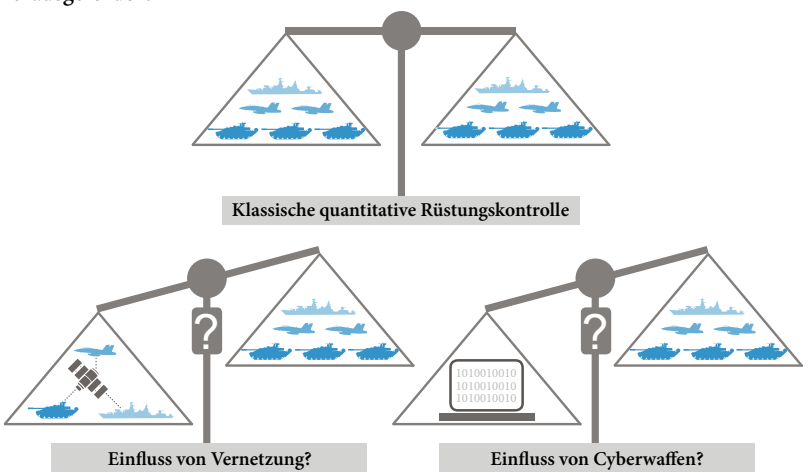
Frieden und Sicherheit

Von der quantitativen zur qualitativen Rüstungskontrolle: Die Herausforderungen moderner Waffenentwicklung

Die klassische Rüstungskontrolle befindet sich in einer Krise. Konzepte und Ideen, die vor allem in den 1960er Jahren vor dem Hintergrund des Kalten Krieges zur Stabilisierung der bilateralen Beziehungen der Supermächte entwickelt wurden, scheinen heute angesichts der stärker multilateralen Ausrichtung und der gewachsenen Zahl möglicher Anwendungsfelder für Rüstungskontrolle nicht mehr zu greifen. Dazu trägt auch ein spezifischer militärischer Trend, die immer stärkere Bedeutung von Computern und ihrer Software, bei. Darunter fallen die zunehmende Vernetzung der Streitkräfte, der Trend zu immer stärker automatisierten Waffensystemen bis hin zu möglichen vollautomatisierten Systemen mit letaler Wirkung sowie die wachsenden Möglichkeiten der elektronischen bzw. Cyberkriegsführung.

Es zeigt sich, dass klassische quantitative Rüstungskontrollbeschränkungen von Waffen und Soldaten, deren Einhaltung mittels Verifikation überprüft wird, durch die wachsende Nutzung der Computertechnik und der dazugehörigen Software immer stärker an Bedeutung verlieren. Dagegen zeichnen sich neue Formen der Transparenz, Vertrauensbildung und Verifikation als mögliche Lösungsansätze ab.

Abbildung 1: Die klassische Rüstungskontrolle wird durch neue Technologien herausgefordert



Quelle: eigene Darstellung

Die klassischen Herangehensweisen: Bilateral – Quantitativ – Verifikation

Klassische Rüstungskontrolle verfolgte drei Ziele (Schelling/Halperin 1961, S. 1): 1) Kriegsverhütung durch Stabilität, 2) Reduzierung der Kosten der Rüstung und 3) Einschränkung der zu erwartenden Schäden im Kriegsfall. Das wichtigste dieser drei Ziele war die Stabilität der angespannten Beziehungen der Supermächte, besonders in Krisenzeiten. Ausgehend von der (neorealistisch inspirierten) Überlegung, dass militärische Gleichgewichte einen Krieg unwahrscheinlich machen, sollten quantitative Höchstgrenzen der Rüstung die Beziehungen der Supermächte stabilisieren und einen erfolgreichen Überraschungsangriff nach Möglichkeit ausschließen. Dieses Gleichgewichtsdenken ist dann besonders einfach umzusetzen, wenn sich die militärischen Potenziale zweier Kontrahenten in ihrer Qualität kaum unterscheiden und eine quantitative Parität von beiden Seiten als Gleichgewicht anerkannt wird. Die Einhaltung des Gleichgewichts *(compliance)* muss dann mittels geeigneter Verifikationsmaßnahmen sichergestellt werden, so dass keine Vertragspartei im Geheimen mehr Machtmittel anhäufen kann als vertraglich vereinbart (z. B. Müller/Schörnig 2006, S. 140 ff.).

Verifikation hat aus klassischer Sicht deshalb eine Schlüsselrolle bei der Rüstungskontrolle: Nur wenn beide Seiten genug Vertrauen in die Wirksamkeit der Verifikationsmaßnahmen haben, sind sie selbst bereit, sich den Vorgaben des Regimes zu unterwerfen. Entsprechend muss Klarheit und Einigkeit darüber bestehen, was genau verboten ist und was nicht (Fey/Müller 2008, S. 215). Es wäre aber unrealistisch zu glauben, Verifikation könne jeden Regelverstoß auch tatsächlich feststellen. Ziel eines geeigneten Verifikationsregimes muss es deshalb sein, für die militärische Stabilität bedeutsame Regelverstöße sicher entdecken zu können. Allerdings stellt die zunehmende Bedeutung von Software im Militärbereich quantitative Gleichgewichte immer mehr in Frage und erhöht das Verifikationsproblem deutlich.

Neue Herausforderungen im konventionellen Bereich

Der vernetzte Charakter moderner Waffensysteme: Fokus auf Fähigkeiten statt Systemen

Spätestens seit dem Erfolg der amerikanischen Streitkräfte im Golfkrieg des Jahres 1991 hat in den USA – und in der Folge auch in anderen westlichen Staaten – eine Entwicklung stattgefunden, die oft als Transformation oder auch Revolution in Militärischen Angelegenheiten (*Revolution in Military Affairs*, RMA) beschrieben wird. Kern dieser RMA ist die Vernetzung moderner Sensoren, Waffensysteme und der militärischen Entscheider im Rahmen eines

»Systems der Systeme« (z. B. Schörnig 2005; Shimko 2010). Den an einem Militäreinsatz beteiligten Akteuren sollen so alle relevanten Informationen ohne Zeitverlust vorliegen, um Entscheidungsprozesse zu beschleunigen, die Qualität der Entscheidungen zu erhöhen und Abläufe zu synchronisieren. Die Bundeswehr spricht in diesem Zusammenhang von »Vernetzter Operationsführung« (NetOpFü). Durch diese umfassende Vernetzung soll weiterhin, wie es Militärs beschreiben, die Wirkung der einzelnen Waffen nicht nur erhöht, sondern »multipliziert« werden. Werden z. B. Angriffe mit gegenüber konventionellen Modellen deutlich präziseren »intelligenten« Bomben oder Raketen auf Basis der in Echtzeit vorliegenden Aufklärungsergebnisse durchgeführt, wird die Lücke zwischen Aufklärung und Angriff auf ein Minimum reduziert und die militärische »Effektivität« deutlich erhöht. Wie speziell der Golfkrieg des Jahres 2003 gezeigt hat, ist diese neue Art der hochtechnisierten Kriegsführung besonders in zwischenstaatlichen Kriegen gegen technologisch unterlegene Gegner erfolgreich (Shimko 2010, S. 142 ff.).

