Ethik in der Medizin (2024) 36:531–545
https://doi.org/10.1007/s00481-024-00839-0

ORIGINALARBEIT

Digitalisierung in Lebenswissenschaften und Medizin – das *Dual-Use*-Problem

Jan-Hendrik Heinrichs · Serap Ergin Aslan

Eingegangen: 4. April 2024 / Angenommen: 3. September 2024 / Online publiziert: 22. Oktober 2024

Zusammenfassung Dual Use bezeichnet zunächst die Verwendbarkeit eines eigentlich für andere Zwecke intendierten Forschungsergebnisses oder -verfahrens für Zwecke, die die innere oder äußere Sicherheit einer Gesellschaft betreffen. Darunter fällt Forschung, die für militärische, geheimdienstliche, terroristische oder kriminelle Zwecke verwendet werden kann. *Dual Use* stellt seit über einem Jahrzehnt ein sich beständig verschärfendes Problem für viele Bereiche der Lebenswissenschaften und der Medizin dar, weil viele von deren Ergebnissen geeignet sind aufzuzeigen, wie Menschen, aber auch (Nutz-)Tiere und Pflanzen manipuliert und attackiert werden können und welche Werkzeuge dafür besonders geeignet sind.

Die Digitalisierung in den Lebenswissenschaften hat im Hinblick auf das *Dual-Use*-Problem zwei voneinander unterscheidbare Einflüsse, nämlich einen verschärfenden und einen erweiternden. Dadurch, dass die Digitalisierung schnellere und umfangreichere Forschungs- und Entwicklungsprozesse ermöglicht, verschärft sie das bestehende *Dual-Use*-Problem, weil zugleich das Tempo steigt, in dem die Ergebnisse dieser Forschung für sicherheitsrelevante Zwecke nutzbar gemacht werden können. Zudem erweitert die Digitalisierung der Lebenswissenschaften das *Dual-Use*-Problem, denn einige der digitalen Werkzeuge, die in den Lebenswissenschaften entwickelt und gebraucht werden, können selbst militärische oder sicherheitsrelevante Verwendung finden.

Deshalb bedarf es einer breit angelegten Governance inklusive einer breiten Beteiligung der Stakeholder im Forschungsprozess und eines Informationsangebots zu

Dieser Artikel erscheint im Rahmen des Themenheftes: „Ethik in der datenintensiven medizinischen Forschung“.

✉ PD Dr. Jan-Hendrik Heinrichs · Dr. Serap Ergin Aslan
Institut für Neurowissenschaften und Medizin 7: Gehirn und Verhalten, Forschungszentrum Jülich, Wilhelm-Johnen-Straße, 52428 Jülich, Deutschland
E-Mail: j.heinrichs@fz-juelich.de

Dual Use in der Ausbildung in guter wissenschaftlicher Praxis über Institutionen, Karrierestufen und Disziplinen hinweg.

Schlüsselwörter Dual Use · Sicherheitsrelevanz · Biowissenschaften · Forschungsethik · Good Scientific Practice

Digitalization in life science and medicine—the dual-use problem

Abstract
Definition of the problem "Dual use" refers to the applicability of a research result or methods for purposes that concern the internal or external security of a society. This includes research that can be used for military, intelligence, terrorist, or criminal purposes. Dual use has been an increasingly aggravating problem for many areas of the life sciences and medicine for over a decade. The main cause for this is that many of their results are capable of demonstrating how humans, but also (domestic) animals and plants, can be manipulated and attacked, and which tools are particularly suitable for this purpose.
Arguments The digitalization in the life sciences has two distinguishable impacts on the dual-use problem: an intensifying and an expanding one. By enabling faster and more comprehensive research and development processes, digitalization exacerbates the existing dual-use problem because it increases the pace at which the results of this research can be utilized for security-related purposes. Moreover, the digitalization of the life sciences expands the dual-use problem, as some of the digital tools developed and used in the life sciences can themselves have military or security-relevant applications.
Conclusion Therefore, a broad-based governance including wide participation of stakeholders in the research process and broader information on dual use in good scientific practice education across institutions, career stages, and disciplines is necessary.

Keywords Dual use · Security · Life sciences · Research ethics · Good scientific practice

Einführung

Die Forschungsethik widmet sich mit wachsendem Nachdruck der Aufgabe, gut begründete Optionen für den Umgang mit sicherheitsrelevanter Forschung und mit dem Missbrauchspotential in den Wissenschaften, insbesondere den Lebenswissenschaften zu ermitteln (Crowley und Dando 2022; Miller und Selgelid 2008). In jüngster Zeit ist der Einfluss von datenintensiven Methoden und künstlich intelligenten Systemen auf den Umfang und die Art sicherheitsrelevanter Forschung besonders thematisch geworden (Carter et al. 2023; siehe z. B. Jakob et al. 2024; Urbina et al. 2023).

Im Folgenden wird nach einer kurzen Verortung in der ethischen Debattenlage und deren forschungspraktischen Kontext zunächst der Begriff des *Dual Use* kurz eingeführt. Auf dieser Vorarbeit aufbauend werden dann die *Dual Use*-relevanten Entwicklungen in den aktuellen Lebenswissenschaften und der Medizin umrissen. Dabei stellt sich heraus, dass diese uns nicht mit genuin *neuen* ethischen Herausforderungen konfrontieren, aber den Kreis der von den bestehenden Herausforderungen betroffenen Wissenschaftlerinnen und Wissenschaftler erweitern. Zum Abschluss wird vor dem Hintergrund aktueller institutioneller Regelungen und Empfehlungen zum Umgang mit *Dual Use* etwaiger Handlungsbedarf identifiziert.

Zu Beginn der 2010er-Jahre erlangte die Frage der Sicherheitsrelevanz von lebenswissenschaftlicher Forschung internationale Aufmerksamkeit[1], nachdem bei Grippeviren genetische Veränderungen mit Auswirkungen auf deren Übertragbarkeit entdeckt worden waren. Die so genannten *Gain-of-function*-Forschungen von Herfst und Kollegen (Herfst et al. 2012) und Imai und Kollegen (Imai et al. 2012) zeigten, dass bereits geringfügige Veränderungen in der Aminosäuresequenz ausreichen, um das H5N1-HPAIV-Virus auf und zwischen Säugetieren und insbesondere auf den Menschen übertragbar zu machen. Die Möglichkeit, dass Personen, die über hinreichende molekularbiologische und virologische Kenntnisse verfügen, diese Information nutzen könnten, um ein Virus mit pandemischem Potenzial und hoher Sterblichkeitsrate für böswillige Zwecke herzustellen, hat Sicherheitsbedenken bei Forscherinnen und Forschern wie bei staatlichen Akteuren aufgeworfen (vgl. Imperiale und Casadevall 2018). Auf diese Sicherheitsbedenken im Zusammenhang mit *Gain-of-function*-Experimenten reagierte die wissenschaftliche Gemeinschaft schnell und suchte nach Vorkehrungen, um zu verhindern, dass diese und andere Ergebnisse in die falschen Hände gerieten. Politische Akteure wie die US-Regierung[2] und eine breitere gesellschaftliche Debatte folgten rasch.

