Forum Innere Führung | 35

Roman Schmidt-Radefeldt | Christine Meissler [Hrsg.]

Automatisierung und Digitalisierung des Krieges

Drohnenkrieg und Cyberwar als Herausforderungen für Ethik, Völkerrecht und Sicherheitspolitik

Nomos

Forum Innere Führung

herausgegeben von dem
Bildungswerk des Deutschen BundeswehrVerbandes
Karl-Theodor-Molinari-Stiftung (KTMS)

Band 35

Roman Schmidt-Radefeldt/Christine Meissler (Hrsg.)

Automatisierung und Digitalisierung des Krieges

Drohnenkrieg und Cyberwar als Herausforderungen für Ethik, Völkerrecht und Sicherheitspolitik

Nomos

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-8329-7198-4

1. Auflage 2012

Inhaltsverzeichnis

Vorwort 5

Roman Schmidt-Radefeldt und *Christine Meissler*
Einführung 9

Teil 1: Automatisierung des Krieges 22

Peter W. Singer
War of the Machines: What Is The Real Story of Robotic Weaponry? 23

Niklas Schörnig
Die Automatisierung des Krieges: Eine kritische Bestandsaufnahme 33

Thilo Marauhn
Der Einsatz von Kampfdrohnen aus völkerrechtlicher Perspektive 60

Thomas Petermann
Unbemannte Systeme als Herausforderung für Sicherheits- und Rüstungskontrollpolitik – Ergebnisse eines Projekts des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag 72

Teil 2: Digitalisierung des Krieges 87

Sandro Gaycken
Die vielen Plagen des Cyberwar 89

Friedrich Wilhelm Kriesel, David Kriesel
Cyberwar – relevant für Sicherheit und Gesellschaft? Eine Problemanalyse 117

Olaf Theiler
Cyber-Defence als Herausforderung für die NATO: Angemessene Bedrohungsabwehr oder Umgang mit einem ‚Scheinriesen'? 130

Wolff Heintschel von Heinegg
Cyberspace – Ein völkerrechtliches Niemandsland? 159

Charles Williamson
A Perspective on the United States' View of International Law in Cyber-Conflict 175

Autorenverzeichnis 201

Einführung

Roman Schmidt-Radefeldt und *Christine Meissler*

I. Zum Wandel des Krieges im Hightech-Zeitalter

Die Entwicklung neuer militärischer Technologien stellt Politiker, Militärs, Juristen und Ethikwissenschaftler regelmäßig vor große Herausforderungen. Eine sog. *Revolution in Military Affairs* erfordert neben Anpassungen der militärischen Doktrinen auch eine rechtliche Überprüfung von neuartigen Methoden der Kriegsführung[1] sowie ethische Neubewertungen – wenn nicht gar ein Infragestellen der herkömmlichen Begrifflichkeiten des Krieges an sich.

Die waffentechnischen Innovationen des 20. Jahrhunderts hatten nachhaltigen Einfluss auf die Raum- und Zeitdimension des modernen Krieges:[2] Flugzeuge vergrößerten die Reichweite, Panzer erhöhten die Schussfolge, die moderne Nachrichtentechnik ermöglichte Kommunikation in Echtzeit, Raketen schufen Distanz zum Gegner und die Nukleartechnik brachte schließlich die ultimative Sprengkraft. Paradoxerweise stellte sich der moderne Krieg gerade in seiner fortgeschrittensten Form als undurchführbar heraus, weil er unweigerlich in die atomare Apokalypse geführt hätte.[3] Die daraus resultierende Krise des modernen Krieges bildete insoweit den politischen und strategischen Kontext für die waffentechnologische Weiterentwicklung seit den 1970er Jahren.[4] Der technologische Fortschritt durch sog. Hightech-Waffensysteme bedeutete gleichsam einen Ausweg aus der atomaren Pattsituation, indem er den Rückgriff auf militärische Mittel politisch und moralisch (wieder) akzeptabel machte.[5] Insbesondere der Einsatz von computergestützten Waffensystemen, die mit Hilfe von Lasern und Kameras ihr Ziel erreichen, versprach punktgenaue Präzision, eine größere Reichweite und eine Minimierung

1 Art. 36 ZP I zu den Genfer Konventionen verpflichtet die Staaten, bei der Entwicklung neuer Waffen oder Methoden der Kriegsführung festzustellen, ob ihre Verwendung mit dem humanitären Völkerrecht in Einklang steht.

2 *Rüdiger Voigt*, Entgrenzung des Krieges, in ders. (Hrsg.), Krieg – Instrument der Politik? Bewaffnete Konflikte im Übergang vom 20. zum 21. Jahrhundert, Baden-Baden 2002, S. 293-341 (293).

3 *Chris Habbles Gray*, InfoWar in der Krise, Ars Electronica 1998, http://90.146.8.18/de/archives/festival_archive/festival_catalogs/festival_artikel.asp?iProjectID=8449.

4 *Lawrence Freedman*, The Revolution in Military Affairs, London, International Institute for Strategic Studies, Adelphi Paper No. 318, 1998 http://www.iiss.org/publications/adelphi-papers/adelphi-summaries/?entryid1=8172&esctl709025directoryviewpager_p=9&char=0-9.

5 *Michael Ignatieff*, Virtueller Krieg, Hamburg 2001, S. 151 f.

ziviler Opfer. Die Entwicklung von unbemannten automatisierten Waffensystemen (z.B. Militärrobotern und Drohnen), die per Joystick und Satellitenkommunikation von jedem beliebigen Ort aus eingesetzt werden können, bedeutete zudem ein nahezu vollständig reduziertes Risiko für die eigenen Kräfte sowie eine Entlastung des „Faktors Mensch" von allen kriegsbedingten Nebenwirkungen. Die Steuerung solcher Hightech-Waffensysteme mittels Computer ermöglichte schließlich die Erstellung eines digitalisierten Schlachtfeldes, das von den Verantwortlichen in Echtzeit auf dem Bildschirm nachvollzogen und gesteuert werden konnte.

