Einführung: Wie die Materialisierung von KI globale Sicherheitsrisiken und Governance verändert

Künstliche Intelligenz hat sich vom Forschungsbereich zur strategischen Realität entwickelt und verändert Überwachung, Logistik, Nachrichtenwesen und sogar militärische Planung. Ihr Dual-Use-Charakter erschwert die Regulierung: Dieselben Systeme, die Innovationen ermöglichen, können auch zu Desinformation, Cyberattacken oder Missbrauch im Bereich Biotechnologie beitragen. Foundation Models verstärken diese Herausforderungen, indem sie die Hürden für fortgeschrittene Funktionen senken, gleichzeitig jedoch schwer verständlich und oft unvorhersehbar bleiben. Traditionelle Rüstungskontrolle, die für materielle Systeme konzipiert wurde, ist für den Umgang mit algorithmischen Technologien nicht gut geeignet. Aber KI bietet auch Chancen, von der Unterstützung von Verifikation und Monitoring bis hin zur Verbesserung der prädiktiven Analyse.

- **Politische Entscheidungsträger*innen und Aufsichtsbehörden sollten klare Vorschriften und Richtlinien festlegen, um KI-Systeme sicher und zuverlässig zu machen.**
- **Regierungen und Unternehmen sollten zusammenarbeiten, um fortschrittliche KI-Systeme zu testen und Erfahrungen aus Problemen oder Fehlfunktionen auszutauschen.**
- **Internationale Organisationen und Staaten sollten Transparenz und vertrauensbildende Maßnahmen fördern, um Risiken zu verringern, selbst ohne formelle Verträge.**

Künstliche Intelligenz, Halbleiter und Chipkriege: Die Geopolitik von KI im Militär und in der internationalen Sicherheit

Künstliche Intelligenz und Halbleiter sind von zentraler Bedeutung für moderne militärische und strategische Fähigkeiten. Da KI Fortschritte bei Automatisierung, Entscheidungsfindung und autonomen Systemen ermöglicht, ist der Zugang zu leistungsstarken Chips zu einer Priorität der nationalen Sicherheit geworden. Die globale Chip-Lieferkette ist stark konzentriert – Schaltplanentwicklung in den USA, Bau von Produktionsmaschinen in den Niederlanden und physische Fertigung in Taiwan. Die geopolitischen Spannungen nehmen zu, insbesondere weil China, ein wichtiger Produzent von Chips mit Bestandstechnologie (≥28 nm), zunehmend von fortschrittlicheren KI-Chiptechnologien ausgeschlossen wird. Der Zugang zu seltenen Erden fügt eine weitere Ebene des strategischen Wettbewerbs hinzu. Diese Entwicklungen schüren einen globalen Wettlauf um die Kontrolle über kritische technische Infrastrukturen. Deutschland und die EU müssen jetzt belastbare Strategien entwickeln, um die Lieferketten von Halbleitern zu sichern und die strategische Autonomie zu bewahren.

- **Errichtung nachhaltiger Halbleiter-Lieferketten: Die europäischen Länder sollten die Abhängigkeit von ausländischen Chipherstellern verringern, indem sie in die heimische Halbleiterentwicklung sowie in die Produktion und Sicherung kritischer Lieferketten investieren.**
- **Schutz der europäischen Halbleiter- und KI-Assets: Da der Aufbau heimischer Halbleiterkapazitäten ein mittel- bis langfristiger Prozess ist, sollte Europa seine Vermögenswerte in der derzeitigen globalen Lieferkette vor politischer oder wirtschaftlicher Einflussnahme schützen und die Verbreitung dieser Technologie strategisch kontrollieren, um diesen Einfluss zu erhalten.**
- **Sichere Halbleiterproduktionskapazitäten und KI-Einrichtungen: Um sie als wichtiges Sicherheitsgut zu schützen, müssen Halbleiterproduktionsketten und -anlagen als kritische Infrastruktur anerkannt werden, die strenge Sicherheitsmaßnahmen erfordert. In Anerkennung des potenziellen Schadens durch Ausfälle oder Störungen sollten große KI-Serversysteme auch ausdrücklich in die bestehenden Vorschriften für kritische Infrastrukturen aufgenommen werden.**

