Verifikation in einer Zeit rasanten technologischen Wandels

FOKUS

Einführung: Verifikation in einer Zeit rasanten technologischen Wandels

Gegenwärtig sind nur noch wenige rüstungskontrollrelevante Verträge mit formalen Verifikationsregimen in Kraft; geopolitische Spannungen und Machtverschiebungen erfordern in der aktuellen Sicherheitslage flexible Ansätze für alte und neue Sicherheitsprobleme. In diesem Kontext muss Verifikation in einem breiteren und umfassenden Sinne verstanden werden. Denn es bleibt nach wie vor von entscheidender Bedeutung, verlässliches und international zugängliches Wissen über Aktivitäten zu gewinnen, die Frieden und Sicherheit auf regionaler oder globaler Ebene gefährden könnten. Neue Technologien können helfen, diese Prozesse zu verbessern, indem sie die verbleibenden Verifikationsmechanismen existierender Regime optimieren, indem sie nichtstaatlichen Akteuren ermöglichen, an Open-Source-basierter Wissensproduktion mitzuwirken, und indem sie sicherstellen, dass neue, nicht-intrusive Verifikationsmechanismen zur Verfügung stehen, sobald die internationale Situation die Errichtung neuer Regime zulässt. Künstliche Intelligenz wird hier eine besondere Rolle spielen, weil sie das Potenzial hat, Rüstungskontrollverifikation in vielen Bereichen auf ein neues Qualitätslevel zu heben. Gleichzeitig gilt es auch die Herausforderungen zu betrachten. Beispielsweise können manche neuen Technologien vertrauliche oder geschützte Informationen über das benötigte Maß hinaus offenlegen und damit die Grenze zwischen notwendiger Transparenz und unzulässigem Eingriff überschreiten.

- **Die Einführung neuer Technologien im Bereich der Verifikation unterstützen:** Neue Technologien können die derzeitigen Verifikationsmechanismen verbessern, insbesondere indem sie die Genauigkeit erhöhen und Kosten senken. Sie sollten auch bei Verhandlungen über neue oder bei der Aktualisierung bestehender Regime berücksichtigt werden – was bisher schwer nachzuweisen war, könnte so nun genau überprüfbar werden.
- **In ein Ökosystem zur Entwicklung von Verifikationstechnologien investieren:** Um einen effektiveren Übergang vielversprechender neuer Technologien von der Grundlagenforschung zur Anwendung zu ermöglichen, braucht es zielgerichtete Maßnahmen. Hier gibt es gegenwärtig eine Lücke, die geschlossen werden sollte.
- **Neue kreative Ansätze, um sicherheitspolitisch relevantes Wissen zu generieren:** Über die bisher praktizierten staatlich betriebenen Verifikationsmethoden hinaus gibt es Chancen, z. B. weniger formalisierte Prozesse, um ein besseres Verständnis von Compliance zu erhalten, oder durch die Zivilgesellschaft bereitgestellte Informationen, die in Compliance-Bewertungen einbezogen werden können.

Jenseits der Black Box: Bedingungen für einen glaubwürdigen Einsatz von KI in der Verifikation

Künstliche Intelligenz kommt bei der Verifikation von Rüstungskontrolle, Abrüstung und Nichtverbreitung zunehmend zum Einsatz. Sie bietet neue Fähigkeiten, um große Datenmengen zu verarbeiten, Anomalien zu entdecken und Compliance-Bewertungen zu unterstützen. Allerdings wirft der „Black-Box"-Charakter von KI Fragen nach der Zuverlässigkeit KI-gestützter Verifikation auf. Erklärbarkeit allein ist nicht das entscheidende Kriterium; vielmehr besteht die zentrale Herausforderung darin, ob KI-Systeme so entwickelt und gesteuert werden können, dass ihre Glaubwürdigkeit in einem Umfeld mit begrenztem Vertrauen gewahrt bleibt. Reproduzierbarkeit, Integrität, Transparenz, Dezentralisierung und robuste Sicherheitsvorkehrungen erweisen sich als zentrale Voraussetzungen für den glaubwürdigen Einsatz von KI in Verifikationsregimen.

- **Fokus auf Glaubwürdigkeit und Reproduzierbarkeit von KI:** Der Black-Box-Charakter von KI sollte ihrem Einsatz in der Rüstungskontrollverifikation nicht entgegenstehen. Damit KI ein wertvolles Verifikationsinstrument werden kann, müssen Glaubwürdigkeit und Reproduzierbarkeit als primäre Entwicklungsziele betrachtet werden.
- **Gemeinsame Standards:** Die Entwicklung KI-gestützter Verifikationssysteme sollte sich an vereinbarten Standards für Datenintegrität, Transparenz, Reproduzierbarkeit und Cybersicherheit orientieren.
- **Unabhängige Validierung:** Teilnehmende Akteure sollten in der Lage sein, KI-generierte Ergebnisse unabhängig zu validieren. Dafür braucht es geteilte Datensätze, transparente Algorithmen und Verfahren sowie dezentrale technische Infrastrukturen.