Allerdings ergeben sich daraus auch neue technologische Herausforderungen: Immer mehr und leistungsfähigere Sensoren stellen immer mehr Informationen zu Verfügung, die es möglichst schnell auszuwerten und zu interpretieren gilt. Nach US-amerikanischen Angaben aus dem Jahr 2011 fielen z. B. in Afghanistan 53 Terabyte an Aufklärungsdaten an – pro Tag (de Selding 2011). Es wird deshalb immer komplexere Assistenzsoftware eingesetzt, um die gewonnenen Daten auszuwerten, miteinander in Beziehung zu setzen und Handlungsvorschläge für menschliche Entscheider zu generieren (Schörnig 2014).

Diese auf Informationstechnologie basierende Multiplikation der militärischen Leistung bedeutet aber auch, dass immer weniger Einheiten notwendig sind, um militärische Ziele umzusetzen. Der seit dem Golfkrieg 1991 deutlich gestiegene Anteil an Präzisionsmunition (Minkwitz 2008, S. 71) ist ebenso Ausdruck dieser Entwicklung wie der zunehmende Einsatz von Spezialeinheiten statt regulärer Truppen (Sanger 2012). Weniger, dafür aber deutlich leistungsfähigere Einheiten bedeuten auch eine schnellere Verlegbarkeit, weniger logistischen Aufwand und schnellere Reaktionsfähigkeit. Kleine vernetzte Armeen sind, wie das Beispiel der Irak-Kriege 1991 und 2003 demonstrierte, unter Umständen in der Lage, quantitativ überlegenen Gegnern nicht nur Paroli zu bieten, sondern sie fast ohne eigene Verluste zu besiegen (Shimko 2010, S. 2). Damit rückt der Fokus auf die – mit Rüstungskontrollmaßnahmen deutlich schwerer zu erfassende – qualitative Komponente, die sich wiederum aus Grad und Qualität der Vernetzung bzw. der eingesetzten Software ergibt.

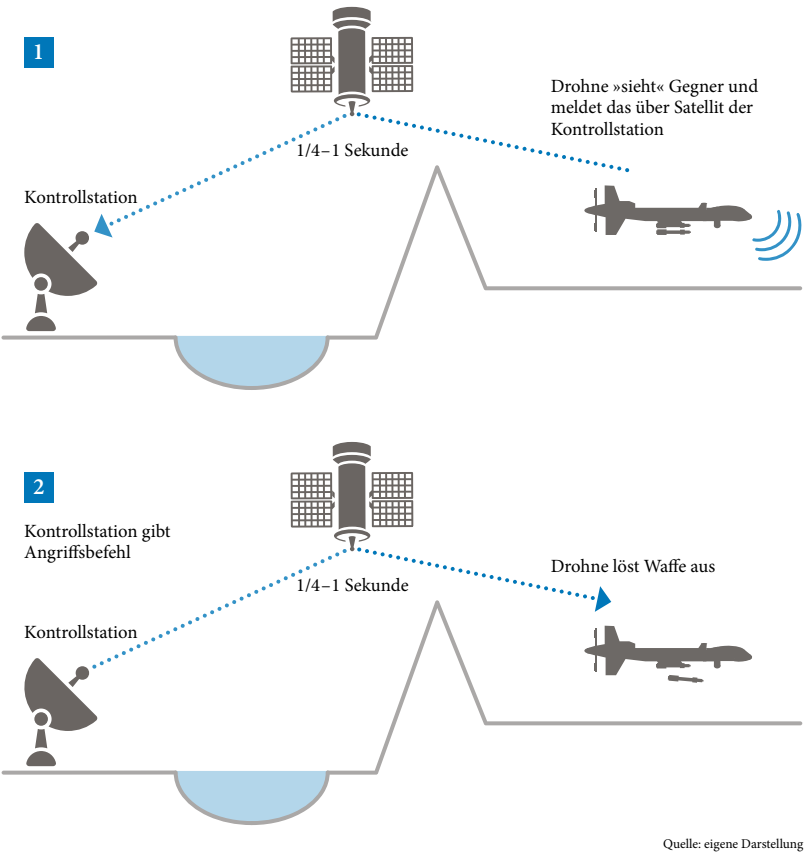
Autonome letale Systeme: Das Ringen mit der Automatisierung des Krieges

(Re-)Aktionszeit ist im militärischen Konflikt eine wichtige Größe, die über Erfolg und Misserfolg entscheiden kann. Angesichts der zum Teil extrem geringen Reaktionszeiten bei (überraschenden) Angriffen, speziell mit schnellfliegenden Raketen, aber auch Mörsergranaten, setzen Militärs immer stärker auf hochgradig automatisierte Systeme zur Selbstverteidigung, z. B. zur Flugkörperabwehr auf Schiffen und zum

