Karl Hans Bläsius, 30. 01. 2023

Link zu diesem Dokument: https://www.fwes.info/akr-techn-entw-2023-1.pdf

Atomkriegsrisiko und neue technische Entwicklungen

Seit dem Krieg in der Ukraine ist auch das Risiko eines möglichen Atomkriegs in der Diskussion. Auch vor Ausbruch dieses Krieges wurde schon von verschiedenen Initiativen vor Kriegsrisiken und dem Atomkriegsrisiko gewarnt, unter anderem auch vor einem Atomkrieg aus Versehen. Dieses Risiko wird vermutlich unabhängig vom Ukraine-Krieg in den nächsten Jahren und Jahrzehnten steigen. Hierbei spielen auch Aspekte von Informatik und Künstliche Intelligenz (KI) eine Rolle. In diesem Artikel werden solche Zusammenhänge und damit verbundene Risiken beschrieben, sowie Möglichkeiten zur Reduzierung dieser Risiken aufgezeigt.

Inhalt:

1. Cyberangriffe, Cyberwaffen

In den letzten Jahren waren Konflikte zwischen Staaten regelmäßig von Cyberangriffen begleitet. Diese Tendenz wird sich weiter verstärken und die Cyberkriegskapazitäten werden von vielen Staaten auf- und ausgebaut. Für Cybergefahren gelten spezielle Eigenschaften, die sicherheitspolitisch relevant sind. So gibt es für Cyberangriffe keine räumlichen Grenzen, eine geographische Abgrenzung ist kaum möglich. Angriffe erfolgen unmittelbar und ohne Zeitverlust. Eine Frühwarnung ist während eines Cyberangriffs nicht möglich. Wenn wirkungsvolle Cyberkriegskapazitäten entwickelt wurden, sind diese für einen Angriff ohne großen Aufwand an vielen Stellen anwendbar. Defensive und offensive Cyber-Fähigkeiten gelten heute als wichtige Grundlage militärischer Macht, wobei zu befürchten ist, dass offensive Operationen gegenüber defensiven Aktionen immer überlegen sein werden.

Das Schadenspotenzial von Cyberangriffen kann besonders groß sein, wenn die kritische Infrastruktur einer Zivilgesellschaft getroffen wird. Dies kann die Bereiche Energie, Wasser,

Gesundheit, Ernährung, Telekommunikation, Logistik, Finanzwesen und die staatliche Verwaltung betreffen. Auch Satelliten und Komponenten der Nuklearstreitkräfte können angegriffen werden. Technische Anlagen können durch Cyberangriffe zerstört werden.

Urheber sind in der Regel sehr schwer zu ermitteln, es können Einzelpersonen, Gruppen, Organisationen oder Staaten sein. Es kann Monate oder Jahre dauern, um den Urheber eines Angriffs zu identifizieren. Die Möglichkeiten im Cyberraum entwickeln sich dynamisch und unabsehbar. Welche Arten von Gefahren uns hier in Zukunft drohen ist daher unklar, und ebenso unkalkulierbar sind deren mögliche Auswirkungen.

2. KI, autonome Waffen

Große Fortschritte im Gebiet „Künstliche Intelligenz“ (KI) haben auch zu entsprechenden Fortschritten in der Militärtechnik geführt. Insbesondere können selbständig agierende Roboter oder Drohnen auch für militärische Zwecke eingesetzt werden. Auf der Basis einer automatischen Bilderkennung mit guter Objektklassifikation können feindliche Ziele automatisch identifiziert und attackiert werden.

Der Begriff „autonome Waffen“ kann unterschiedlich eng oder weit gefasst werden. Streng genommen versteht man darunter ein Gerät, das nach seiner Aktivierung mit Hilfe von Sensoren und Software selbstständig ohne menschliche Kontrolle einen Weg zu einem Ziel sucht und dort selbständig Operationen auslösen kann, z.B. um etwas zu zerstören oder auch Menschen zu töten.

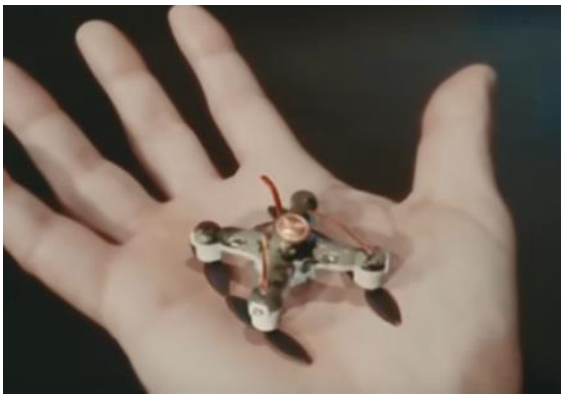
Für Autonomie in Waffensystemen gibt es ein großes Anwendungsspektrum. Viele Arten von Waffen können mit immer mehr Autonomie versehen werden. Dies betrifft Roboter, Fahrzeuge, Flugobjekte und auch Schiffe oder U-Boote. In solchen Systemen können Menschen durch KI-Komponenten ersetzt werden. Dies kann ähnlich wie beim Autonomen Fahren auch schrittweise erfolgen. Unsere modernen Autos enthalten schon viele autonome Funktionen bis hin zum völlig autonomen Fahren, wobei aus rechtlichen Gründen aber ein Mensch noch jederzeit eingreifen können muss. Denn im Straßenverkehr werden Unfälle von autonomen Fahrzeugen noch nicht toleriert. In Kriegssituationen kann das anders sein, Kollateralschäden werden eher in Kauf genommen. Auch weniger gut ausgereifte autonome Funktionen könnten hier zum Einsatz kommen. Damit steigt das Risiko, dass solche Systeme in Kriegszeiten auch eingesetzt werden. Und es steigt das Risiko, dass ihre Entwicklung von vielen Staaten vorangetrieben wird, auch weil sich der Einsatz von Drohnen bisher vielfach als wirkungsvoll herausgestellt hat.

