

3



2026 / Risiken und Chancen neuer Technologien /

RÜSTUNGSDYNAMIKEN

- 3.1** ↘ Technische Innovationen und Dual-Use-Problematik
- 3.2** ↘ Technische Innovationen und Rüstungskontrolle

↓ EMPFEHLUNGEN

3

92

1 Zivile Sicherheits- und Verteidigungsforschung fördern

Zivile Sicherheits- und Verteidigungsforschung und die Kooperation mit dem Militär erfordern eine erhöhte Forschungssicherheit, ohne die Wissenschaftsfreiheit zu beeinträchtigen. Verbote (von Zivilklauseln) oder Verpflichtungen (zur Zusammenarbeit mit der Bundeswehr) sind kontraproduktiv.

2 Künstliche Intelligenz und digitale Souveränität stärken

Deutschland und Europa sollten KI-Schlüsselkompetenzen ausbauen und die Abhängigkeit von den USA und China reduzieren. Dazu gehören Forschungs- und Innovationskapazitäten, der Zugang zu kritischen Rohstoffen und Rechenressourcen sowie resiliente Wertschöpfungsketten.

3 Abhängigkeit von US-Defensivsystemen reduzieren

Die Abhängigkeit von Abfangraketen aus US-Beständen sollte durch europäische Ko-Produktion und koordiniertes Bestandsmanagement verringert werden.

4 Stationierungsmoratorium für Mittelstreckentraketen

Deutschland sollte ein Stationierungsmoratorium für neue landgestützte Raketen im ehemaligen INF-Reichweitenbereich anstreben, verbunden mit reziproken Transparenzmaßnahmen.

5 Abrüstungsengagement in der OVCW aufrechterhalten

Deutschland sollte den Abrüstungsprozess in Syrien weiter unterstützen. Mutmaßliche Chemiewaffeneinsätze Russlands in der Ukraine sollten unabhängig untersucht und internationale Initiativen zur Aufklärung und Rechenschaftspflicht gefördert werden.

6 Biowaffenkontrolle stärken

Deutschland sollte den BWÜ-Prozess stärken, destruktiven Bestrebungen entgegenwirken und den Aufbau eines wissenschaftlichen Beratungsgremiums fördern. In der Verifikation sollten KI-Anwendungen geprüft und eigene, technisch fundierte Vorschläge sowie praktische Übungen eingebracht werden.

7 Neue Proliferationsrisiken frühzeitig thematisieren

Deutschland sollte international darauf hinwirken, die Proliferationsrisiken höherer Urananreicherungsgrade für neuartige Reaktorsysteme zu thematisieren. Die Nuklearindustrie muss aufgefordert werden, Safeguards-Optionen bereits während der Entwicklungsphase mitzudenken.

8 Für Akzeptanz von KI in der Verifikation werben

Neue Technologien können Verifikationsverfahren stärken, müssen dafür aber international Akzeptanz finden. Für die Nutzung von KI in der Verifikation könnte Deutschland mittels eines Workshops einen Prozess anstoßen, um systematisch Möglichkeiten und Herausforderungen zu eruieren.

RÜSTUNGSDYNAMIKEN /

Risiken und Chancen neuer Technologien /

Neue Technologien bieten enorme Chancen, bergen zugleich aber erhebliche Risiken für Frieden und Sicherheit. Die Dual-Use-Problematik macht deutlich, dass zivile technologische Entwicklungen auch militärische Verwendungen haben können und vor Missbrauch geschützt werden müssen. Eine zukunfts-fähige Regulierung muss kooperativ, vorausschauend und anpassungsfähig sein – und die Balance zwischen Freiheit der Forschung, Dynamik der Wirtschaft und internationaler Sicherheit neu austarieren.

3.1 ✓ Technische Innovationen und Dual-Use-Problematik

Wissenschaftlicher und technologischer Fortschritt eröffnet enorme Potenziale für gesellschaftliche Entwicklung, wirtschaftliche Prosperität und internationale Kooperation. Gleichzeitig verschärft er ein grundlegendes Dilemma: Viele Technologien besitzen einen inhärenten Dual-Use-Charakter – sie können sowohl für friedliche, zivile Zwecke eingesetzt als auch für militärische oder kriminelle Anwendungen missbraucht werden. Diese Ambivalenz macht neue Technologien zu einem zentralen Thema für Sicherheitspolitik und Rüstungskontrolle.

Moderne Technologien – von datengetriebenen Systemen über vernetzte Maschinen bis hin zu biotechnologischen Verfahren – erweitern die Handlungsmöglichkeiten von Staaten, nichtstaatlichen Akteuren und Individuen. Sie ermöglichen eine effizientere Produktion, bessere Versorgung, neue Kommunikationsformen und verbesserte Krisenreaktion. Gleichzeitig können dieselben Technologien Fähigkeiten schaffen, die bestehende Machtverhältnisse verschieben, Proliferationsrisiken erhöhen oder neue Formen von Gewalt und Destabilisierung ermöglichen. Diese Ambivalenz wird dadurch verschärft, dass viele Technologien in frühen Entwicklungsstadien schwer einzuschätzen sind. Forschung, die mit guten Absichten betrieben wird, kann unbeabsichtigte Risiken erzeugen – etwa durch unvorhergesehene Nebenwirkungen, Zweckentfremdung oder Spionage und Diebstahl.

Klassische Instrumente der Rüstungskontrolle können mit der technologischen Entwicklung kaum Schritt halten

Die Regulierung neuer Technologien ist besonders anspruchsvoll, weil sie sowohl deren objektive Eigenschaften als auch die subjektiven Nutzungsabsichten berücksichtigen muss. Klassische Instrumente wie Exportkontrollen oder nationale Genehmigungsverfahren geraten dabei zunehmend an ihre Grenzen: Sie reagieren oft zu langsam, sind zu eng gefasst oder werden stark von politischen Prioritäten geprägt, sodass sie mit der Geschwindigkeit technologischer Entwicklungen kaum Schritt halten können. Während internationale Abkommen in einigen Bereichen robuste Rahmenbedingungen bieten, fehlen für viele neue Technologien vergleichbare Strukturen. Stattdessen gewinnen Soft-Law-Regime, freiwillige Standards und Formen der wissenschaftlichen Selbstregulierung an Bedeutung – allerdings mit sehr unterschiedlichen Umsetzungsniveaus und ohne verbindliche Durchsetzungsmechanismen. Vor diesem Hintergrund besteht die zentrale Herausforderung darin, Innovation zu ermöglichen, ohne die damit verbundenen Sicherheitsrisiken zu vernachlässigen. Eine wirksame Regulierung muss daher mehrere Ziele gleichzeitig verfolgen: Risiken und Chancen frühzeitig erkennen und transparent machen, um Missbrauch zu verhindern; flexible und adaptive Regulierungsmechanismen schaffen, ohne Forschung und wirtschaftliche Entwicklung zu blockieren; und die Verantwortung von Forschenden, Institutionen und staatlichen Stellen klar definieren, ohne die Bürokratie ins Unermessliche wachsen zu lassen.