In den Mittelpunkt der forschungsethischen Diskussion rückte durch diese Ereignisse vor allem die terroristische Missbrauchsgefahr. Die folgenden Fragen sind seither von zentraler Bedeutung: Was genau fällt unter „Sicherheitsrelevanz" bzw. „*Dual Use*", was sind geeignete Kriterien und was ist bei sicherheitsrelevanter Forschung zu beachten?

Es gibt eine Reihe von Unterscheidungen, die unter dem Begriff „*Dual Use*" zusammengefasst werden und auf die wir im folgenden Abschnitt kurz eingehen (vgl. Miller und Selgelid 2007; Shamoo und Resnik 2009; Forge 2010; Resnik 2009; Selgelid 2009a).[3] Bei der zugrundeliegenden Definition von sicherheitsrelevanter Forschung folgen wir zunächst dem Leitfaden des Gemeinsamen Ausschusses zum Umgang mit sicherheitsrelevanter Forschung von DFG und Leopoldina (Nationale

[1] Für eine detailliertere Auseinandersetzung mit der bewegten Geschichte der Dual-Use-Forschung in den Lebenswissenschaften, insbesondere während des Kalten Krieges, sei an dieser Stelle auf das Werk von Armin Krishnan (2017) „Military Neuroscience and the Coming Age of Neurowarfare" verwiesen.

[2] Für weiterführende Informationen bezüglich der politischen Reaktion wird auf den White House Blog (2014) mit dem Titel „Doing diligence to assess the risks and benefits of life sciences gain-of-function research" verwiesen.

[3] Für eine Legaldefinition siehe Art. 2 Nr. 1 Abs. 1 der Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20. Mai 2021 (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021R0821, zugegriffen: 28. Feb. 2024).

Akademie der Wissenschaften Leopoldina und Deutsche Forschungsgemeinschaft 2022). Demnach handelt es sich um „wissenschaftlichen Arbeiten, bei denen die Möglichkeit besteht, dass sie Wissen, Produkte oder Technologien hervorbringen, die unmittelbar von Dritten missbraucht werden können, um Menschenwürde, Leben, Gesundheit, Freiheit, Eigentum, Umwelt oder ein friedliches Zusammenleben erheblich zu schädigen (sog. besorgniserregende sicherheitsrelevante Forschung – Dual-Use Research of Concern)“ (Nationale Akademie der Wissenschaften Leopoldina und Deutsche Forschungsgemeinschaft 2022, S. 10). Im weiteren Text wird ergänzt, dass zwischen *Dual Use* und *Dual Use of Concern* die Unmittelbarkeit der Bedrohung unterscheidet. Diese Definition von sicherheitsrelevanter Forschung ist zwar keine abschließende Antwort auf die immer wieder gestellte Frage nach den Kriterien für die Sicherheitsrelevanz und die Missbrauchsanfälligkeit von Forschung, wohl aber eine Explikation der Standards, an denen Missbrauch in der Wissenschaft gemessen wird und die für die Wissenschaft als Ganzes und für die einzelnen Wissenschaftlerinnen und Wissenschaftler gelten.

Ein Großteil der umrissenen ethischen Debatte und politischen Entscheidungsfindung zur *Dual-Use*-Forschung konzentriert sich auf die oben genannten *Gain-of-function-* und ähnliche Forschungen mit bioterroristischem oder biowaffentechnischem Potenzial (vgl. Selgelid 2009b, a). Mit der rasanten Entwicklung der Lebenswissenschaften hat sich – wie wir im Weiteren nachzeichnen werden – das *Dual-Use*-Potenzial jedoch erheblich erweitert. Bereiche wie Neurowissenschaften, Bioinformatik, Genome Editing und synthetische Biologie bieten heute neue Möglichkeiten für *Dual-Use*-Anwendungen (World Health Organisation 2022, S. 9). Die Besorgnis über Bioterrorismus und die technologischen Fortschritte bei der Gen-Synthese und Gen-Editierung haben den *Dual-Use*-Charakter der biologischen Forschung in den Fokus der Öffentlichkeit gerückt (z. B. Ahteensuu 2017; Kosal 2020). Darüber hinaus erschwert die Konvergenz verschiedener Disziplinen mit den Lebenswissenschaften die Bewertung von *Dual-Use*-Risiken zusätzlich. Disziplinen wie Künstliche Intelligenz oder Maschinelles Lernen überschneiden sich zunehmend mit der biologischen Forschung, verwischen traditionelle Grenzen und erhöhen das Potenzial für unbeabsichtigte Folgen (World Health Organisation 2022, S. 9).

In ethischen Debatten über sicherheitsrelevante Forschung werden unter dem Stichwort des *Dual-Use*-Dilemmas häufig die Grundwerte Forschungsfreiheit und Schadensvermeidung gegenübergestellt (Salloch 2018, S. 3). Unseres Erachtens sollte man den Begriff der Schadensvermeidung in dieser Hinsicht sehr weit ausdeuten oder sich gleich auf den der Sicherheit beziehen. Unter *Dual Use* können durchaus Forschungsergebnisse und Technologien fallen, die nicht in einem engen Sinne schädigend genutzt werden können, deren Verbreitung jenseits legitimer staatlicher Sicherheitsorgane aber dennoch als problematisch gelten darf und laut Rechtslage gilt. Darunter fallen insbesondere einige Informationstechniken wie etwa Verschlüsselungsverfahren. Diese weite Ausdeutung des *Dual-Use*-Dilemma als eines zwischen Freiheit und Sicherheit deckt sich mit dem Titel und Sprachgebrauch des Gemeinsamen Ausschusses Sicherheitsrelevante Forschung von DFG und Leopoldina. Insofern stehen der Freiheit zur Forschung und zur Dissemination und Nutzung der Ergebnisse konkrete Verpflichtungen auf die Wahrung der inneren und äußeren Sicherheit gegenüber, wie die Weitergabe von Informationen an Behörden, die

Nichtveröffentlichung von Ergebnissen oder gar eine Pflicht zur Einstellung konkreter Forschungsprojekte (Salloch 2018, S. 3).

