Präventive Rüstungskontrolle – Möglichkeiten und Grenzen mit Blick auf die Digitalisierung und Automatisierung des Krieges

Marcel Dickow, Mischa Hansel, Max M. Mutschler*

Abstract: While the digitalization and automation of war has increased the demand for preventive arms control, no such regimes have emerged yet. Building on regime theory and empirical observations from the case of Anti-Ballistic Missile (ABM) arms control, this article explores whether or not regime-building is feasible in the cases of cyberwar and robotics respectively. Due to problems to define "cyberweapons" and to verify their use, banning specific information technologies is hardly achievable. Instead, regime-building should rely on international norms against certain behavior in cyberspace. In the case of the automation of warfare, preventive arms control is feasible, but leading states would need to learn more about the negative consequences of unhindered arms competition.

Keywords: Preventive arms control, cyberspace, robotics, regime theory
Schlagworte: Präventive Rüstungskontrolle, Cyberspace, Robotik, Regimetheorie

1. Einleitung

Kerngedanke der „präventiven" Rüstungskontrolle ist, dass das Sicherheitsdilemma auch eine qualitative Dimension hat. Oft ist es der technologische Vorsprung, der über Sieg und Niederlage in bewaffneten Konflikten entscheidet. Entsprechend groß ist der Anreiz für Staaten in die Entwicklung neuester Waffentechnologie zu investieren, auch wenn dadurch die Bedrohungswahrnehmung anderer Staaten steigt. Es können Rüstungswettläufe und die Proliferation entsprechender Waffensysteme folgen, sodass am Ende die Sicherheit aller leidet. Befürworter des Konzepts der präventiven Rüstungskontrolle plädieren deshalb für eine vorausschauende Analyse technologischer Entwicklungen und für eine Kontrolle aller Entwicklungsphasen, die ein Waffensystem durchläuft. Optimalerweise werden so technologische Rüstungswettläufe bereits in den Phasen der *Forschung* und *Entwicklung* verhindert. Auf jeden Fall muss die Kontrolle noch vor der *Beschaffung* und *Stationierung* der Waffensysteme erfolgen.[1]

Vor dem Hintergrund einer sich beschleunigenden technologischen Entwicklung, insbesondere in der Robotik und Informationstechnologie, gibt es gegenwärtig mehr denn je einen Bedarf für präventive Rüstungskontrolle. Dennoch kann man kaum entsprechende Entwicklungen in diesen Bereichen beobachten. Vielmehr haben wir es mit „Nicht-Regimen" zu tun. Das heißt, es gibt bisher keine problemfeldbezogenen Institutionen, die mittels impliziten oder expliziten Prinzipien, Normen, Regeln und Entscheidungsprozeduren die wechselseitigen Verhaltenserwartungen der Akteure in Übereinstimmung bringen.[2]

Dieser Artikel sucht nach Erklärungen für das Phänomen der Nicht-Regime im Bereich der präventiven Rüstungskontrolle, um auf dieser Grundlage über die Tragfähigkeit des Konzeptes für die Sicherheitspolitik im 21. Jahrhundert urteilen zu können. Was sind die zentralen Kooperationshindernisse? Wie können sie überwunden werden? Dazu werden zunächst auf der Grundlage theoretischer Überlegungen aus der Regimetheorie in Kombination mit der Analyse der erfolgreichen Regimebildung im Fall der Raketenabwehr während des Kalten Krieges einige zentrale Erfolgsbedingungen für das Entstehen internationaler Regime zur präventiven Rüstungskontrolle herausgearbeitet. Anschließend werden die beiden Technologiefelder „Cyber" und „Robotik" auf Erfolgsaussichten analysiert.

2. Regimetheorie und präventive Rüstungskontrolle[3]

Eine wichtige Rolle für die Erfolgsaussichten internationaler Regimebildung spielen in der Regimetheorie sogenannte Situationsstrukturen, die sich aus der spieltheoretischen Modellierung realer Situationen ergeben.[4] Zur Erklärung von Rüstungswettläufen wird vor allem auf zwei Spielsituationen zurückgegriffen. Erstens auf das Gefangenendilemma, bei dem sich die Akteure durch beidseitige Kooperation besserstellen können. Die Kooperation kann aber daran scheitern, dass die

* Marcel Dickow leitet die Forschungsgruppe Sicherheitspolitik der Stiftung Wissenschaft und Politik (SWP), Mischa Hansel ist wissenschaftlicher Mitarbeiter am Institut für Politikwissenschaft der Justus-Liebig-Universität Gießen, Max M. Mutschler ist wissenschaftlicher Mitarbeiter am Bonn International Center for Conversion (BICC).
Dieser Artikel wurde doppelt-blind begutachtet (double-blind peer-reviewed).