KI im geopolitischen Innovationswettlauf

China, die USA und die EU betrachten künstliche Intelligenz als Teil des globalen Wettbewerbs, oft als „KI-Wettrüsten" bezeichnet. Wir argumentieren, dass diese Metapher die Dynamiken der KI-Entwicklung falsch darstellt. Stattdessen schlagen wir den Begriff eines „geopolitischen Innovationswettlaufs" um die technologische Vorherrschaft in einer vernetzten globalen Wirtschaft vor. Basierend auf einer Analyse von Policy-Dokumenten stellen wir fest, dass Akteure (1) zwischen Nullsummen- und Positivsummenansätzen schwanken, (2) Netzwerke je nach nationalen Innovationskulturen unterschiedlich organisieren, (3) neben Sicherheit auch wirtschaftliche und statusbezogene Ziele verfolgen, und (4) die Interpretation von KI offenhalten. Fallübergreifend verstetigt die „Wettlauf"-Metapher die „Geopolitisierung" von Innovation und verknüpft Sicherheit mit wirtschaftlichen Interessen. Vor diesem Hintergrund identifizieren wir die folgenden Kernpunkte:

- **Die Metapher des „Wettrüstens" sollte vermieden werden. Sie vereinfacht die KI-Entwicklung zu stark und birgt Eskalationsrisiken. Ein geopolitischer Innovationswettlauf basiert dagegen sowohl auf Wettbewerb als auch auf Zusammenarbeit.**
- **Rhetorik zählt. Kommunikation, die auf einer nationalistischen Redeweise von „Wettrüsten" aufbaut, fördert nur eine „Rückkehr zur Geopolitik". Es ist zwar wichtig, Probleme transparent zu machen, sie sollten aber auf differenzierte Weise kommuniziert werden.**
- **Kooperative Rahmenordnungen sollten gestärkt werden. Internationale Standards und Regulierung können**

Rivalitäten abmildern und, je nach ihrem Aufbau, Raum für verantwortungsvollere und diversere Innovation schaffen.

Kriegsführung im Prozessortakt: Der zunehmende Einsatz von KI beim Militär

Die Debatte über den militärischen Einsatz von KI hat sich mit dem Auftauchen brauchbarer (tödlicher) autonomer Waffensysteme (Lethal Autonomous Weapon Systems, LAWS) um 2010 intensiviert. Anfangs konzentrierten sich die Kritiker*innen der autonomen Waffen nur auf die Auswahl und den Einsatz von Zielen. Dieser Fokus hat sich in letzter Zeit auf die allgemeinere „Zuverlässigkeit" militärischer KI und nationaler KI-Strategien ausgeweitet. Während der volle Umfang und die Fähigkeiten der militärischen KI noch diskutiert werden, wird KI zunehmend und unauffällig in vermeintlich unkritischen militärischen Bereichen eingesetzt. Obwohl die Militärs Effizienzgewinne und deren Anwendung in scheinbar harmlosen Rollen und Funktionen feiern, werfen solche Implementierungen ernsthafte Fragen für die Rüstungskontrolle auf. Die Hauptsorgen sind die Beschleunigung der Kriegsführung und die Erosion der menschlichen Kontrolle.

- **Angesichts des Interesses der Staaten an militärischer KI sollten die Debatten über ihre Stabilität und ihre Auswirkungen auf die Sicherheit intensiviert werden. Es ist wichtig, den Fokus von ethischen oder rechtlichen Fragen auf umfassendere Sicherheitsbelange und staatliche Interessen zu verlagern.**