Der Umstand allein, dass ein Forschungsergebnis zu einem *Dual Use* geeignet ist, bedeutet anders, als man vielleicht meinen könnte, keine eigenständige moralische Bewertung. Die moralische Bewertung eines zu *Dual Use* geeigneten Forschungsprojekte hängt vielmehr unter anderem von a) der Art der möglichen Nutzung, als auch b) von der Gestaltung des Forschungsprojekte und der Forschungsdissemination ab.

a) Der Begriff „*Dual Use*" wird, wie in der Literatur oft bemerkt, mehrdeutig verwendet (Miller und Selgelid 2008, S. 11 f.). Zunächst wird *Dual Use* darauf bezogen, dass ein Forschungsergebnis für zivile wie für militärische Zwecke verwendet werden kann. Diese Verwendungsweise findet sich beispielsweise in der Eingrenzung von Forschungsförderung oder Forschungsinstitutionen auf zivile Zwecke wie in sogenannten Zivilklauseln (zur Abgrenzung zur Friedensklausel siehe unten) oder in der Festlegung der EU-Forschungsförderung jenseits der Verteidigungsfonds auf zivile Applikationen.

In dieser Verwendungsweise ist *Dual Use* kein dichter, evaluativ gehaltvollen Begriff und erlaubt somit auch keine moralischen Schlüsse. Dass etwas für militärische Zwecke verwendet werden kann, sagt über dessen ethische Bewertung noch nichts aus. Der militärische Aufgabenbereich umfasst moralisch neutrale, moralisch rechtfertigungsbedürftige und sogar moralisch lobenswerte Aktivitäten wie den Katastrophenschutz.

Innerhalb des militärischen Anwendungsfeldes dürfte die konkrete Bewertung von *Dual-Use*-Gütern kompliziert sein und von zusätzlichen Vorannahmen hinsichtlich rechtfertigungsfähiger Mittel und Zwecke abhängen. Es gibt allerdings einige sowohl rechtlich als auch moralisch eindeutige Fälle. In rechtlicher Hinsicht handelt es sich um Verwendungsweisen von Forschungsergebnissen, die durch internationales Recht und Übereinkommen geächtet sind, nämlich biologische und chemische Waffen. In moralischer Hinsicht dürften alle Formen von Massenvernichtungswaffen als kritikwürdig gelten, darunter besonders waffenfähige Mikroorganismen und Substanzen, sogenannten *Dual Use of Concern.*

In gegenwärtigen Diskussionen ist zudem vorgeschlagen worden, dass Steuerungssysteme für automatisierte Waffensysteme, sogenannte Killer Roboter (Sparrow 2007) ebenfalls moralisch nicht rechtfertigungsfähig sind. Das dort vorgebrachte Argument bezieht sich darauf, dass deren Einsatz mit den Regeln des gerechten Krieges nicht vereinbar sei. Es werde nämlich verunmöglicht, persönliche Verantwortung für mögliche Kriegsverbrechen durch solche Systeme zuzuschreiben. Auch wenn wir diese Schlussfolgerung, Verantwortungszuschreibung werde verunmöglicht, nicht durchweg teilen (Tigard 2021), scheint uns doch die Bezugnahme auf die Regeln gerechten Krieges eine vielversprechende argumentative Figur zu sein. *Dual-Use*-Güter unterlägen demnach grundsätzlicher moralischer Kritik, wenn ihr Einsatz in militärischen Kontexten es deutliche erschwerte oder verunmöglichte, Regeln des gerechten Krieges einzuhalten (vgl. Walzer 2015; McMahan 2004). Diese Denkfigur umfasst eben nicht nur Massenvernichtungswaffen, sondern auch andere *Dual-Use*-Technologien wie eben automatisierte Waffensysteme oder bestimmte Formen des

pharmazeutischen, militärischen *Human Enhancement*, die beispielsweise Soldaten hindern, Zivilisten oder Kapitulierende zu verschonen.

Eine von der militärischen Verwendbarkeit weitgehend unabhängige Verwendungsweise des Begriffs „*Dual Use*" bezeichnet die Verwendbarkeit von Forschungsergebnissen zum kriminellen bzw. terroristischen Missbrauch. Invers zur militärischen Verwendungsweise ist deren Bewertung als moralisch problematisch – *ceteris paribus* – offenkundig[4]. Diese Zugehörigkeit zu demselben Begriffsfeld erhellt sich, wenn man den Begriff der Sicherheitsrelevanz hinzuzieht. Es handelt sich in beiden Fällen um Forschungsergebnisse, die die Sicherheit einer Gesellschaft betreffen, im Falle der kriegerischen, militärischen Verwendbarkeit die äußere Sicherheit, im Falle des terroristischen oder kriminellen Missbrauchs die innere Sicherheit.

Aktuelle Analysen versuchen, konkrete Anwendungsfelder auszuzeichnen, in denen Forschungsergebnisse geeignet sind, sicherheitsrelevante Effekte zu zeitigen, um die oft unscharfe Kategorisierung als *Dual-Use*-Objekt zu überwinden. Die genannten Anwendungsfelder sind „political applications [...] to govern or manage the conduct of individuals, groups, or populations", „security applications", „intelligence applications", und „military applications" (Mahfoud et al. 2018, S. 74–77).

b) Die moralische Bewertung von *Dual Use* geeigneter Forschung hängt nicht nur davon ab, welcher Verwendung diese zugeführt werden können, sondern auch wie das Forschungsumfeld gestaltet ist und wem diese Ergebnisse offen stehen und zur Verwendung verfügbar werden. So sind beispielsweise für die Sicherheitskräften legitimer Staaten andere Handlungsoptionen gerechtfertigt als für normale Bürger.

Diese Abhängigkeit der Bewertung beginnt bereits mit der Auswahl der beteiligten Wissenschaftlerinnen und Wissenschaftler. Wenn nur verantwortungsbewusste Wissenschaftlerinnen und Wissenschaftler sowie Organisationen Zugang zu den Ergebnissen haben, ist die Wahrscheinlichkeit höher, dass Ergebnisse einer positiven Nutzung zugeführt und Missbrauch vermieden wird. Des Weiteren hängt die moralische Evaluation davon ab, welche Form von Sicherheitsvorkehrung getroffen wird. Strenge Zugangskontrollen und Sicherheitsmaßnahmen können dazu beitragen, dass Ergebnisse nur von vertrauenswürdigen und Personen und Institutionen genutzt werden. Neben den Sicherheitsvorkehrungen spielen die interne und externe Rechenschaftspflicht sowie die institutionellen Standards eine erhebliche Rolle. Institutionen, in denen klare Verantwortungsstrukturen und Richtlinien herrschen, sind tendenziell eher in der Lage, Missbrauch zu verhindern. Nicht zuletzt spielt der soziale, politische und kulturelle Kontext, in dem die Forschung stattfindet, eine entscheidende Rolle. Das betrifft einerseits die Forschungsinstitution selbst, die durch eine transparente und informierte Kultur der Aufklärung über *Dual-Use*-Risiken die Missbrauchsgefahr reduzieren kann. Das betrifft aber auch die Gesellschaft als Ganze. In stabilen, rechtsstaatlichen Gesellschaften kann dieselbe Forschung weniger problematisch sein als in Regionen, die von Instabilität oder Konflikten ge-

[4] Möglicherweise ist die kriminelle Verwendbarkeit von Forschungsergebnissen etwa zur Abwehr von Übergriffen durch Unrechtsregime moralisch gerechtfertigt.

prägt sind, weil die Anreize zum Missbrauch oder zum Zulassen eines Missbrauchs andere sind.