1 Götz Neuneck/Reinhard Mutz (Hrsg.), Vorbeugende Rüstungskontrolle. Ziele und Aufgaben unter besonderer Berücksichtigung verfahrensmäßiger und institutioneller Umsetzung im Rahmen internationaler Rüstungsregime, Baden-Baden 2000 (Nomos); Jürgen Altmann, Präventive Rüstungskontrolle, in: Die Friedens-Warte 83 (2008) 2-3, S. 105-126, 105-107.

2 Zum Konzept des „International Nonregimes" siehe Radoslav S. Dimitrov et al., International Nonregimes. A Research Agenda, in: International Studies Review 9 (2007) 2, S. 230-258. Zum ursprünglichen Konzept des „internationalen Regimes" siehe Stephen D. Krasner, Structural Causes and Regime Consequences. Regimes as Intervening Variables, in: Stephan D. Krasner (Hrsg.), International Regimes, Ithaca, NY 1982 (Cornell University Press), S. 1-21.

3 Dieses Kapitel stützt sich auf eine längere Studie zu den Erfolgsbedingungen präventiver Rüstungskontrolle: Max M. Mutschler, Arms Control in Space. Exploring Conditions for Preventive Arms Control, Basingstoke 2013 (Palgrave Macmillan).

4 Michael Zürn, Interessen und Institutionen in der internationalen Politik. Grundlegung und Anwendungen des situationsstrukturellen Ansatzes, Opladen 1992 (Leske + Budrich).

Akteure die Entscheidung der anderen Seite nicht kennen.[5] Im Fall der präventiven Rüstungskontrolle besteht die Kooperation darin, dass die Akteure vereinbaren, sich bei der Entwicklung neuer Rüstungstechnologien zurückzuhalten. In der spieltheoretischen Modellierung (siehe Abbildung 1), entspricht dies dem Ergebnis 2,2. So kann ein kostspieliger und gefährlicher Rüstungswettlauf (1,1) vermieden werden. Da sich aber beide Staaten nicht sicher sein können, dass sich die andere Seite auch daran hält, fällt dies schwer.

Abbildung 1: Gefangenendilemma[6]

		Staat A	
		rüsten	nicht rüsten
Staat B	rüsten	1,1	3,0
	nicht rüsten	0,3	2,2

Da die Staaten allerdings die wechselseitige Kooperation bevorzugen, kann dieses Problem mit Hilfe einer Tit-for-Tat-Strategie überwunden werden. Das heißt, Nicht-Kooperation wird mit Nicht-Kooperation, Kooperation mit Kooperation beantwortet.[7] Die Langwierigkeit des Prozesses zur Entwicklung neuer Waffensysteme gibt den Staaten diese Reaktionszeit. In einer Situation, die dem Gefangenendilemma entspricht, ist Kooperation also nicht einfach, aber eben dennoch möglich. Wesentlich schwieriger ist dies hingegen in einer sogenannten Deadlock-Situation (siehe Abbildung 2).[8] Hier ziehen die Staaten die beidseitige Nicht-Kooperation (2,2) der beidseitigen Kooperation (1,1) vor. Das heißt, sie rüsten auf, auch in dem Wissen, dass die Gegenseite nachziehen wird. Sie versprechen sich von einem Rüstungswettlauf einen größeren Sicherheitsgewinn, als von wechselseitiger Zurückhaltung.

Abbildung 2: Deadlock-Situation

		Staat A	
		rüsten	nicht rüsten
Staat B	rüsten	2,2	3,0
	nicht rüsten	0,3	1,1

In einer solchen Deadlock-Situation befanden sich die USA und die Sowjetunion während des Kalten Krieges im Hinblick auf die Entwicklung von Anti-Ballistic Missiles (ABMs), Raketen zur Abwehr von ballistischen Raketen. Beide hatten bereits kurz nach Ende des Zweiten Weltkriegs mit der Erforschung der ABM-Technologie begonnen. Das nukleare Wettrüsten, vor allem die Entwicklung von ballistischen Interkontinentalraketen, verleitete sie zu der Ansicht, mit der Entwicklung von ABM-Systemen ihre nationale Sicherheit erhöhen zu können. Sowohl die Sowjetunion wie auch die USA entwickelten unterschiedliche ABM-Systeme und testeten diese mehrfach. So etwa das amerikanische Nike-X-System oder das sowjetische Galosh-System. Das Wissen um die Rüstungsanstrengungen der Gegenseite beförderte den Wettstreit der Entwicklungsteams auf beiden Seiten.[9]