Schutz von Feldlagern oder Städten wie etwa in Israel. Solche Eigenschutzsysteme erhalten ihren Einsatzbefehl in der Regel noch von Menschen vor den Bildschirmen, können aber auch in einem vollautonomen Modus betrieben werden, in dem das System sich selbstständig Ziele sucht und diese ohne den sich durch menschliche Bestätigung zwangsläufig ergebenden Zeitverlust bekämpft (Schörnig 2014). Zwar richten sich diese autonomen Kampfsysteme noch nicht gegen Menschen. Kritiker befürchten aber, dass in Zukunft Computeralgorithmen auch die Entscheidung über Leben und Tod übertragen wird, was aus ihrer Sicht weder ethisch akzeptabel, rechtlich zulässig noch technologisch sicher ist (vgl. speziell Human Rights Watch 2012). Sicher ist, dass viele künftige Systeme deutlich stärker automatisiert sein werden als aktuelle Waffensysteme. Dies wird z. B. an sich abzeichnenden Entwicklungen im Drohnenbereich deutlich. Aktuelle *Unmanned Aerial Vehicles* (UAVs), wie die US-amerikanischen *MQ-1 Predator* und *MQ-9 Reaper*, werden von Menschen per Funk oder über Satellitenkommunikation ferngesteuert, auch wenn einige Manöver wie Start oder Landung schon jetzt praktisch nur noch überwacht werden müssen. Im Angriffsfall gibt aber der Operator am Boden aktiv den Feuerbefehl. Allerdings sind aktuelle Aufklärungs- und Kampfdrohnen nur für den »unumkämpften Luftraum« konzipiert. Sofern der Gegner (noch) über eine rudimentäre Luftabwehr verfügt, sind diese recht langsamen Drohnen ein relativ leichtes Ziel (Haider 2014, 6 f.), was ihre Einsatzmöglichkeiten stark einschränkt. Aktuell in Entwicklung und Probe befindliche Modelle verfügen deshalb über Eigenschaften, die sie auch im umkämpften Luftraum einsetzbar machen sollen, in dem zur Zeit nur bemannte Kampfjets operieren können. Ziel der Industrie sind deshalb Drohnen, die mit den Fähigkeiten der bemannten Kampfflugzeuge nicht nur gleichziehen, sondern diese in vielen Bereichen sogar übertreffen, weil z. B. bei extremen Flugmanövern nicht mehr auf die physischen Belastungsgrenzen des Piloten im Cockpit Rücksicht genommen werden muss (z. B. Haider 2014, S. 101). Eine Fernsteuerung solcher Systeme ist dabei militärisch von Nachteil. Bei Satellitensteuerung kommt es zu Verzögerungen (einer »Latenz«) von mindestens einer halben Sekunde, ehe ein Signal aus der Drohne von der Bodenstation beantwortet wird und wieder die Drohne erreicht – z. B. der Schussbefehl [vgl. Abbildung 2].

In umkämpften Szenarien scheint dies zu lange, der militärische Vorteil, der sich durch die höhere Agilität des unbemannten Systems ergibt, wäre hinfällig. Hinzu kommt die Gefahr, dass das Steuersignal gestört oder manipuliert werden kann. Zwar fliegen schon heutige Drohnen bei einem Verlust des Steuersignals automatisch zu ihrer Heimatbasis zurück, allerdings hat dies einen Missionsabbruch und die Nichterfüllung des militärischen Auftrags zur Folge. Beide Probleme könnten umgangen werden, wenn die Entscheidung über den Waffeneinsatz (bzw. die Missionsdurchführung allgemein) von hochgradig komplexer Software in der Drohne selber getroffen würde – bis hin zu Waffengewalt gegen Menschen. Dann würde man von einem *Lethal Autonomous Weapon System* (LAWS) reden. Wichtig ist es also, darauf zu schauen, bis zu welchem Grad Menschen noch in die Entscheidungsprozesse eingebunden sind [vgl. Abbildung 3]: Ist der Mensch

Abbildung 2: Die Fernsteuerung automatisierter Systeme bringt zeitliche Verzögerungen mit sich
Das »Latenzproblem« ferngesteuerter unbemannter Kampfdrohnen

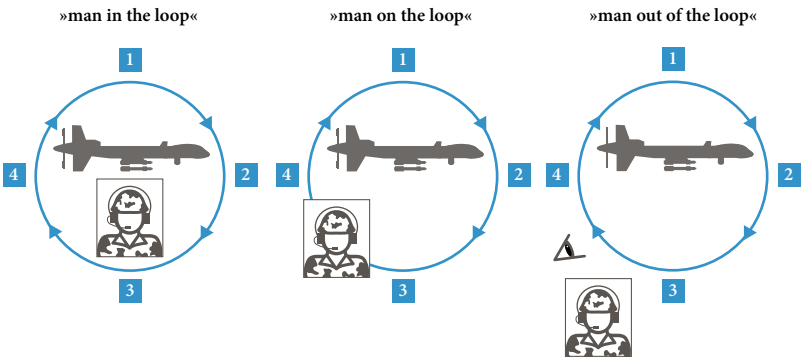


Quelle: eigene Darstellung

noch in die komplette Entscheidungsschleife eingebunden, obliegt ihm im Wesentlichen die Kontrolle und Bestätigung maschineller Vorschläge? Oder agiert das System so autonom, dass dem Menschen im besten Fall eine Abbruchoption bleibt – wenn er schnell genug reagieren kann?

Nicht nur Drohnen können LAWS sein: Es sind z. B. auch autonom agierende bewaffnete Bodenroboter vorstellbar, die selbstständig Ziele auswählen und Waffengewalt gegen Menschen anwenden. Einige Robotiker, wie z. B. der US-Amerikaner Ronald Arkin, arbeiten in diesem Zusammenhang an Software, die militärischen Robotern eine »Ethik« geben soll (2009), nur als Kombattanten klassifizierte »Ziele« anzugreifen und Zivilisten zu verschonen. So sei eine Kriegsführung möglich, die »humaner« sei als die von Menschen praktizierte,

Abbildung 3: Der Mensch muss nicht mehr in Entscheidungsprozesse eingebunden werden
Die militärische Entscheidungsschleife* bei verschiedenen Autonomiegraden unbemannter Systeme



Erläuterung: Bei zunehmendem Automatisierungsgrad wird die Bedeutung des menschlichen Entscheiders immer geringer. Bei einem niedrigen Automatisierungsgrad trifft der Pilot alle zentralen Entscheidungen *(man in the loop)*; bei Vollautonomie bekämpft die Maschine Ziele ohne vorherige menschliche Betätigung *(man out of the loop)*. Bei Zwischenstufen greift der Mensch nur noch punktuell ein, besonders bei Fragen des Waffeneinsatzes *(man on the loop)*.

* Der OODA-Loop (Observe/Orient/Decide/Act) wird dem US-amerikanischen Kampfjetpiloten John Boyd zugeschrieben.

