AUSSEN- UND SICHERHEITSPOLITIK 14.04.2026 | Tianjiao Jiang

Kein Wille, keine Kontrolle

KI-Waffen sind regulierbar: Warum die größten Hürden nicht technisch, sondern politisch sind.

Künstliche Intelligenz (KI) verändert nicht nur die Arbeitswelt, sondern könnte auch die Kriegsführung grundlegend neu definieren. Wenn KI-Waffen tatsächlich die Zukunft des Krieges sind, wird Rüstungskontrolle für KI-Waffen dringend erforderlich. Viele Beobachter argumentieren jedoch, dass traditionelle Methoden der Rüstungskontrolle auf KI-Waffen nicht anwendbar seien. Insbesondere weisen viele Studien auf die grundlegenden Unterschiede zwischen der Rüstungskontrolle bei Atomwaffen und der Rüstungskontrolle bei KI-Waffen hin und betonen die großen Hürden für Letztere.

Zwar haben diese skeptischen Ansichten eine gewisse Berechtigung, doch die eigentliche Herausforderung der KI-Rüstungskontrolle ist der Mangel an politischem Willen. Betrachten wir die Themen Überprüfbarkeit, rechtliche und ethische „rote Linien“, Dual-Use-Anwendungen und mögliche zukünftige institutionelle Regelungen.

Erstens argumentieren einige hinsichtlich der Überprüfbarkeit, dass KI-Algorithmen und Datensätze überhaupt nicht überprüfbar seien, da ihnen eine physische Form fehle. Aber auch bei Verträgen wie dem Neuen Vertrag zur Verringerung strategischer Waffen (*New START*) zwischen den USA und Russland, der bis zu seinem Auslaufen im Februar 2026 Vor-Ort-Verifizierungen und Datenaustausch in Bezug auf Atomwaffen vorschrieb, hatten viele bezweifelt, dass eine glaubwürdige Verifizierung erreicht und Täuschung durch die Gegenseite vermieden werden kann. Sie waren Ergebnis jahrzehntelanger Verhandlungen, Kommunikation und Vertrauensbildung.

Zudem kann nicht das gesamte Atomwaffenarsenal vollständig und transparent inspiziert werden. Stattdessen wählten beide Seiten einen Teil ihrer wichtigsten strategischen Atomwaffen aus und führten einen sogenannten Rüstungskontroll-Inspektionsmechanismus ein, der auf spezifischem Datenaustausch und teilweise offenen Inspektionen beruhte, unterstützt durch ständig aktualisierte Technologien. Eine auf Verifizierungen basierende Atomwaffenkontrolle bliebe äußerst

schwierig, wenn die USA und Russland nicht bereit wären, Teile ihrer Atomwaffenarsenale offenzulegen. Tatsächlich lassen andere Atomwaffenstaaten solche Inspektionen nicht zu, was zu zahlreichen Streitigkeiten führt.

In den letzten Jahren war die Umsetzung der Verifizierungsmechanismen der Rüstungskontrolle zwischen den USA und Russland negativ von geopolitischen Konflikten wie dem Ukraine-Krieg betroffen. Beide Seiten glauben, dass die jeweils andere Seite die Modernisierung ihres Nukleararsenals energisch vorantreibt. Dies zeigt, dass die Verifizierung von Atomwaffen Vorbedingungen unterliegt, insbesondere politischer Vermittlung. Nuklearwaffen sind nicht unbedingt leichter zu verifizieren, nur weil das Objekt der Rüstungskontrolle eine physische Form hat und gezählt werden kann.