KÜNSTLICHE INTELLIGENZ

Künstliche Intelligenz (KI) gilt als zentraler Treiber tiefgreifender wirtschaftlicher und sicherheitspolitischer Transformationen. Vor allem Fortschritte im maschinellen Lernen und bei großen Sprachmodellen (large language models, LLMs) haben KI von spezialisierten Anwendungen zu einer allgemeinen Schlüsseltechnologie (general purpose technology) gemacht, die nahezu alle Lebens- und Produktionsbereiche durchdringt – von Verwaltung und Industrie bis zu Kommunikation, Sicherheit und Kriegsführung.

Diese Entwicklung ist eng mit der politischen Ökonomie ihrer materiellen Grundlagen verknüpft. Rechenkapazitäten, Daten, Chips, Halbleiter, Energie und kritische Rohstoffe sind hochgradig konzentriert und zunehmend Gegenstand geopolitischer Instrumentalisierung. Eigentum und Kontrolle über diese Ressourcen erhalten strategische Bedeutung. Rivalitäten, besonders zwischen den USA und China, zeigen sich in Exportkontrollen, Industriepolitik, Eingriffen in ausländische Halbleiterunternehmen und Konflikten um seltene Erden.

Die massive Nachfrage nach KI wirkt als Beschleuniger dieser Spannungen. Sie verändert nicht nur das Verhalten staatlicher Akteure, sondern verschiebt auch Macht- und Produktionsverhältnisse, indem neue Abhängigkeiten entstehen. Europäische Staaten und Schlüsselunternehmen wie das niederländische ASML oder Zeiss geraten dabei in Gefahr, ihre strategische Autonomie zu verlieren und zwischen den Machtzentren marginalisiert zu werden.

Der Dual-Use-Charakter von KI stellt die Regulierung vor Herausforderungen

Besonders herausfordernd ist der ausgeprägte Dual-Use-Charakter von KI. Viele Systeme, die für zivile Optimierung, Automatisierung oder Entscheidungsunterstützung entwickelt werden, lassen sich ohne grundlegende technische Modifikation militärisch nutzen. Die gleichen Modelle, die Verkehrsflüsse steuern oder industrielle Prozesse verbessern, können Zielerkennung, Logistikplanung oder Lageanalyse im militärischen Kontext ermöglichen. Da KI überwiegend Software-basiert, leicht übertragbar und oft offen zugänglich ist, greifen klassische Kontrollmechanismen – etwa Exportregime oder Rüstungskontrolle – nur begrenzt. Nicht einzelne Produkte, sondern abstrakte Funktionen müssten kontrolliert werden, was angesichts global fragmentierter Wertschöpfungsketten und schwer zuzuordnender Verantwortlichkeiten kaum praktikabel ist.

Diese Dual-Use-Eigenschaft verstärkt militärische Dynamiken zusätzlich. KI ermöglicht die Verarbeitung großer Datenmengen in Echtzeit, automatisiert Entscheidungsprozesse und erhöht damit die operative Geschwindigkeit. Besonders sichtbar wird dies bei Drohnensystemen, die durch KI autonomer und widerstandsfähiger werden. Parallel gewinnt KI im Cyber-Raum an Bedeutung, wo Angriffe automatisiert und skaliert erfolgen. Auch Möglichkeiten hybrider Kriegsführung wachsen: Automatisierte Desinformation, microtargeting – also die gezielte Ansprache einzelner Gruppen mit personalisierten Botschaften – und die Manipulation öffentlicher Diskurse werden von antiliberalen Akteuren wie Russland genutzt und finden auch in den USA zunehmend Anwendung. Wer KI kontrolliert, beeinflusst damit nicht nur Märkte, sondern auch Informationssphären und strategische Handlungsspielräume.

KI ist damit weniger neutraler technologischer Fortschritt als Verstärker machtpolitischer Rivalität. Regulierung stößt dort an Grenzen, wo wirtschaftliche Interessen, militärische Vorteile und geopolitische Konflikte dominieren. Die Dual-Use-Problematik erschwert wirksame Kontrolle, während der technologische Wettbewerb weiter eskaliert. KI wird so zu einem zentralen Faktor zukünftiger Konflikt und Ordnungsfragen, der klassische Regulierungs- und Rüstungskontrollansätze herausfordert.

AUTONOME SYSTEME

3
96

Im Bereich der Robotik und autonomen Waffensysteme findet – nicht zuletzt durch den russischen Krieg gegen die Ukraine – ein kontinuierlicher technologischer Fortschritt statt. Autonomie betrifft bislang vor allem unkritische Funktionen wie selbstständige Navigation, Routenplanung und Schwarmkoordination von Drohnen sowie boden- und seegestützte Systeme. Getrieben wird dies wesentlich durch den zivilen Robotiksektor: Autonome Lieferfahrzeuge, industrielle Robotik, Logistiksysteme oder Assistenzroboter nutzen Sensorik, Bewegungsplanung und Objekterkennung, die nahezu identisch in militärischen Plattformen eingesetzt werden können. Der Dual-Use-Charakter ist damit strukturell angelegt.