Quelle: eigene Darstellung

da Gefühle wie Stress, Angst oder Rache (z. B. für getötete Kameraden) keine Rolle spielen würden (Arkin 2009). Kritiker bezweifeln allerdings, dass es Computern auf absehbare Zeit möglich sein wird, Kombattanten und Zivilisten sicher zu unterscheiden (z. B. Human Rights Watch 2012). Noch besitzt kein Staat (zumindest offiziell) ein LAWS, und auch Militärs betonen bislang, dass sie Entscheidungen über Leben und Tod nicht Maschinen überlassen wollen. Gleichwohl schreitet die Automatisierung militärischer Abläufe voran. Wenn Sekundenbruchteile über militärischen Erfolg und Misserfolg entscheiden, könnte es zu einem Rüstungswettlauf um Automatisierung kommen, an dessen Ende der Einsatz autonomer Waffengewalt auch gegen Menschen steht.

Cyber: Krieg mit »virtuellen Waffen«

Kaum ein Begriff hat in den letzten Jahren so viel Aufsehen erregt wie der des Cyberwar. Da sowohl die zivile als auch militärische Infrastruktur moderner Staaten immer stärker von elektronischer Vernetzung anhängig ist, wurde die »Cybersphäre« als Austragungsort möglicher zukünftiger Konflikte identifiziert. Laut dem Cybersicherheitsexperten Sandro Gaycken verfolgen »zwischen 108 und 140 Staaten Cyberwar-Programme« (Gaycken 2014, S. 10), die umfangreichsten vermutlich die USA, China und Russland. Allerdings wirft der Cyberbereich eine Vielzahl neuer militärischer Probleme auf. Zunächst ist das Spektrum möglicher Angriffsformen sehr vielfältig, selbst wenn man Cyberkriminalität zur illegalen Gewinnerzielung ausnimmt. Die Bandbreite reicht von Cyberspionage, also dem Ausspähen oder Stehlen fremder Daten (Neuneck 2014, S. 241), über relativ simplen und deshalb häufigen *hacktivism*, z. B. den *Denial-of-Service*-Attacken, bei denen ein Server durch eine Überzahl an gleichzeitigen Zugriffen überfordert wird, bis hin zu Angriffen, die darauf abzielen, die physische Infrastruktur eines Gegners nachhaltig zu schädigen. Je nach Umfang der Schäden wäre dann von »Cybersabotage« oder gar Cyberwar zu sprechen (Neuneck 2014, S. 242). Das bislang einzige bekannte Beispiel für einen solchen Cyberangriff, der tatsächlich physische Schäden verursachte, ist der 2010 bekanntgewordene Wurm *Stuxnet*, der iranische Urananreicherungszentrifugen durch gezielte Wechsel der Rotationsgeschwindigkeit über einen längeren Zeitraum zu zerstören suchte (Farwell/Rohozinski 2011). Umfassendere Angriffe, auch gegen zivile Infrastrukturen wie das Ampelsystem einer Großstadt oder gar Kraftwerke, sind denkbar. Was alle Angriffe eint, ist, dass sie in einer »virtuellen« Sphäre stattfinden und sich auf (unterschiedlich komplexe) Software stützen.

Das zentrale Problem bei Cyberangriffen jeder Art besteht darin, den Täter genau zu identifizieren – und wird als »Attributionsproblem« bezeichnet. Versierte Experten können im Internet ihren eigenen Standort verschleiern. Angriffe können von mit Schadsoftware infizierten Rechnern unbeteiligter Personen ohne deren Wissen durchgeführt werden.

Schließlich kann ein Cyberangriff, zumindest theoretisch, von jedem Ort mit Netzzugang gestartet werden – die dazu notwendige Software passt auf einen USB-Stick oder die Festplatte eines Laptops. Eine Rückverfolgung in ein bestimmtes Land bedeutet deshalb nicht zwingend, dass der Angriff auch von nationalen Stellen dieses Landes durchgeführt oder zumindest angeordnet wurde.

Das Attributionsproblem stellt zudem klassische Konzepte der Abschreckung in Frage. Kann weder die Urhebernation eines Angriffs sicher festgestellt noch gesagt werden, ob der Angriff von staatlichen Stellen ausging, greift die Drohung eines Cybergegenschlags ins Leere. Auch wenn Staaten wie die USA daran arbeiten, dieses Problem zu lösen, ist sicher, dass die wenigsten Staaten auf absehbare Zeit über die Cyberressourcen der US-Streitkräfte verfügen werden. Die Kombination aus Spekulation über Fähigkeiten, dem breiten Spektrum

möglicher Angriffe und den im besten Fall sehr eingeschränkten Attributionsmöglichkeiten bei einem Angriff machen Cyber also insgesamt zu einer instabilen und kaum zu kontrollierenden oder gar zu beschränkenden Sphäre.

Die Reaktionen der Rüstungskontrolle

Was alle genannten Bereiche aktueller militärischer Entwicklung eint, ist die Tatsache, dass Software anstelle von bzw. im Verbund mit Hardware eine zunehmend wichtigere Rolle spielt. Dies stellt die Rüstungskontrolle vor enorme Probleme, da stabile (quantitative) Gleichgewichte weder identifiziert werden können noch eine besondere Rolle spielen würden. Darüber hinaus könnte eine Vertragseinhaltung kaum verifiziert werden – das A und O klassischer Rüstungskontrolle. Das auf der Hand liegende Problem, wie man immaterielle und dazu ausgesprochen komplexe Software kontrollieren soll, stellt in vielen aktuell relevanten Bereichen also die Crux für belastbare Rüstungskontrollabkommen dar. Experten haben schon seit mehr als einem Jahrzehnt auf die neuen Herausforderungen hingewiesen und eine Bearbeitung gefordert (z. B. Müller/Schörnig 2001; Fey/Müller 2008). Geschehen ist, vermutlich auch angesichts der lange bestehenden westlichen technologischen Führerschaft der 1990er und 2000er Jahre, wenig. Trotzdem gibt es in den einzelnen genannten Bereichen zumindest rüstungskontrollpolitische Ansätze.