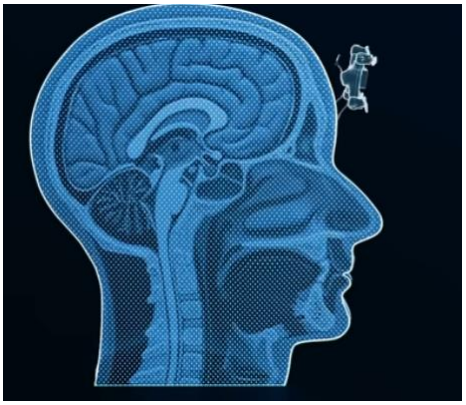
In Zusammenhang mit Autonomen Waffen wird es auch neuartige Waffen geben, wie man sie bisher nicht kannte. Zur Unterstützung einer Kampagne zum Verbot autonomer Waffen hat das Future of Life Institute im November 2017 den knapp achtminütigen Film „Slaughterbots“ veröffentlicht, in dem die Risiken autonomer Waffen verdeutlicht werden.[1] Der Film zeigt eine Minidrohne, die ihren Weg mit automatischer Bilderkennung sucht und ein Ziel mit automatischer Gesichtserkennung identifiziert. Nach Erreichen des Ziels kann eine tödliche Sprengladung gezündet werden. Mit den heutigen Techniken können solche Waffen in recht kurzer Zeit konstruiert und eingesetzt werden.

---

[1] https://futureoflife.org/newsletter/fli-november-2017-newsletter/ und https://futureoflife.org/video/the-ideas-behind-slaughterbots-if-human-kill-a-deep-dive-interview/

Ausschnitte aus diesem Film:





Die im Film verwendete Drohne ist recht klein. Nach der Identifikation eines Ziels positioniert sich die Drohne auf der Stirn des Opfers.

Eine tödliche Sprengladung kann gezündet werden.

Die Kargu-Drohne der türkischen Firma stm hat angeblich bereits eine solche automatische Gesichtserkennung und kann auf diese Weise gegen Zielpersonen eingesetzt werden.

In einem Bericht für den Bundestag zur Technikfolgen-Abschätzung für autonome Waffen schreiben die Autoren zum Zusammenhang zwischen autonomen Waffen und Nuklearwaffen: „Auf der globalen Ebene spielt das strategische Gleichgewicht zwischen den Nuklearwaffenstaaten nach wie vor eine herausragende Rolle. Es basiert wesentlich auf der gesicherten Fähigkeit eines Zweitschlags und der daraus resultierenden Abschreckung eines möglichen Erstschlags. Es wäre vorstellbar, dass sehr potente AWS (autonomous weapons systems) zukünftig als konventionelle Erstschlagwaffen zur Zerstörung gegnerischer Nuklearwaffenarsenale eingesetzt werden könnten, die mögliche Ziele (Raketensilos oder mit Nuklearwaffen bestückte U-Boote) selbstständig aufklären, in deren Nähe unentdeckt verweilen und auf Befehl koordiniert diese Ziele angreifen und zerstören. AWS könnten auch als Trägerplattformen für Nuklearwaffen verwendet werden, beispielsweise in Form von autonomen Unterwasserfahrzeugen. Diese könnten schneller, überraschender und koordinierter als bisherige Trägersysteme zuschlagen und vorhandene Verteidigungsmaßnahmen aushebeln. Eine solche Nutzung von AWS würde die strategische Stabilität massiv infrage stellen. Dies wiederum könnte weitere nukleare Abrüstung

unmöglich machen und eine Ära nuklearer Modernisierung oder gar nuklearer Aufrüstung einläuten."[2]

3. Rüstungskontrolle bei Software

Bei üblichen Waffensystemen sind Rüstungskontrolle und Verifikation möglich. Flugzeuge, Schiffe, Panzer und Atomwaffen können gezählt werden. Bei Cyberwaffen und autonomen Waffen geht es indessen um Software. Softwaresysteme haben spezielle Merkmale, für die eine Rüstungskontrolle und die Verifikation von Vereinbarungen kaum realisierbar sind.

Bei Software sind beliebig viele Kopien in kurzer Zeit herstellbar und entsprechend beliebig oft anwendbar. In [Rus20] argumentiert der KI-Wissenschaftler Stuart Russell (Seite 122 - 123), dass autonome Waffensysteme als Massenvernichtungswaffen einzustufen sind, da sie „skalierbar", also in beliebig großer Anzahl produzierbar sind.

Software unterliegt meist einer kontinuierlichen Entwicklung, wobei fast jeder Zwischenstand anwendbar ist. Von außen ist nicht erkennbar, welches Potential in der Software steckt – bei ihrem Einsatz zeigt sich jeweils nur ein Teil der Fähigkeiten des aktuellen Entwicklungsstandes. Weitere Fähigkeiten könnten enthalten sein, die bei einem Einsatz noch nicht sichtbar wurden.