Zunehmend kommt KI auch bei der Zielidentifizierung zum Einsatz, etwa wenn Systeme Tarnnetze erkennen und Bediener:innen auf mögliche Ziele hinweisen. Die Entscheidung über die Zielbekämpfung liegt jedoch meist weiterhin beim Menschen, obwohl es technisch seit Jahren möglich wäre, Angriffsentscheidungen ganz an das System zu delegieren – das heißt vollständig autonome Waffen einzusetzen. Die Entwicklung in diese Richtung hält an: Die Verwundbarkeit ferngelenkter Drohnen gegenüber elektronischen Gegenmaßnahmen erhöht zum Beispiel den Druck, Systeme zu entwickeln, die ohne stabile Datenverbindung operieren können. In der Ukraine werden Drohnen per Glasfaserkabel gesteuert, was Reichweite und Flexibilität einschränkt. Entsprechend arbeiten Anbieter an Optionen, Drohnen vollautonom gegen spezifische Ziele – wie Radareinrichtungen – einzusetzen, um Störungen zu umgehen. Der deutsche Hersteller Helsing bewirbt seine HX-2-Drohne explizit mit der Fähigkeit, dank integrierter KI Ziele auch ohne kontinuierliche Datenverbindung bekämpfen zu können.

Dass solche Möglichkeiten bislang nur begrenzt genutzt werden, zeigt, dass die seit 2014 international geführte Debatte über autonome Waffensysteme und die Notwendigkeit sinnvoller menschlicher Kontrolle Wirkung entfaltet hat. Gleichzeitig mehrten sich aber Hinweise, dass diese Zurückhaltung unter Druck erodieren könnte – sei es durch militärische Notlagen oder durch Staaten, die bereit sind, vollautonome Systeme einzusetzen. Die jüngste Auseinandersetzung zwischen dem US-Kriegsminister Pete Hegseth und dem KI-Unternehmen Anthropic verdeutlicht dies und zeigt, dass normative Einwände aus Wissenschaft, Politik oder Wirtschaft gegenüber machtpolitischen Interessen nur begrenzte Wirkung haben.

Die bisherige Zurückhaltung bei autonomen Waffensystemen könnte politisch unter Druck geraten

CYBER

Cyber-Angriffe sind längst zentrale Instrumente hybrider Einflussoperationen – sowohl in Friedenszeiten als auch in bewaffneten Konflikten, etwa zwischen Indien und Pakistan. Ihr Umfang wächst stetig. Angreifer nutzen technologische Fortschritte, insbesondere KI, um Operationen effizienter und wirkungsvoller zu gestalten. Die Fähigkeit, mit KI Schadsoftware zu entwickeln oder automatisiert Phishing-Attacken und komplexe Angriffstechniken ohne tiefes Fachwissen auszuführen, senkt die Schwelle für offensive Cyber-Fähigkeiten erheblich. Der Dual-Use-Charakter digitaler Technologien verstärkt diese Dynamik: Dieselben KI-Modelle, die in Unternehmen zur Automatisierung oder Fehlererkennung eingesetzt werden, können nahezu unverändert für Cyber-Angriffe genutzt werden.

Damit verschwimmen die Grenzen zwischen Cyber-Sicherheit und Informationsoperationen zunehmend zu einer Form der kognitiven Kriegsführung. Ziel ist es dabei, Wahrnehmung und Urteilsvermögen von Menschen durch Desinformation, deepfakes und andere künstlich erzeugte Medien zu beeinflussen. Wenn technische Mittel täuschend echte Inhalte erzeugen können, bricht das gemeinsame Verständnis von Wahrheit auseinander – ein Zustand, der Manipulation erleichtert und demokratiefeindliche Dynamiken begünstigt. Einige staatliche Akteure nutzen dies gezielt und systematisch aus. Besonders sichtbar wird dies auf Social-Media-Plattformen, deren Regulierung trotz Ansätzen wie dem EU Digital Services Act schwierig bleibt, da auch hier Dual-Use-Probleme bestehen: Werkzeuge zur Moderation und Personalisierung können ebenso zur Manipulation eingesetzt werden.

Cyber-Angriffe und Informationsoperationen werden zu kognitiver Kriegsführung

Mit der rasanten Verbreitung digitaler Technologien und ihrer Bedeutung für alle gesellschaftlichen Bereiche geraten die zugrunde liegenden Infrastrukturen selbst zunehmend ins Visier. Besonders deutlich zeigt sich dies an wiederholten, mutmaßlich staatlich gelenkten Sabotageakten gegen Untersee-Glasfaserverbindungen, dem Rückgrat globaler Internetversorgung. Solche Störungsversuche nehmen sowohl in der Ostsee als auch in der Straße von Taiwan zu, sind jedoch aufgrund komplexer seerechtlicher Regelungen schwer international zu ahnden.

BIOTECHNOLOGIE

Auch in der Biotechnologie stellen technologische Innovationen, die zunehmend von KI unterstützt werden, einen Trend dar, der sich auf die internationale Sicherheit auswirken kann. KI-gestützte Bidesign-Tools ermöglichen inzwischen in beeindruckendem Ausmaß die schnelle Vorhersage von Proteinstrukturen, die Optimierung von Sequenzen sowie funktionelles Design. Sie beschleunigen den Fortschritt in der Medizin, Impfstoffentwicklung und industriellen Biotechnologie. Gleichzeitig senken sie die technischen Hürden für das Design oder die Veränderung von biologischen Agenzien, was die seit langem bestehenden Bedenken bezüglich des Dual-Use-Potenzials in diesem Feld verstärkt.

Das Dual-Use-Problem ist in der Biologie besonders ausgeprägt, da Forschungen, die oft wichtige Erkenntnisse etwa für den Gesundheitsschutz bringen, zum Teil auch für unfriedliche Zwecke missbraucht werden könnten. Eine Regulierung des Forschungsfeldes ist daher kompliziert und wird dadurch weiter erschwert, dass schädliche Eigenschaften oft vom Kontext abhängen und auf der Ebene von Sequenzen oder Modellen nicht leicht zu erkennen sind. Ein Protein oder genetisches Konstrukt, das an sich harmlos erscheint, kann sich trotzdem als schädlich herausstellen, wenn es in ein lebendes System eingebaut wird.