Verifikation mit Quantensensorik

Quantensensorik ist ein fortschrittlicher Ansatz, der Quantenmechanik für Messungen einsetzt, um Objekte über große Entfernungen hinweg oder in Umgebungen mit starken Störsignalen zu erkennen. Sie könnte in der Verifikation spezifische Aufgaben unterstützen, so etwa Deklarationen mit Beobachtungen abzugleichen, Anomalien zu ermitteln, die weitere Nachverfolgung erfordern, zu dokumentieren, wo und wie Messungen genommen wurden, und ohne übermäßige Eingriffe Hinweise zu sammeln. Ihr potenzieller Wert ist eher praktischer als transformativer Natur: stabilere Messungen im Feld, selektiveres Screening and besser reproduzierbare Inspektionsprotokolle.

Die Interferometrie mit kalten Atomen kann zur Unterstützung lokaler Gravimetrie und der Trägheitsnavigation eingesetzt werden; NV-Zentren- und Atommagnetometer können die Kartierung lokaler magnetischer Anomalien verbessern; und nichtlineare Interferometer auf Basis induzierter Kohärenz können molekulare Fingerabdrücke im mittleren Infrarot erfassen, wobei die Detektion im sichtbaren oder nahen Infrarot erfolgt. Keine dieser Anwendungen wird bisher in Vertragsinspektionen eingesetzt. Ihr operativer Nutzen wird letztlich davon abhängen, ob sie gegenüber etablierten Messgeräten einen nachweisbaren Mehrwert bieten, praktikable Messzeiten ermöglichen, auf klar vereinbarten Datenregeln basieren und von den beteiligten Staaten und Organisationen akzeptiert werden.

- **Missionsorientierte Validierung finanzieren:** Es sollten vergleichende Versuche im Feld durchgeführt werden, bei denen die Leistung an repräsentativen Standorten mit etablierten klassischen Messgeräten verglichen und folgende Aspekte geprüft werden: falsch-positive Ergebnisse, falsch-negative Ergebnisse, Kalibrierungsstabilität, Robustheit, Bedienungsaufwand sowie Datenschutzanforderungen.
- **Klar abgegrenzte Pilotprojekte priorisieren:** darunter lokale Gravimetrie und Magnetometrie zur Kartierung von Anomalien, quantengestützte Trägheitsnavigation für Inspektionen ohne GPS-Empfang sowie Screening im mittleren Infrarotbereich mittels nichtlinearer Interferometer mit Auslesung im sichtbaren oder nahen Infrarotbereich für die anschließende chemische Analyse.
- **Die Verifikationsfrage vor dem Einsatz definieren:** Für jedes neue Messgerät sollten Leistungsschwelle, Funktion in der Beweissammlung, Sicherheitsvorkehrungen für den kontrollierten Zugang und Genehmigungswege vereinbart werden.

Datenintegration in der Satellitenüberwachung

Bald nach dem Start von Sputnik I 1957 wurde das Sammeln von Informationen aus dem Weltraum für die nationale Sicherheit zu einem wichtigen Motor für die Erforschung der „letzten Grenze“. Beide nuklearen Supermächte wie auch eine wachsende Zahl weiterer Staaten haben seitdem stark in satellitengestützte Aufklärung investiert. Die jüngsten Entwicklungen bei der künstlichen Intelligenz (KI) und der Fusion von Daten aus verschiedenen weltraumgestützten Beobachtungstechnologien könnten jedoch die Weltraumüberwachung wesentlich voranbringen, beispielsweise bei der weltraumgestützten Erkennung von Stealth-Systemen. Zudem verbessert Datenfusion die gesellschaftliche Verifikation auf Grundlage von kommerziellen Satelliten und privatem Zugang zu Satellitenbildern. Diese Fortschritte eröffnen zwar neue Möglichkeiten für die Verifikation, bringen aber auch neue Risiken mit sich. Um die mit der Nutzung von Satellitenbildern verbundenen Risiken und Chancen umfassend einschätzen zu können, müssen auch die derzeitigen technischen Grenzen der verschiedenen eingesetzten Technologien erfasst werden.

- **Investition in KI-gestützte Informationsgewinnung:** Strategische Vorteile hängen zunehmend von der Integration und Analyse von Multisensordaten ab und nicht mehr nur von der reinen Sammlung von Bildmaterial. Politische Entscheidungsträger*innen sollten KI, Datenfusion und Analysekapazitäten priorisieren.
- **Gründliche Technologiebewertungen:** Nationale Frequenzbehörden, Verteidigungsforschungsorganisationen und die Europäische Verteidigungsagentur (EDA) sollten eine systematische und unabhängige Bewertung neuartiger Sensortechnologien und neuer Nutzungsformen des Funkfrequenzspektrums sicherstellen, um deren technische Glaubwürdigkeit, Entwicklungsgeschwindigkeit und potenzielle sicherheitspolitische Auswirkungen zu ermitteln, einschließlich der Umstände, unter denen sie strategische Bedeutung erlangen könnten.
- **Überprüfung der politischen Positionen zu Fernerkundung:** Deutschland sollte prüfen, ob seine ‚*National Data Security Policy for Space-Based Earth Remote Sensing Systems*‘ auf einem zunehmend internationalen Markt für kommerzielle Erdbeobachtung noch zweckmäßig ist; es sollte geprüft werden, ob der derzeitige Rechtsrahmen weiterhin wirksam zur Erreichung der nationalen Sicherheitsziele beiträgt und gleichzeitig die wissenschaftlichen, wirtschaftlichen und humanitären Vorteile der kommerziellen Erdbeobachtung gewährleistet.