Die Entwicklung von Software erfolgt oft im Verborgenen, wobei allenfalls die Entwickler selbst gewisse Einblicke haben. Bei großen Entwicklungsprojekten, die oft viele Millionen Zeilen Code enthalten, haben auch die einzelnen Mitglieder eines Teams nur einen eingeschränkten Einblick in das Gesamtsystem. Noch schwieriger wird es für Fremde, mögliche Funktionalitäten einer Software zu erkennen.

Ein Staat wird kaum zulassen, dass bzgl. Verifikation von Rüstungskontrollvereinbarungen Mitarbeiter eines gegnerischen Staates Einblick in die eigene Software erhalten. Das Risiko wäre zu hoch, dass damit der Gegner eine Kopie dieser Software erhalten könnte. Des Weiteren wäre eine Überprüfung der möglichen Funktionalitäten sehr aufwendig und könnte Jahre dauern, währenddessen die Software ohnehin weiterentwickelt würde. Es wäre auch nicht feststellbar, ob eine zu prüfende Software tatsächlich die relevante Version ist, oder ob diese verändert ist und nicht alles enthält.

Für Außenstehende ist nicht feststellbar, welche weiteren Funktionalitäten in einer Software in kurzer Zeit realisierbar sind, für die bereits Grundlagen gelegt sind. Es ist völlig unkalkulierbar, was in Zukunft hinsichtlich softwarebasierter Waffen auf uns zukommt.

Abrüstungsvereinbarungen bezogen auf Software werden kaum möglich sein. Der INF-Vertrag von 1987 führte zur Vernichtung sehr vieler Atomwaffen. Bei Software kann es beliebig viele Kopien geben. Auch im Falle von entsprechenden Vereinbarungen wird nicht überprüfbar sein, ob alle Kopien der Software für ein autonomes Waffensystem gelöscht sind. Einmal entwickelte Software für autonome Waffen wird immer erhalten bleiben.

4. These von Clausewitz

Eine These des Militärwissenschaftlers Clausewitz besagt, dass die Verteidigung die überlegene Form der Gefechtsführung ist. Demnach gilt grundsätzlich, dass ein Verteidiger

---

[2] [GK20], Seite 19 und Seite 118 - 119

bei militärischem Gleichgewicht gegenüber einem Angreifer im Vorteil ist. Dies ist sicherheitspolitisch relevant, denn solange diese These als gültig angenommen wird, kann dies potenzielle Angreifer abschrecken und das Kriegsrisiko senken.

Generalleutnant a.D. Kersten Lahl und Prof. Johannes Varwick schreiben in ihrem Buch „Sicherheitspolitik verstehen“, dass diese These von Clausewitz in Zusammenhang mit Cyberangriffen nicht zutrifft. Im Cyberraum ist nicht mehr der Verteidiger im Vorteil, sondern der Angreifer.

Das Gleiche gilt bezüglich des steigenden Einsatzes von KI in Waffensystemen bis hin zu Autonomen Waffen. Lahl und Varwick sehen die Gefahr, dass hierdurch die Clausewitz'sche Lehre nicht mehr gilt und ins Gegenteil verkehrt wird. Denn ein vermehrter Einsatz von KI-Techniken kann zu einer Komplexität und Dynamik in Angriffssituationen führen, in denen Abwehrmaßnahmen kaum noch wirksam sind. Dies hätte erhebliche Folgen für die globale Sicherheit, auch im Hinblick auf die nukleare Abschreckung.[3]

5. Atomkriegsrisiko

Auch wenn die nukleare Abschreckung einen bewussten Atomwaffeneinsatz bisher verhindert hat, gibt es keine Garantie, dass dies immer so bleibt. Dies wird auch von Experten aus Militär und Sicherheitspolitik so gesehen. Lahl und Varwick sehen das Risiko einer mangelnden Beherrschbarkeit der Kategorie nuklearer Waffen durch eine zunehmende Zahl von Atomwaffenstaaten einerseits und eine zunehmende Komplexität möglicher nuklearer Bedrohungssituationen durch neue technische Entwicklungen andererseits.[4]

Die nukleare Abschreckungsstrategie beinhaltet auch den Betrieb von Frühwarnsystemen zur Erkennung eines Angriffs mit Atomwaffen. Hierbei kann es aber zu Fehlalarmen kommen, bei denen nukleare Angriffe gemeldet werden, obwohl kein Angriff vorliegt. Solche Fehlalarme sind besonders gefährlich im Falle von internationalen Krisen. In der Vergangenheit gab es einige Situationen, in denen es nur durch großes Glück nicht zu einem Atomkrieg aus Versehen kam. Die Abschreckungsstrategie schützt also nicht vor einem „Atomkrieg aus Versehen“.