KI im Labor: Die Zukunft des Biodesigns

KI-unterstützte Biodesigninstrumente machen rasche Fortschritte und ermöglichen Durchbrüche auf Gebieten wie Proteindesign und Gentechnik. Das Zusammenspiel von KI und Biodesign-Technologien senkt die Hürden für die Veränderung biologischer Agenzien, indem es sowohl schnelle Innovationen als andererseits potenziell auch Missbrauch ermöglicht. Dies schafft neue Sicherheitsrisiken wie etwa die automatisierte Entwicklung schädlicher Organismen, Cyber-Bio-Angriffe auf digitale Bioentwicklungssysteme und die Umgehung bestehender Biosicherheitsvorkehrungen. Im Gegensatz zu Large Language Models (LLMs) fehlen bei KI-gestützten Instrumenten für Biodesign oft klare Sicherheitsvorkehrungen. Angesichts der zunehmenden Leistungsfähigkeit und Verfügbarkeit dieser Werkzeuge besteht ein dringender Bedarf an verantwortungsvoller Steuerung, um sicherzustellen, dass sie sicher, ethisch vertretbar und zum allgemeinen Nutzen verwendet werden.

- **Die Entwickler*innen von Biodesigninstrumenten sollten verpflichtet werden, die Risiken in jeder Phase zu bewerten und zu mindern, von der Datenerfassung über das Training der Modelle bis hin zur Veröffentlichung und dem Zugang für Nutzer*innen.**

- **Es sollte ein Spektrum von Zugangsmodellen propagiert werden (z. B. API-begrenzter Zugang, offener Zugang unter Lizenz), die auf die Anfälligkeit des Werkzeugs für Missbrauch und die vorgesehenen Nutzer*innen zugeschnitten sind.**

- **Bio- und Cybersicherheitsmaßnahmen sollten in Biodesigninstrument-Pipelines integriert werden und robuste Überwachung auf Missbrauch sowie Schutzmaßnahmen gegen Cyber-Bio-Angriffe auf digitale Bioentwicklungssysteme einschließen.**

KI-Entwicklungen in der Chemie

Die Integration von KI-Anwendungen in Chemiewerkzeuge revolutioniert die Arbeitsweise sowohl in der akademischen Forschung als auch von Industrieunternehmen. Die Anwendung von KI in der Chemie hat das Potenzial, bedeutende Fortschritte in Bereichen wie der Analyse chemischer Daten, Reaktionsplanung und Eigenschaftsvorhersage zu ermöglichen. Der inhärente Dual-Use-Charakter dieser Technologie bringt jedoch erhebliche Sicherheitsrisiken mit sich. In diesem Kapitel werden verschiedene Politikempfehlungen vorgeschlagen, um einem Missbrauch von KI in der Chemie vorzubeugen.

- **KI birgt ein erhebliches Potenzial zur Stärkung des Chemiewaffenübereinkommens und zur Unterstützung der Organisation für das Verbot chemischer Waffen in kritischen Bereichen wie Detektion, Verifikation und Bedrohungsanalyse.**

- **Der Dual-Use-Charakter dieser Technologie birgt Sicherheitsrisiken, die sich durch die Umsetzung der folgenden Empfehlungen mindern lassen könnten: Ethikschulungen als Bestandteil der wissenschaftlichen Ausbildung, strengere KI-Regulierung sowie verbesserte Sicherheitsmechanismen und Zugangsbeschränkungen für KI-Werkzeuge.**

- **Um KI-bedingte Risiken für die Chemiewaffenabrüstung zu mindern, müssen politische Maßnahmen umgesetzt werden, ohne jedoch dabei den wissenschaftlichen Fortschritt zu behindern.**

KI in der Verifikation

Künstliche Intelligenz bietet leistungsstarke Analysetechniken, die in zukünftigen Verifikationsregimen nützlich sein können. Die zunehmende Menge an verifikationsrelevanten Daten – worunter sowohl instrumentengestützte Daten als auch Informationen aus öffentlich zugänglichen Quellen fallen–, erfordert zusätzliche Werkzeuge für die Auswertung, die den Weg für KI-basierte Ansätze eröffnen. Um jedoch Vertrauenswürdigkeit der KI-Ergebnisse zu gewährleisten, muss die Herausforderung der „Erklärungsfähigkeit" („*Explainability*") – d.h., die Begründung der KI-Ergebnisse und -Schlussfolgerungen transparent und erklärungsfähig zu machen – in der Entwicklungsphase und während der Implementierung adressiert werden. Die endgültigen Entscheidungen innerhalb eines Verifika-

tionsregimes müssen in den Händen rechenschaftspflichtiger menschlicher Inspektor*innen bleiben.