Neuartige Partikelsonden in der nuklearen Verifikation

Atomenergie erlebt einen weltweiten Wiederaufstieg, der auch die Entwicklung neuartiger, fortschrittlicher Reaktor- und Einsatzkonzepte einschließt. Um diesen Innovationen Rechnung zu tragen, wären umfangreiche Änderungen an den bestehenden nuklearen Sicherungsmaßnahmen sowie zusätzliches Personal erforderlich. Vor diesem Hintergrund untersuchen Forschende und akademische Einrichtungen neue Techniken der nuklearen Verifikation. Zerstörungsfreie Analysemethoden erscheinen dabei besonders vielversprechend, um Szenarien für zukünftige Sicherungsmaßnahmen zu bearbeiten. Diese Bemühungen stützen sich auf Fortschritte bei industriellen Technologien und in laufender Forschung und Entwicklung (FuE) im Bereich Signaldetektion und Datenverarbeitung. Durch die Analyse der Evolution innovativer Verifikationstechniken können gemeinsame technologische Treiber sowie ihrer Entwicklung förderliche Ansätze identifiziert werden.

- **Nukleare Verifikation in sicherheitsorientierte Programme aufnehmen:** Regierungen sollten sicherstellen, dass sie nukleare Verifikation in ihre sicherheitsorientierten FuE-Förderprogramme und -maßnahmen auf-

nehmen und gleichzeitig den zivilen Sicherheitsaspekt betonen. Durch Ausgewogenheit und Transparenz können Vertrauen geschaffen und kooperative Innovationen gefördert werden.

- **Den Nutzen der Anpassung physikalischer Grundlagenforschung an Verifikationsanwendungen anerkennen:** Dank der Anpassung von Innovationen im Bereich der Detektionstechnologien, die aus der Grundlagenforschung in der Physik hervorgegangen sind, konnten neuartige Werkzeuge entwickelt werden, die die Bausteine für neue Techniken der nuklearen Verifikation bilden – dieser Nebeneffekt und Nutzen muss von akademischen Einrichtungen wie Universitäten, die Grundlagenforschung betreiben, deutlicher anerkannt werden, um die Attraktivität solcher Forschungsarbeiten für Wissenschaftler*innen zu steigern.
- **Interdisziplinäre Forschungsumgebungen unterstützen:** Der effektivste Weg, existierende FuE-Bemühungen zu nutzen, dürfte es sein, kontinuierlich interdisziplinäre Entwicklungsumgebungen zu unterstützen und darüber Innovationen für Verifikationszwecke zu fördern. Zwar gibt es interdisziplinäre Fördermittel und Austauschmöglichkeiten, sie konkurrieren jedoch häufig und zu ihrem Nachteil mit disziplinspezifischen Forschungen oder Trends.

Attribution gentechnischer Veränderungen: Beitrag zur Verifikation und praktische Einschränkungen

Die Attribution gentechnischer Veränderungen (genetic engineering attribution, GEA) bleibt für die laufende Diskussionen um Biosicherheit und Verifikation weiterhin relevant. Jüngste Forschungsarbeiten deuten darauf hin, dass gentechnisch verändertes biologisches Material erkennbare Spuren von Designentscheidungen und Laborpraktiken aufweisen könnte. Allerdings basiert ein Großteil dieses Fortschritts auf kuratierten Datensätzen, wie z.B. Plasmid-Repositorien, die sich signifikant von realen Bedingungen unterscheiden. Die derzeitigen Methoden können zwar bei der Vorauswahl und der Eingrenzung der Möglichkeiten helfen, doch für ihre Verwendung zur Verifikation sind bessere Daten, realistischere Tests und eine sorgfältige Auswertung erforderlich.

- **Datenstandards für gentechnisch veränderte biologische Sequenzen verbessern:** Initiativen im Bereich Biosicherheit und Attribution sollten eine einheitlichere Dokumentation von Bauart, Vektorsystem, Backbone, Konstruktionsmethode und relevanten Informationen zum Einreicher in biologischen Repositorien und Sequenzdatenbanken fördern.
- **Realweltliche Bedingungen in Bewertungen nachahmen:** Forschungsprogramme zur Unterstützung von GEA sollten Tests unter realistischeren Bedingungen priorisieren, darunter unvollständige, degradierte, gemischte oder unzureichend dokumentierte Proben, und sie sollten zwischen der Erkennung gentechnischer Veränderung und der Zuordnung zu einer Quelle unterscheiden.
- **GEA mit anderen Methoden kombinieren:** Ermittler*innen und Verifikationsfachleute, die GEA einsetzen, sollten die Ergebnisse dieser Methode zusammen mit epidemiologischen, umweltbezogenen und ermittlungstechnischen Beweisen interpretieren, anstatt sie als eigenständigen Beweis zu betrachten.