Das Wissen um die gravierenden Auswirkungen eines Atomkriegs bildet auch in Krisen- und Kriegszeiten eine große Hemmschwelle für den Einsatz von Atomwaffen. Dennoch sind verschiedene Szenarien denkbar, in denen es zu einem Einsatz kommen kann:

1. Bewusster Einsatz von Atomwaffen: Eine Seite setzt Atomwaffen ein, um einen Vorteil zu erzielen, ein bestimmtes Ziel zu erreichen oder Vergeltung zu üben.
2. Atomkrieg aus Versehen: Aufgrund eines Fehlalarms in einem Frühwarnsystem für nukleare Bedrohungen kommt es durch Fehleinschätzungen zu einem Atomkrieg.
3. Kombination von bewusstem und versehentlichem Atomkrieg: Ein Fehlalarm in einem Frühwarnsystem könnte als Anlass für einen nuklearen Angriff gewählt werden, wenn ein solcher ohnehin schon in Erwägung gezogen wurde. Die Aspekte 1 und 2 könnten sich entscheidend verstärken.

Wenn es zu einem Einsatz von Atomwaffen kommt, wird dies wie ein Unfall plötzlich und unerwartet geschehen, egal ob der Einsatz bewusst, aus Versehen oder als Kombination von

---

[3] [LV22], Seite 133

[4] [LV22], Seite 130, siehe auch https://atomkrieg-aus-versehen.de/zitat-LV-kB/

beidem erfolgt. Ähnliche Risiken kennen wir aus vielen Lebensbereichen. Auch wenn eine riskante Fahrweise im Straßenverkehr hundertmal gut gegangen ist, ist dies keine Garantie, dass es beim nächsten Mal auch wieder gut geht, stattdessen kann es tödlich enden. Auch wenn ein schrittweises Ausloten, wie weit der Westen mit Waffenlieferungen gehen kann, bisher noch nicht zu einer nuklearen Eskalation geführt hat, ist keinesfalls sicher, dass dies immer so bleibt. Auch wenn die nukleare Abschreckungsstrategie bisher einen Atomkrieg verhindert hat, ist damit nicht sicher, dass dies immer gelten wird. Im Gegenteil: mangelndes Vertrauen zwischen Atommächten und eine enorme Erhöhung der Komplexität möglicher Bedrohungslagen durch neue technische Entwicklungen erhöhen die Risiken einer nuklearen Konfrontation.

In Zusammenhang mit Atomwaffen können in Frühwarn- und Entscheidungssystemen als Folge einer Eskalationsspirale und falscher Einschätzungen plötzlich, völlig unerwartet und ohne Vorwarnung innerhalb weniger Minuten Prozesse ablaufen, die zum Einsatz vieler Atomwaffen führen und das Überleben der gesamten Menschheit gefährden. Solche Prozesse sind irreversibel, die gefallenen Entscheidungen endgültig. Es gibt hinterher keine Möglichkeiten mehr zu einer Korrektur.

6. Einfluss Cyber, KI/autonome Waffen auf Atomkriegsrisiko

Es ist zu erwarten, dass das Risiko eines Atomkriegs in den nächsten Jahren und Jahrzehnten stark steigen wird. Der Klimawandel wird zu mehr Krisen führen und neue technische Entwicklungen werden die Komplexität von Frühwarnsystemen und Bedrohungssituationen so stark erhöhen, dass die Beherrschbarkeit solcher Systeme immer schwieriger wird.

In den letzten Jahren hat ein neues Wettrüsten in verschiedenen militärischen Dimensionen begonnen. Die meisten dieser Entwicklungen sind noch am Anfang und die Folgen kaum kalkulierbar. Dies gilt für neue Trägersysteme von Atomwaffen, wie etwa die Hyperschallraketen, die geplante Bewaffnung des Weltraums, Laserwaffen, den Ausbau von Cyberkriegskapazitäten und die zunehmende Anwendung von Systemen der Künstlichen Intelligenz bis hin zu autonomen Waffensystemen. Alle diese Aspekte haben auch Wechselwirkungen mit Frühwarnsystemen zur Erkennung von Angriffen mit Atomraketen und werden die Komplexität dieser Systeme deutlich erhöhen.

Die Weiterentwicklung von Waffensystemen mit höherer Treffsicherheit und immer kürzeren Flugzeiten (Hyperschallraketen) wird zunehmend Techniken der Künstlichen Intelligenz (KI) erforderlich machen, um für gewisse Teilaufgaben Entscheidungen automatisch zu treffen. Es gibt im Zusammenhang mit Frühwarnsystemen bereits Forderungen, autonome KI-Systeme zu entwickeln, die vollautomatisch eine Alarmmeldung bewerten und gegebenenfalls einen Gegenschlag auslösen, da für menschliche Entscheidungen keine Zeit mehr bleibt. Die für eine Entscheidung verfügbaren Daten sind in der Regel jedoch vage, unsicher und unvollständig. Deshalb können auch KI-Systeme in solchen Situationen nicht zuverlässig entscheiden. In der kurzen verfügbaren Zeit wird es kaum möglich sein, Entscheidungen der Maschine zu überprüfen. Dem Menschen bleibt nur zu glauben, was die Maschine liefert. Aufgrund der unsicheren und unvollständigen Datengrundlage werden weder Menschen noch Maschinen in der Lage sein, Alarmmeldungen zuverlässig zu bewerten.