Bis zur Mitte der 1960er Jahre befanden sich die USA und die Sowjetunion in einer Deadlock-Situation. Dennoch einigten sie sich 1972 auf den ABM-Vertrag, der ihnen nur die Stationierung einer sehr begrenzten Anzahl von landgestützten Abfangraketen an lediglich zwei Orten erlaubte und die Entwicklung, das Testen und die Stationierung von see-, luft- und weltraumgestützten sowie mobilen landgestützten ABM-Systemen verbot. Damit hatte der Vertrag eine klare präventive Wirkung. Zusätzlich zu den direkten Verboten bestimmter neuer Technologien machte die zahlenmäßige und geografische Begrenzung existierender ABM-Systeme deren weitere Produktion und Modernisierung unattraktiv. So konnte die Rüstungsdynamik zwischen den Supermächten in diesem Bereich eingehegt werden.[10]

Das widerlegt nicht die Überlegung, dass Kooperation in Deadlock-Situationen nicht zu erwarten ist. Vielmehr verweist diese Entwicklung darauf, dass wir die Präferenzen der Akteure nicht als exogen gegeben und unveränderbar betrachten dürfen. Widersprüche zwischen Zielen und Mitteln können Staaten dazu bewegen, zu lernen und ihre nationalen Interessen neu zu definieren.[11] Maßgeblich angetrieben durch eine national wie international gut vernetzte „epistemische Gemeinschaft" von Naturwissenschaftlern und Experten für Nuklear-Strategie setzte sich zunächst in den USA die Ansicht durch, dass ein ABM-Wettrüsten, trotz der Überlegenheit der USA bei der ABM-Technologie, negative Auswirkungen auf die nationale Sicherheit hätte. Ein technologischer Durchbruch bei der Raketenabwehr könnte dazu beitragen, die nukleare Zweitschlagsfähigkeit des Gegners zu schwächen und die Abschreckung zu unterwandern. Vermittelt durch den wissenschaftlichen Austausch zwischen den US-Wissenschaftlern mit ihren sowjetischen Kollegen setzte sich diese Sichtweise dann auch in der Sowjetunion durch.[12] Damit entsprach die Situation nicht mehr dem Deadlock-Spiel, sondern einem Gefangenendilemma. Wechselseitige Kooperation wurde zum erstrebenswerten Ziel.

Es bleiben allerdings noch sogenannte Kooperationsprobleme zweiter Ordnung, die eine Lösung des grundsätzlichen Kooperationsproblems (erster Ordnung), in diesem Fall die Überwindung des Gefangenendilemmas mit Hilfe von Tit-for-Tat-Strategien, behindern.[13] Ein solches Kooperationsproblem zweiter Ordnung stellt das rechtzeitige Erkennen von Nicht-Kooperation (Vertrauensproblem) dar. Deshalb haben sich im Zusammenhang mit Rüstungskontrollregimen zumeist auch Regeln für die Verifikation herausgebildet, die entweder auf

5 Siehe zum Beispiel Harald Müller/Niklas Schörnig, Rüstungsdynamik und Rüstungskontrolle. Eine exemplarische Einführung in die Internationalen Beziehungen, Baden-Baden 2006 (Nomos), S. 40-47.

6 In dieser spieltheoretischen Modellierung steht der Wert 3 für die erste und der Wert 0 für die letzte Präferenz des jeweiligen Akteurs.

7 Robert M. Axelrod, The Evolution of Cooperation, New York 1984 (Basic Books).

8 George W. Downs et al., Arms Races and Cooperation, in: World Politics 38 (1985) 1, S. 118-146.

9 David S. Yost, Soviet Ballistic Missile Defense and the Western Alliance, Cambridge, MA 1988 (Harvard University Press); Earnest J. Yanarella, The Missile Defense Controversy. Strategy, Technology, and Politics, 1955-1972, Lexington, KY 1977 (University Press of Kentucky).