Attribute wie „Hightech-" oder „postmoderner" Krieg versuchen, den Wandel des Krieges durch die waffentechnologischen Innovationen des ausgehenden 20. Jahrhunderts begrifflich auf den Punkt zu bringen.[6] Zu den Charakteristika dieses Wandels gehören die zunehmende *Automatisierung* von Waffensystemen sowie eine *Digitalisierung* der Kriegsführung. Die digitale Infiltration von Drohnen-Steuerungsanlagen der amerikanischen Bodenstationen mit Schadsoftware führt beide Phänomene plastisch sichtbar zusammen.[7] Automatisierung und Digitalisierung beeinflussen nicht nur die Art und Weise der Kriegsführung, sondern vor allem auch das Verhältnis von Mensch und Maschine im bewaffneten Konflikt.

Dank der Informationstechnologie sind militärische Operationen nicht mehr in erster Linie auf den physischen Sieg über die feindliche Streitmacht gerichtet, sondern vielmehr auf die Herstellung einer Informationshegemonie über Kommandozentralen, Computernetzwerke und Schaltstellen. Diese lassen sich mittels elektronischer Funkstörung, Computerviren oder Desinformation digital ausschalten (sog. informationelle Kriegsführung), wodurch dem Feind die Kontrolle über kriegsentscheidende Faktoren genommen wird. Digitale Waffen erweisen sich damit gewissermaßen als eine „Umkehrung" der Neutronenbombe, durch deren Einsatz Menschen umkommen und Gegenstände "überleben".

Die Informationstechnologie verkoppelt Mensch und Waffentechnik zu einem aus Teilsystemen gebildeten komplexen militärischen Mensch-Maschine-System,[8] wobei die Bedeutung der Maschine im bewaffneten Konflikt tendenziell zu- und die Rolle des Menschen tendenziell abnimmt. Dies verleitete den US-Politologen *Peter Singer* zu der Annahme, der Krieg im 21. Jahrhundert werde von Maschinen bestimmt und durch Roboter revolutioniert.[9] Automatisierung und Digi-

6 Vgl. zum Begriff *Chris Hables Gray*, Postmodern War, London 1998.

7 http://www.news.de/politik/855230826/bericht-computervirus-befaellt-us-drohnen/1/; vgl. dazu auch *Wright, Craig*, Lebensgefahr aus dem Internet, in: Die ZEIT v. 13.10.2011, S. 26.

8 *Andreas Herberg-Rothe*, Der Krieg – Geschichte und Gegenwart. Frankfurt 2003, S. 130. So erhält etwa der mit Nachtsichtgeräten, Mikrophonen und Bildschirmen ausgestattete „Hightech-Krieger" per Funk Befehle und liefert automatische Videobilder und Positionsdaten an seine Leitstelle.

9 Vgl. *Peter W. Singer*, Wired for War: The Robotics Revolution and Conflict in 21st Century, New York 2009. Zu den rechtlichen und ethischen Fragen vgl. *Armin Krishnan*, Legality and Ethicality of Autonomous Weapons, Ashgate 2009.

talisierung der Kriegsführung charakterisieren den Hightech-Krieg des 21. Jahrhunderts also vor allem dadurch, dass sie die Rolle des Menschen im Krieg neu definieren – und ihn am Ende vielleicht überflüssig machen. Mit der Erprobung einer sensorgesteuerten Zielsuche beim Drohneneinsatz, die auf eine Fernsteuerung durch den Menschen mehr oder weniger verzichten kann, ist der Schritt von der bloßen Automatisierung hin zur Autonomisierung der Kriegsführung „auf Autopilot" bereits angelegt. Er wäre vollendet, wenn auch der Befehl zum Töten nicht mehr durch den Kommandeur, sondern durch einen Computeralgorithmus erfolgt.

Augenfälligstes Merkmal dieser Entwicklung: Das Schlachtfeld wird immer leerer.[10] Das dem amerikanischen Schriftsteller *Carl Sandburg* (1878-1967) zugeschriebene Bonmot: „Stell´ Dir vor es ist Krieg und keiner geht hin"[11], erhält mit Blick auf den Hightech-Krieg gewissermaßen eine doppelte Bedeutung. Die räumliche und physische Entkoppelung der Akteure vom eigentlichen Kriegsgeschehen, welches als „virtueller Raum" bzw. „digitales Schlachtfeld" dem realen Erleben der Kriegsbeteiligten entzogen ist, wirkt sich auf die Beziehung des Menschen zum Krieg aus: Der anonym im Netz oder am Joystick agierende Kriegsbeteiligte tritt als unmittelbarer Akteur einer militärischen Auseinandersetzung in den Hintergrund des Geschehens und erlebt den Krieg am Bildschirm fast wie ein Spiel. Die Kriegsparteien agieren folglich nicht mehr in ihrer (traditionellen) Doppelrolle als potentielle Täter *und* Opfer auf dem Schlachtfeld.[12] Vielmehr wird der Kriegsteilnehmer ersetzt durch autonome Maschinen und „virtuelle Kombattanten" jeglicher Couleur, deren Handeln sich der Kontrolle durch die kriegführenden Parteien zunehmend entzieht.

Automatisierung und Digitalisierung verändern das Gesicht des Krieges, in dem sie – im doppeldeutigen Sinne – zu dessen „Ent-Menschlichung" beitragen. Insbesondere in asymmetrischen Auseinandersetzungen, bei denen sich eine Konfliktpartei hinter ihrer Hochtechnologie „verschanzt", haftet dem Kampf zwischen Maschine und Mensch etwas geradezu Unmenschliches an. Beide Phänomene – Automatisierung und Digitalisierung – stellen weitreichende Fragen an die Strategie der Kriegsführung, an die Zurechenbarkeit von Kriegshandlungen, an die Einhaltung des humanitären Völkerrechts, an die Ethikfähigkeit künstlicher Intelligenz sowie an die „Humanität" des Krieges schlechthin.[13] Aufgabe von Wissenschaft und Praxis bleibt es, den Prozess zunehmender Automatisierung und Digitalisierung der Kriegsführung rechtlich einzuhegen und im Sinne ethischer Postulate und sicherheitspolitischer Interessen „menschlich" zu gestalten.

10 *Joanna Bourke*, An Intimate History of Killing, London 1999, S. 6.
11 "Sometime they'll give a war and nobody will come".
12 Diese Doppelrolle zeitigte stets auch eine gewalthemmende Wirkung auf die Konfliktparteien – man denke an die Regelungen zur Kriegsgefangenschaft der III. Genfer Konvention.
13 Vgl. näher *Jack M. Beard*, Law and War in the Virtual Era, in: American Journal of Int´l Law, Vol. 103 (2009), S. 1-37 (34).