Autonome Raumfahrzeuge und die Herausforderung der Verifikation

Die Autonomie von Satelliten, also ihre Fähigkeit, mit geringer Abhängigkeit von der Bodenkontrolle zu operieren und zu navigieren, ist zugleich vorteilhaft und risikobehaftet. Einerseits erhöht sie die Resilienz, eröffnet neue Möglichkeiten für die Verifikation im Orbit und für operationale Unabhängigkeit. Andererseits bringt sie neue Herausforderungen für Governance und Sicherheit mit sich. Da sich weniger Entscheidungen direkt menschlichen Bedienern zuschreiben lassen, wird es schwieriger zu bestimmen, ob Verhalten unbeabsichtigt, ungeplant entstanden, fahrlässig oder vorsätzlich ist. In konfliktträchtigen Bereichen des Orbits könnten autonome Rendezvous- und Annäherungsoperationen (rendezvous and proximity operations, RPO) das Misstrauen zwischen Staaten verstärken und zu einer Eskalation beitragen. Ein zentrales Problem ist das Risiko von Fehleinschätzungen unter Bedingungen der Unsicherheit, insbesondere dort, wo eine strategische Interpretation ohnehin schon schwierig ist. Bestehende Regulierungsrahmen und Normen haben mit den technischen Möglichkeiten nicht Schritt gehalten, was ihre Fähigkeit einschränkt, neu entstehende autonome Systeme effektiv zu steuern.

- **Gemeinsame Verifikationsprotokolle entwickeln und Mehrdeutigkeit minimieren:** Manöver, Flugbahnen und Annäherungsgeschwindigkeiten, die im mit Verifikation im Zusammenhang stehen, sollten transparent und beobachtbar sein, um Mehrdeutigkeiten zu minimieren und die Bedrohungswahrnehmung zu verringern.
- **Einrichtung einer offenen Arbeitsgruppe für Inspektionssatelliten:** Der Erste Ausschuss der Vereinten Nationen könnte eine offene Arbeitsgruppe beauftragen, in Absprache mit technischen Überprüfungsgremien wie der Internationalen Atomenergie-Organisation (IAEO) Vorschläge für eine Flotte international anerkannter Inspektionssatelliten auszuarbeiten.
- **Informationsbarrieren definieren:** Raumfahrtnutzende Staaten sollten vereinbarte Grenzen für Überwachungssensoren und Inspektionsmaßnahmen als Informationsbarrieren festlegen, um sicherzustellen, dass Verifikation im Orbit durchgeführt werden kann, ohne dass eine intrusive Überwachung ermöglicht wird.

Was die Regulierung des Cyberspace von der traditionellen Rüstungskontrolle lernen kann

Cyberoperationen werden zunehmend für militärische Zwecke eingesetzt, insbesondere im Kontext hybrider Kriegsführung. Allerdings gibt es gegenwärtig keinen verbindlichen internationalen Rechtsrahmen für den Cyberspace. In Anlehnung an das Chemiewaffenübereinkommen (CWÜ), das oft als eines der erfolgreichsten Rüstungskontrollregime bezeichnet wird, sollte die Regulierung des Cyberspace sich weniger auf spezifische technologische Anwendungen und mehr auf schädliche Verhaltensweisen und Anwendungskontexte konzentrieren.

- **Fokus auf Verhalten und Absicht:** Cyber-Rüstungskontrolle sollte sich darauf konzentrieren, statt spezifischer technologischer Anwendungen vielmehr schädliches Verhalten, intendierte Effekte und Anwendungskontexte zu regulieren.
- **Einen Attributionsmechanismus für Cyberangriffe einführen:** Ein unabhängiger, aber global anerkannter Attributionsmechanismus nach dem Vorbild der in der Fachliteratur vorgeschlagenen staatenunabhängigen Attributionsverfahren könnte im Cyberraum eine praktikable Alternative zu traditionellen Verifikationsansätzen darstellen.
- **Soft Law und Normsetzung einbeziehen:** Da Soft-Law-Instrumente und Normsetzung wahrscheinlich Voraussetzungen für künftige verbindliche Cyber-Rüstungskontrollvereinbarungen sind, sollten sie in Ansätze zur Regulierung des Cyberspace einbezogen werden.