Dual Use in den datenintensiven Lebenswissenschaften

Zunächst betrifft das *Dual-Use*-Problem in den Lebenswissenschaften deren Produkte und Ergebnisse, beispielsweise modifizierte pathogene Organismen oder Toxine. In den selteneren Fällen, in denen das *Dual-Use*-Problem Werkzeuge der Lebenswissenschaften betrifft, ist das überwiegend deshalb der Fall, weil sie geeignet sind, solche Produkte und Ergebnisse zu generieren. Methoden der Veränderung von Organismen sind beispielsweise deshalb sicherheitsrelevant, weil damit humanpathogene Organismen hergestellt werden können, die sicherheitsrelevant sind.

Diese Differenzierung ist eingestandenermaßen nicht vollständig trennscharf. Das ist sie deshalb nicht, weil die Unterscheidung zwischen den Werkzeugen und Methoden der Lebenswissenschaften und deren Ergebnissen und Produkten nicht trennscharf ist. Vieles, was als Ergebnis gelten darf, wie etwa eine Gen-Schere, funktioniert gleichzeitig als Werkzeug in den Lebenswissenschaften. Dennoch ist die Unterscheidung für den gegenwärtigen Zweck hilfreich, weil sie sich eignet aufzuzeigen, wie die datenintensive und KI-gestützte Entwicklung der Lebenswissenschaften das Problem der Sicherheitsrelevanz nicht nur verschärft, sondern auch erweitert hat. Die Rede von datenintensiver *und* KI-gestützter Entwicklung verweist dabei einerseits auf den Umstand, dass diese beiden Faktoren, Datenintensität und Verwendung künstlich intelligenter Methoden, einander bedingen und stützen. Andererseits sind ihre Effekte aus der gegenwärtigen Perspektive so ähnlich und miteinander verwoben, dass eine Ausdifferenzierung für den vorliegenden Beitrag nicht hilfreich wäre.

Zunächst zur Verschärfung des *Dual-Use*-Problems durch die höhere Datenintensität und die KI-Verwendung in den Lebenswissenschaften. Diese Form der Verschärfung lässt sich am einfachsten an einer parallelen Entwicklung in der Chemie aufweisen. In einem mittlerweile berühmten Fall haben Urbina und Kollegen (Urbina et al. 2022) vorgeführt, dass ein KI-Modell, das mögliche neue Therapeutika vorhersagt und dabei Toxizität vermeidet, sich so modifizieren lässt, dass es besonders giftige Substanzen prädiktiert. Ein offensichtlich analoger Fall bestünde darin, dass mithilfe von KI-Werkzeugen nicht mehr vorhergesagt wird, welche Mikroorganismen sich für Produktionsprozesse in der Bioökonomie oder als Werkzeuge zur Zersetzung von Abfällen eignen, sondern für die Produktion von Toxinen oder direkt für einen humanpathogenen Einsatz. Ähnliche Szenarien lassen sich für KI-Werkzeuge in der Proteomik denken, wenn die Eignung von Proteinen als Toxine vorhergesagt wird. Man darf davon ausgehen, dass einschlägig ausgebildete Lebenswissenschaftlerinnen und -wissenschaftler wenig Mühe haben, sich zahlreiche ähnliche Beispiele vorzustellen.

Darüber hinaus versprechen datenintensive Forschungsprogramme in Medizin und Lebenswissenschaften eine höhere Personalisierung von Therapeutika aller Art. Diese Personalisierung wird deshalb möglich, weil durch die Analyse großer Datenbanken der Einfluss einzelner Eigenschaften auf die Wirkung solcher Mittel identi-

fiziert und im Weiteren entsprechend berücksichtigt werden kann. Diese Form des Zuschneidens auf Individuen oder biologisch ähnliche Gruppen lässt sich selbstverständlich auf nicht-therapeutische Mittel übertragen. Die seit einiger Zeit bereits diskutierte Sorge ist deshalb die vor biologischen und chemischen Waffen, die nur bestimmte Bevölkerungsgruppen betreffen.

Diese und ähnliche Fälle der Verschärfung der *Dual-Use*-Problematik resultieren daraus, dass datenintensive und KI-gestützte Werkzeuge den Forschungsprozess unabhängig davon erheblich beschleunigen, ob das gesuchte Ergebnis sicherheitsrelevant ist. Es handelt sich um eine Verschärfung der *Dual-Use*-Problematik, weil die Zahl der sicherheitsrelevanten Ergebnisse auf diese Weise zunimmt. Damit dürfte zugleich die Häufigkeit steigen, mit der ein Ergebnis sich tatsächlich in ein verwendbares Produkt transferieren lässt, es sich beispielsweise hinreichend einfach und sicher herstellen und der Prozess sich skalieren lässt. Damit steigt auch der Aufwand in der *Dual-Use*-Governance, etwa, die Ergebnisse auf mögliche Sicherheitsrelevanz zu prüfen oder sie entsprechend zu deklarieren und reglementieren.

Auch mithilfe datenintensiver und KI-gestützter Werkzeuge bedarf es allerdings erheblicher lebenswissenschaftlicher Expertise, um überhaupt Ergebnisse, geschweige denn sicherheitsrelevante Ergebnisse zu generieren (Berger und Roderick 2014, S. 36). Es ist also nicht so, als erlaubten KI-Werkzeuge es jedermann, Toxine oder humanpathogene Viren zu entdecken, geschweige denn zu synthetisieren oder zu modifizieren. Der Effekt ist also nicht zunächst einer der weiteren Dissemination, sondern wie oben beschrieben einer der Beschleunigung des Forschungsprozesses.