II. Aspekte einer Automatisierung des Krieges: Drohnenkrieg

Mitarbeiter von US-Geheimdiensten bezeichnen Drohnen inzwischen als das effektivste Mittel zur Bekämpfung des internationalen Terrorismus – sowohl im Bereich der Aufklärung als auch zum Zwecke gezielter Tötungen. Zwischen 2006 und 2011 wurden in Pakistan ca. 2.280 Personen durch US-amerikanische Drohnen exekutiert.[14] Diese Entwicklung hat sich gerade unter der *Obama*-Administration weiter verstärkt.[15] Angesichts ihrer taktischen und strategischen Vorzüge – Drohnen sind schwerer aufzuklären als Flugzeuge, präziser in ihrer Wirkung, weniger anfällig als Piloten und um ein Vielfaches kostengünstiger als Kampfjets – droht ein weltweiter Rüstungswettlauf um die stärkste Drohnenflotte.[16] Befördert wird diese Entwicklung durch ein technisch und kulturell motiviertes „Prestigedenken"; vor allem aber durch die Aussicht auf eine Minimierung der Opfer aus den eigenen Reihen. Neben den klassischen Drohnen-Mächten USA, Israel und Großbritannien sollen inzwischen bereits mehr als 40 Staaten, darunter auch Russland und China aber auch nicht-staatliche Akteure wie die Hamas, unbemannte Luftfahrzeuge gebaut oder erworben haben – mit weltweit steigender Nachfrage.[17] Die allermeisten dienen der Luftaufklärung, doch erweitert sich die Produktpalette zunehmend auch um (Kampf)drohnen etwa vom Typ „Predator" oder „Reaper" – also um fliegende Kampfautomaten, bestückt mit lasergelenkten Luft-Boden-Raketen.[18]

Der Einsatz von Drohnen ist indes längst nicht mehr genuines Geschäft von Militärs, sondern zunehmend auch von nicht-militärischen Sicherheitsakteuren

14 http://www.longwarjournal.org/pakistan-strikes.php; dazu *Mary Ellen O´Connell*, Unlawful Killing with Combat Drones, A Case Study of Pakistan, 2004-2009, Notre Dame Law School Legal Studies Research Paper No. 09-43, 7/2010, https://webspace.utexas.edu/rmc2289/LT/Mary%20Ellen%20OConnell%20on%20Drones.pdf.

15 Dazu *Hauke Friedrichs*, Obamas riskanter Drohnenkrieg, in: Die ZEIT v. 16.9.2010; *Christian Schaller*, Gezielte Tötungen und der Einsatz von Drohnen – zum Rechtfertigungsansatz der Obama-Administration, in: Humanitäres Völkerrecht-Informationsschriften (HuV-I) 2011, S. 91-96.

16 Zu den militärischen Eignungsmerkmalen von Drohnen vgl. *Wolfgang Richter*, Kampfdrohnen versus Völkerrecht? Zum „Drohnenkrieg" in Afghanistan und Pakistan, in: HuV-I 2011, S. 105-112 (106).

17 *Philip Alston*, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, (UN Doc. A/HRC/14/24/Add.6, 28. Mai 2010, Rz. 27. Zur zunehmenden Bedeutung von Drohnen für die deutsche Außen- und Sicherheitspolitik vgl. *Ralph Thiele*, Veränderungen in Sicht?, in: Zeitschrift für Außen- und Sicherheitspolitik (ZFAS) 2011, S. 183-193 (192). Ansätze einer britisch-französischen Verteidigungskooperation im Drohnensektor sind bereits erkennbar (http://www.guardian.co.uk/politics/2011/nov/25/britain-france-stronger-defence-ties)

18 Vgl. *Scott Shane*, Coming Soon: The Drone Arms Race, The New York Times, 8.10.2011, http://www.nytimes.com/2011/10/09/sunday-review/coming-soon-the-drone-arms-race.html?scp=1&sq=Drone%20Arms%20Race&st=cse; *Felix Boor*, Der Drohnenkrieg in Afghanistan und Pakistan, in: Humanitäres Völkerrecht-Informationsschriften (HUV-I) 2011, S. 97-104 (97 f).

(wie z.B. Geheimdiensten) oder Aufständischen. So hat die CIA erstmalig eigenständige „Ziellisten" erstellt, um mithilfe von Kampfdrohnen gezielte Tötungen in Ländern durchzuführen, in denen die Vereinigten Staaten nicht offiziell Krieg führen. Der immer leichter werdende Zugang zu sog. Mini-Drohnen aber auch das erfolgreiche Hacken und Umleiten einer Predator-Drohne durch irakische Aufständische[19] bestätigen den von *Philip Alston*, ehemaliger UN-Sonderberichterstatter, diagnostizierten Trend, wonach unbemannte Flugkörper zunehmend in die Verfügungsgewalt nicht-staatlicher Gewaltakteure geraten können.[20]

Unbemannte Luftfahrzeuge („Unmanned Aerial Combat Vehicles"), zu denen auch Drohnen zählen, sind durch das humanitäre Völkerrecht nicht *per se* verboten.[21] Der Einsatz automatisierter, (teil)autonom agierender Waffensysteme wirft jedoch – jenseits der reinen Fernlenkung – zahlreiche völkerrechtliche und ethische Probleme auf.

Eine Bewertung des Einsatzes von Kampfdrohnen am Maßstab des humanitären Völkerrechts führt zur Frage nach der Einhaltung des Unterscheidungsgrundsatzes.[22] Fest steht, dass sich Opfer bei der Zivilbevölkerung trotz stärkerer Aufklärungsfähigkeit von Drohnen nicht vermeiden lassen. Teilweise wird sogar behauptet, die Nutzung ferngelenkter Drohnen begünstige nachgerade unterschiedslose (und damit völkerrechtswidrige) Angriffe.[23] Ob eine verbesserte Kamera- und Satellitentechnik die menschliche Präsenz am Kriegsschauplatz vollständig zu ersetzen vermag oder gar zu einer präziseren Lagebewertung führt, ist umstritten.[24] Problematisch in diesem Zusammenhang erweist sich vor allem die Frage nach einer Korrektur- und Anpassungsmöglichkeit von automatischen Waffensystemen

19 Vgl. Der Spiegel v. 17.12.2009: „Irakische Aufständische hacken US-Militärdrohne", http://www.spiegel.de/netzwelt/netzpolitik/0,1518,667648,00.html.