Zwar wurde in den letzten Jahren mehr politische Aufmerksamkeit auf diese Risiken gerichtet, aber die Regelungen in diesem Bereich sind nach wie vor fragmentiert. Im Unterschied zu LLMs verfügen Bidesign-Tools über weniger Sicherheitsvorkehrungen. Fachleute betonen deshalb die Notwendigkeit gestufter Schutzmaßnahmen – etwa die Kontrolle der verwendeten Trainingsdaten, Begrenzungen der verfügbaren Rechenleistung, verpflichtende Risikoprüfungen vor der Anwendung sowie einen kontrollierten, nicht frei zugänglichen Zugriff über Programmierschnittstellen. Vorgeschlagen wird zudem, Wasserzeichen in gentechnisch veränderte Sequenzen einzufügen und die genetische Attribuierung (genetic engineering attribution) zu verstärken, um von Missbrauch abzuschrecken und verantwortungsbewusstes Verhalten zu fördern. Allerdings ergeben sich Bedenken hinsichtlich des freien Zugriffs auf wissenschaftliche Erkenntnisse, der Marktmacht und des ungleichen Zugangs zur Technologie.

Derzeit gibt es keinen einheitlichen internationalen Rahmen, um den Zugang zu Hochrisiko-Biotools oder sensiblen Daten zu regulieren. In der EU zeigt die Biotech and Biomanufacturing Initiative zwar ein wachsendes Bewusstsein für die sicherheitspolitischen Risiken, doch der Schwerpunkt liegt weiterhin auf Wettbewerbsfähigkeit statt auf Rüstungskontrolle. Die bestehende Lücke zwischen der Anerkennung der Risiken und verbindlichen Regeln wird durch Forderungen nach EU-weiten Know-Your-Order-Vorgaben besonders deutlich.

Bestehende Regime wie das Biowaffen-Übereinkommen (BWÜ) tun sich schwer mit der Verifikation, Attribuierung und Kontrolle in einem KI-gesteuerten Forschungsfeld. Gleichzeitig könnten neue technische Werkzeuge wie fortgeschrittene Bioüberwachung, Bioforensik und Design-Attribuierung künftig vertrauensbildende und Compliance-Maßnahmen unterstützen. An der Biotechnologie zeigt sich exemplarisch, wie neue Technologien gleichzeitig neue Risiken und neue Mittel zum Management eben diese Risiken schaffen können.

Bestehende Instrumente der Rüstungskontrolle sind nicht ausreichend für KI-getriebene Biotechnologie

DUAL USE UND FORSCHUNGSSICHERHEIT

Auf nationaler Ebene verschärft sich die Dual-Use-Problematik in dem Maße, in dem – angesichts der weltpolitischen Lage nicht zu Unrecht – gefordert wird, dass sich die zivile, insbesondere universitäre Forschung stärker an Sicherheits- und Verteidigungsforschung beteiligt. Viele Hochschulen verfügen jedoch nicht über die Sicherheitsvorkehrungen, die verhindern, dass wissenschaftliche Erkenntnisse ausspioniert, gestohlen oder für militärische oder terroristische Zwecke missbraucht werden können. Der Wissenschaftsrat und andere Organisationen fordern daher den Aufbau oder die Stärkung institutioneller Strukturen, etwa Ethik und Sicherheitskommissionen, die das Bewusstsein für Risiken sicherheitsrelevanter Forschung schärfen und die Forschungssicherheit bei Dual-Use-Projekten erhöhen (→ Wissenschaftsrat 2024; → DFG/Leopoldina 2022).

Weitergehende Forderungen, bestehende Zivilklauseln auszuweiten oder Dual-Use-Forschung ganz zu verbieten, greifen zu kurz, weil sich die Grenze zwischen ziviler und militärischer Nutzung in vielen Bereichen faktisch nicht ziehen lässt. Zivilklauseln haben vor allem symbolischen Charakter: Sie erinnern an die Verantwortung der Wissenschaft für den Frieden, können aber die im Grundgesetz garantierte Wissenschaftsfreiheit nicht einschränken oder Sicherheits- und Verteidigungsforschung verbieten. Umgekehrt schützt die Wissenschaftsfreiheit aber auch vor einem Zwang zur Militärforschung oder der Verpflichtung zur Kooperation mit der Bundeswehr. Um die Sicherheits- und Verteidigungsforschung an deutschen Hochschulen zu fördern, ist deshalb nicht die Abschaffung der Zivilklausel notwendig, sondern die Stärkung der Forschungssicherheit im Umgang mit Dual-Use-Risiken.

Die Forschungssicherheit an deutschen Hochschulen muss erhöht werden

3.2 ✓ Technische Innovationen und Rüstungskontrolle

Neuere Technologien entziehen sich aufgrund ihrer Dual-Use-Qualität tendenziell traditionellen Mechanismen der Rüstungskontrolle. Wie steht es aber um die bestehende Rüstungskontrollarchitektur, und welche Auswirkungen haben technische Innovationen hier?

NUKLEARE RÜSTUNGSKONTROLLE

Mit dem Auslaufen des New START-Vertrags im Februar 2026 unterliegen die größten Nukleararsenale der USA und Russlands erstmals seit 1972 keinen vertraglichen Begrenzungen mehr. Bereits zuvor waren zentrale Elemente der bilateralen Rüstungskontrolle – der INF-Vertrag (Verbot landgestützter Mittelstreckenraketen) und der ABM-Vertrag (Begrenzung von Raketenabwehrsystemen) – weggefallen. Mit New START gehen nicht nur Obergrenzen für Sprengköpfe und Trägersysteme verloren, sondern auch die verlässlichen Verifikations und Transparenzmechanismen, die über Jahrzehnte zur Stabilisierung der nuklearen Rivalität beigetragen hatten. Ob Washington und Moskau informell an bisherigen Grenzen festhalten oder ein beschleunigter Rüstungswettlauf einsetzt, bleibt offen. Chinas rascher Ausbau seines Arsenalts erschwert jedenfalls jede Rückkehr zu bilateralen Formaten.

Parallel verschärfen regionale Konflikte die Lage. 2025 kam es zur schwersten militärischen Auseinandersetzung zwischen Indien und Pakistan seit Jahrzehnten. Im Juni 2025 und März 2026 führten die USA und Israel Präventivkriege gegen den Iran, um unter anderem das iranische Nuklearprogramm, das offiziell zivilen Zwecken dient, zu zerstören. Damit ist das 2015 ausgehandelte Abkommen über das iranische Atomprogramm (JCPOA) endgültig gescheitert: Nach der US-Kündigung des Abkommens im Mai 2018 unter Präsident Trump gaben 2025 auch die EU-Staaten ihre Rettungsversuche auf. Der Iran selbst erklärte den Deal im Oktober 2025 für nichtig.