Vernetze Kriegsführung: Fokus auf Qualität und »verifizierte Transparenz«

In der konventionellen Rüstungskontrolle spielen also reine Quantitäten aufgrund der sich durch Vernetzung ergebenden Multiplikatoreffekte eine zunehmend unwichtigere Rolle. Kleine, hochgradig vernetzte Einheiten sind in der Lage, quantitativ überlegene Gegner militärisch effektiv zu bekämpfen. Auch spielen regionale Ansätze, wie z. B. die im Vertrag über die Konventionellen Streitkräfte (KSE) in Europa festgelegten regionalen Höchstgrenzen zur Verhinderung destabilisierender Truppenkonzentrationen, angesichts der deutlich gestiegenen Mobilität leicht verlegbarer, aber dennoch wirkungsmächtiger Verbände eine abnehmende Rolle (Schmidt 2013). Praktiker und Experten suchen deshalb in jüngerer Zeit verstärkt nach neuen Instrumenten, die die hergebrachte konventionelle europäische Rüstungskontrolle ergänzen, vielleicht sogar ersetzen könnten. Grundsätzlich sind natürlich auch quantitative Ansätze zur Beschränkung qualitativer Merkmale von Streitkräften und einzelnen Waffensystemen denkbar. So könnte man z. B. die Größe, Reichweite oder Zuladung unbemannter Flugsysteme (in der Zukunft auch unbemannter Bodensysteme) nach oben, aber auch nach unten beschränken (z. B. Altmann 2013). So wären besonders destabilisierende Angriffsoptionen, z. B. die Nutzung von unbemannten Kampfflugzeugen als Trägersysteme für Nuklearwaffen, weitreichende Enthauptungsschläge oder gezielte heimliche Anschläge mit Mikro-UAVs auszuschließen. Ob solche

punktuellen Einschränkungen aber zu signifikanten Beschränkungen der Multiplikatoreffekte »an sich« führen, ist fraglich. Hier müsste ein radikales Umdenken stattfinden. Eine weitere Alternative wäre die Konzentration auf das Verbot bestimmter militärischer »Effekte« oder »Strategien«, z. B. gezielte Enthauptungsschläge, die sich im Rahmen einer vernetzten Kriegsführung besonders anbieten (Müller/Schörnig 2001). Ob Staaten, die die Fähigkeit dazu besitzen, sich aber auf Verbote bestimmter militärischer Optionen und Einsatzformen einlassen, sofern diese nicht im Widerspruch zum geltenden Humanitären Völkerrecht stehen, ist fraglich.

Entsprechend sieht die aktuelle Debatte davon ab, den extrem schwierigen Versuch einer Beschränkung vernetzter Operationen zu wagen. Experten und Praktiker haben stattdessen die Unsicherheit, die über die Fähigkeiten vernetzter Armeen bestehen, als einen wesentlichen destabilisierenden Faktor erkannt, der konstruktiv angegangen werden kann. Ein ambitioniertes, aber erreichbares Ziel ist deshalb, zunächst bei allen Beteiligten Klarheit über die Fähigkeiten zu schaffen, die sich aus Vernetzung ergeben. In diesem Zusammenhang wurde von deutscher Seite vor kurzem das Konzept der »verifizierten Transparenz« für die europäische konventionelle Rüstungskontrolle entwickelt, das statt Streitkräften und Waffen potenziell destabilisierend wahrgenommene »Fähigkeiten«, z. B. schnelle Luftverladefähigkeit (Schmidt 2014, S. 10 f.), ins Zentrum der Transparenz und Verifikation stellt. Ziel ist es, dem Gegenüber eine realistische Einschätzung der vorhandenen Fähigkeiten zu ermöglichen und so Unsicherheiten ab- und Vertrauen aufzubauen. Verifizierte Transparenz knüpft an klassische Vertrauensbildende Maßnahmen (VBMs) an, ist aber ein eigenständiges neues Instrument. Der Ansatz ist umstritten, da er, um die nötige Verifizierbarkeit der Transparenz sicherzustellen, vertrauliche Einblicke in militärische Operationen vermitteln würde. Angesichts der aktuellen Spannungen zwischen Russland und der Organisation des Nordatlantikvertrags (NATO) erscheint eine Umsetzung des Konzeptes allerdings ungewiss. Gleichwohl ist es einer der ersten Ansätze, der die qualitative Vernetzungsproblematik moderner Armeen systematisch aufgreift und dabei auf Transparenz, Verifikation und Vertrauensbildung setzt. Sich daran anschließende quantitative und qualitative Beschränkungen werden zwar nicht ausgeschlossen, aber auf die nächste Runde möglicher Rüstungskontrollvereinbarungen verschoben, wenn durch verifizierte Transparenz verlässlichere Einschätzungen über die Fähigkeiten erzielt wurden.

Cyber: Erste Schritte – Gemeinsame Definitionen und Vertrauensbildung

Noch stärker als bei RMA und netzwerkzentrierter Kriegsführung, wo die eingesetzte Hardware immer noch eine gewichtige Rolle spielt, zeichnet sich der Cyberbereich durch die zentrale Relevanz von Software aus. Zwar kann auch hier ein logistisches Rückgrat bis hin zum Nachbau der anzugreifenden Anlage nötig sein, speziell wenn Würmer oder andere Malware – wie im *Stuxnet*-Fall – ganz gezielt individuelle Ziele angreifen sollen (Lindsay 2013). Ist die Software aber programmiert, so kann sie