20 *Philip Alston*, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, UN Doc. A/HRC/14/24/Add.6, www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf. Ebenso *Philipp Stroh,* Der Einsatz von Drohnen im nicht-internationalen bewaffneten Konflikt, in: HuV-I 2011, S. 73-77 (73).

21 Zu den Statusfragen von Drohnen vgl. näher *Robert Frau,* Unbemannte Luftfahrzeuge im internationalen bewaffneten Konflikt, in: HUV-I 2011, S. 60-72 (62 f).

22 Vgl. Art. 51 ZP I zu den Genfer Konventionen.

23 Nach *David Kilcullen / Andrew McDonald Exum*, Death from Above, Outrage Down Below, in: The New York Times v. 17.3.2009 (http://www.nytimes.com/2009/05/17/opinion/17exum.html?pagewanted=all) kämen auf jede gezielt getötete Zielperson ca. 50 nicht beabsichtigte Opfer. Zur Diskussion vgl. *Felix Boor*, Der Drohnenkrieg in Afghanistan und Pakistan, in: HUV-I 2011, S. 97-104 (98) m.w.N.

24 So kam es etwa im Februar 2010 zur Tötung von 23 afghanischen Zivilisten, weil bei der Auswertung der Aufnahmen einer Aufklärungsdrohne mehrere Fahrzeuge fälschlicherweise als militärisches Ziel identifiziert und infolge eines *Information Overload* übersehen wurde, dass sich dort auch Frauen und Kinder befanden (vgl. *Scott Shane*, C.I.A. Is Disputed on Civilian Toll in Drone Strikes, The New York Times, 11.8.2011 http://www.nytimes.com/2011/08/12/world/asia/12drones.html?pagewanted=all). Allerdings wird auch ein Jetpilot den völkerrechtlichen Status von Individuen aus der Luft nicht immer eindeutig feststellen können, sofern diese nicht eindeutig als unmittelbar Kampfbeteiligte zu erkennen sind.

– etwa wenn sich im Zielgebiet einer Kampfdrohne neue Konstellationen hinsichtlich der Zivilbevölkerung oder dem Status ziviler Objekte ergeben. Hier müssen die an den Staat gestellten Anforderungen im Bereich „targeting", vor allem die kontinuierliche Aufklärung „in Echtzeit", weiter ausdifferenziert werden.[25] Solange die (menschliche) Fähigkeit, Kombattanten und Zivilisten auseinanderzuhalten, technisch nicht realisierbar ist, darf die Entscheidung zum Waffeneinsatz jedenfalls automatisiert werden.[26]

Ethisch fragwürdig erweist sich eine zunehmend automatisierte Kriegsführung, deren militärstrategisches Charakteristikum in der räumlichen – und letztlich auch psychologischen – Distanz zwischen Konfliktakteuren und Konfliktschauplatz besteht. Dabei bestehe die Gefahr, dass sich bewaffnete Konflikte immer mehr in eine Art reales Videospiel verwandeln – mit Drohnenführern, die losgelöst vom tatsächlichen Kampfgeschehen und ohne eigene physische Gefährdung[27] tausende von Kilometern entfernt in ihren Büros die Joysticks bedienen und der Drohne über Satellit Befehle erteilen, um nach getaner Arbeit zu ihren Familien zurückzukehren.[28] Die räumliche Distanz zwischen der Drohnen-Bodenstation und dem Kriegsschauplatz, auf dem die Drohne zum Einsatz kommt, schließt das Risiko eines Drohnenführers aus, unmittelbar in bewaffnete Unternehmungen einbezogen zu werden. Der geringe Personaleinsatz, aber auch die zu verschmerzenden materiellen Verluste im Falle eines Drohnenausfalls senken zudem die Hemmschwelle für den Einsatz militärischer Mittel in bewaffneten Konflikten.[29] Mit zunehmender Entfernung zum potentiellen Opfer nähmen schließlich Empfindungen wie Empathie und Mitleid ab, während die Bereitschaft zum Angriff mit zunehmender Entfernung zum Kriegsschauplatz ansteige.[30] Die Sicht auf den Gegner über einen Bildschirm lässt die Realität wie Fiktion erscheinen und fördert die von *Alston* diagnostizierte „Playstation-Mentalität."[31]

25 Vgl. Art. 57 ZP I zu den Genfer Konventionen. In diesem Sinne auch *Robert Frau,* Unbemannte Luftfahrzeuge im internationalen bewaffneten Konflikt, in: HUV-I 2011, S. 60-72 (65) und *Philipp Stroh,* Der Einsatz von Drohnen im nicht-internationalen bewaffneten Konflikt, in: HuV-I 2011, S. 73-77 (77).

26 *Felix Boor*, Der Drohnenkrieg in Afghanistan und Pakistan, in: HuV-I 2011, S. 97-104 (98).

27 *Peter W. Singer*, Wired for War 2009, S. 347 berichtet allerdings über posttraumatische Belastungsstörungen.

28 Zum Arbeitsalltag eines Drohnenpiloten vgl. Interview mit Major *B. Callahan* in: Der Spiegel v. 10.3.2010 sowie *Tobias Hürter*, Das automatisierte Töten, in: Die ZEIT v. 1.7.2010, S. 33. Zu den ethischen Implikationen vgl. *Jutta Weber*, Digitale Kriegsmaschinerie, in: Die ZEIT v. 1.7.2010, S. 34.

29 *Peter W. Singer*, Wired for War, 2009, S. 396.

30 So *Dave Grossman*, On Killing: The Psychological Cost of Learning to Kill in War and Society, 1995, S. 187.

31 *Philip Alston*, Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, UN Doc. A/HRC/14/24/Add.6, 28. Mai 2010, Rz. 84. Zu der außerrechtlichen Problematik von Drohneneinsätzen vgl. *Felix Boor,* Der Drohnenkrieg in Afghanistan und Pakistan, in: HuV-I 2011, S. 97-104 (99 f).