10 Mutschler, Arms Control in Space, S. 78-83.

11 Joseph S. Nye, Nuclear Learning and U.S.–Soviet Security Regimes, in: International Organization 41 (1987) 3, S. 371-402.

12 Emmanuel Adler, The Emergence of Cooperation. National Epistemic Communities and the International Evolution of the Idea of Nuclear Arms Control, in: International Organization 46 (1992) 1, S. 101-145; Bernd W. Kubbig, Wissen als Machtfaktor im Kalten Krieg. Naturwissenschaftler und die Raketenabwehr der USA, Frankfurt/New York 2004 (Campus Verlag), S. 163-322.

13 Bernhard Zangl, Interessen auf zwei Ebenen. Internationale Regime in der Agrarhandels-, Währungs- und Walfangpolitik, Baden-Baden 1999 (Nomos), S. 68-73.

Vor-Ort-Inspektionen oder auf jeweils nationale Fähigkeiten zur Informationsbeschaffung (national technical means), wie zum Beispiel Aufklärungssatelliten, setzen. Bei der präventiven Rüstungskontrolle ist die Verifikation jedoch besonders schwierig, da es um Technologien in der Entwicklungsphase geht. Forschung im Allgemeinen ist ambivalent (dual-use), und ihre Kontrolle schürt den Spionageverdacht. Hinzu kommt, dass der Verbotstatbestand überhaupt erst einmal definiert sein muss.

Mit dem Vertrauensproblem geht also ein Definitionsproblem einher, insbesondere bei Technologien ohne eindeutige Bestimmung. Zweckbasierte Definitionen können Abhilfe schaffen. Im Falle des ABM-Vertrags wurden Raketen und Radaranlagen nur dann als Teile eines ABM-Systems betrachtet, wenn sie für diesen Zweck konstruiert und stationiert oder dafür getestet wurden. Die Entwicklung von Radar- und Raketentechnologie für die Raumfahrt blieb dadurch unbeeinträchtigt. Dieses Beispiel zeigt, dass es wenig Sinn macht, präventive Rüstungskontrolle als Verbot kompletter Technologiezweige zu konzipieren. Zielführender ist es, nur ganz bestimmte Technologien zu verbieten, welche im Hinblick auf eine militärische Nutzung entwickelt werden. Dies schließt eine Weiterentwicklung der Technologie im zivilen Bereich nicht aus.

Ein weiteres Kooperationsproblem zweiter Ordnung ist das Verteilungsproblem, wenn die entscheidenden Staaten sich auf unterschiedlichem technologischem Niveau befinden und deswegen der Kooperationsgewinn ungleich verteilt ist. Auf den ersten Blick würde der technologisch überlegene Staat durch Einschränkungen in diesem Bereich benachteiligt. So verfügten die USA zwar bereits in den 1960er Jahren über die besseren technologischen Voraussetzungen für die Entwicklung von anti-ballistischen Raketen,[14] dennoch schlugen sie der Sowjetunion vor, die ABM-Rüstung zu begrenzen. Auf amerikanischer Seite hatte sich die Überzeugung durchgesetzt, dass die Risiken der neuen Technologie zu groß sind. Dem Aspekt der ausgeglichenen Gewinne konnte dann dadurch Rechnung getragen werden, dass sich die beiden Supermächte parallel auf eine Begrenzung der Interkontinentalraketen (Strategic Arms Limitation Talks, SALT, 1969-1972) verständigen konnten. Hier war die Sowjetunion gerade dabei neue schwere Raketen zu bauen und die USA hatten ein Interesse daran, dies einzudämmen. Eine solche Verknüpfung verschiedener Themen („issue-linkage") kann also helfen, das Verteilungsproblem zu lösen.

Es ist also vor allem die Einsicht der beteiligten Akteure in die Sicherheitsgewinne, die präventive Rüstungskontrolle möglich macht. Wenn sich diese Sichtweise bei einem der entscheidenden Akteure ändert, dann kann das entsprechende Regime wieder zusammenbrechen. Auch dies illustriert die Geschichte des ABM-Regimes mit der Aufkündigung des Vertrags durch die USA im Dezember 2001.