Systems for Implementation Review

Systems for Implementation Review (SIRs), also Mechanismen zur Überprüfung der Implementierung von Verpflichtungen, sind internationale oder regionale Institutionen und Verfahren, über die Vertragsparteien eines multilateralen Übereinkommens Informationen über die Umsetzung austauschen, ihre jeweiligen Implementierungsmaßnahmen vergleichen, die Umsetzung durch andere Vertragsparteien überprüfen, aus den Erfahrungen anderer Vertragsparteien lernen, Fälle der Nicht- oder unzureichenden Erfüllung von Verpflichtungen behandeln und, soweit zweckmäßig, ihre Verpflichtungen anpassen. Erfahrungsgemäß können die Entwicklung und Anwendung von SIRs wichtige Beiträge zu Effektivität von Verträgen oder Regimen leisten, insbesondere bei komplexen multilateralen Abkommen. SIRs verbessern Umsetzung und Compliance, indem sie dazu beitragen, rechtzeitig internationale Aufmerksamkeit zu wecken und Expertenreaktionen auf aufkommende Probleme oder Chancen bei der nationalen Implementierung internationaler Verpflichtungen zu mobilisieren. Im Kontext von Umweltabkommen haben sie sich als besonders effektiv erwiesen. Obwohl SIRs in mehreren multilateralen Rüstungskontroll- und Abrüstungsregimen zum Einsatz kommen, finden sie nach wie vor relativ wenig Beachtung und sind oft nur unzureichend ausgearbeitet. Ein stärkerer Fokus auf die Entwicklung und den Einsatz von SIRs könnte dazu beitragen, die Bemühungen um Rüstungskontrolle dynamischer und effektiver zu gestalten.

- **SIRs in die Bemühungen zur Stärkung von multilateralen Abkommen und Soft Law in der Rüstungskontrolle und Abrüstung einbeziehen:** Das Auswärtige Amt und seine Partner auf EU- und internationaler Ebene sollten der Entwicklung und dem zielgerichteten Einsatz von SIRs mehr Aufmerksamkeit widmen, im Rahmen ihrer Bemühungen
  - die Dynamik und Effektivität existierender multilateraler Rüstungskontroll- und Abrüstungsregime, wie CWÜ, BWÜ, NVV und Abkommen der humanitären Rüstungskontrolle, zu steigern; und
  - internationale Verhaltenskodizes und Leitlinien für bewährte Praktiken als Teil ihrer Soft-Law-Ansätze zu entwickeln, um die internationale Zusammenarbeit in Fragen der Sicherheit im Weltraum zu fördern und die Risiken einzudämmen, die durch den Einsatz von Cyberwaffen und den Missbrauch neuer Technologien entstehen.

Gesellschaftliche Verifikation

Gesellschaftliche Verifikation, die Analyst*innen außerhalb des Regierungs-Nachrichtendienst-Nexus eine Rolle bei der Produktion verifikationsrelevanten Wissens zuschreibt, hat angesichts der weit verbreiteten Nutzung und zunehmenden Verfügbarkeit von Satellitenbildern wieder neue Aufmerksamkeit erfahren. Die Überwachung nordkoreanischer Nuklearanlagen und das Tracking iranischer Standorte durch nichtstaatliche Akteure, darunter Nichtregierungsorganisationen (NGOs), Thinktanks und unabhängige Forschende, verdeutlicht, wie von NGOs erstellte Analysen in die öffentliche Debatte und die Medienberichterstattung einfließen. Aus Interviews mit OSINT-Analyst*innen (Open-Source Intelligence) aus NGOs und Thinktanks sowie mit Regierungsvertreter*innen geht hervor, dass Initiativen zur gesellschaftlichen Verifikation zwei unterschiedliche Auswirkungen haben: (1) Sie informieren die Öffentlichkeit über drängende Sicherheitsfragen, wobei sie auch neue Information veröffentlichen, die Regierungsakteure benutzen können; (2) sie stimulieren und prägen innerstaatliche Debatten über Sicherheitspolitik. Ein verbesserter Dialog zwischen nichtstaatlichen und Regierungsexpert*innen würde politischen Entscheidungsträger*innen helfen, die Informationen von Thinktanks und NGOs besser zu nutzen. Zudem könnte auch Ängsten in der Bevölkerung und Worst-Case-Annahmen begegnet werden, indem Lücken in der Berichterstattung über Bedrohungen und Sicherheitsthemen dort geschlossen werden, wo Nachrichtendienste und Regierungen zurückhaltender sind.

- **Dialog zwischen nichtstaatlichen Akteuren und Regierungen:** Nichtstaatliche Akteure, die OSINT verwenden,

und Regierungen sollten ihren Dialog verstärken, um Debatten auszuweiten und mehr Stakeholder in die Produktion verifikationsrelevanten Wissens einzubinden.

- **Das von nichtstaatlichen Akteuren produzierte verifikationsrelevante Wissen sollte Regierungen in ihren Entscheidungsprozessen anleiten.** Analysen nichtstaatlicher Akteure bieten für die Öffentlichkeit zusätzliche Perspektiven und Kontext zu Politikfolgen und Bedrohungspotenzialen, wobei sie manchmal eine kritischere Haltung einnehmen als Regierungsmitteilungen.
- **Zusammenarbeit zwischen staatlichen und nichtstaatlichen Akteuren sollte auf die Stärkung der Glaubwürdigkeit künftiger Verifikationsansätze und Rüstungskontrollmaßnahmen abzielen.** Das könnte auch die öffentliche Unterstützung für politische Maßnahmen fördern.