Der Einsatz von Drohnen erweitert nicht allein das militärische Arsenal, sondern verändert insbesondere auch die Art und Weise der Kriegsführung. Die Aktionsmöglichkeiten einer Drohne sind letztlich statisch und lassen dem Drohnenführer wenig Spielraum für eine flexible oder abgestufte Reaktionen. Warum sollte eine Konfliktpartei unter hohem Risiko für die eigenen Kräfte versuchen, Gefangene zu nehmen, wenn sich der Gegner auf ein bloßes Ziel am Bildschirm reduzieren und per Knopfdruck ausschalten lässt? Forderungen des Internationalen Komitees vom Roten Kreuz nach einer verstärkten Beachtung des Verhältnismäßigkeitsprinzips im humanitären Völkerrecht – z.B. die Forderung, den Gegner nicht zu töten, wenn er unter den gegebenen Umständen ohne zusätzliche Risiken auch durch Gefangennahme außer Gefecht gesetzt werden kann[32] – würden durch den Einsatz von Drohnen weitgehend konterkariert.[33] Der Handlungsspielraum einer Kampfdrohne reduziert sich nämlich auf eine Art „binären Code“: Tötung oder Einsatzabbruch – *tertium non datur*. Die Automatisierung des Krieges führt daher tendenziell zu einer „Radikalisierung“ der Kriegsführung, d.h. zu einem Verlust an Flexibilität und Differenztierungsmöglichkeiten.[34] Überdies besteht beim Einsatz automatisierter Systeme die Gefahr einer Eskalation der Kampfhandlungen – etwa wenn Drohnen nach fälschlicher Interpretation gegnerischer Handlungen automatisch Gegenreaktionen einleiten.[35] Die von dem englischen Robotiker *Noel Sharkey* gegründete NGO „International Committee for Robot Arms Control“ (ICRAC) setzt sich daher auf internationaler Ebene für eine Ächtung autonom agierender Waffensysteme ein.[36]

Automatisierte Waffensysteme verändern – wie alle waffentechnologischen Neuerungen – auch die Rolle des Menschen im Krieg. Dessen Aufgabenspektrum verschiebt sich von einer genuin kämpfenden Rolle hin zu einer (derzeit noch) steuernden, bald aber vielleicht nur noch kontrollierenden und überwachenden Tätigkeit. Für die fortschreitende Automatisierung der Entscheidungsprozesse, wie

32 Interpretative Guidance on the notion of direct participation in hostilities under International Humanitarian Law, 2009, http://www.icrc.org/eng/resources/documents/article/review/review-872-p991.htm. Vgl. zu dieser Forderung bereits *Jean Pictet*, Development and Principles of International Humanitarian Law, Dordrecht 1985, S. 75.

33 Fraglich ist, ob sich Drohneneinsätze von vornherein auf Szenarien beschränken lassen, bei denen die Möglichkeit zur risikolosen Festnahme ex-ante ausgeschlossen ist.

34 Ähnlich *Armin Krishnan*, Killer Robots. Legality and Ethicality of Autonomous Weapons, 2009, S. 91 f.

35 So auch *Felix Boor*, Der Drohnenkrieg in Afghanistan und Pakistan, in: HUV-I 2011, S. 97-104 (103 f). Strukturell vergleichbare Gefahren gibt es bereits beim automatisierten („Turbo“-)Börsenhandel, wenn vollautomatische Computerprogramme in Sekundenbruchteilen auf (vermeintliche) Kursdifferenzen mit massenhaften Kauf- und Verkaufsaufträgen reagieren und dadurch (nicht beabsichtigte) Kurseinbrüche am Aktienmarkt provozieren (dazu *Niklas Hoyer* und *Günter Heismann*, Börse im Bann der Maschinen, in: Wirtschafts-Woche v. 2.12.2011, http://www.wiwo.de/finanzen/boersenhandel-boerse-im-bann-der-maschinen/5143548.html).

36 http://www.icrac.co.cc.

sie heute schon in der Raketenabwehr auf Kriegsschiffen Anwendung findet, gibt es handfeste militärische Interessen – zum Beispiel die schnellere Reaktionsfähigkeit eines autonom agierenden Systems gegenüber der eines Piloten. Dank zunehmender Spezifizierung der Steuerungssysteme vermag ein einzelner Operator bereits heute mehrere (teil)autonome Drohnen gleichzeitig zu steuern und zu überwachen.[37] Die Letztentscheidung über das Töten ist derzeit (noch) dem Menschen vorbehalten. Gleichwohl erscheint der Schritt zur vollautomatischen Zielauswahl, Zielerfassung und Auftragserfüllung durch autonome Waffensysteme technisch nicht unvorstellbar. Doch lassen sich ethische und rechtliche Wertungen in Computersoftware programmieren?[38] Menschliche Werte können sich nur unter menschlicher Beteiligung entfalten. Die Rückkopplung von automatisierten Entscheidungsprozessen bleibt insoweit die zentrale Voraussetzung menschlicher Verantwortung und völkerrechtlicher Zurechnung. Auch die völkerstrafrechtliche Verantwortlichkeit knüpft regelmäßig an vorsätzliches Handeln der Kriegsbeteiligten an:[39] Das fahrlässige Handeln eines Programmierers von Computersoftware für autonome Waffensysteme bliebe dann aber sanktionslos – und mit ihm der möglicherweise völkerrechtswidrige Einsatz einer Kampfdrohne.

Wie weit also Automatisierungsprozesse den Drohnenführer (den sog. „man in the loop“) verdrängen dürfen, ist daher nicht allein eine Frage technischer Machbarkeit. Die Frage, wo die Grenze zum (autonomen) „War of the Machines“ gezogen wird, ist immer auch Ausdruck des politischen und rechtlichen Willens zur Regelung menschlicher Konflikte.

III. Aspekte einer Digitalisierung des Krieges: Cyber War

1993 brachten *John Arquilla* und *David Ronfeld* in einer visionären Studie mit dem Titel „Cyber War is Coming“ die digitale *Revolution in Military Affairs* auf den Begriff *Cyber War,*[40] der sich in der Folge zu einem sicherheitspolitischen „Modewort“ entwickelt hat.[41] Es nimmt daher nicht wunder, dass gerade die US-Streitkräfte auf die digitalen Herausforderungen der Kriegsführung mit Errichtung eines militärischen *Cyber Command* reagiert und den Cyberspace zum fünften militäri-

37 *Peter W. Singer*, Wired for War, 2009, S. 126.

38 Am *Georgia Institute of Technology* in Atlanta wird unter Leitung des Robotikers *Ronald C. Arkin* an einer „Ethik-Programmierung“ gearbeitet (www.cc.gatech.edu/ai/robot-lab/ethics/#multi); vgl. dazu auch *Armin Krishnan*, Killer Robots, 2009, S. 107 ff.