- **KI-Techniken werden höchstwahrscheinlich eine Rolle in zukünftigen Verifikationsregimen spielen. Die Menge der verfügbaren Daten nimmt rapide zu und wurde bereits in anderen Zusammenhängen erfolgreich mit KI analysiert, was darauf hindeutet, dass KI zu einem unverzichtbaren Werkzeug werden wird.**

- **Die internationale Akzeptanz von KI bei der Verifikation hängt vom Vertrauen in KI-Modelle ab, das durch Transparenz der Trainingsdaten und -modelle und, wo möglich, durch gemeinsame Entwicklung und Feldübungen erreicht wird. Da die Weitergabe von sensiblen Trainingsdaten und die Transparenz der Modelle jedoch gezielte Angriffe ermöglichen kann, müssen solche Bedenken international diskutiert werden. Aus technischer Sicht trägt die Erklärungsfähigkeit der KI-Ergebnisse in allen Phasen der Entwicklung und des Einsatzes zur Vertrauensbildung bei.**

- **KI kann menschliche Entscheidungsträger*innen nicht ersetzen. Dies erfordert eine kritische Prüfung der KI-Ergebnisse durch die Aufsichtsbehörden und bei Verifikationsverfahren, bei denen die Entscheidungen letztlich auf fundierten menschlichen Einschätzungen beruhen. Die Interaktion zwischen Mensch und Computer muss so gestaltet sein, dass die Übernahme von Verantwortung berücksichtigt wird.**

Aktuelle Entwicklungen im Drohnenbereich

Der Vormarsch von Drohnen im Kampfeinsatz der Gegenwart lässt keine Anzeichen einer Verlangsamung erkennen. In der Tat werden sie immer wichtiger. Seit dem letztjährigen zusammenfassenden Artikel im CNTR Monitor hat sich die Integration von künstlicher Intelligenz in Drohnen intensiviert und zeigt sich besonders in den Bereichen Zielerkennung und -identifizierung, Schwarmverhalten und Zielbekämpfung. Außerdem geht das Katz-und-Maus-Spiel zwischen Drohnen und Drohnenabwehr immer noch weiter, wobei jede Seite abwechselnd die Oberhand gewinnt, um dann von der anderen überholt zu werden.

- **Angesichts der schlechten Aussichten für eine internationale Regulierung der Drohnenkriegsführung und der dynamischen Trends der technologischen Entwicklung muss der Drohnenabwehr sowohl im militärischen als auch im zivilen Bereich besondere Aufmerksamkeit geschenkt werden.**

Neue Reaktorgenerationen und internationale Sicherheit

Die weltweiten Bemühungen, die CO_2-Emissionen zu reduzieren und gleichzeitig die steigende Stromnachfrage zu decken, haben zu einem erneuten Interesse an der nuklearen Stromerzeugung geführt. Zu diesem Zweck wurden neue Reaktorkonzepte und Umsetzungsstrategien verfolgt, darunter modulare Kleinreaktoren (*Small Modular Reactors*, SMRs) und alternative Reaktorkonzepte (*Novel Advanced Reactors*, NARs) als Alternativen zu herkömmlichen Großkraftwerken. Da jedoch einige dieser Konzepte und Einsatzstrategien eine höhere Brennstoffanreicherung und dezentrale Standorte vorsehen, stellen sie neue Herausforderungen für Sicherungsvorkehrungen und die Kernmaterialüberwachung dar. Außerdem kann die Kompaktheit dieser Reaktoren den Zugang zu Verifikationszwecken erschweren. Da sich diese Konzepte noch im Stadium der Forschung und Entwicklung befinden, gibt es ein Zeitfenster, in dem diese Überlegungen bei der Planung künftiger Nuklearanlagen berücksichtigt werden können.

