27

H

Halbleiter 11, 16 ff., 63
 Human enhancement 60, 64, 70 f., 74
 Hyperschallsysteme 60, 64 f.

I

Immunevasion 9 f., 80 ff.
 Improvised Explosive Devices (IEDs) 30
 INF-Vertrag 23

K

Kapsid-Bibliothek 81, 99
 KI-Agent 42, 97
 KI-Durchführungsverordnung, siehe Executive Order 14110
 Kleinwaffen 35 f.
 Klimawandel 38, 61, 63 ff., 68 f.
 Kommunikationstechnologien 8, 60 ff., 66 ff., 70 f., 73 f., 76
 Krankheitserreger 39 ff., 46, 49, 51 f., 79, 97 f.
 Künstliche Intelligenz 11, 16 ff., 38 ff., 60, 63 f., 68 f., 72, 97
 Künstliche Neuronale Netze 16 f., 97

L

Large Language Models 17, 40 ff., 97
 Liberator 33
 Lipidomik 49 ff., 97
 Luftkampf 18, 27
 Luftverteidigung 23 f., 64 f., 66

M

M777 32
 Mammoth Biosciences 51

Marschflugkörper 23 f.
 Maschinelles Lernen 16, 39, 97
 Massenspektrometrie 49 ff., 98
 Massenvernichtungswaffen 5, 35, 64 f., 90
 Metagenomik 39, 48 f., 98
 Mikroorganismen 46, 48, 50 f., 52, 97
 Missile Technology Control Regime (MTCR) 5, 8, 28
 Molekularbiologie 40
 Myanmar 30, 33

N

Nachrichtendienste 52, 64, 69, 74
 Nanomaterialien 67, 70 f.
 Nationale Sicherheitsstrategien 58 ff.
 Belgien 61 f., 70 f.
 Frankreich 62 f., 70
 Deutschland 63, 71
 Japan 63 f., 74, 76
 Niederlande 65
 Pakistan 65 f.
 Polen 58 f., 66
 Russland 67 f.
 Spanien 68
 Südkorea 64 f., 70 f., 74, 76 f.
 USA 70
 Vereinigtes Königreich 69 f.
 NATO 19, 59 ff., 66, 71, 76
 Neue Materialien 60
 Nordkorea 63 ff., 90

O

Öffentliche Gesundheit 10, 79

P

Pandemie 10, 38 f., 46, 50 ff., 63, 69, 78, 80, 82
 Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy 93 f.

Polymerase-Kettenreaktion (PCR) 46 f., 50, 96, 98
 Präzisionsmunition 25
 ProGen2 41, 96
 Programme of Action (PoA) to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons (SALW) in All Its Aspects 35 f.
 Projekt „Maven“ 72
 Proliferationsrisiko 24 f., 34
 Proteomik 49 f., 98
 Public Health, siehe Öffentliche Gesundheit

Q

Quantentechnologien 58, 60, 62 ff., 67, 69 ff., 74 f., 76

R

Raketenabwehr, siehe Luftverteidigung
 Raketentechnik 64, 66 f., 70 f.
 REAIM 77, 93
 Replicator-Initiative 18, 27
 Reverse-Genetik-Systeme 81
 RFDiffusion 41, 96
 RNA 39, 41, 48 f., 51, 96, 98
 Robotik 27, 32, 40, 42 f., 60, 64, 67, 70 f., 75, 99
 Russland 8, 17, 19, 23 ff., 63, 66 ff., 70 f., 75 f., 90
 Rüstungsindustrie 33, 59, 67

S

SARS-CoV2 10, 49, 51, 52, 63, 69
 Sicherheitsrelevante Forschung 6, 92
 Sprengfallen, siehe Improvised Explosive Devices (IEDs)
 Sprengstoff 34, 36, 74
 Stealth 63, 74
 Synthetische Biologie 39, 43, 69, 81, 99

T

Tarnkappenfähigkeiten, siehe Stealth
Terrorismus 4, 8 f., 35, 65, 89
 Bioterrorismus 47, 52, 89
Tianjin Guidelines 92
Toxine 41, 46, 50 f., 88, 90
Trägerzellen 82
Transgenprodukte 81, 99
TSMC 20

U

Ukraine 16 ff., 23 ff., 30, 33 f., 38, 58 f., 73, 75
UN, siehe Vereinte Nationen

UNSC-Resolution 1540 7, 90

Unbemannte Systeme 22 ff., 58, 64, 67, 70 f., 75

USA 8, 10, 20, 23 f., 27 f., 32, 43, 52, 66, 68 f., 70 f., 76, 90, 92, 93 f.