Nach einem Bericht der „National Security Commission on Artificial Intelligence“ der USA vom November 2019 besteht die Gefahr, dass KI-fähige Systeme bisher unverletzliche militärische Positionen verfolgen und angreifen und somit die globale strategische Stabilität

und nukleare Abschreckung untergraben könnten. Staaten könnten dadurch zu einem aggressiveren Verhalten verleitet werden, was die Anreize für einen Erstschlag erhöhen könnte.[5] In dem Bericht werden auch Vereinbarungen zwischen USA, Russland, China und anderen Nationen vorgeschlagen, um ein Verbot für einen durch KI-Systeme autorisierten oder ausgelösten Abschuss von Atomwaffen zu erwirken.[6]

Auch der SIPRI-Bericht über die Auswirkungen der KI auf die strategische Stabilität und die nuklearen Risiken warnt vor einem zunehmenden Einsatz von autonomen oder KI-basierten Entscheidungsunterstützungssystemen, die nur scheinbar ein klares Bild in kurzer Zeit liefern. Um ein gewisses Maß an Stabilität aufrechtzuerhalten, sei ein Austausch zwischen Militärs über die jeweiligen KI-Fähigkeiten erforderlich, um das Prinzip der nuklearen Abschreckung aufrecht erhalten zu können.[7]

Unkalkulierbar sind auch potenzielle Cyberangriffe, wobei Komponenten oder Daten eines Frühwarnsystems manipuliert werden könnten, was auf vielfältige Art möglich sein kann.

7. Risiken durch Falschnachrichten

In Kriegszeiten spielen Propaganda und Falschnachrichten eine große Rolle. Möglicherweise haben in Zukunft auch Fake-News unkalkulierbare Auswirkungen auf Frühwarn- und Entscheidungssysteme und beeinflussen die Bewertung von Alarmmeldungen. Im Dezember 2016 wird der frühere israelische Verteidigungsminister in einem gefälschten Online-Artikel mit der Aussage zitiert, dass Israel Pakistan nuklear zerstören werde, falls Pakistan Truppen gegen den IS nach Syrien schicken würde. Der pakistanische Verteidigungsminister hat die Fälschung nicht erkannt und seinerseits mit Atomwaffen gedroht.

Mit Techniken des „deepfake“ können Audio- und Video-Dateien erzeugt werden, in denen eine Person einen beliebigen Text spricht, wobei Aussprache und Bild so zu dieser Person passen, dass diese Fälschung kaum erkennbar ist. Besonders gefährlich kann es werden, wenn es Hackern gelingt, sich in eine Konferenz zur Bewertung einer nuklearen Alarmmeldung einzuschalten, dabei die Verbindung mit einem „falschen“ Präsidenten herstellen und diesen sprechen lassen, was sie möchten.

Mit den technischen Möglichkeiten des „deepfake“ kann alles gefälscht werden. Ein Ausnutzen solcher Möglichkeiten durch Hacker (z.B. von Terror-Organisationen) kann politisches Handeln in Krisensituationen sehr erschweren, denn bereits die Tatsache, dass Bedienungsmannschaften irgendwann wissen, dass alles (z.B. Ton- und Videoaufnahmen) gefälscht sein mag, kann zu großen Unsicherheiten bei der Bewertung von Krisensituationen führen. Techniken wie deepfake können zu einer Vertrauenskrise führen und jede übermittelte Information an ein Frühwarnsystem für nukleare Bedrohungen könnte falsch sein. Dies wird in vielen Fällen nicht feststellbar sein.

Auch ein Sipri-Bericht von 2019 beschreibt die Gefahr, dass im Rahmen eines Informationskriegs gefälschte naturgetreue Scheinbefehle in Form von Audio- oder Video-

---

5 [SW19], Seite 11

6 [SW19], Seite 46

7 [Bou19], Seite 50-51

Sequenzen Kernwaffenbetreiber dazu verleiten könnten, eine Kernwaffe zu starten oder auf einen Angriff nicht zu reagieren.[8]

8. Schutz- und Abschreckungsmaßnahmen

Als Möglichkeiten Cyberangriffe abzuschrecken, nennen Lahl und Varwick vier Optionen:[9]

1. Androhung von Strafe,
2. Sicherheit durch Resilienz
3. internationale Verflechtung
4. internationale Normensetzung

Option 1 ist die Androhung von Strafe. Diese kann in einem Gegenangriff bestehen, aber auch in wirtschaftlichen oder militärischen Maßnahmen. Hauptproblem ist hierbei die Bestimmung des Urhebers von Angriffen.

Option 2 ist Sicherheit durch Resilienz. Hierbei soll die Sicherheit durch technische und organisatorische Vorsorge verbessert werden. Dazu gehören wirkungsvolle Firewalls, redundante Systeme und die Abtrennung besonders verwundbarer Systeme. Lahl und Varwick sehen hierbei aber folgendes Problem: „Allerdings leidet dieser Ansatz unter der Tatsache, dass alle auch noch so guten Abwehrmittel aufgrund der Rasanz im technologischen Wandel immer wieder rasch an Wirkung verlieren. Die Sicherheitskonzepte drohen damit stets der Realität hinterherzulaufen." Als weiteren Nachteil dieses Ansatzes sehen Lahl und Varwick auch die Tatsache, dass solche Schutzmechanismen realistisch getestet werden müssen, was wiederum die Entwicklung entsprechend offensiver Cyberwaffen voraussetzt.