- **Die steigende Nachfrage nach Elektrizitätsproduktion mit geringem CO_2-Ausstoß macht neue Arten von Kernkraftwerken, wie z. B. modulare Kleinreaktoren mit dezentraler Standortwahl, attraktiv.**

- **Die potenzielle Zunahme von Nuklearstandorten und der Vorstoß in Richtung Uran im oberen Bereich der schwachen Anreicherung, auch „HALEU"-Brennstoff genannt, mit einer Urananreicherung von bis zu 20% wirft neue Sicherheits- und Proliferationsbedenken auf.**

- **Modulare Kleinreaktoren und alternative Reaktorkonzepte befinden sich noch in der Forschungs- und Entwicklungsphase. Dies bietet die Möglichkeit, den Bedarf an bestimmten Materialien und Techniken zu bewerten, neue Sicherungs- und Kernmaterialüberwachungskonzepte zu entwickeln und sicherzustellen, dass Fragen der nuklearen Sicherung bereits in der Entwurfsphase berücksichtigt werden.**

Autonome Laboratorien

Autonome Laboratorien (SDLs, *Self-Driving Laboratories*) sind eine aufkommende Technologie, die künstliche Intelligenz, Chemie und Robotik kombiniert, um die Laborforschung schneller, reproduzierbarer und potenziell autonom durchführbar zu machen. Trotz der beachtlichen Fortschritte, die sowohl die Wissenschaft als auch die Industrie in den letzten Jahren erzielt haben, befinden sich autonome Labore noch in einem frühen Stadium der Entwicklung. Ihr potenzieller Dual-Use-Charakter unterstreicht jedoch die Notwendigkeit eines proaktiven und umfassenden Steuerungsrahmens. Aus Verteidigungssicht könnten autonome Labore eine wertvolle Rolle spielen, indem sie die Entdeckung und Synthese von Gegenmitteln beschleunigen.

- **Autonome Labore könnten zur Verteidigung beitragen, indem sie die automatische Synthese bestehender Gegenmittel gegen chemische Kampfstoffe ermöglichen oder bei der Entwicklung neuer Gegenmittel helfen.**

- **Ein solider Steuerungsrahmen, der Bildungsinitiativen, rechtliche Regulierungsinstrumente und Zugangsbe-**

schränkungen umfasst, sollte für autonome Labore eingeführt werden, auch wenn sie derzeit noch im Entstehen sind.

- Zwar sind die potenziellen chemischen Sicherheitsrisiken, die von autonomen Laboren ausgehen, zu berücksichtigen, doch ihre technische Komplexität und die fortgeschrittenen Anforderungen machen ihren Einsatz bei der Entwicklung chemischer Kampfstoffe weniger wahrscheinlich.

Spiegelleben und die Wissenschaft der Chiralität

Der Begriff „Spiegelleben" (*mirror life*) bezeichnet synthetische Organismen, die aus spiegelbildlichen Biomolekülen aufgebaut sind, was sie biochemisch unvereinbar mit natürlichem Leben macht. Obwohl sie anfangs als vielversprechend für Anwendungen in der Medizin und bei der Eindämmung von Krankheiten angesehen wurden, warnen neuere Analysen davor, dass robuste Spiegelorganismen Immunreaktionen entgehen, dem Abbau widerstehen und sich unvorhersehbar verbreiten könnten. Mehrere Expert*innen drängen auf frühzeitiges politisches Handeln, um die Herausforderungen für die Biosicherheit und Steuerung zu bewältigen, bevor Spiegelleben technisch machbar wird.

- Regierungen und internationale Wissenschaftsgremien sollten ein vollständiges Moratorium für die Forschung an Spiegelleben in Erwägung ziehen. Dies würde Zeit für eine weitere sorgfältige Prüfung der potenziellen Risiken und Vorteile, ethische Überlegungen und einen internationalen Dialog bieten.