Vor diesem Hintergrund steht die Überprüfungskonferenz des nuklearen Nichtverbreitungsvertrags (NVV) 2026 unter schlechten Vorzeichen. Eine Einigung erscheint angesichts russischer Blockadehaltung und der erwartbaren Kritik vieler Staaten an den US-israelischen Luftschlägen gegen einen (noch) nicht nuklear bewaffneten Staat unwahrscheinlich. Auch der Umfassende Teststoppvertrag (CTBT) ist geschwächt: Russlands Rückzug 2023 und die Ankündigung der US-Regierung 2025, nach über 30 Jahren wieder Nuklearwaffentests in Erwägung zu ziehen, bedrohen die fortbestehende Teststopp-Norm. Gleichzeitig bemühen sich die Vertragsstaaten des NVV um die Aufarbeitung der humanitären Folgen früherer Tests – ein Ausdruck der tiefen Polarisierung der globalen Nukleardebatte. Das „nukleare Tabu“ bleibt bislang zwar gewahrt, doch seine Resilienz ist angesichts zunehmender Drohgebärden nicht garantiert.

Die nukleare Rüstungskontrolle ist in der Krise, die Proliferationsrisiken steigen

Die Proliferationsrisiken nehmen parallel zu. Die größten Gefahren gehen weiterhin von Spaltmaterialbeständen und den Technologien des Brennstoffkreislaufs aus. Nach den israelischen Angriffen auf iranische Nuklearanlagen ist unklar, wo sich das auf 60 % angereicherte Uran befindet; es könnte für eine primitive nukleare Explosion ausreichen. Zudem gibt es Hinweise auf neue iranische Anreicherungskapazitäten. Auch andere Staaten verfolgen ambitionierte und poliferationsrelevante zivile Programme: Saudi-Arabien und Südkorea verhandeln mit den USA über Kooperationen, die Urananreicherung oder Wiederaufarbeitung einschließen könnten; Japan baut seinen Brennstoffkreislauf weiter aus.

Hinzu kommen neue Reaktorkonzepte wie small modular reactors, die zu einer deutlichen Zunahme von Standorten führen könnten – mit entsprechenden Risiken für Verifikation und Sicherheit in Konfliktzonen. Besonders problematisch ist der Einsatz höher angereicherten Urans (HALEU) in einigen Designs. HALEU liegt knapp unterhalb der Schwelle zu waffenfähigem Material und kann mit geringem Aufwand weiter angereichert werden; theoretisch wären sogar primitive nukleare Explosionen damit möglich (→ Kemp et al. 2024). Da Russland derzeit der einzige kommerzielle Produzent von HALEU ist, entstehen zudem geopolitische Abhängigkeiten. Deutschland sollte sich daher dafür einsetzen, HALEU in neuen Reaktoren zu vermeiden und Verifikationsmechanismen bereits in der Entwicklungsphase mitzudenken.

RAKETENABWEHR

Die schnelle Verbreitung moderner Raketentechnologien überfordert bestehende Abwehrsysteme. Neue Angriffskonzepte kombinieren ballistische Raketen, Marschflugkörper und Drohnen, um Abwehr gezielt zu überwinden. Erfahrungen aus Israel und der Ukraine zeigen, dass Raketenabwehr konventionelle Schäden mindern kann, aber strukturellen Beschränkungen unterliegt. Offensive Technologie entwickelt sich schneller als defensive.

Vier Faktoren bestimmen die Wirksamkeit von Raketenabwehr: Die Geographie legt fest, was abgedeckt werden kann. Über die Zeit erodiert die Wirksamkeit, da Abfangmunition schneller verbraucht als ersetzt wird. Angreifer passen die Flugbahnen und Angriffsmuster an. Die Fähigkeit, Starts an der Quelle zu unterbinden, entlastet die Abfangschicht entscheidend.

Diese Faktoren wirken gegen Europa. Sein großes Territorium macht flächendeckenden Schutz unmöglich, Schläge gegen russische Startkapazitäten wären eskalationsträchtig. Russlands Ausbau bodengestützter Systeme seit Ende des INF-Vertrags – von Iskander über Marschflugkörper bis zum Oreschnik mit Mehrfachsprengköpfen – verschärft die Bedrohung. Die duale Fähigkeit dieser Systeme erzeugt zusätzliche Ambiguität. Europäische Abwehr wäre auf US-Abfangmunitionsbestände angewiesen, die durch laufende Konflikte zunehmend dezimiert werden.

Nuklearwaffen verändern die Leistungsschwelle von Raketenabwehr grundlegend: Geringe Durchbruchsraten werden inakzeptabel, da ein einzelner nuklearer Treffer alle konventionellen Schäden um Größenordnungen übersteigt. Nahezu perfekte Abwehr ist gegen einen Gegner mit Gegenmaßnahmen nicht erreichbar. Raketenabwehr bleibt wertvoll für den Objektschutz, kann aber die strategische Verwundbarkeit nicht beseitigen. Da offensive Raketentechnologie die defensive überholt, hängt Stabilität weniger von technischen Lösungen als von Rüstungskontrolle ab. Ein Moratorium für bodengestützte Systeme in der ehemaligen INF-Reichweite, Transparenzmaßnahmen und Stationierungsbeschränkungen könnten Risiken wirksamer reduzieren als jeder Ausbau defensiver Fähigkeiten.

Raketenabwehr kann die strategische Verwundbarkeit nicht vollständig beseitigen

AUTONOME SYSTEME

Ein rechtlich verbindliches Verbot autonomer Waffensysteme bleibt auch 2026 unrealistisch. Obwohl seit 2014 im Rahmen der VN-Waffenkonvention (CCW) darüber verhandelt wird, blockieren Definitionsstreitigkeiten und Vetos technologisch führender Staaten jeden Fortschritt. Die 2019 verabschiedeten Guiding Principles sind unverbindlich, der aktuell verhandelte Textentwurf enthält kein Verbot. Dennoch hat der CCW-Prozess das Thema international sichtbar gemacht: 2024 verabschiedete die VN-Generalversammlung eine Resolution (A/RES/79/62), die die wachsenden Risiken letaler Autonomie betont.