TRENDS

Künstliche Intelligenz und Halbleiter – Wichtige Entwicklungen seit 2025

Halbleiter sind nicht mehr nur ein wirtschaftliches Thema; sie sind zunehmend zu einer Frage der nationalen und internationalen Sicherheit geworden. Der Wettbewerb um KI-Fähigkeiten ist eng mit der Kontrolle über Halbleiter-Lieferketten, kritische Rohstoffe und die für fortschrittliche Rechenleistung erforderlichen Infrastrukturen verbunden. Die Stärkung der Resilienz in den gesamten Halbleiter-Ökosystemen – einschließlich der Produktionskapazitäten, der Energieversorgung und der internationalen Partnerschaften – ist daher zu einem zentralen strategischen Ziel sowohl für Staaten als auch für Unternehmen geworden.

- Die deutsche Außenpolitik sollte die Lieferketten für Halbleiter und die Recheninfrastruktur für künstliche Intelligenz als zentrale Themen der wirtschaftlichen Sicherheit und des Schutzes kritischer Infrastrukturen behandeln.
- Deutschland und die EU sollten internationale Partnerschaften entlang der Halbleiter-Wertschöpfungskette verstärken und diversifizieren – von kritischen Mineralien und Fertigungsanlagen bis hin zu hochmodernen Chips und Speicherkapazitäten.
- Die Resilienz gegenüber geopolitischen Umbrüchen sollte gestärkt werden, indem Zusammenarbeit in den Bereichen Versorgungssicherheit, Exportkontrollen und Zugang zu kritischen Halbleiter- und KI-Infrastrukturen gestärkt und international koordiniert wird.

KI im Labor: Vom biologischen Design zur biologischen Zugangskontrolle

Mit zunehmender Bedeutung von KI-Tools in den Lebenswissenschaften verlagert sich die politische Debatte von allgemeinen Dual-Use-Bedenken hin zu praktischeren Fragen der Kontrolle, des Zugangs und der Umsetzung. Dazu zählt Zugang zu sensiblen Daten zu Krankheitserregern, kontrollierter Zugang zu biologischen KI-Tools mit höherem Risiko, stärkeres Nukleinsäure-Screening und Anwendungskontrollen bei führenden KI-Unternehmen. Die politische Kernfrage lautet: Wie lassen sich Zugang, Kontrolle und Verantwortlichkeit regeln, bevor risikoreichere Fähigkeiten zur Routine werden?

- Die EU sollte strengere und einheitlichere Anforderungen an Nukleinsäure-Screening und Überprüfung der Kundenindentität in allen Mitgliedsstaaten fördern.
- Nationale und EU-Rechtsrahmen sollten einen kontrollierten Zugang zu biologischen KI-Tools mit erhöhtem Risiko und zu sensiblen Datensätzen über Krankheitserreger unterstützen.
- Die internationale Koordinierung sollte auf die Förderung kompatibler Standards für Nukleinsäure-Screenings, Regulierung biologischer KI, Berichterstattung und Bewertung abzielen.

Künstliche Intelligenz in Chemie und Chemiewaffenkontrolle: Fragmentierung und die „Umsetzungslücke“

Obwohl die künstliche Intelligenz (KI) in der Chemie rasante Fortschritte macht, ist ihre Anwendung in der Forschung und ihr Einsatz bei der Kontrolle chemischer Waffen nach wie vor fragmentiert und unzureichend reguliert. Während viele Modelle entwickelt werden, werden sie selten in stabile Workflows integriert. Gleichzeitig erleichtert die weitverbreitete Verfügbarkeit von Open-Source- und wenig gesicherten Tools die Entdeckung neuartiger Synthesewege und toxischer Moleküle. Chancen für Verifikation, forensische Analyse und Einsatzplanung bleiben großteils ungenutzt. Um die Wirksamkeit des Chemiewaffenübereinkommens zu wahren, ist eine genauere Abstimmung zwischen den technischen Fähigkeiten und den politischen Rahmenbedingungen von entscheidender Bedeutung.

- Staaten und die Organisation für das Verbot chemischer Waffen (OVCW) sollten die Anwendung von KI in der Chemie systematisch beobachten, um die Risiken fragmentierter und unregulierter Modelle frühzeitig zu identifizieren und zu minimieren.
- Die OVCW und die zuständigen nationalen Behörden sollten gezielte Fähigkeiten für den operativen Einsatz von KI bei der Verifikation, Analyse und Missionsplanung aufbauen, um die derzeitige „Umsetzungslücke“ zu schließen.
- Entwickler*innen, Forschungseinrichtungen und politische Entscheidungsträger*innen sollten zusammenarbeiten, um verbindliche Sicherheitsvorkehrungen und Zugangsbeschränkungen für besonders sensible Anwendungen zu entwickeln und durchzusetzen, darunter toxische Moleküle, Retrosynthese-Planer und autonome Labore.