Option 3 ist eine internationale Verflechtung. Dazu Lahl und Varwick: „Dieser Ansatz nutzt die Erkenntnis, dass in einer global vernetzten Welt jede gewaltsame Auseinandersetzung unter dem Strich nur Verlierer hervorbringt. Je stärker also die Akteure miteinander wirtschaftlich, technologisch, kulturell und ggf. auch militärisch vernetzt sind, desto geringer ist die Chance, durch Aggression einseitige Vorteile erzielen zu können. Dieser oft zu Unrecht als naiv empfundene Gedanke läuft damit auf eine Art der Selbstabschreckung hinaus." Die Grenzen dieses Ansatzes sehen Lahl und Varwick darin, dass oft nationale Interessen verfolgt werden und es daher eventuell an der Bereitschaft der betreffenden Akteure zu Vertrauensbildung und gegenseitiger Verflechtung mangelt.

Option 4 ist eine internationale Normensetzung. Internationale Vereinbarungen könnten ein Mittel sein, um einen unkontrollierten Rüstungswettlauf bei Cyberkriegskapazitäten zu dämpfen. Dazu gehören könnten Normen für Forschung und Entwicklung, Regeln zur völkerrechtlichen Einordnung und die Ächtung bestimmter Cyberaktivitäten. Es gibt keine Garantie, dass solche Regeln eingehalten werden, trotzdem könnten diese eine abschreckende Wirkung haben.

Keine dieser vier Optionen reicht alleine für eine bessere Sicherheit – es ist eine Kombination von mehreren oder allen Optionen erforderlich. So reichen nationale Lösungen, wie sie Option 1 und Option 2 erlauben, nicht aus. Nur weitreichende internationale Lösungen mit einem weiten Blick in die Zukunft sind erfolgsversprechend.

---

8 [Bou19], Seite 61

9 [LV22], ab Seite 117

Auch bezüglich der Risiken durch Autonome Waffensysteme sind diese vier Optionen relevant. Die Bestrebungen ein Verbot zu erreichen, sind bisher allerdings erfolglos. Es gibt bis jetzt keinerlei rechtliche Einschränkungen (Option 4). Problematisch ist auch, dass bei keinem Waffensystem direkt erkennbar ist, ob autonome Funktionen enthalten sind. Die Androhung von Strafe (Option 1) wird hierbei kaum wirksamer sein, als bei der Anwendung herkömmlicher Waffensysteme. Ein technischer Schutz (Option 2) vor autonomen Waffen wird eher schwieriger sein. Denn diese Systeme könnten auch KI-basierte Komponenten zur Erkennung von Abwehrangriffen enthalten und damit solchen Angriffen ausweichen.

Option 3 wird auch bezüglich der Gefahren durch autonome Waffensysteme besonders wichtig sein. Je stärker potenzielle Gegner wirtschaftlich, technologisch und kulturell miteinander vernetzt sind, je besser damit Vertrauen und Zusammenarbeit sind, desto geringer werden Motivation und Wille sein, Mittel und Prioritäten auf die Entwicklung von autonomen Waffen zu legen.

9. Optionen zur Reduzierung des Atomkriegsrisikos

Die vier in Abschnitt 8 beschriebenen Optionen sind auch relevant, um das Atomkriegsrisiko zu reduzieren.

In vielen Fällen wird Option 1, die Androhung von Strafe, als ausreichend zum Schutz vor einem Atomkrieg dargestellt und es wird in diesem Sinne auch von einem nuklearen Schutzschirm gesprochen. Auch wenn die nukleare Abschreckung, also Androhung von Strafe, nach 1945 Atomwaffeneinsätze verhindert hat, gibt es keine Garantie, dass dies immer so bleibt (siehe Abschnitt 5).

Moderne Abwehrsysteme werden einen Teil angreifender Atomraketen abfangen können, aber nicht alle. Insbesondere wird es schwer sein, lenkbare Hyperschallraketen zu treffen. Option 2 wird also nur bedingt anwendbar sein. Auch wird gelten, dass bei einem Rüstungswettlauf zwischen offensiven und defensiven Komponenten die Defensive der Offensive immer hinterherlaufen wird.

Bereits vor Beginn des Ukraine-Krieges am 24.2.2022 war das Vertrauensverhältnis zwischen den Atommächten USA und Russland sehr schlecht. Dazu schreiben Michael Staack und Gunther Hauser 2020 in [SH20]: „Die Beziehungen zwischen Russland und den westlichen Staaten sind gegenwärtig so schlecht wie seit den frühen 1980er Jahren nicht mehr – der Zeit vor dem Amtsantritt Michail Gorbatschows in der damaligen Sowjetunion (1985). Sicherheitspolitisch fällt die Analyse noch kritischer aus. Der damalige Kalte Krieg bewegte sich in relativ geordneten Bahnen und beide Seiten bemühten sich insbesondere, Risiken durch versehentliche militärische Zusammenstöße zu vermeiden. An solchen eingespielten Mechanismen und Selbstkontrollen fehlt es derzeit und das im OSZE-Rahmen aufgebaute Netzwerk von Vertrauens- und sicherheitsbildenden Maßnahmen und Krisenprävention wird nicht geachtet und genutzt. Deshalb ist eine militärische Eskalation aus Versehen wahrscheinlicher geworden als sie das in den 1980er Jahren war. Dazu tragen auch neue Waffensysteme mit verkürzten Vorwarnzeiten bei.“

Inzwischen sind sehr viele wirtschaftliche, technologische, kulturelle und sonstige Beziehungen zum Westen abgebrochen worden. Eine mögliche Wirksamkeit von Option 3 gibt es daher inzwischen kaum noch. Auch bezüglich Option 4 sind die Risiken gestiegen, denn viele wichtige Verträge wie INF und „Open Skies“ sind in den letzten Jahren gekündigt

worden. Alle vier Optionen sind auch zum Schutz vor einem Atomkrieg wichtig, allerdings sind die Bedingungen für zwei dieser Optionen in den letzten Jahren deutlich verschlechtert worden. Auch deshalb ist das Atomkriegsrisiko gestiegen.