Die Debatte hat den VN-Rahmen inzwischen aber verlassen: Seit 2023 finden die REAIM-Konferenzen (Responsible AI in the Military Domain) statt, in denen Industrie und Zivilgesellschaft stärker eingebunden sind. Dort betonen Staaten ihre Verantwortung für die sichere Entwicklung und Nutzung militärischer KI. Auch wurde die Global Commission on Responsible AI in the Military Domain (GC REAIM) gegründet. Die USA veröffentlichten 2024 eine Absichtserklärung (Political Declaration), die – wie REAIM – politisch verbindliche Leitlinien formuliert, ohne ein internationales Verbot anzustreben. 2024 unterstützten 61 Staaten einen Aktionsplan (Blueprint for Action), der menschliche Kontrolle und Zuverlässigkeitsanforderungen festschreibt. 2025 hob die GC REAIM das Prinzip responsibility by design hervor: Rechtliche und ethische Anforderungen sollen schon in der Entwicklungsphase in die Systeme integriert werden.

All das zeigt, wie schwer verbindliche Rüstungskontrolle angesichts des militärischen Interesses an KI geworden ist. Gleichzeitig zeigt der wachsende normative Konsens, dass wenigstens geteilte Leitplanken für militärische KI möglich sind. Ob diese Bestand haben, wenn einzelne Staaten sie ignorieren und vollautonome Waffen einsetzen, bleibt offen.

Die Notwendigkeit der Kontrolle von militärischer KI ist erkannt, doch die Umsetzung bleibt schwierig

BIO- UND CHEMIEWAFFENKONTROLLE

Technische Innovationen in der Biologie und Biotechnologie stellen die biologische Rüstungskontrolle vor besondere Herausforderungen, da sie in der Regel nützliche Anwendungen in der Medizin, Pharmakologie und im öffentlichen Gesundheitsschutz betreffen, zum Teil jedoch für unfriedliche Zwecke missbraucht werden könnten. Dies gilt etwa für manche Forschungen und Entwicklungen in der Immunologie, der Genetik und Gentechnik, der synthetischen Biologie oder des KI-gestützten Bidesigns, zum Beispiel in der Proteinforschung oder Impfstoffentwicklung. Gleichzeitig bieten biotechnische Innovationen Chancen, zum Beispiel für verbesserten Schutz vor biologischen Angriffen oder für ihre Untersuchung. Eine Regulierung oder Beschränkung technischer Innovationen über das im Biowaffen-Übereinkommen von 1972 (BWÜ) angewandte sogenannte Allgemeine Zweckkriterium hinaus ist angesichts des hohen Dual-Use-Potenzials schwierig bis gar nicht möglich.^{→ 1}

Entgegen dem globalen Negativtrend der Rüstungskontrolle lassen sich für die Biowaffenkontrolle einige positive Entwicklungen feststellen. Es ist Ausdruck der generellen Unterstützung für das BWÜ, dass die Beteiligung an den Vertrauensbildenden Maßnahmen (VBM) seit einigen Jahren stetig ansteigt und dass eine wachsende Zahl an Vertragsstaaten sich aktiv an den Diskussionen der BWÜ-Arbeitsgruppe beteiligt. Diese Arbeitsgruppe, die allen BWÜ-Mitgliedern offensteht, intensivierte ihre seit 2023 laufenden Diskussionen im Jahr 2025 und nahm Textverhandlungen über konkrete Schritte und Empfehlungen zur Stärkung des BWÜ auf. Die Frage nach der Bedeutung von technologischen Innovationen für das BWÜ durchdringt dabei die meisten Bereiche. Im Fokus steht vor allem die Einrichtung zweier neuer Mechanismen. Die internationale Kooperation bei der friedlichen Nutzung der Biologie sowie zur wissenschaftlichen Beratung über Chancen und Risiken technischer Entwicklungen für das BWÜ soll gefördert werden. Zusätzlich soll eine neue Arbeitsgruppe eingesetzt werden, die sich dezidiert mit dem Thema Verifikation aus politischer, rechtlicher und technischer Perspektive befassen soll. Letzteres ist bemerkenswert, da Gespräche darüber im BWÜ zwei Jahrzehnte lang aus politischen Gründen nicht möglich waren. Die Textverhandlungen werden 2026 fortgesetzt. Zwar besteht über viele Fragen, auch zu den zuletzt genannten Maßnahmen, vergleichsweise große Einigkeit oder zumindest Gesprächs- und Kompromissbereitschaft bei den meisten Vertragsstaaten. Der Einfluss der globalen sicherheitspolitischen Lage schlägt sich aber auch in diesem Feld negativ nieder, unter anderem in Form von fundamentalen Differenzen sowie von destruktiven Verhandlungstaktiken der russischen Delegation. Ob eine Einigung im Konsens möglich sein wird, ist daher derzeit fraglich.

Bei der Kontrolle biologischer und chemischer Waffen gibt es Erfolge und Blockaden

Auch im Bereich der chemischen Abrüstung fällt die Bilanz derzeit gemischt aus, und das Feld zeigt sich sowohl in politischer als auch in technologischer Hinsicht als sehr dynamisch. Im Laufe des Jahres 2025 verdichteten sich die Hinweise weiter, dass im Krieg gegen die Ukraine chemische Kampfstoffe eingesetzt werden. Die Organisation für das Verbot Chemischer Waffen (OVCW) hat in drei Untersuchungen in Kampfgebieten seit 2024 CS-Gas nachgewiesen. Sie war allerdings nicht befugt, den Ursprung und die Urheber:innen eventueller Einsätze zu ermitteln. CS-Gas ist zwar als polizeiliches Mittel zur Unruhebekämpfung erlaubt, als Mittel der Kriegsführung aber durch das Chemiewaffen-Übereinkommen (CWÜ) verboten. Zusätzlich beschuldigen Deutschland und einige andere Staaten Russland, in der Ukraine den chemischen Kampfstoff Chloropikrin eingesetzt zu haben. Auch hier steht eine unabhängige Bestätigung zwar noch aus, es spricht aber Vieles dafür, dass tatsächlich toxische Chemikalien als Waffen im Krieg eingesetzt wurden oder werden. Solche Einsätze werden – ebenfalls unbestätigt – auch dem Sudan vorgeworfen. Der Fall von Alexej Nawalny, der vermutlich 2024 zum zweiten Mal mit einem chemischen Kampfstoff vergiftet wurde, zeigt, dass nicht nur klassische Kriegseinsätze, sondern auch Attentate eine Herausforderung für die Chemiewaffenkontrolle darstellen. Erneut zeigt sich an diesen Beispielen, dass die Möglichkeiten für die Durchsetzung des Chemiewaffenverbots begrenzt sind.