V

Vereinte Nationen 7, 76, 89 ff., 94

Verifikation 9, 53, 76, 88

Verteidigungsindustrie, siehe Rüstungsindustrie

Verordnung (EU) 2021/821 90

Virale Vektoren 79 ff., 99

Viraler Tropismus 81

Völkerrecht 4 f., 7, 19, 93 f.

W

Wassenaar-Arrangement 5, 8, 28

Weltraum 60 ff., 67ff., 70 f.

WHO 10, 78, 91 f.

Z

Zivilklausel 36, 76

CNTRMONITOR 2024

PRIF – Leibniz-Institut für Friedens- und Konfliktforschung

PRIF – Peace Research Institute Frankfurt

Baseler Straße 27–31

60329 Frankfurt am Main

Telefon: +49 69 95 91 04–0

E-Mail: cntr@prif.org

www.cntrarmscontrol.org

ISBN: 978-3-946459-97-2

DOI: 10.48809/cntr2024

Herausgeber: Prof. Dr. Malte Götsche, Prof. Dr. Christopher Daase,
Sprecher des Clusters Natur- und Technikwissenschaftliche Rüstungskontrollforschung (CNTR)

Coverbild: Susanne Hartmann/media machine GmbH

Textlizenz: Creative Commons CC-BY-ND 4.0 (Namensnennung/Keine Bearbeitungen/4.0 International).
Die verwendeten Bilder unterliegen eigenen Lizenzbedingungen.



The appearance of U.S. Department of Defense (DoD) visual information does not imply or constitute DoD endorsement.

Redaktion und Satz: Elisabeth Waczek, CNTR

Layoutgestaltung: Susanne Hartmann/media machine GmbH

November 2024

Empfohlene Zitierweise: Götsche, M. & Daase, C. (Hrsg). (2024). *Perspektiven auf Dual Use. CNTR Monitor – Technologie und Rüstungskontrolle 2024*. PRIF – Leibniz-Institut für Friedens- und Konfliktforschung.

DANKSAGUNG

Wir danken PD Dr. Jürgen Altmann und Prof. Dr. Kathryn Nixdorff herzlich für die umfangreiche und wertvolle Kommentierung von früheren Fassungen der Trend- und Analysekapitel.

Perspektiven auf Dual Use

Forschung und Entwicklung, die zunächst im zivilen Bereich stattfindet, kann in vielen Fällen militärisch eingesetzt werden oder von nichtstaatlichen Akteuren für böswillige Zwecke missbraucht werden. Wissenschaftlicher und technologischer Fortschritt macht die Regulierung von Dual-Use-Gütern immer komplexer und stellt zunehmend eine Herausforderung für Frieden und Sicherheit dar.

Der CNTR Monitor 2024 wirft einen interdisziplinären Blick auf die vielen Perspektiven, die mit dem Thema Dual Use verbunden sind. Von künstlicher Intelligenz und Halbleitern, Drohnen und additiver Fertigung bis hin zu unbeabsichtigten Folgen biologischer und medizinischer Forschung, aber auch neuen Chancen für die Rüstungskontrolle – so vielfältig die Gegenstände und Technologien, so vielfältig sind auch die relevanten Akteure und die politischen und rechtlichen Rahmenbedingungen. Der CNTR Monitor 2024 beleuchtet unterschiedliche Dual-Use-Problematiken, zeigt Möglichkeiten der politischen Kontrolle auf und bewertet Chancen und Risiken ausgewählter neuer Technologien.

cntrarmscontrol.org

Gefördert durch:



Auswärtiges Amt

aufgrund eines Beschlusses
des Deutschen Bundestages

CNTR ist ein Verbundprojekt zwischen:



TECHNISCHE
UNIVERSITÄT
DARMSTADT