39 Vgl. Art. 30 des Römischen Statuts des IStGH.

40 *Arquilla / Ronfeld*, Cyberwar is Coming, in: Journal of Comparative Strategy 1993 (Vol. 12), S. 141-165.

41 Vgl. etwa zuletzt die gleichnamigen Werke aus der jüngeren Literatur von *Richard A. Clarke* & *Robert K. Knake*, 2010 sowie von *Sandro Gaycken*, 2011. Auf die „virtuelle“ Kriegsführung beziehen sich auch die Begriffe *Netwar*, *Information War* oder *Electronic Warfare*.

schen Operationsraum (neben Land, See, Luft und Weltraum) erklärt haben.[42] Ähnlich wie mit dem sog. *War on Terror* verfolgen die Amerikaner auch mit *Cyber War* eine breit angelegte Konzeption unter Einbeziehung auch nachrichtendienstlicher und polizeilicher Aspekte unter die „Kriegsagenda".

Gleichzeitig erlebt die Diskussion – wie im Herbst 2010 in Zusammenhang mit dem Schadprogramm „Stuxnet" – eine bemerkenswerte rhetorische „Aufrüstung" im kriegsrelevanten Kontext: „Der digitale Erstschlag ist erfolgt"[43] – „NATO rüstet sich für Computer-Kriege"[44] – „Krieg im Cyber-Space"[45] – „Die neuen Cyberkrieger"[46] oder „Das Netz als Schlachtfeld".[47] Wo sich die deutsche Politik jahrelang damit schwertat, den Bundeswehreinsatz in Afghanistan als „Krieg" zu bezeichnen, erscheint die einhellige (und mediale Aufmerksamkeit heischende) Cyberkriegsrhetorik umso erstaunlicher: Denn die „Stuxnet-Attacke" zeitigte weder Tote noch Verletzte oder gar bedeutsame militärische Aktivitäten. Überdies ließ sich nur mutmaßen, ob sich hinter „Stuxnet" überhaupt staatliche Akteure, Motive und Interessen verbergen, die denen bei internationalen bewaffneten Konflikten gleichen und eine Qualifizierung als Cyber*krieg* rechtfertigen.

Der Begriff *Cyber War* weist wie kaum ein anderer Topos in der aktuellen Sicherheitsdebatte – abgesehen vielleicht vom *War on Terror* – so wenig inhaltlich-präzise Konturen und gleichzeitig einen so weiten Konnotationsbereich auf. Über eine Definition von „Cyberwaffen" oder die Anwendung kriegsvölkerrechtlicher Regelungen im Cyberspace herrscht ebenso wenig Konsens wie über die kategorielle Abgrenzung zwischen *Cyber War* und *Cybercrime*[48] und die damit einhergehenden polizeilichen, militärischen oder geheimdienstlichen Zuständigkeiten im virtuellen Raum. Forderungen nach neuen Normen für den „Cyberspace" sind ebenso schnell laut geworden wie unlängst Bestrebungen, ein Sonderrechtsregime für die Terrorbekämpfung zu etablieren. Erfordert der Cyberspace als neuartige Dimension eine Neubewertung unserer Vorstellungen vom Krieg? Oder unterscheiden sich Computernetzwerkattacken und klassische militärische Auseinandersetzungen in der „physischen" Welt nur durch die *modi operandi* der eingesetzten „Waffen"?

42 Das Auftragsspektrum des US-Cyberkommandos dient u.a. dem Schutz der US-amerikanischen Verteidigungsinfrastruktur sowie der Aufsicht bzw. Zuteilung aller dem Militär zur Verfügung stehenden Cyber-Ressourcen (vgl. näher *William J. Lynn III,* Defending a New Domain: The Pentagon's Cyberstrategy, in: Foreign Affairs, Vol. 89 No. 5 (2010), S. 98).

43 *Frank Rieger* in: FAZ.NET v. 22.9.2010.

44 *Peter Blechschmidt* in: SZ v. 1.10.2010.

45 *Camilo Jimenéz* in: SZ v. 23.9.2010.

46 *Misha Glenny* in: Financial Times v. 12.10.2010.

47 *Paul-Anton Krüger* in: SZ v. 4.10.2010.

48 Dazu näher *Sandro Gaycken*, Cyberwar. Das Internet als Kriegsschauplatz, München 2011, S. 78 f; *Jenny Döge*, Cyber Warfare, in: Archiv des Völkerrechts Bd. 48 (2010), S. 486-501 (487, 492).

Zweifellos führt der hohe Vernetzungsgrad moderner Streitkräfte zu einer fortschreitenden Abhängigkeit der Operationsführung von Computersystemen und Internet. Eine vergleichbare Verletzlichkeit hochtechnisierter Staaten besteht hinsichtlich der Steuerungssoftware einer informationstechnisch gestützten Kritischen Infrastruktur (sog. SCADA-Systeme).[49] Computernetzwerkoperationen eröffnen damit ein ganzes Spektrum an neuen taktischen Möglichkeiten: Diese reichen von einer Störung, Manipulation, Unterdrückung bzw. Löschung von Daten durch Einspeisen von *malware* (Schadprogramme mit Viren, Trojanern) in gegnerische Computernetzwerke, internetgestützte Kommunikationsnetze oder *targeting*-Datenbanken bis hin zu Eingriffen in die Steuerungsprozesse kritischer Infrastrukturanlagen (Chemiefabriken, Stromnetze, Notrufzentralen, Pipelines, Kraftwerke, Atomanlagen oder Verkehrsleitsysteme). Die Auswirkungen digitaler Netzwerkattacken können die System- oder Nutzerebene betreffen („Lahmlegen" der Funktionsfähigkeit), aber mittelbar auch zu Schäden an Personen und Sachwerten (z.B. Flugzeugabstürze, Überschwemmungen, nukleare Verstrahlung) führen.[50] Pläne des amerikanischen *Cyber Command,* im Frühjahr 2011 Libyens Luftabwehr elektronisch statt mit Bomben auszuschalten, sollen – neben juristischen und politischen Bedenken – offenbar auch deswegen verworfen worden seien, weil sich die Wirkungen einer solchen Cyberattacke nicht genau abzuschätzen ließen.[51]