In Syrien gab es dagegen Ende 2025 eine positive Wendung. Nach über zehn Jahren andauernder syrischer Vertragsbrüche und stagnierender Abrüstungsbemühungen aufgrund der fehlenden Kooperationsbereitschaft der Regierung unter Assad hat ihr überraschender Sturz im Dezember 2024 die Lage grundlegend verändert. Die neue Regierung scheint glaubhaft motiviert, das syrische Chemiewaffenprogramm vollständig abzurüsten. Die OVCW attestiert ihr Kooperationsbereitschaft und konstruktive Zusammenarbeit, weist aber auch darauf hin, dass der Abrüstungsprozess durch mangelndes Wissen über das Programm, die anhaltend schwierige Sicherheitslage und fehlende Ressourcen langsam vorangeht. Immerhin konnte die OVCW ihre Inspektions- und Verifikationsaktivitäten 2025 auch vor Ort wieder aufnehmen. Diese Bemühungen werden fortgesetzt, ab Juli 2026 unter der Führung der neu gewählten Generaldirektorin Sabrina Dallafior und mit finanzieller Unterstützung mehrerer Staaten, auch Deutschlands.

Die Ereignisse zeigen, dass auch nach der erfolgten Vernichtung aller deklarierten Chemiewaffenbestände Expertise in der chemischen Abrüstung und Tatsachenermittlung notwendig ist. Sie muss unter Nutzung technischer Innovationen, etwa im Bereich der chemischen Forensik, erhalten und ausgebaut werden. Ähnlich wie in der Biologie ergeben sich für die Chemiewaffenkontrolle zudem Herausforderungen aus Forschungen und Entwicklungen mit Dual-Use-Potenzial, das sich unter anderem in der zunehmend intensiven Nutzung von KI, etwa in der Medikamentenentwicklung, und durch die fortschreitende Automatisierung von Laborprozessen noch verstärkt.

WELTRAUMWAFFEN

Mit dem wachsenden Innovations- und Investitionstempo im Weltraum nimmt auch das Konfliktpotenzial zu. Die größte Gefahr für Frieden und Sicherheit entsteht dabei weniger durch neue Waffensysteme, als durch die zunehmende Bereitschaft, strategische Risiken einzugehen, um wirtschaftliche oder politische Vorteile zu erzielen. In dicht genutzten und wirtschaftlich wichtigen Orbitbereichen – besonders im erdnahen Orbit – beeinflusst wirtschaftlicher Wettbewerb immer mehr militärisches Verhalten. Die Akteure sind zunehmend geneigt, ihre eigenen Interessen durchzusetzen, statt auf Zurückhaltung oder Diplomatie zu bauen.

Im Weltraum beeinflusst wirtschaftlicher Wettbewerb das militärische Verhalten

Klassische Rüstungskontrolle, die auf das Verbot bestimmter Systeme abzielt, greift hier kaum. Der Weltraumvertrag von 1967 untersagt lediglich die Stationierung von Massenvernichtungswaffen. Für die Vielzahl moderner counterspace capabilities, also militärischer Technologien zur Zerstörung oder Beeinträchtigung von Weltraum-Aktivitäten, Infrastruktur oder Satelliten eines Gegners, bieten sie jedoch wenig Orientierung. Dadurch entsteht ein Umfeld, in dem Regeln schwer durchsetzbar sind und es leicht zu Konflikteskalation kommen kann. Wenn Frieden und Sicherheit im Weltraum weniger durch einzelne Waffen als durch unkontrollierte Eskalation bedroht werden, muss politische Zurückhaltung wieder gestärkt werden. Maßgeschneiderte technische und operative Standards für Starts in sensible Orbitbereiche – mit strengeren Anforderungen für bemannte Missionen oder strategische Satelliten – könnten Stabilität schaffen, ohne legitime zivile oder militärische Aktivitäten unnötig einzuschränken.

VERIFIKATION

Dass technologische Entwicklungen einen wichtigen Beitrag zu Frieden und Sicherheit leisten können, zeigt sich besonders im Bereich der Überwachung und Verifikation von Nichtverbreitungs- und Rüstungskontrollverpflichtungen. Zwei Aspekte sind vor allem zu nennen.

3
106

In der Sensorik hat es in den vergangenen Jahren erhebliche Fortschritte gegeben. Die Zahl kommerzieller und staatlicher Satelliten ist stark gestiegen, ebenso ihre räumliche und spektrale Auflösung. Heute kann nahezu jeder Punkt der Erde im Abstand weniger Stunden erfasst werden (→ Moric 2022). Diese Daten stehen nicht mehr nur Regierungen und internationalen Organisationen zur Verfügung, sondern zunehmend auch zivilgesellschaftlichen Akteuren – ein Trend, der als *societal verification* die Transparenz internationaler Verpflichtungen stärkt.

Parallel wächst die Menge an Daten, die für Verifikationszwecke genutzt werden können. Die Internationale Atomenergiebehörde betreibt inzwischen über 1.300 Überwachungskameras. KI-gestützte Analyseverfahren werden künftig eine zentrale Rolle spielen, um große Datenmengen effizient auszuwerten. KI kann zudem in Bereichen wie Waffenstillstandsüberwachung oder Friedensmissionen eingesetzt werden – hier wurden bereits erste Systeme genutzt (→ Unruh und Göttsche 2026). Voraussetzung für ihren Einsatz ist jedoch Vertrauen in die Werkzeuge selbst. Ansätze wie „Explainable AI“ sollen nachvollziehbar machen, wie KI-Systeme zu ihren Bewertungen gelangen, existieren aber nur für einige wenige Bereiche.