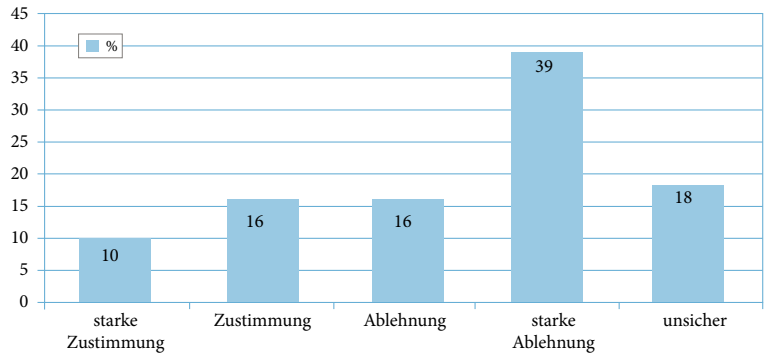
im Zweifel auf einem USB-Stick gelagert und von dort zum Einsatz gebracht werden. Die Vorstellung, Cyberwaffen seien vollständig »virtuell« und grundsätzlich keiner Form der Verifikation zugänglich, ist also irrig, weil immer auch ein physisches Medium (USB-Stick, Festplatte etc.) vorliegen muss, das im Zweifel geprüft werden könnte. Gleichwohl würde die Suche nach einem spezifischen Speichermedium der berühmten Suche nach der Stecknadel im Heuhaufen gleichen. Auch hier steht der Gedanke, Rüstungskontrolle habe auf verifizierbaren Verträgen mit gleichen Rechten und Pflichten für alle Vertragsparteien zu basieren, einem pragmatisch-konstruktiven Herangehen im Weg. Angesichts der gestiegenen Aufmerksamkeit und vermutlich auch weil westliche Staaten im Cyberbereich nicht mehr zwingend die Technologieführerschaft haben, wird auf internationaler Ebene trotzdem seit einigen Jahren intensiver auf eine stärkere Reglementierung gedrängt. Zudem werden verschiedene Ansätze verfolgt: Einen ersten Schritt stellen dabei die Vorschläge von Völkerrechtlern dar, den Begriff des Cyberwar aus rechtlicher Perspektive zu definieren und gegenüber weniger starken Formen von Cyberangriffen abzugrenzen (z. B. Melzer 2011). Auch die NATO beteiligt sich an dieser rechtlichen Debatte und hat dazu Expertenmeinungen gesammelt (Schmitt 2013), ebenso wie die Vereinten Nationen (UN), die inzwischen drei Expertenberichte vorgelegt haben (United Nations 2013). Diskutiert wird weiterhin ein *International Code of Conduct for Information Security*, der 2011 der UN-Generalversammlung von Russland und China vorgeschlagen, allerdings von US-Seite verhalten aufgenommen wurde (Farnsworth 2011). Die Bildung von Vertrauen scheint bzw. schien bis zur Krise zwischen Russland und den USA auch in diesem Bereich aktuell der erfolgversprechendste Weg: Neben den UN-Expertenberichten, die zunächst freiwillige vertrauensbildende Maßnahmen vorschlagen, haben sich die Teilnehmerstaaten der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE) im Dezember 2013 zu ersten VBMs auf freiwilliger Basis verpflichtet (Neuneck 2014, S. 251). Auch die EU engagiert sich inzwischen im Bereich der Vertrauensbildung im Cyberbereich, und deutsche Diplomaten versuchen das (europäische) Konzept der VBMs im Cyberbereich auch in anderen Regionen zu befördern (Geier 2014). Hierbei könnten z. B. Einblicke in offizielle Dokumente der nationalen Cyberdoktrin ein erster Schritt sein.

Letale Autonomie: Verbot des Einsatzes, ein Tabu und Ex-post-Analysen

Auch im Bereich der immer stärker automatisierten Kampfsysteme, wie sie aktuell bewaffnete Drohnen am greifbarsten darstellen, ist der Unterschied zwischen einem ferngesteuerten und einem autonom agierenden System im Wesentlichen der umfangreichere Softwarecode des autonomen Systems, während äußerliche Charakteristika eher irrelevant sind (Gubrud/Altmann 2013). Solche, möglicherweise auch noch versteckte Software-Algorithmen zu finden und zu identifizieren, wird kaum zu leisten sein, auch wenn die Steuerkonsolen und Drohnen physisch relativ leicht auffindbar sind. Auch müsste der Kontrolleur Zugriff auf den gesamten Softwarecode des Systems haben, was

Abbildung 4: Breite Skepsis in der Bevölkerung gegenüber autonomen Waffensystemen

Einstellungen in den USA zur Nutzung autonomer letaler Waffensysteme, Mai 2013



Quelle: http://www.whiteoliphaunt.com/duckofminerva/wp-content/uploads/2013/06/UMass-Survey_Public-Opinion-on-Autonomous-Weapons.pdf, 3.11.2014, eigene Darstellung

intimste Einblicke in relevante Routinen bedeuten würde. Es ist unwahrscheinlich, dass sich Staaten auf solche Überprüfungspraktiken einlassen werden.

Obwohl die USA zu den wenigen Ländern weltweit gehören, in der die Mehrheit der Bevölkerung den Einsatz bewaffneter ferngesteuerter Kampfdrohnen befürwortet, lehnt nach einer Umfrage der *University of Massachusetts Amherst* aus dem Jahr 2013 eine Mehrheit trotzdem den Einsatz von LAWS ab [vgl. Abbildung 4]. Umfragen zu LAWS aus anderen Ländern sind bislang nicht bekannt. Das könnte sich jedoch ändern, nachdem es Nichtregierungsorganisationen (NGOs) dank intensiver Kampagnen- und Aufklärungsarbeit in sehr kurzer Zeit geschafft haben, »letale Autonomie« auf die internationale Agenda zu hieven und Nationalstaaten zu gewinnen, das Thema breiter zu diskutieren. So fand im Mai 2014 ein inoffizielles Expertentreffen im Rahmen der UN-Waffenkonvention, der *Convention on Certain Conventional Weapons* (CCW) [vgl. Kasten], in Genf statt, in dessen Rahmen ein Einsatzverbot »letaler Autonomie« von Staatenvertretern und NGOs intensiv diskutiert wurde (Sauer 2014). Die Beratungen werden im April 2015 fortgesetzt. Allerdings bietet die CCW nur die Möglichkeit, den Einsatz bestimmter Waffensysteme zu verbieten – was einigen NGOs nicht weit genug geht, denen ein umfassendes Entwicklungs- und Herstellungsverbot letaler autonomer Systeme lieber wäre. Im Rahmen des Expertengesprächs schälte sich zumindest das Interesse vieler Staaten heraus, beim Einsatz tödlicher Gewalt gegen Menschen durch Maschinen *meaningful human control* zu erhalten, also einen Grad menschlicher Kontrolle, der sich nicht nur auf das Abnicken von bereits vom Computer getroffenen Entscheidungen beschränkt (Sauer 2014). Wohin sich der CCW-Prozess entwickeln wird, ist aktuell offen. Bei einem Scheitern des konsensualen CCW-Prozesses ist es denkbar, dass NGOs eine ähnliche internationale Kampagne ini-

Das Waffenübereinkommen der Vereinten Nationen (CCW)