Dies gilt insbesondere auch für das Risiko eines Atomkriegs aus Versehen als Folge eines Fehlalarms in einem Frühwarnsystem. Dass es in Krisensituationen leicht zu fatalen Fehlkalkulationen kommen kann, hat der versehentliche Abschuss eines ukrainischen Verkehrsflugzeugs im Januar 2020 im Iran gezeigt. Der politische Kontext und eine entsprechende Erwartungshaltung hatten bei der Situationsbewertung höheres Gewicht als rein sachliche Fakten. Auch bei der Bewertung einer Alarmsituation in einem Frühwarnsystem für nukleare Bedrohungen kann der politische Kontext eine entscheidende Rolle spielen. Kriegsrhetorik, nukleare Drohungen und der Abbruch vieler Beziehungen (z.B. wirtschaftlich, wissenschaftlich, kulturell) können maßgeblich zu einer Erwartungshaltung beitragen, die in einer Alarmsituation zu einer fatalen Fehlkalkulation führen kann.[10]

10. Unkontrollierter Rüstungswettlauf droht

In Abschnitt 8 ist „Internationale Verflechtung“ als wichtige Option genannt, um Cyberangriffe abzuschrecken. Auch bezogen auf andere Risiken wie Autonome Waffen und Atomwaffen ist diese Option relevant. Die Globalisierung der Wirtschaft in den letzten Jahrzehnten hat genau in diese Richtung einer Internationalen Verflechtung gewirkt. Nun ist dieser Prozess gebremst oder gestoppt und viele Beziehungen zwischen dem Westen und Russland sind abgebrochen. Beziehungen zu China werden in Frage gestellt.

Eine auf Konfrontation statt auf Zusammenarbeit ausgerichtete Politik zwischen den großen Industrienationen und Militärmächten wird einen ungebremsten Rüstungswettlauf befeuern. Dies gilt insbesondere für softwarebasierte Waffen, wie Cyber- und autonome Waffen.

Bei einem Konfrontationskurs der großen Nationen wird keiner das Risiko eingehen, in den technologisch wichtigen Bereichen Cyberraum und Künstliche Intelligenz den Konkurrenten hinterher zu hinken. Die Softwareentwicklung auf diesen Gebieten kann völlig unkontrolliert und im Verborgenen ablaufen. Keine der Nationen kann wissen, welche Fähigkeiten der Gegner bereits hat und welche in kurzer Zeit erreichbar sein werden. Deshalb muss jede Seite allergrößte Anstrengungen aufnehmen, um mithalten zu können.

Bei zivilen KI-Anwendungen gab es in den letzten Jahren einige Überraschungen, wobei unerwartete Fähigkeiten erreicht wurden, wie zuletzt mit dem System ChatGPT. Ein Rüstungswettlauf im Bereich KI könnte deutlich schneller als erwartet zu äußerst gefährlichen militärischen Produkten führen.

Ein ungebremster Rüstungswettlauf von Atommächten auf Konfrontationskurs erhöht auch das Atomkriegsrisiko in erheblichem Umfang. Mögliche Zusammenhänge mit Cyber- und KI-Fähigkeiten sind in Abschnitt 6 dargestellt. Weitere bisher unbekannte Wechselwirkungen könnten hinzukommen.

Ein solcher Rüstungswettlauf bindet auch Mittel und Ressourcen, die woanders gebraucht werden, z.B. beim Kampf gegen den Klimawandel. Eine Konfrontation zwischen großen Militärmächten und ein Rüstungswettlauf zwischen diesen wird den Kampf gegen den

[10] https://mitsicherheitkontrovers.de/international/zur-bewertung-nuklearer-bedrohungen/

Klimawandel folgenschwer behindern. Wirksame Maßnahmen gegen den Klimawandel können nicht gegen große Nationen wie Russland und China durchgesetzt werden, sondern nur mit diesen gemeinsam.

11. Sicherheit durch Handel

Aufgrund des vernichtenden Potenzials von Atomwaffen kann sich die Menschheit dauerhafte Spannungen zwischen großen Atommächten nicht leisten. In Krisensituationen kann es leicht zu fatalen Fehlkalkulationen und daraus resultierenden Fehlhandlungen kommen. Solange nicht ein gewisses Maß an Vertrauen und Zusammenarbeit besteht, wird es auch nicht möglich sein, irgendwelche Abrüstungsvereinbarungen zu treffen. Im Gegenteil: es besteht das Risiko einer ungebremsten nuklearen Aufrüstung.

Zur Sicherung einer lebenswerten Zukunft für die nachfolgenden Generationen und das gesamte Ökosystem sind dringend Vereinbarungen zwischen allen großen Nationen erforderlich: zum Kampf gegen den Klimawandel, zur Verhinderung autonomer Waffensysteme, zur Begrenzung von Cyberkriegskapazitäten und zur Reduzierung oder Abschaffung von Atomwaffen. Alle Nationen müssen in diesen Punkten zusammenarbeiten.