KI wird zentrale Rolle für Verifikation, Waffenstillstandsüberwachung und Friedensmissionen spielen

Da sich insbesondere KI-Technologien rasant weiterentwickeln und technologischer Rückstand schwer aufzuholen ist, müssen Staaten, die zukünftige internationale Verifikationsregime mitgestalten wollen, frühzeitig investieren: Sowohl in technische Fähigkeiten als auch in die Kompetenz, neue Technologien verantwortungsvoll in Kontrollmechanismen einzubinden.

SCHLUSSFOLGERUNGEN

Neue Technologien verschärfen die Dual-Use-Problematik und unterlaufen vielfach klassische Rüstungskontrollmechanismen. Zugleich eröffnen sie Chancen für bessere Überwachung, Verifikation und internationale Kooperation. Bislang erfolgt die Regulierung von Dual-Use-Technologien vor allem über nationale Exportkontrollen und internationale Soft-Law-Regime wie das Wassenaar-Arrangement oder die Australische Gruppe. Diese Instrumente schaffen Transparenz und sollen verhindern, dass sensible Technologien in die Hände nicht vertrauenswürdiger Akteure gelangen. Gleichzeitig bleiben sie politisch geprägt, lückenhaft und schwer anpassbar an rasante technologische Entwicklungen. Dies gilt insbesondere bei unterstützenden Technologien wie KI, die sich nicht klar einem von den genannten Instrumenten abgedeckten Technologiebereich zuordnen lassen. Für bestimmte Waffen existieren verbindliche internationale Verbote (BWÜ, CWÜ, NVV), die erhalten und gestärkt werden sollten. Doch auch hier bleibt ein Spannungsverhältnis zwischen Nichtverbreitung und internationaler Kooperation bestehen, etwa beim Austausch von Wissen und Technologien für friedliche Zwecke.

Weil technologische Innovation schneller voranschreitet als politische Regulierung, geraten bestehende Rüstungskontrollregime unter Druck. Neue Technologien entziehen sich häufig ganz der Verregelung. Um Wirkung zu entfalten, muss Rüstungskontrolle flexibler, technologisch informierter und präventiver werden, etwa durch responsibility by design, technische Verifikationswerkzeuge und internationale Standards.

Europa steht vor besonderen Herausforderungen, weil es technologisch abhängig, geographisch exponiert und in einer prekären Sicherheitslage ist. Europa sollte gezielt in technische Verifikationskapazitäten investieren – darunter KI-gestützte Monitoring-Instrumente und Ansätze gesellschaftlicher Verifikation –, die sich unilateral entwickeln und einsetzen lassen. Ergänzend empfiehlt sich die Verfolgung eng umrissener vertrauensbildender Maßnahmen, etwa eines Moratoriums für Systeme im INF-Reichweitenbereich, flankiert durch robuste Transparenzbestimmungen.

¹ Artikel I des BWÜ definiert biologische Kampfstoffe und Waffen über ihren Verwendungszweck und verbietet Aktivitäten, Materialien und Ausrüstungen dann, wenn sie nicht für Schutz-, Vorsorge- oder sonstige friedliche Zwecke gerechtfertigt sind.

Autor:innen

Prof. Dr. Christopher Daase (Koordination)

PRIF – Leibniz-Institut für Friedens- und Konfliktforschung

Dr. Caroline Fehl

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

Dr. Timur Kadyshev

IFSH – Institut für Friedensforschung und Sicherheitspolitik
an der Universität Hamburg

Dr. Mateusz Łabuz

IFSH – Institut für Friedensforschung und Sicherheitspolitik
an der Universität Hamburg

Dr. Sarah McKee

PRIF – Leibniz-Institut für Friedens- und Konfliktforschung

Dr. Thomas Reinhold

PRIF – Leibniz-Institut für Friedens- und Konfliktforschung

Dr. Kadri Reis

PRIF – Leibniz-Institut für Friedens- und Konfliktforschung

Dr. Niklas Schörnig

PRIF – Leibniz-Institut für Friedens- und Konfliktforschung

Dr. Matthias Schulze

IFSH – Institut für Friedensforschung und Sicherheitspolitik
an der Universität Hamburg

Liska Suckau

PRIF – Leibniz-Institut für Friedens- und Konfliktforschung

Quellenverzeichnis

Buchanan, Ben 2020: *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Cambridge, MA.

Deutsche Forschungsgemeinschaft/Leopoldina 2022: Wissenschaftsfreiheit und Wissenschaftsverantwortung: Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung, in: https://www.sicherheitsrelevante-forschung.org/wp-content/uploads/2022/11/2022_Empfehlungen_Wissenschaftsfreiheit_Wissenschaftsverantwortung.pdf; 08.04.2026.

Kemp, R. Scott/Lyman, Edwin S./Deinert, Mark R./Garwin, Richard L./von Hippel, Frank 2024: The Weapons Potential of High-Assay Low-Enriched Uranium, in: *Science* 384, DOI: 10.1126/science.ado8693.

Lewandowsky, Stephan/Ecker, Ullrich. K. H./Cook, John 2017: Beyond Misinformation: Understanding and Coping With the “Post-Truth” Era, in: *Journal of Applied Research in Memory and Cognition* 6:4, 353–369, DOI: <https://doi.org/10.1016/j.jarmac.2017.07.008>.

Moric, Igor 2022: Capabilities of Commercial Satellite Earth Observation Systems and Applications for Nuclear Verification and Monitoring, in: *Science & Global Security* 30, DOI: 10.1080/08929882.2022.2063334.

Unruh, Fabian/Götsche, Malte 2026: Beispiele für KI-Anwendungen in Kontexten von Monitoring und Verifikation, in: CNTR Monitor, <https://monitor.cntrarmscontrol.org/2025/beispiele-fur-ki-anwendungen-in-kontexten-von-monitoring-und-verifikation/>; 08.04.2026.

Wissenschaftsrat 2025: Wissenschaft und Sicherheit in Zeiten weltpolitischer Umbrüche. Positionspapier, Köln, DOI: 10.57674/9tr5-kn29.