Die Verifizierung von Algorithmen und Datensätzen der Künstlichen Intelligenz steht sicherlich vor technischen Hürden, das heißt aber nicht, dass sie überhaupt nicht verifizierbar wären. Tatsächlich müssen wir nicht alle Modelle und Datensätze verifizieren; die relevanten Länder müssen lediglich die Modelle und zugehörigen Datensätze zur Verfügung stellen, die am ehesten Sicherheitsrisiken bergen, damit diese getestet und bewertet werden können. Sicherheitstests für Künstliche Intelligenz stehen vor ähnlichen Herausforderungen wie die *Governance* der Cybersicherheit. Theoretisch könnte die internationale Gemeinschaft unabhängige Labore zur Bewertung von Cybersicherheitslücken einrichten und Schwachstellen- und Virendatenbanken erstellen. Unabhängige Labore könnten eingeladen werden, Cybersicherheitsbewertungen für kritische digitale Infrastruktur und wichtige Glieder der Lieferkette durchzuführen. Dass dieses Idealmodell nicht in die Praxis umgesetzt wurde, liegt am großen gegenseitigen Misstrauen der Großmächte und ihren divergierenden Interessen im Bereich der Cybersicherheit.

Grundsätzlich stellt der Mangel an politischem Willen zur Zusammenarbeit und an Vertrauen ein größeres Hindernis dar als technische Probleme.

Grundsätzlich stellt der Mangel an politischem Willen zur Zusammenarbeit und an Vertrauen ein größeres Hindernis dar als technische Probleme. Ein aufschlussreiches Beispiel stammt aus dem Jahr 2018, als sich Huawei – in dem Bestreben, Zugang zum britischen 5G-Markt zu erhalten – bereit erklärte, sich einer technischen Überprüfung durch britische Sicherheitsbehörden zu unterziehen, und ein Zentrum für Cybersicherheitstransparenz in Brüssel einrichtete, wo es seinen Quellcode und seine Testumgebungen zur Verfügung stellen

würde. Aus politischen Gründen lehnten viele europäische Länder die Einführung von Huaweis 5G-Technologie dennoch ab.

Zweitens argumentieren einige, dass die rechtlichen und ethischen „roten Linien“ im Zusammenhang mit Atomwaffen sehr klar seien, was es einfacher mache, einen internationalen Konsens zur nuklearen Rüstungskontrolle zu erzielen als zur Regulierung von Künstlicher Intelligenz. Allerdings enthalten auch die „roten Linien“ und „Tabus“ im Zusammenhang mit Atomwaffen viele Unklarheiten, die zu zahlreichen Streitigkeiten geführt haben. So lässt sich beispielsweise nach einem Urteil des Internationalen Gerichtshofs aus dem Jahr 1994 immer noch nicht eindeutig feststellen, ob der Einsatz von Atomwaffen zur Verteidigung des eigenen Landes rechtmäßig ist. Auch der Atomwaffensperrvertrag (*Non-Proliferation Treaty*, NPT) ist nicht präzise genug, wenn es um den Einsatz von Atomwaffen in anderen Ländern geht.

Drittens argumentieren einige, dass es sich bei der Nukleartechnologie um eine spezifische Technologie mit leicht unterscheidbaren militärischen und zivilen Anwendungen handele und dass deshalb leicht ein separates Rüstungskontrollsystem rund um ihre militärischen Anwendungen eingerichtet werden könne. KI hingegen sei eine weit verbreitete, universell einsetzbare Technologie, bei der keine klare Unterscheidung zwischen militärischen und zivilen Anwendungen bestehe. Diese Sichtweise übersieht eine grundlegende Tatsache: Die Revolution der Atomtechnologie spielte eine entscheidende Rolle bei der weltweiten wirtschaftlichen Erholung nach dem Zweiten Weltkrieg, wie das Programm *Atoms for Peace* verdeutlicht. Darüber hinaus waren Systeme zur Rüstungskontrolle im Nuklearbereich nie auf den militärischen Bereich beschränkt. Die Überzeugung, dass militärische und zivile Anwendungen der Nukleartechnologie leicht zu unterscheiden seien, ist Ergebnis der gemeinsamen Bemühungen der Nationen während eines halben Jahrhunderts, ein umfassendes Nichtverbreitungsregime zu etablieren, das sowohl militärische als auch zivile Anwendungen abdeckt, und von Exportkontrollsystemen wie dem Zangger-Komitee für Nuklearexport.