Seit Beginn des Ukraine-Krieges wird immer wieder behauptet, die Strategie „Wandel durch Handel“ sei gescheitert. Das ist falsch. Es gilt allerdings tatsächlich, dass diese Strategie nicht ausreichend war, um den Ukraine-Krieg zu verhindern. Hierzu wären noch weitere Maßnahmen erforderlich gewesen. Eine solche Strategie ist aber notwendig für eine dauerhafte globale Sicherheit.

Aus der Mathematik ist in Zusammenhang mit dem Beweisen von Sätzen bekannt, dass „notwendige“ und „hinreichende“ Bedingungen unterschieden werden müssen. Dies wäre auch wichtig, wenn es um Folgerungen aus „Wandel durch Handel“ geht.

Wenn eine Aussage A hinreichend für eine Aussage B ist, dann gilt: A => B, also „aus A folgt B“ oder anders formuliert: „wenn A gilt, dann gilt auch B.

Wenn eine Aussage A notwendig für eine Aussage B ist, dann gilt: B => A, also „aus B folgt A“ oder anders formuliert: „wenn B gilt, dann gilt auch A. Die Folgerung gilt hier also genau in der entgegengesetzten Richtung.

Die Aussage „Wandel durch Handel“ ist aus sicherheitspolitischer Sicht auch vielleicht ein ungünstiger Begriff. Das Ziel sollte nicht sein, andere zu ändern, sondern gemeinsam die nötige Sicherheit für die Zukunft zu erreichen. Besser wäre deshalb vielleicht der Begriff „Sicherheit durch Handel“. Deshalb wird nachfolgend nur noch dieser Begriff verwendet.

Die Strategie „Sicherheit durch Handel“ war also nicht hinreichend, um den Krieg in der Ukraine zu verhindern. Aber eine solche Strategie ist notwendig, um das Risiko weiterer Eskalationen und weiterer militärischer Konflikte zu reduzieren. „Sicherheit durch Handel“ ist notwendig, um dauerhaft ein gewisses Maß an globaler Sicherheit und damit eine friedlichere Welt zu erreichen.

12. Fazit

Das Zusammenwirken neuer technischer Entwicklungen mit dem Vernichtungspotenzial von Atomwaffen wird immer weniger beherrschbar. Zum Schutz vor diesen Risiken reicht die

nukleare Abschreckung nicht aus. Alle Optionen, die ein Atomkriegsrisiko reduzieren, müssen genutzt werden. Einmal entwickelte Softwarekomponenten für autonome Waffensysteme werden nicht wieder vernichtet werden können, sondern bleiben uns immer erhalten. Abrüstungsvereinbarungen bezüglich Software werden kaum möglich sein. Deshalb ist es wichtig einen Rüstungswettlauf in den Bereichen KI und Cyberraum zu bremsen oder zu stoppen. Dies wird aber nur mit einem gewissen Maß an Vertrauen und Zusammenarbeit zwischen allen Nationen möglich sein.

Jetzt wäre es besonders wichtig, die Zerstörung der Beziehungen zwischen großen Nuklearmächten zu stoppen und diesen Prozess wieder umzukehren. Die Verbesserung von Beziehungen kann auf allen Ebenen erfolgen: wissenschaftlich, wirtschaftlich, technologisch kulturell, militärisch und auch privat. Je mehr Kontakte es auf diesen Ebenen gibt, desto geringer ist das Risiko eines ungebremsten Rüstungswettlaufs auf technologisch wichtigen Feldern wie der KI und desto geringer ist das Atomkriegsrisiko. Die insbesondere durch die Globalisierung erreichten internationalen Verflechtungen sollten nicht gestoppt und rückgängig gemacht, sondern gestärkt und durch vertrauensbildende Maßnahmen zwischen allen Staaten ergänzt werden. Der Aspekt „Sicherheit durch Handel“ ist nicht gescheitert, sondern notwendig für eine dauerhafte globale Sicherheit.

13. Literatur

[Bou19] Vincent Boulanin (ed.): The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk. Sipri Report, https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf, 2019

[GK20] Reinhard Grünwald, Christoph Kehl: Autonome Waffensysteme – Endbericht zum TA-Projekt, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Arbeitsbericht Nr. 187, Okt. 2020, https://dip21.bundestag.de/dip21/btd/19/236/1923672.pdf

[LV22] Kersten Lahl, Johannes Varwick: Sicherheitspolitik verstehen – Handlungsfelder, Kontroversen und Lösungsansätze. Wochenschauverlag, 3. Auflage, 2022

[Rus20] Stuart Russell: Human Compatible – Künstliche Intelligenz und wie der Mensch die Kontrolle über superintelligente Maschinen behält. Mitp Verlag, 2020

[SW19] Eric Schmidt, Robert O. Work, u.a.: National Security Commission on Artificial Intelligence – Interim Report, November 2019, https://www.epic.org/foia/epic-v-ai-commission/AI-Commission-Interim-Report-Nov-2019.pdf

[SH20] Michael Staack, Günther Hauser (Hrsg.): Russland und der Westen – Ist kooperative Sicherheit möglich? WIFIS-aktuell, Verlag Barbara Budrich, 2020

Dank

Für die Erstellung dieses Artikels habe ich wertvolle Hinweise und Korrekturvorschläge von Claudia Nelgen und Ulrich Schwarz erhalten. Hierfür bedanke ich mich herzlich.