Ähnlich wie der *War on Terror* beschreibt *Cyber War* asymmetrische Auseinandersetzungen ohne klare Fronten, klar identifizierbare Akteure oder eindeutige Regelungen. Überdies überwindet der Cyberspace erstmals alle Begrenzungen und Hürden geographischer Räume und erlaubt es einer unübersehbaren Zahl an Akteuren (z.B. „patriotische" Hacker, Cyber-Söldner, Cyber-Terroristen etc.), bereits mit relativ geringem finanziellen Aufwand im virtuellen Raum zu agieren. Die verflochtene und ubiquitäre Netzstruktur wirkt dabei einer zentralisierten Kontrolle oder Vorherrschaft im Cyberspace entgegen. Cyberangriffe können nicht nur aus allen Richtungen, sondern unter Einbindung zahlreicher Akteure (sog. Botnetze) sowohl zeitgleich als auch zeitlich verzögert stattfinden. Überdies können strukturelle Kopplungen von kleinen, scheinbar unbedeutenden digitalen Funktionen gravierende Wirkungen zeitigen (sog. Kaskadeneffekte),[52] wodurch eine präzise Unterscheidung zwischen militärischen und zivilen Zielen deutlich erschwert wird. Schließlich bleiben gravierende Unsicherheiten hinsichtlich der Motive und der

49 SCADA = *Supervisory Control and Data Acquisition*. Erinnert sei hier an die etymologische Bedeutung von *cyber* (griechisch *Kybernetike* = Steuerung, Kunst des Steuerns).

50 Vgl. näher zu den Wirkungsformen von Computernetzwerkattacken *Katharina Ziolkowski*, Computernetzwerkoperationen und die Zusatzprotokolle zu den Genfer Abkommen, in: Humanitäres Völkerrecht – Informationsschriften (HUV-I) 2008, S. 202-213 (203).

51 *Paul-Anton Krüger*, Gedankenspiele um Cyber-Krieg, in: SZ v. 19.10.2011, S. 7.

52 *Sandro Gaycken*, Die Zukunft des Krieges – Strategische Konzepte und strukturelle Probleme des Cyberwarfare, in: SIGINT09-Proceedings, Köln 2009.

Identität eines Angreifers im Cyberspace: Ob ein Datenpaket legalen, kriminellen oder Spionagezwecken dient, lässt sich kaum unterscheiden. Ein „Cyber-Radar" zur Aufklärung gegnerischer Internetaktivitäten existiert nicht; die Akteure im Cyberspace tragen weder Waffen noch Uniformen, sondern operieren anonym. Die Unübersichtlichkeit der Netzstruktur erschwert die Identifikation der Angreifer (Attributions- oder Rückverfolgungsproblematik), zumal sich die Herkunft von Daten leicht verschleiern oder eine IP-Adresse leicht vortäuschen lässt. Und selbst bei gelungener Rückverfolgung zu einem bestimmten Computer bleibt die Frage nach der konkreten Zurechenbarkeit einer Cyber-Attacke gegenüber einer bestimmten Person (sog. „Mensch-Maschine-Gap") offen. Das Attributionsproblem lässt auch die klassischen Instrumente der (militärischen) Abschreckung und der Rüstungskontrolle versagen – zumindest solange sich Abrüstungsschritte nicht verifizieren lassen und die Abgrenzung zwischen Cyber-Waffen und ziviler Computertechnologie fast unmöglich erscheint.[53]

Kriegsführung im Cyberspace entzieht sich nicht *per se* den geltenden kriegsvölkerrechtlichen Parametern. Die Völkerrechtswissenschaft ist schon seit längerem dabei, die bestehenden rechtlichen Maßstäbe und Begrifflichkeiten auch auf digitale Auseinandersetzungen anzuwenden. Dabei gilt es, die Sphäre des Cyberspace zu „entmystifizieren" und geltende Rechtsprinzipien im Lichte neuer Herausforderungen weiterzuentwickeln, wie es etwa beim Selbstverteidigungsrecht gegen nicht-staatliche Akteure (Terroristen) geschehen ist. Das von einem internationalen Expertenkreis im *Cooperative Cyber Defence Centre of Excellence* in Tallin erarbeitete *Manual of International Law applicable to Cyber Warfare* („The Tallin Manual") soll bis 2013 erscheinen. Ähnlich wie bei Terrorattacken muss völkerrechtlich geklärt werden, wann Computernetzwerkattacken die Schwelle zur *armed attack* (i.S.v. Art. 51 UN-Charta und Art. 5 NATO-Vertrag) überschreiten.[54] Macht es bei einer wirkungsorientierten Sichtweise rechtlich einen Unterschied, ob Infrastrukturanlagen physisch zerstört oder durch Sabotage der Steuerungssoftware (nur) neutralisiert werden?[55] Fraglich ist ferner, inwieweit die Regeln des humanitären Völkerrechts (insb. der Schutz von zivilen Infrastrukturnetzwerken) bei digitalen Attacken eingehalten werden können.[56] Doch auch unterhalb

53 Dazu näher *Ingo Ruhmann*, Rüstungskontrolle gegen den Cyberkrieg?, http://www.heise.de/tp/artikel/31/31797/1.html. Zu Vorschlägen für ein Cyber-Inspektionsregime, angelehnt an die IAEA sowie ein *Cyber War Limitation Treaty*, angelehnt an SALT, vgl. *Richard A. Clarke / Robert K. Knake*, Cyber War, New York 2010, S. 247 ff. und 268 ff.

54 Näher dazu *Falko Dittmar*, Angriffe auf Computernetzwerke, Berlin 2005, S. 156 ff.

55 Unter Verweis auf Art. 52 (2) des 1. Zusatzprotokolls zu den Genfer Konventionen hält *Döge* (AVR 2010, 486, 492) bereits die Neutralisierung von Infrastruktur für ausreichend.