Ein leicht anders gelagertes *Dual-Use*-Problem ergibt sich durch datenintensive Methoden in anderen Lebenswissenschaften von der Medizin bis hin zur Pflanzenwissenschaft. Das Problem besteht darin, dass detaillierte Modelle von Organismen oder Systemen genutzt werden können, um deren Verwundbarkeiten zu identifizieren. Ein detailliertes Modell eines Ökosystems oder eines landwirtschaftlichen Areals ist beispielsweise geeignet, Angriffsvektoren darauf zu identifizieren. Und nicht weniger erlauben beispielsweise große Datensätze aus dem Public-Health-Sektor gezielte Angriffe auf eine Bevölkerung.

Die bisher genannten verschärfenden Effekte datenintensiver Methoden in den Lebenswissenschaften hat eine gemeinsame Studie der American Association for the Advancement of Science, des Federal Bureau of Investigation und des United Nations Interregional Crime and Justice Research Institute 2014 so gefasst: „The security risks of Big Data in the life sciences fall into two major categories: 1) inappropriate access to data and analytic technologies through vulnerabilities in the data and cyber infrastructure; and 2) the use of Big Data technologies to integrate current data and enable the design of a harmful biological agent“ (Berger und Roderick 2014, S. 35).

Neben dieser Verschärfung wird die *Dual-Use*-Problematik durch die Verbreitung datenintensiver und KI-gestützter Werkzeuge in den Lebenswissenschaften aber auch erweitert. Das kann einerseits der Fall sein, weil durch neue Forschungs- und Analysemethoden sicherheitsrelevante Ergebnisse generiert werden, die sich früheren Methoden – entweder aus prinzipiellen Gründen oder aufgrund des schieren Informations- und Rechenaufwands – schlicht entzogen hätten.

Exemplarisch dafür sind jüngste Ergebnisse der Proteinforschung, in der es nicht nur mit sehr viel höherer Geschwindigkeit und Präzision möglich geworden ist, die Faltung eines Proteins auf der Basis der Aminosäurekette vorherzusagen (Jumper et al. 2021). Es ist mittlerweile auch möglich, die Interaktion von Proteinen miteinander und mit anderen Molekülen zu modellieren (Abramson et al. 2024). Damit werden aber nicht nur neue Ergebnisse für die Therapie oder in der Landwirtschaft, sondern eben auch neue Formen von biologischen Waffen erreichbar, die ohne diese Methoden voraussichtlich nicht hätten entwickelt werden können. Ähnliche Erweiterungen finden in der pharmakologischen Forschung statt, wo sogenannte *Chemical Language Models* aufgrund großer Datensätze existierender Pharmazeutika neue Substanzen zu generieren und den Raum chemischer Konstellationen auszuloten helfen (Grisoni 2023). Auch in der Genetik haben KI-basierte Ansätze neue Optionen generiert, etwa zur Vorhersage des Krankheitswertes von Mutationen oder der spezifischen Wirksamkeit von Substanzen in Abhängigkeit von der individuellen genetischen Ausstattung von Personen (Alharbi und Rashid 2022). Was erhebliche Hoffnung in der personalisierten Medizin oder für gezieltere Verfahren in der Landwirtschaft erzeugt, hat die Kehrseite, gezieltere – etwa in einzelnen Ethnien wirksame – Schädigungen zu ermöglichen.

Andererseits haben einige der neuen Werkzeuge selbst potenziell Sicherheitsrelevanz. Gemeint ist, dass die Nachbildung kognitiver Prozesse durch künstliche neuronale Netze geeignet ist, sicherheitsrelevante Aufgaben zu übernehmen. Die Nachbildungen beispielsweise des kognitiven Mechanismus zur unbewussten Identifizierung von Gefahren oder zur visuellen Objekterfassung und -verfolgung haben nicht nur klare militärische Verwendung, sondern sind teilweise bereits Gegenstand von Forschungsprojekten mit militärischen Geldgebern (Gafford 1995).

Diese Formen sicherheitsrelevanter Ergebnisse und Werkzeuge stehen bislang weitaus weniger im Fokus der Aufmerksamkeit als etwa die seit 2012 prominent diskutierten *Gain-of-function*-Experimente (s. oben). Zwar werden KI-Anwendungen sukzessive häufiger als *Dual-Use*-Güter erachtet (vgl. Kaffee et al. 2023; Schmid et al. 2022), dass davon aber auch künstlich intelligente Werkzeuge anderer Wissenschaften betroffen sind, hat bislang wenig Aufmerksamkeit gefunden. Lediglich in den spezialisierteren Diskussionen der *Dual-Use*-Problematik in den Neurowissenschaften (Moreno 2012; Dando 2020; Krishnan 2017) ist aufgefallen, dass die enge Verknüpfung der Erforschung kognitiver Prozesse und deren Implementierung in computationalen Systemen neue Potenziale für die Sicherheitsdienste und das Militär generieren.

Dass die datenintensiven und KI-basierten Lebenswissenschaften die *Dual-Use*-Problematik noch einmal verschärfen, wird vor dem Hintergrund der obigen Diskussion von *Dual Use* als Sicherheitsrelevanz besonders deutlich. Datenintensive Methoden der Lebenswissenschaften werden nicht nur direkt militärisch – etwa in Steuerungsprozessen von Militärfahrzeugen aller Art – verwendet, sie spielen auch bei anderen Sicherheitsaufgaben, insbesondere in der Aufklärung und Überwachung, eine wachsende Rolle (vgl. Krishnan 2017, S. 76 ff.; Mahfoud et al. 2018).

Dual-Use-Governance

Die Forschungsethik hat nicht nur Analysen zu den terminologischen und moralischen Herausforderungen von *Dual Use* vorgelegt, sondern auch konkrete Formen der Governance von *Dual-Use*-Herausforderungen in der Forschung entwickelt. In Deutschland ist dies insbesondere an die Gründung und Tätigkeit des Gemeinsamen Ausschusses „Sicherheitsrelevante Forschung" von DFG und Leopoldina gekoppelt. Der Gemeinsame Ausschuss ist ein Gremium, das das Bewusstsein für die Möglichkeit von *Dual Use* und für Missbrauchsrisiken sowie den verantwortungsvollen Umgang mit sicherheitsrelevanter Forschung stärken soll. Er unterstützt die Umsetzung von Empfehlungen zur Wissenschaftsfreiheit und Wissenschaftsverantwortung (Nationale Akademie der Wissenschaften Leopoldina und Deutsche Forschungsgemeinschaft 2022). Dazu gehört auch die Einrichtung und Arbeit von Ethikkommissionen für sicherheitsrelevante Forschung an deutschen Forschungseinrichtungen. Der Ausschuss fördert den Erfahrungsaustausch in diesem Bereich.