Die im Dezember 1983 in Kraft getretene *Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons* (CCW, deutsch: UN-Waffenkonvention oder UN-Waffenübereinkommen) ist ein völkerrechtlicher Vertrag und zielt auf das Verbot oder die Beschränkung des Einsatzes bestimmter konventioneller Waffen in internationalen und nichtinternationalen bewaffneten Konflikten. Dabei stehen Waffensysteme im Fokus, die übermäßiges Leiden verursachen oder unterschiedslos wirken können. Hintergrund ist die völkerrechtliche Norm, dass Staaten bei der Wahl der im Konflikt eingesetzten Mittel nicht völlig freie Hand haben, sondern humanitäre Aspekte berücksichtigen müssen. Die Konvention ist zunächst ein Rahmenvertrag, den 118 Staaten unterschrieben und 113 ratifiziert haben. Die Waffen, deren Einsatz verboten wird, werden in Protokollen erfasst. Bislang gibt es fünf Protokolle, die unter anderem den Einsatz von Brandwaffen (Protokoll III) oder blindmachenden Laserwaffen (Protokoll IV) verbieten. Neue Protokolle werden von allen beteiligten Staaten verhandelt und nur konsensual beschlossen. Den Staaten steht es darüber hinaus dann frei, welche Protokolle sie durch ihre Unterschrift annehmen, d. h., nicht alle beteiligten Staaten haben alle fünf Protokolle anerkannt.

Quellen: Auswärtiges Amt 2013; UNOG 2014

tiieren wie z. B. die, die zur Landminenkonvention geführt hat. Damit würde, eine kritische Masse von Unterstützerstaaten vorausgesetzt, eine internationale Norm etabliert, mit der sich auch Nichtunterzeichner auseinandersetzen müssten (Meier 2013). Das Beispiel der Anti-Landminen-Kampagne zeigt, dass zumindest einige Nichtunterzeichner die Normen der Konvention anerkennen. Eine solche Norm könnte im Idealfall auch den Einsatz letaler autonomer Waffen durch Nichtteilnehmer »tabuisieren« und zusätzliche Staaten zur Teilnahme bewegen. Eine Norm bedeutet zwar keine Sicherheit, dass letale Systeme nicht doch eingesetzt werden, würde aber die politischen Kosten nachgewiesener Verstöße mittels internationaler *Shaming-and-blaming*-Kampagnen deutlich erhöhen.

Vor dem Hintergrund der Frage, wie man Verstöße gegen eine Einsatznorm letaler autonomer Systeme nachweisen könnte, haben Gubrud und Altmann ein Konzept »forensischer Rüstungskontrolle« (2013) entwickelt. Bei diesem Ansatz würden sich Staaten verpflichten, spezifische Kommunikationsdaten zwischen Bodenstation und Drohne sowie weitere Flugdaten in einer speziell gesicherten Einrichtung zu speichern und bei dem Verdacht auf den Einsatz »letaler Autonomie« einer internationalen Überprüfungsorganisation auszuhändigen. Diese könnte aus den Daten rekonstruieren, ob die Kontrolle über einen Waffeneinsatz tatsächlich noch beim menschlichen Entscheider am Boden gelegen hat, ohne die zugrundeliegende Software kennen zu müssen. Ob der Vorstoß eine Chance auf Umsetzung hat, bleibt abzuwarten.

Handlungsempfehlungen

Der Blick auf die drei oben skizzierten Felder aktueller Rüstungsdynamiken hat gezeigt, dass Rüstungskontrolle mehr und unterschiedliche Elemente aufgreifen muss, um auch in Zukunft Relevanz zu haben. Rein quantitative Ansätze verlieren an Bedeutung, auch wenn sie beispielsweise in Regionen, in denen Sicherheitsdilemmata herrschen (Meier 2013, S. 100) und lokale Rivalen keine zu starken qualitativen Unterschiede in der Bewaffnung aufweisen, weiter relevant sein können. Bei den technologisch fortschrittlichsten Staaten müssen aber neue Instrumente entwickelt und eingesetzt werden. Es zeigt sich, dass diese überwiegend auf Transparenz, Vertrauensbildung und starke Normen setzen müssen. Dies setzt aber umso mehr den Willen zur Rüstungskontrolle voraus. Dieser wiederum hängt ab von den grundlegenden Beziehungen zwischen den zentralen Akteuren (Müller 1996, 405 ff.). Die aktuell deutlich abgekühlten Beziehungen zwischen dem Westen und Russland stellen deshalb auch aus Sicht der Rüstungskontrolle ein großes Problem dar. Sich aber weiterhin über Fragen der Rüstungskontrolle auszutauschen kann dazu beitragen, dass sich die Beziehungen nicht weiter verschlechtern oder sogar wieder verbessern.

Es sollte auch im westlichen Interesse liegen, sich von staatlicher Seite systematisch mit den Gefahren der zunehmenden Bedeutung von Software in der Rüstungskontrolle auseinanderzusetzen. Dass Staaten selbst in den beschriebenen hochproblematischen Bereichen versuchen, kleine rüstungskontrollpolitische Schritte zu unternehmen und neue Konzepte entwickeln – auch wenn die aktuelle Umsetzung problematisch ist –, lässt hoffen. Zusätzlich sinnvoll wäre es aber, die verschiedenen Ansätze in den genannten Bereichen unter einer breiteren Perspektive »Rüstungskontrolle für Software« zu diskutieren. Besonders wichtig erscheint es angesichts der rasanten technologischen Entwicklungen aber, beim Thema »letale Autonomie« weiterhin aktiv zu bleiben und die begonnene internationale Diskussion nicht abreißen zu lassen. Es besteht die Chance, in den nächsten Monaten im Kontext der CCW zu konkreten Ergebnissen zu gelangen. Diese Chance darf nicht verspielt werden.

Literatur

Altmann, Jürgen 2013: Arms Control for Armed Uninhabited Vehicles: an Ethical Issue, in: Ethics and Information Technology, Jg. 15/2, S. 137–152.

Arkin, Ronald C. 2009: Ethical Robots in Warfare, in: IEEE, Technology and Society Magazine, Jg. 28/1, S. 30–33.

Auswärtiges Amt 2013: Waffenübereinkommen der Vereinten Nationen mit den dazugehörigen Protokollen, Berlin (http://www.auswaertiges-amt.de/DE/Aussenpolitik/Friedenspolitik/Abruestung/KonvRueKontrolle/VN-Waffenuebereinkommen-CCW_node.html, 7. 11. 2014).

de Selding, Peter B. 2011: Pentagon Struggles with Avalanche of Data (http://www.spacenews.com/article/

pentagon-struggles-avalanche-data, 16. 6. 2014).