Hochskalierung von Desinformation mit KI: Eine Gefahr für das Verbot chemischer Waffen?

Agentenbasierte, auf großen Sprachmodellen basierende künstliche Intelligenz (KI) kann Desinformation skalierbarer, kostengünstiger und schwerer entdeckbar machen. Das gefährdet Vertrauen in Institutionen und demokratische Prozesse. Diese Entwicklung wirkt sich besonders auf die Kontrolle chemischer Waffen aus. Die Organisation für das Verbot chemischer Waffen (OVCW) ist seit langem Ziel koordinierter Kampagnen, die versuchen, die Zuschreibung von Verantwortung, institutionelle Legitimität und Governancestrukturen zu untergraben. Herkömmliche Methoden zur Aufdeckung von Desinformationskampagnen, die Bots verwenden, sind angesichts neuer technischer Entwicklungen wirkungslos. Daher braucht es resiliente Institutionen, die in der Lage sind, Angriffe frühzeitig zu erkennen, transparent zu kommunizieren und kooperativ Gegenstrategien zu entwickeln, anstatt sich auf technische Zensurmaßnahmen zu verlassen.

- Die OVCW sollte einen Überwachungs- und Analyserahmen schaffen, um KI-gestützte Desinformationskampagnen, die ihre Glaubwürdigkeit untergraben sollen, systematisch zu erfassen, zu bewerten und ihnen zu begegnen.
- Die Organisation und ihre Mitgliedsstaaten sollten weiterhin proaktive und transparente Kommunikationsstrategien verfolgen, die Prozeduren, Mandate und Grenzen der OVCW verständlich erklären. Das stärkt die Resilienz gegenüber delegitimierenden Narrativen.
- Staaten, internationale Organisationen, Plattformbetreiber und KI-Anbieter sollten gemeinsam Methoden zur Aufdeckung von KI-gestützten „Schwarm"-Kampagnen entwickeln und koordinierte Maßnahmen ergreifen, um solche Aktivitäten insbesondere während sensibler Ereignisse zu kennzeichnen oder einzudämmen.

Innovation im Drohnentempo: Wie der Krieg gegen die Ukraine die Kriegsführung der Zukunft prägt

In den letzten zwei Jahren haben wir über die rasante Entwicklung von Drohnen im Krieg in der Ukraine berichtet. Dieser Trend hält immer noch an und hat sogar noch an Dynamik gewonnen. Zu den wichtigsten Entwicklungen zählen unter anderem die zunehmende Bedeutung von Abwehr-Drohnen, die andere Drohnen jagen, die deutliche Zunahme unbemannter Bodenfahrzeuge (Bodendrohnen) sowie die Tatsache, dass die Ukraine zu einem weltweit führenden Anbieter von Drohnen- und Anti-Drohnen-Technologie geworden ist. Damit hat sie sich von einem Importeur von Sicherheitstechnologie zu einem internationalen Anbieter gewandelt.

- Angesichts der schlechten Aussichten für eine internationale Regulierung der Drohnenkriegsführung und der dynamischen Entwicklungen im technologischen Bereich muss der Drohnenabwehr sowohl im militärischen als auch im zivilen Bereich weiterhin besondere Aufmerksamkeit gewidmet werden.

Spiegelleben: Von der Warnung zur Governance-Debatte

Obwohl noch kein sich selbst reproduzierender Spiegelorganismus bekannt ist, ist Spiegelleben zu einem aktiven Thema der Politik geworden. Seit der Veröffentlichung des letzten CNTR Monitor haben die UNESCO, der Wissenschaftliche Beirat der Vereinten Nationen, britische Regierungsvertreter, Geldgeber und der „Mirror Biology Dialogues Fund" die Diskussionen über Moratorien, Vorläufertechnologien und Sicherheitsvorkehrungen vorangetrieben. Die jüngsten Fortschritte im Bereich synthetischer Zellen und die Debatte über ökologische Einschränkungen unterstreichen die Notwendigkeit gezielter Vorschriften, die sich selbst replizierende Spiegelorganismen verhindern und gleichzeitig risikoärmere Forschungsarbeiten an nicht replizierenden Spiegelmolekülen ermöglichen.

- Regierungen und internationale wissenschaftliche Gremien sollten eine starke Norm gegen die Erzeugung sich selbst reproduzierender Spiegelorganismen aufrechterhalten.
- Politische Entscheidungsträger*innen, Geldgeber und Forschungseinrichtungen sollten Regelungen für solche Vorläufertechnologien entwickeln, die die Erzeugung von Spiegelorganismen erleichtern könnten.
- Risikoärmere Arbeit an nützlichen nicht replizierenden Spiegelmolekülen sollte mit Regeln weitergeführt werden, die sie eindeutig von Arbeit an sich selbst reproduzierenden Spiegelorganismen abgrenzen.