Diese und ähnliche internationale Governance-Strukturen reichen weit in die Strukturen der Forschungsinstitutionen hinein und sogar darüber hinaus. Zeitgenössische Forschungsumgebungen insgesamt haben die Verantwortlichkeiten für die Vorbereitung und Durchführung von Forschungsvorhaben zunehmend dezentralisiert. Abhängig von der institutionellen Struktur haben Forscherinnen und Forscher oft Zugang zu verschiedenen Formen der Unterstützung bei der Projektvorbereitung. Diese Unterstützungsinfrastruktur kann spezialisierte Einheiten umfassen, die sich der Erstellung von Förderanträgen widmen, sowie Ethikkommissionen, die die moralischen Überlegungen erleichtern. Wie als Gegengewicht der Unterstützungsinfrastruktur, die Forschenden zur Verfügung steht, verlangt die zeitgenössische Forschungslandschaft aber auch ein erhöhtes Maß an Wachsamkeit und Rechenschaft hinsichtlich der ethischen und gesellschaftlichen Implikationen wissenschaftlicher Untersuchungen. Die wachsende Verbreitung von *Dual-Use*-Forschung unterstreicht die Notwendigkeit robuster Governance-Mechanismen noch.

Gerade bei der Bewältigung von *Dual-Use*-Herausforderungen in der Forschung spielen verschiedene Akteure eine wichtige Rolle. Diese Akteure, auch Stakeholder genannt, sind Personen oder Gruppen, die direktes oder indirektes Interesse an einer Organisation, einem Projekt oder einem Prozess haben und von den Entscheidungen und Ergebnissen betroffen sind. Sie umfassen laut World Health Organisation (2022, S. xxiii) „scientists, the scientific community, ethics committee members, institutional and repository managers, biosafety officers, funding bodies, publishers, editors, security officials, regulators, institutional and other authorities, civil society networks, the private sector, other relevant organizations and publics". Wir können hier nicht auf die Rollen all dieser Stakeholder eingehen, wollen aber exemplarisch die Beteiligung zweier Gruppen erwähnen, die zwar innerhalb der Forschungsinstitutionen agieren, aber dennoch nicht als Forscherinnen oder Forscher an sicherheitsrelevanten Projekten.

Leitungen von Forschungsinstituten und Universitäten etwa sind allein deshalb schon relevante Stakeholder, weil sie oft die rechtliche Verantwortung für die Verbreitung von Dual-Use-Gütern im Kontext des Außenhandelsrechts tragen. Sie entwickeln interne Gremien, Richtlinien und Verfahren für die Beteiligung an sicher-

heitsrelevanter Forschung, um sicherzustellen, dass ihre eigenen Statuten – wie etwa Friedensklauseln –, aber eben auch Normen der Forschungsethik und rechtliche Standards eingehalten werden.

Neben der außenwirtschaftsrechtlichen Prüfung durch einschlägige Rechtsabteilungen bewerten Ethikkommissionen sowohl innerhalb von Forschungsinstitutionen als auch im Auftrag von Fördergebern (z. B. EU Ethics Panel) die ethischen Aspekte von sicherheitsrelevanter Forschung. Sie stellen sicher, dass die einschlägigen Prinzipien bzw. Richtlinien der Forschungsethik eingehalten werden. Eine gängige Reaktion von Institutionen für Forschungsethik auf Bedenken hinsichtlich der potenziellen Missbrauchsanfälligkeit eines Forschungsprojekts besteht darin, die eigentlich ersten Stakeholder, Forscherinnen und Forscher, aufzufordern, ihre diesbezüglichen Fachkenntnisse einzubringen. Dies kann die Aufforderung zur Erstellung eines Risikobewertungs- oder Risikominderungsplans beinhalten.

Die Notwendigkeit der Einbindung von Stakeholdern liegt in deren Fähigkeit, ein breites Spektrum an Kenntnissen und Perspektiven zu bieten, die zur ganzheitlichen Bewertung und Bewältigung der *Dual-Use*-Herausforderungen erforderlich sind. Ihre Zusammenarbeit trägt dazu bei, ein ausgewogenes Verhältnis zwischen wissenschaftlichem Fortschritt und gesellschaftlichen Interessen zu gewährleisten und die potenziellen ethischen Risiken der *Dual-Use*-Forschung zu minimieren.

Der Umstand, dass das *Dual-Use*-Problem durch datenintensive und KI-basierte Werkzeuge breitere Bereiche in den Lebenswissenschaften und der Medizin erfasst, generiert zunächst keine *neuen* ethischen Herausforderungen, sondern erweitert lediglich den Kreis der von den bestehenden Herausforderungen betroffenen Wissenschaftlerinnen und Wissenschaftler. Während bislang vom *Dual-Use*-Verdacht eher enge Bereiche der Lebenswissenschaften, etwa die Mikrobiologie, die Toxikologie oder verwandte Subdisziplinen der Chemie oder Pharmakologie betroffen waren, betrifft dies nunmehr auch andere Teildisziplinen von der computationalen Neurowissenschaft bis zur Pflanzenwissenschaft.

Dies ist umso mehr der Fall, als *Dual Use,* wie oben eingeführt, nicht einfach nur zu schädlichen Zwecken verwendbare Ergebnisse, sondern eben alle sicherheitsrelevanten Ergebnisse umfasst. Für den Bereich der Neurowissenschaften ist bereits verschiedentlich gezeigt worden, dass ihre Ergebnisse auch im Bereich der politischen Einflussnahme oder der Informationsbeschaffung geeignet sind (Dando 2020; Moreno 2012). Ähnliches dürfte mit der Verbreitung datenintensiver und KI-gestützter Methoden auf mehr und mehr andere lebenswissenschaftliche und medizinische Forschungsfeldern zutreffen.

Das bedeutet zunächst, dass die bereits bestehende ethische und rechtliche Governance für *Dual-Use*-Fragen ein breiteres Publikum erreichen muss. Das betrifft nicht nur die Information und Sensibilisierung von breiteren Gruppen von Wissenschaftlerinnen und Wissenschaftlern. Reichte es früher aus, Nachwuchswissenschaftlerinnen und Nachwuchswissenschaftler in der Mikrobiologie für die Sicherheitsrelevanz von *Gain-of-function*-Studien zu sensibilisieren, so dürfte es mittlerweile angezeigt sein, *Dual Use* in der Ausbildung zur guten wissenschaftlichen Praxis flächendeckend abzubilden.

Allein dieser Informations- und Sensibilisierungsbedarf impliziert aber bereits dreierlei. Zum ersten scheint es angezeigt, dass Institutionen ihr Curriculum zur

guten wissenschaftlichen Praxis so konzipieren, dass Fragen des *Dual Use* darin überhaupt und hinreichend tief behandelt werden, um bei den Teilnehmenden ein entsprechendes Bewusstsein für das Problem zu schaffen. Nach wie vor ist der Begriff „*Dual Use*" vielen Wissenschaftlerinnen und Wissenschaftlern über die Karrierestufen hinweg schlicht unbekannt oder Sicherheitsrelevanz und Missbrauchspotential der eigenen Forschung kein präsentes Thema (National Academies of Sciences, Engineering, and Medicine 2017).