Farnsworth, Timothy 2011: China and Russia Submit Cyber Proposal (http://www.armscontrol.org/act/2011_11/China_and_Russia_Submit_Cyber_Proposal, 5. 11. 2014).

Farwell, James P./Rafal Rohozinski 2011: Stuxnet and the Future of Cyber War, in: Survival. Global Politics and Strategy, Jg. 53/1, S. 23–40.

Fey, Marco/Harald Müller 2008: Unkontrollierbare Rüstungsdynamik? Die RMA als »harter Brocken« für die Rüstungskontrolle, in: Jan Helmig/Niklas Schörnig (Hg.), Die Transformation der Streitkräfte im 21. Jahrhundert. Militärische und politische Dimensionen der aktuellen »Revolution in Military Affairs«, Frankfurt am Main, S. 203–223.

Gaycken, Sandro 2014: Die Cyberkämpfer kämpfen schon, in: Loyal, Magazin für Sicherheitspolitik, Nr. 4/2014, S. 6–10.

Geier, Karsten 2014: Presentation by Karsten Geier, Head of the Division for Communication and New Challenges in Arms Control and Non-Proliferation, Federal Foreign Office Berlin at the ASEAN Regional Forum Workshop on Cyber Confidence Building Measures, ASEAN Regional Forum Workshop on Cyber Confidence Building Measures, Kuala Lumpur, 25. 3. 2014 (vom Auswärtigen Amt verschicktes Redemanuskript).

Gubrud, Mark/Jürgen Altmann 2013: Compliance Measures for an Autonomous Weapons Convention, International Committee for Robot Arms Control (ICRAC) Working Paper 2/2013, o. O. (http://icrac.net/wp-content/uploads/2013/05/Gubrud-Altmann_Compliance-Measures-AWC_ICRAC-WP2.pdf, 5. 11. 2014).

Haider, André 2014: Remotely Piloted Aircraft Systems in Contested Environments. A Vulnerability Analysis, Kalkar (http://www.japcc.org/publications/report/Report/JAPCC_RPAS_In_Contested%20_Environements.pdf, 5. 11. 2014).

Human Rights Watch 2012: Losing Humanity. The Case against Killer Robots. Washington, D. C.

Lindsay, Jon R. 2013: Stuxnet and the Limits of Cyber Warfare, in: Security Studies, Jg. 22/3, S. 365–404.

Meier, Oliver 2013: Gibt es einen Formwandel der Rüstungskontrolle?, in: Sicherheit und Frieden, Jg. 31/2, S. 99–101.

Melzer, Nils 2011: Cyberwarfare and International Law (UNIDIR Resources), Genf (http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf, 6. 11. 2014).

Minkwitz, Olivier 2008: Die technologische Komponente der militärischen Transformation, in: Jan Helmig/Niklas Schörnig (Hg.), Die Transformation der Streitkräfte im 21. Jahrhundert. Militärische und politische Dimensionen der aktuellen »Revolution in Military Affairs«, Frankfurt am Main, S. 63–80.

Müller, Harald 1996: Von der Feindschaft zur Sicherheitsgemeinschaft – Eine neue Konzeption der Rüstungskontrolle, in: Berthold Meyer (Hg.), Eine Welt oder Chaos?, Frankfurt am Main, S. 399–428.

Müller, Harald/Niklas Schörnig 2001: RMA and Nuclear Weapons – A Calamitous Link for Arms Control?, in: Disarmament Forum, Jg. 3/4, S. 17–26.

Müller, Harald/Niklas Schörnig 2006: Rüstungsdynamik und Rüstungskontrolle. Eine exemplarische Einführung in die Internationalen Beziehungen, Baden-Baden.

Neuneck, Götz 2014: Die Geheimdienste und das Militär: neue Bedrohungen im Cyberspace, in: Ines-Jacqueline Werkner/Janet Kursawe/Margret Johannsen/Bruno Schoch/Marc von Boemcken (Hg.), Friedensgutachten 2014, Münster, S. 239–253.

Sanger, David E. 2012: Confront and Conceal. Obama's Secret Wars and Surprising Use of American Power, New York.

Sauer, Frank 2014: Autonome Waffensysteme. Humanisierung oder Entmenschlichung des Krieges? (Global Governance Spotlight 4/2014), Bonn.

Schelling, Thomas C./ Morton H. Halperin 1961: Strategy and Arms Control, New York.

Schmidt, Hans-Joachim 2013: Verified Transparency. New Conceptual Ideas for Conventional Arms Control in Europe (PRIF Report 119/2013), Frankfurt am Main.

Schmidt, Hans-Joachim 2014: Verifiable Transparency, in: Security Community, Nr. 1/2014, S. 10–11.

Schmitt, Michael N. (Hg.) 2013: Tallinn Manual on the International Law Applicable to Cyber Warfare. Prepared by the International Group of Experts at the Invitation of The NATO Cooperative Cyber Defence Centre of Excellence, Cambridge.

Schörnig, Niklas 2005: Die *Revolution in Military Affairs* – Hemmschwelle für eine kooperative Weltordnung, in: Ulrich Ratsch/Reinhard Mutz/Bruno Schoch/Corinna Hauswedell/Christoph Weller (Hg.), Friedensgutachten 2005, Münster, S. 219–227.

Schörnig, Niklas 2014: Automatisierte Kriegsführung – Wie viel Entscheidungsraum bleibt dem Menschen?, in: Aus Politik und Zeitgeschichte, Jg. 64/35-37, S. 27–34.

Shimko, Keith L. 2010: The Iraq Wars and America's Military Revolution, Cambridge.

United Nations 2013: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (Sixty-Eighth Session, Item 94 of the Provisional Agenda, Developments in the Field of Information and Telecommunications in the Context of International Security), New York (http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98, 6. 11. 2014).

UNOG (United Nations Office at Geneva) 2014: The Convention on Certain Conventional Weapons, Genf (http://www.unog.ch/80256EE600585943/%28httpPages%29/4F0DEF093B4860B4C1257180004B1B30, 8. 12. 2014).

Niklas Schörnig