- Wenn die Forschung fortgesetzt wird, sollten globale Normungsgremien internationale Richtlinien für biologische Sicherheit und den Arbeitsschutz in diesem Bereich entwickeln. Diese sollten sich mit dem Containment von Laboren, dem Verbot der Freisetzung von Schadstoffen in die Umwelt, den Governancestrukturen und den Mechanismen der Rechenschaftspflicht befassen.

- Politische Entscheidungsträger*innen und Forschungseinrichtungen sollten Programme zur Beobachtung und Risikobewertung einrichten. Diese sollten eine unabhängige wissenschaftliche Überprüfung, öffentliche Berichterstattung und eine laufende Neubewertung der ökologischen und gesellschaftlichen Risiken umfassen. Sie sollten auch Frühwarnsysteme einschließen, um unbeabsichtigte Ergebnisse oder Containment-Verletzungen zu erkennen.

DNA-Synthese-Screening

In dem Maße, in dem DNA-Synthese verfügbarer wird, wachsen die Bedenken hinsichtlich eines möglichen Missbrauchs, insbesondere durch KI-entwickelte Krankheitserreger und Cyber-Bio-Bedrohungen. Während Screeninginstrumente und Sicherheitsrahmen sich weiterentwickeln, bleiben erhebliche Lücken in der (globalen) Politik, der Cybersicherheit und der Überwachung. Als Lehre aus dem Bereich der digitalen Sicherheit fordern Expert*innen verbesserte Detektionsmethoden, universale Screening-Standards und mehr Cyber-Biosicherheit, um aufkommende Risiken einzudämmen.

- Regierungen und internationale Regulierungsbehörden sollten universale Screening-Standards für DNA-Synthese-Bestellungen einführen, einschließlich von Know-Your-Customer- und Know-Your-Order-Prozessen, um eine einheitliche Aufsicht über Anbieter*innen zu gewährleisten.

- Politische Entscheidungsträger*innen und wissenschaftliche Einrichtungen sollten internationale Kooperationen einrichten, um Screeninginstrumente regelmäßig zu aktualisieren und zu überprüfen, und dabei KI-fähige Systeme einbeziehen, um neue synthetische Bedrohungen zu erkennen.

- Universitäre und kommerzielle Laboratorien, die sich mit DNA-Synthese beschäftigen, sollten strenge Cybersicherheitsmaßnahmen einführen, um das wachsende Risiko von Cyber-Bio-Angriffen zu verringern.

Technologiepräferenzen von fünf Demokratien westlichen Stils: Eine Analyse sicherheitspolitischer Technologiestrategien

Der Charakter der Kriegsführung entwickelt sich ständig und mit hoher Geschwindigkeit weiter. Dieses Kapitel befasst sich mit Militärtechnologien, die auf den Schlachtfeldern der Zukunft eine Schlüsselrolle spielen könnten. Wird der Krieg gegen die Ukraine zum künftigen Maßstab der Militärtechnologie, oder denken manche Länder bereits weiter? Durch Analyse der beiden neuesten Militärtechnologiestrategien von fünf Nationen zeigt die Studie, dass neben Kommunikations- und KI-Technologien auch modernisierte „Bestands"-Systeme wie Panzer, Kampfflugzeuge und Seestreitkräfte entscheidend bleiben. Aber auch auf fortschrittliche Raketentechnologie, KI und Aufklärung wird ein großer Wert gelegt. Während die militärische Nutzung von KI seit langem international ein Grund zur Besorgnis ist, wurde die destabilisierende Wirkung konventioneller Raketen weltweit noch nicht ausreichend beachtet. Dieses Thema erfordert eine intensivere Diskussion, die sich auf Leitlinien, wirksame Abwehrmaßnahmen und Rüstungskontrolle konzentriert.

- Die internationale Debatte über die destabilisierende Wirkung von Raketen sollte intensiviert werden.

- In Deutschland ist eine intensivere Debatte über künftige Technologieentscheidungen erforderlich.