Die Wahrnehmung, dass bei Nukleartechnologie leicht zwischen militärischer und ziviler Nutzung unterschieden werden könne, geht auf den jahrzehntelangen Einfluss des NPT zurück. Die drei Säulen Nichtverbreitung, nukleare Abrüstung und friedliche Nutzung der Kernenergie haben sich tief in das Bewusstsein der Menschen eingegraben. Die Vereinigten Staaten haben die nukleare Verbreitung durch verschiedene Mittel wie diplomatischen Druck,

Wirtschaftssanktionen und sogar militärische Maßnahmen verhindert. Nukleare Tabunormen geben den meisten Ländern klare Vorgaben, was sie tun und was sie unterlassen sollten.

Gleichzeitig haben viele Länder versucht, durch den Ausbau der zivilen Kernenergie an Atomwaffen zu gelangen. Bis heute ist die iranische Atomfrage ungelöst, weil erhebliche Unklarheiten hinsichtlich des akzeptablen Urananreicherungsgrades bestehen. Einige Länder sind zu sogenannten Nuklear-Schwellenstaaten geworden, indem sie starke zivile nukleartechnologische Fähigkeiten entwickeln und Vorräte sensibler nuklearer Materialien anlegen.

Das größte Problem ist, dass wir noch keinen Konsens darüber erzielt haben, welche Art von KI-Technologien und -Anwendungen inakzeptabel sind.

Der Dual-Use-Charakter der KI-Technologie ist nicht das Haupthindernis für KI-Rüstungskontroll-Mechanismen; die Gegenstände solcher Mechanismen sind fast immer Dual-Use-Technologien. Das größte Problem ist, dass wir noch keinen Konsens darüber erzielt haben, welche Art von KI-Technologien und -Anwendungen inakzeptabel sind. In diesem Sinne scheinen wir in der Ära vor 1945 zu leben: Großmächte liefern sich einen erbitterten Wettstreit um eine disruptive Technologie, aber niemand weiß wirklich, wie ihre endgültige Form aussehen wird.

Das erste Land, das sich eine Allgemeine Künstliche Intelligenz (AKI) oder Künstliche Superintelligenz (KSI) aneignet – deren überwältigende Macht wir noch nicht vollständig verstehen –, wird wahrscheinlich versuchen, ein Monopol zu errichten. Wenn andere Länder nach und nach AKI oder KSI erlangen, werden sie wahrscheinlich neue Mechanismen zur Nichtverbreitung und zur internationalen Sicherheit erproben. Möglicherweise werden diese anderen Länder dann zwar in der Lage sein, KI-Technologien zu nutzen, aber es wäre ihnen möglicherweise verwehrt, AKI oder KSI vollständig zu erlangen, ganz ähnlich den Beschränkungen des Atomwaffensperrvertrags (NPT). Entsprechende Nichtverbreitungsmechanismen könnten in Bezug auf Rechenleistung, Datensätze und Stromressourcen aufgebaut werden. Großmächte könnten durch den Erwerb von AKI oder KSI eine neue Art gegenseitiger Verwundbarkeit und strategischer Stabilität erreichen.

Entwicklungsländer und der Globale Süden würden die Entstehung einer weiteren diskriminierenden internationalen Regelung, die den Abstand im KI-Bereich vergrößern und ihr Recht auf Entwicklung beeinträchtigen würde, selbstverständlich nicht begrüßen. Eine

alternative zukünftige institutionelle Regelung bestünde in der Bildung regionaler Rechenleistungs- und Stromzentren in Ostasien, Südasien, dem Nahen Osten, Europa, Afrika und Amerika sowie in der Gründung kooperativer Organisationen auf der Grundlage bestehender regionaler Integrationsmechanismen, die für die Forschung im Bereich Superintelligenz und für die Identifizierung von Sicherheitsrisiken zuständig wären.



Tianjiao Jiang
Shanghai

Tianjiao Jiang ist *Associate Professor* am Entwicklungsinstitut der Fudan-Universität und seit 2026 Gastwissenschaftler am *Paul Tsai China Center* der *Yale Law School*. Seine Forschungsschwerpunkte liegen auf neuen Technologien und internationaler Sicherheit.