Zum zweiten darf das entsprechende Informationsangebot zu *Dual Use* kein Dasein als Nischenthema fristen, das nur Wissenschaftlerinnen und Wissenschaftler aus bestimmten Teildisziplinen angeboten wird oder gar nur jenen, die in ihrer eigenen Arbeit bereits Sicherheitsrelevanz oder Missbrauchspotential ausgemacht haben. Das Thema gehört demnach in das Curriculum der Ausbildung in guter wissenschaftlicher Praxis über Institutionen und Disziplinen hinweg.

Drittens muss das Curriculum auch über den *Dual Use of Concern* hinaus informieren. *Dual Use* beschränkt sich wie oben vorgeführt nicht auf die Waffentauglichkeit von biologischen Strukturen. Er umfasst das Potenzial von Forschungsergebnissen, innere und äußere Sicherheit zu betreffen. Eine informierte ethische Auseinandersetzung mit dem *Dual-Use*-Potenzial eines Forschungsprojekts kann individuell wie institutionell nur gelingen, wenn *Dual Use* insgesamt berücksichtigt wird.

Das Erfordernis, einer breiter angelegten Governance betrifft aber auch die Schnittstellen von Forschung zu Forschungsunterstützung und -verwaltung. Forschungsinstitutionen sind in rechtlicher wie in ethischer Hinsicht gut beraten, Forscherinnen und Forschern die Möglichkeit einzuräumen, ihre Projekte auf Sicherheitsrelevanz prüfen zu lassen. Das geschieht normalerweise einerseits durch eine für Außenhandelsrecht zuständige Abteilung, zum anderen durch eine Kommission für Ethik sicherheitsrelevanter Forschung, eine interne Ethikkommission oder ein vergleichbares Gremium. Diese Prüf-Möglichkeit ist tatsächlich nicht hinreichend etabliert, wenn entsprechende Abteilungen vorhanden sind und Forscherinnen und Forscher darüber informiert wurden. Die Wahrscheinlichkeit, dass im laufenden Forschungs- und Antragsprozess Beratungsoptionen ungenutzt bleiben, ist allein schon aufgrund des oft hohen Zeitdrucks und der ohnehin großen Arbeitsbelastung groß. Einfache Verfahren, die Forscherinnen und Forscher als Teil des Prozesses der Einreichung bei Drittmittelgebern durch die entsprechenden Verwaltungseinheiten daran erinnern, dass eine Prüfung auf Sicherheitsrelevanz angezeigt sein könnte, sind eines von vielen möglichen Mitteln, um solche Prüf-Angebote auch in der Forschungspraxis zu verankern.

Neben der Information und Bewusstseinsbildung steht im Zentrum der Governance von *Dual Use* also die institutionelle Kontrolle. Damit sind vor allen Dingen die Kommissionen zum Umgang mit sicherheitsrelevanter Forschung gemeint. Auch für sie dürfte sich – neben der gerade erwähnten besseren Gestaltung der Schnittstelle zu den Forscherinnen und Forschern – eine parallele Verschiebung der Erfordernisse abzeichnen. Einerseits dürfte sich das Erfordernis von Kontrollstrukturen verschärfen, weil neue datenintensive Methoden die schiere Zahl von Forschungsprojekten und -ergebnissen mit Sicherheitsrelevanz erhöhen. Darüber hinaus aber dürfte die Reichweite der den Kontrollinstanzen vorgelegten Forschungsprogramme erweitert

werden müssen. Bislang müssen typischerweise Projekte der Mikrobiologie und Toxikologie oder andere Projekte, in denen militärische Verwendbarkeit erwartet wird, in entsprechenden Kommissionen verhandelt werden. Das bedeutet aber, dass ein relativ breiter Bereich von potenziell sicherheitsrelevanter Forschung in der Medizin und den Lebenswissenschaften durch das gegenwärtige Kontrollsystem nicht abgedeckt wird. Nicht nur umfasst *Dual Use* mit der Relevanz für äußere und innere Sicherheit breitere Verwendungsfelder, es generieren auch mehr Forschungsfelder Ergebnisse, die in diesem breiten Sinn sicherheitsrelevante Ergebnisse erzielen. Entsprechende spezialisierte Zuschnitte der Zuständigkeit von Beratungs- und Kontrollinstanzen bedürfen demnach einer strukturell analogen Modifikation zu Ausweitung von Information und Bewusstseinsbildung.

Danksagung Wir danken den Teilnehmenden der Klausurwoche „Dual Use und Missbrauch von Forschungsergebnissen“, und deren Förderer, dem Bundesministerium für Bildung und Forschung (01GP2187) sowie den Mitarbeiterinnen und Mitarbeitern der Arbeitsgruppe „Neuroethik und Ethik der Künstlichen Intelligenz“ am Institut für Neurowissenschaften und Medizin 7: Gehirn und Verhalten am Forschungszentrum Jülich für Anregungen und Diskussion!

Funding Open Access funding enabled and organized by Projekt DEAL.

Einhaltung ethischer Richtlinien

Interessenkonflikt J.-H. Heinrichs und S. Ergin Aslan geben an, dass kein Interessenkonflikt besteht.

Ethische Standards Für diesen Beitrag wurden von den Autor/-innen keine Studien an Menschen oder Tieren durchgeführt. Für die aufgeführten Studien gelten die jeweils dort angegebenen ethischen Richtlinien.

Literatur

Abramson J, Adler J, Dunger J, Evans R et al (2024) Accurate structure prediction of biomolecular interactions with AlphaFold 3. Nature 630(8016):493–500. https://doi.org/10.1038/s41586-024-07487-w

Ahteensuu M (2017) Synthetic biology, genome editing, and the risk of bioterrorism. Sci Eng Ethics 23(6):1541–1561. https://doi.org/10.1007/s11948-016-9868-9

Alharbi WS, Rashid M (2022) A review of deep learning applications in human genomics using next-generation sequencing data. Hum Genomics 16(1):26. https://doi.org/10.1186/s40246-022-00396-x

Berger KM, Roderick J (2014) National and transnational security implications of Big Data in the life sciences. www.aaas.org/report/national-and-transnational-security-implications-big-data-life-sciences. Zugegriffen: 28. Febr. 2024

Carter SR, Wheeler NE, Chwalek S, Isaac CR, Yassif J (2023) The convergence of artificial intelligence and the life sciences: safeguarding technology, rethinking governance, and preventing catastrophe. https://www.nti.org/wp-content/uploads/2023/10/NTIBIO_AI_FINAL.pdf. Zugegriffen: 13. Aug. 2024