Technologiepräferenzen von sechs militärisch innovativen Ländern: Eine aktualisierte Analyse sicherheitspolitischer Technologiestrategien

Die Art der Kriegsführung verändert sich ständig und rasant – und neue Technologien spielen dabei eine bedeutende Rolle. Doch welche Technologien wurden und werden von Staaten aus militärischer Sicht als besonders bedeutsam angesehen? Eine Analyse von Strategiepapieren sechs ausgewählter Staaten aus den Jahren 2016 bis 2025 zeigt, dass die Weiterentwicklung traditioneller konventioneller Waffensysteme ebenso wichtig ist wie die Entwicklung neuer militärischer Technologien wie verbesserter Command-and-Control-Systeme, neuartiger Sensoren, KI-basierter Analysen und Vernetzung. Zudem ist insbesondere in den letzten Jahren ein wachsendes Interesse an (ballistischen) Raketen zu beobachten. Die Analyse zeigt jedoch auch, dass die Diskussionen über zu-

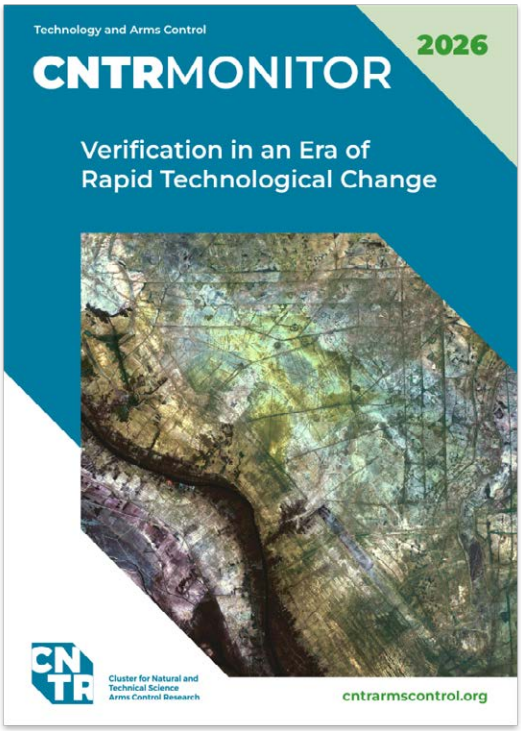
künftige Militärtechnologie in den untersuchten Staaten sehr unterschiedlich ausfallen. Während beispielsweise Australien sowohl hinsichtlich der Quantität als auch der Tiefe anspruchsvolle Diskussionen führt, hinkt Deutschland sowohl bei der Anzahl der Dokumente als auch bei der inhaltlichen Tiefe hinterher.

- Das gestiegene Interesse an ballistischen Raketen gibt Anlass zur Sorge und sollte auf internationaler Ebene diskutiert werden, wobei die EU-Staaten die Initiative ergreifen sollten.
- Ein offener Diskurs über militärische und militärtechnische Ausrichtung ist in Demokratien angebracht und dient zudem dazu, die Legitimität zu sichern. Folglich sollten jene Länder, die sich bisher vor einer solchen Auseinandersetzung gescheut haben – darunter auch das deutsche Verteidigungsministerium –, diesen Diskurs intensivieren.

Über den CNTRMONITOR 2026:

Rasante wissenschaftliche und technologische Fortschritte könnten die zukünftige Verifikationslandschaft umgestalten. Nur wenige Rüstungskontrollverträge mit formalen Verifikationsregimen sind überhaupt noch in Kraft. Dennoch bleibt es wichtig, in Bezug auf Aktivitäten, die Frieden und Sicherheit destabilisieren könnten, gemeinsames Wissen zu produzieren. Der CNTR Monitor 2026 untersucht daher neue Möglichkeiten für Verifikation – mit und ohne Verträge.

Verifikationswissen muss verlässlich und international zugänglich sein. Neue Technologien können dabei helfen, existierende Verifikationsregime zu verbessern, bringen aber auch neue Herausforderungen. Der CNTR Monitor 2026 analysiert ausgewählte Technologien und politische Veränderungen und beleuchtet damit die Dynamiken, die Verifikation in der heutigen Sicherheitslage prägen.



Göttsche, M., Jakob, U., & Schörnig, N. (Eds.). (2026). *Verification in an Era of Rapid Technological Change. CNTR Monitor – Technology and Arms Control 2026*. PRIF – Peace Research Institute Frankfurt.

*Autor*innen: Philip Gasse, Malte Göttsche, Markus Gräfe, Owen Greene, Una Jakob, Abdullah Kasim Korkusuz, Anja-Liisa Krichbaum, Sarah McKee, Robin E.Möser, Luis Pazos Clemens, Helene Pleil, Lukas Rademacher, Thomas Reinhold, Kadri Reis, Christian Reuter, Yan-Jie Schnellbach, Niklas Schörnig, Adhitya Sekhar, Liska Suckau, Fabian Unruh*

Gefördert durch:
Auswärtiges Amt
aufgrund eines Beschlusses des Deutschen Bundestages