56 Näher dazu *Jenny Döge*, Cyber Warfare, in: Archiv des Völkerrechts Bd. 48 (2010), S. 486-501 (493 ff); *Katharina Ziolkowski*, Computernetzwerkoperationen und die Zusatzprotokolle zu den Genfer Abkommen, HuV-I 2008, S. 202-213; *Knut Dörmann*, Applicability of the Additional Protocols to Computer Network Attacks, 2004, online unter: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

der Schwelle des Gewaltverbots gilt es zu klären, welche zulässigen Reaktionen den Staaten z.B. gegen Netzwerkattacken nicht-staatlicher Akteure zur Verfügung stehen (etwa die sog. „hackback"-Verteidigung). Dabei ist fraglich, welche Gegenmaßnahmen ein Staat dulden muss, von dessen Territorium Computerattacken ausgehen, die er sich nicht zurechnen lassen muss.[57]

Letztlich bleibt der Staat Dreh- und Angelpunkt für die Sicherheit im Cyberspace, was bei der Diskussion um die Globalität von Cyberbedrohungen leicht aus dem Blickfeld gerät. Denn die Server, Router und Glasfaserkabel, über welche die Bits und Bytes der Internetkommunikation oder die Trojaner verseuchter Computerprogramme transportiert werden, befinden sich an geographisch lokalisierbaren Standorten. Dort gelten die Gesetze des betreffenden Staates, an welche Unternehmen und Provider gebunden sind. Allein der Staat kann Regelungen gegenüber Administratoren und Providern durchsetzen, um den Zugang zu den Datennetzen zu reglementieren, das Internet zu blockieren bzw. zu filtern oder Botnetze abzuschalten. Schließlich sind die Staaten gefordert, wenn es um die internationale Regelbildung für die Cybersphäre (*Cyber Codes of Conduct*, technisches *Standard Setting*, vertrauensbildende Maßnahmen, Netzüberwachungsmaßnahmen, Frühwarnmechanismen etc.) geht. Hierzu bedarf es entsprechender Koordinierung und Abstimmung auf der Ebene der Vereinten Nationen oder der NATO.[58]

Der amerikanische Politologe *Joseph Nye* hat den Cyberspace unlängst mit den städtischen Handelsmessen des ausgehenden Mittelalters verglichen, die neben den bestehenden feudalherrschaftlichen Strukturen ko-existierten und neuen Wohlstand schufen.[59] So wie die Kaufleute des Mittelalters bestimmte Verhaltensregeln für den Geschäftsverkehr (*lex mercatoria*) entwickelten, so entstehen heute Verhaltensregeln (*codes of conduct*) für die Nutzung des Internets. Digitalisierte Formen der Auseinandersetzung werden sich freilich ebenso wenig vermeiden lassen, wie die Handelskriege der Vergangenheit. Doch verbindliche Normen sind indes Voraussetzung, um virtuelle und reale Kriege zu humanisieren.

IV. Zum Tagungsband

Der vorliegende Band ist das Ergebnis einer interdisziplinären Tagung an der *Bundesakademie für Sicherheitspolitik*, die in Zusammenarbeit mit der *Deutschen Gesellschaft für Wehrrecht und Humanitäres Völkerrecht* sowie der *Karl-Theodor-*

57 Näher *Tobias Plate*, Völkerrechtliche Fragen bei Gefahrenabwehrmaßnahmen gegen Cyber-Angriffe, in: Zeitschrift für Rechtspolitik 2011, S. 200-202 (201).

58 *Standard Setting* im Cyberbereich betreiben etwa das *Cooperative Cyber Defence Center of Excellence* in Tallin/Estland sowie die *Europäische Agentur für Netz- und Informationssicherheit* (ENISA) in Heraklion/Kreta.

59 *Joseph Nye*, Macht im 21. Jahrhundert, München 2011, S. 182.

Molinari-Stiftung, Bildungswerk des Deutschen BundeswehrVerbandes am 11. November 2010 in Berlin durchgeführt wurde. Der Einladung folgte ein großer Kreis von Experten aus Wissenschaft, Ministerien, Parlament, Militär, Medien und Rüstungsindustrie.

Mit der übergreifenden Thematik der „Automatisierung und Digitalisierung des Krieges" sollen zwei unterschiedliche, aber gleichwohl symptomatische Phänomene des Hightech-Krieges inhaltlich zusammengeführt und aus dem Blickwinkel der Sozialwissenschaft, der Ethik, der Sicherheitspolitik und des Völkerrechts analysiert werden. Ziel der Veranstaltung und dieses Tagungsbandes ist es, die sich noch immer in Fachzirkeln bewegende Debatte über Cyber War und Drohnenkrieg durch eine interdisziplinäre Betrachtung zu bereichern und die immer noch recht überschaubare deutschsprachige Fachliteratur mit einer Gesamtschau der einzelnen Aspekte der Thematik abzurunden.

Der vorliegende Tagungsband befasst sich im ersten Teil mit Fragen der Automatisierung des Krieges: *Peter Singer* handelt die ethischen Aspekte der Roboterkriegsführung ab; *Niklas Schörnig* befasst sich mit der Entwicklung unbemannter Waffensysteme aus sozialwissenschaftlicher und sicherheitspolitischer Sicht; *Thilo Marauhn* analysiert die humanitär-völkerrechtlichen und rüstungskontrollrechtlichen Aspekte eines Einsatzes von Kampfdrohnen und *Thomas Petermann* beleuchtet vor dem Hintergrund einer Untersuchung des Büros für Technikfolgenabschätzung des Deutschen Bundestages zur militärischen Nutzung von UAVs die Relevanz der Thematik für den parlamentarisch-politischen Raum.[60]

Der zweite Teil widmet sich der Digitalisierung des Krieges: *Sandro Gaycken* analysiert den Begriff Cyber War und den Cyberspace aus dem Blickwinkel von Philosophie und IT-Sicherheit und beleuchtet schwerpunktmäßig das Problem der Attribution; *Friedrich-Wilhelm Kriesel* betrachtet Cyber War als ein gesamtstaatlich-sicherheitspolitisches Problem; *Olaf Theiler* befasst sich mit Cyber-Defense im Rahmen der NATO und ihrem neuen Strategischen Konzept; *Wolff Heintschel v. Heinegg* analysiert Computernetzwerkattacken aus Sicht des humanitären Völkerrechts und des Neutralitätsrecht und *Charles Williamson* bewertet schließlich Cyberattacken aus der Rechtssicht der Vereinigten Staaten von Amerika insb. mit Blick auf die Einhaltung humanitär-völkerrechtlicher Bestimmungen.

Wir danken den zahlreichen Autoren für ihre bereichernden Beiträge zu diesem Tagungsband und wir danken dem Nomos Verlag sowie der Karl-Theodor-Molinari-Stiftung, Bildungswerk des *Deutschen BundeswehrVerbandes*, für die Aufnahme dieser Veröffentlichung in die Schriftenreihe „Forum Innere Führung".

Berlin, im Januar 2012 Die Herausgeber

60 Vgl. dazu auch BT-Drs. 16/12481, S. 1 ff.