Crowley M, Dando M (2022) Toxin and bioregulator weapons: Preventing the misuse of the chemical and life sciences. Palgrave Macmillan, Cham

Dando MR (2020) Neuroscience and the problem of dual use neuroethics in the new brain research projects. Springer, Cham

Forge J (2010) A note on the definition of "dual use". Sci Eng Ethics 16(1):111–118. https://doi.org/10.1007/s11948-009-9159-9

Gafford R (1995) The operational potential of subliminal perception. Studies in Intelligence 2(2). https://www.cia.gov/resources/csi/static/Potential-of-Subliminal-Perception.pdf. Zugegriffen: 27. Febr. 2024

Grisoni F (2023) Chemical language models for de novo drug design: challenges and opportunities. Curr Opin Struct Biol 79:102527. https://doi.org/10.1016/j.sbi.2023.102527

Herfst S, Schrauwen EJ, Linster M et al (2012) 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 SC, Ozawa M, Shinya K, Zhong G, Hanson A, Katsura H, Watanabe S, Li C, Kawakami E, Yamada S, Kiso M, Suzuki Y, Maher EA, Neumann G, Kawaoka Y (2012) Experimental adaptation of an influenza H5 HA confers respiratory droplet transmission to a reassortant H5 HA/H1N1 virus in ferrets. Nature 486(7403):420–428. https://doi.org/10.1038/nature10831

Imperiale MJ, Casadevall A (2018) A new approach to evaluating the risk-benefit equation for dual-use and gain-of-function research of concern. Front Bioeng Biotechnol 6:21. https://doi.org/10.3389/fbioe.2018.00021

Jakob U, Kraemer F, Kraus F, Lengauer T (2024) Applying ethics in the handling of dual use research: the case of Germany. Res Ethics. https://doi.org/10.1177/17470161241261044

Jumper J, Evans R, Pritzel A, Green T et al (2021) Highly accurate protein structure prediction with AlphaFold. Nature 596(7873):583–589. https://doi.org/10.1038/s41586-021-03819-2

Kaffee LA, Arora A, Talat Z, Augenstein I (2023) Thorny roses: investigating the dual use dilemma in natural language processing. Findings of the Association for Computational Linguistics: EMNLP 2023 https://doi.org/10.18653/v1/2023.findings-emnlp.932

Kosal ME (2020) Emerging life sciences and possible threats to international security. Orbis 64(4):599–614. https://doi.org/10.1016/j.orbis.2020.08.008

Krishnan A (2017) Military neuroscience and the coming age of neurowarfare. Routledge, London, New York

Mahfoud T, Aicardi C, Datta S, Rose N (2018) The limits of dual use. Issues in Science and Technology 34(4):73–78. https://www.jstor.org/stable/26597992. Zugegriffen: 28. Febr. 2024

McMahan J (2004) The ethics of killing in war. Ethics 114(4):693–733. https://doi.org/10.1086/422400

Miller S, Selgelid MJ (2007) Ethical and philosophical consideration of the dual-use dilemma in the biological sciences. Sci Eng Ethics 13(4):523–580. https://doi.org/10.1007/s11948-007-9043-4

Miller S, Selgelid MJ (2008) Ethical and philosophical consideration of the dual-use dilemma in the biological sciences. Springer, Dordrecht

Moreno JD (2012) Mind wars: Brain science and the military in the twenty-first century. Bellevue Literary, New York

National Academies of Sciences, Engineering, and Medicine (2017) Dual use research of concern in the life sciences: current issues and controversies. National Academies Press, Washington https://doi.org/10.17226/24761

Nationale Akademie der Wissenschaften Leopoldina, Deutsche Forschungsgemeinschaft (2022) Wissenschaftsfreiheit und Wissenschaftsverantwortung – Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung. Halle (Saale). https://www.sicherheitsrelevante-forschung.org/wp-content/uploads/2022/11/2022_Empfehlungen_Wissenschaftsfreiheit_Wissenschaftsverantwortung.pdf. Zugegriffen: 28. Febr. 2024

Resnik DB (2009) What is "dual use" research? A response to Miller and Selgelid. Sci Eng Ethics 15(1):3–5. https://doi.org/10.1007/s11948-008-9104-3

Salloch S (2018) The dual use of research ethics committees: why professional self-governance falls short in preserving biosecurity. BMC Med Ethics 19(1):53. https://doi.org/10.1186/s12910-018-0295-0

Schmid S, Riebe T, Reuter C (2022) Dual-use and trustworthy? A mixed methods analysis of AI diffusion between civilian and defense R&D. Sci Eng Ethics 28(2):12. https://doi.org/10.1007/s11948-022-00364-7

Selgelid MJ (2009a) Dual-use research codes of conduct: lessons from the life sciences. Nanoethics 3(3):175–183. https://doi.org/10.1007/s11569-009-0074-y

Selgelid MJ (2009b) Governance of dual-use research: an ethical dilemma. Bull World Health Org 87(9):720–723. https://doi.org/10.2471/blt.08.051383

Shamoo AE, Resnik DB (2009) Responsible conduct of research. Oxford University Press, Oxford, New York

Sparrow R (2007) Killer robots. J Applied Philosophy 24(1):62–77. https://doi.org/10.1111/j.1468-5930.2007.00346.x

Tigard DW (2021) There is no techno-responsibility gap. Philos Technol 34(3):589–607. https://doi.org/10.1007/s13347-020-00414-7

Urbina F, Lentzos F, Invernizzi C, Ekins S (2022) Dual use of artificial-intelligence-powered drug discovery. Nat Mach Intell 4(3):189–191. https://doi.org/10.1038/s42256-022-00465-9

Urbina F, Lentzos F, Invernizzi C, Ekins S (2023) AI in drug discovery: a wake-up call. Drug Discov Today 28(1):103410. https://doi.org/10.1016/j.drudis.2022.103410

Walzer M (2015) Just and unjust wars. A moral argument with historical illustrations. Basic Books, New York

White House Blog (2014) Doing diligence to assess the risks and benefits of life sciences gain-of-function research. https://obamawhitehouse.archives.gov/blog/2014/10/17/doing-diligence-assess-risks-and-benefits-life-sciences-gain-function-research. Zugegriffen: 28. Febr. 2024

World Health Organisation (2022) Global guidance framework for the responsible use of the life sciences: mitigating biorisks and governing dual-use research. World Health Organisation, Genf. https://iris.who.int/bitstream/handle/10665/362313/9789240056107-eng.pdf?sequence=1. Zugegriffen: 28. Febr. 2024