3. Cyberspace

Moderne Gesellschaften sind in hohem Maße von vernetzten Informationsinfrastrukturen abhängig. Allein deshalb sollten alle Staaten ein gemeinsames Grundinteresse an der Begrenzung der Entwicklung, der Erprobung und Verbreitung von hochwirksamen Schadprogrammen haben. Hinzu kommt, dass der Cyberspace im besonderen Maße Fehlkalküle und unbeabsichtigte Eskalation begünstigt.[15] Ein internationales Regime präventiver Rüstungskontrolle wäre daher grundsätzlich wünschenswert. Allerdings setzt keiner der relevanten staatlichen Akteure gegenwärtig auf die genuinen Instrumente präventiver Rüstungskontrolle. Die USA weisen Verbote technologischer Fähigkeiten sowie völkerrechtliche Verträge als für das Problemfeld Cybersicherheit ungeeignet zurück. Genauso wie die Staaten der Europäischen Union präferieren sie die Ausbildung von Verhaltensstandards und -normen.[16] Russland, China und andere Mitglieder der Shanghai Cooperation Organization (SCO) streben zwar eine völkerrechtliche Ächtung von sogenannten „information weapons" an,[17] dahinter verbirgt sich jedoch kein Verbot von Technologie, sondern von unliebsamen Internetinhalten, etwa regimekritischen Äußerungen.[18]

Mit Blick auf das Kooperationsproblem erster Ordnung könnte daher eine Deadlock-Situation vorliegen, insofern das Nichtregime aus einem mangelnden politischen Kooperationswillen der Staaten resultiert. Allerdings weisen nicht nur die USA, sondern zahlreiche unabhängige Experten auf eine Reihe praktischer Probleme hin, wie insbesondere die Definition und Verifikation etwaiger technischer Beschränkungen. Zunächst einmal führt der Versuch der Definition einer „Cyberwaffe" ins Leere.[19] Unautorisierte Zugriffe auf Computernetzwerke basieren nicht auf physischer Feuerkraft, sondern auf dem Wissen über technische Sicherheitslücken und fehleranfällige Organisationsroutinen. Der Erwerb solchen Wissens kann schwerlich verboten und sanktioniert werden. Ein solcher Ansatz würde überdies jegliche defensive Planungen konterkarieren, da die Verteidigung im Cyberspace dasselbe Wissen voraussetzt wie der Angriff.[20] Umso größer wäre der Nutzen desjenigen, der gegen eine solche Abmachung verstößt.

Im Lichte dessen ist man auf der Suche nach Alternativen. Tatsächlich hat sich in den letzten Jahren ein internationaler Konsens über die Notwendigkeit gemeinsamer Normen und vertrauensbildender Maßnahmen (VBMs) in der Cybersicherheit herausgebildet. Dies ist nicht zuletzt an der Mitwirkung russischer, chinesischer und US-amerikanischer Delegierter in hochrangig besetzten UN-Expertengruppen ablesbar.[21] Trotzdem ist der Weg hin zu entsprechenden Regeln steinig, denn Angreifer unterschiedlichster Intention – militärische, nachrichtendienstliche, kriminelle – verwenden nahezu identische

14 Mutschler, Arms Control in Space, S. 88-91.

15 Mischa Hansel, Internationale Beziehungen im Cyberspace. Macht, Institutionen und Wahrnehmung, Wiesbaden 2012 (VS Verlag), S. 291-338.

16 Annegret Bendiek, Europäische Cybersicherheitspolitik, Berlin 2012 (Stiftung Wissenschaft und Politik), S. 15.

17 United Nations General Assembly, International Code of Conduct for Information Security, A/66/359, 12.9.2011, S. 4.

18 Keir Giles/William Hagestad II, Divided by a Common Language. Cyber Definitions in Chinese, Russian and English, in: K. Podins/J. Stinissen/M. Maybaum (Hrsg.), 5th International Conference on Cyber Conflict. Proceedings, Talinn 2013 (NATO CCDCOE), S. 421.

19 James Andrew Lewis, Confidence-Building and International Agreement in Cybersecurity, in: Disarmament (2011) 4, S. 58.

20 Dorothy E. Denning, Obstacles and Options for Cyber Arms Control, in: Heinrich-Böll-Stiftung (Hrsg.), Rüstungskontrolle im Cyberspace, Berlin 2001, S. 36-37.

21 Die inzwischen dritte Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security nahm im Juli 2014 ihre Arbeit auf. Nähere Informationen und Dokumente unter http://www.un.org/disarmament/topics/informationsecurity/.

Instrumente. Technisch besteht kaum ein Unterschied zwischen dem Abschöpfen und dem Sabotieren von digitalen Daten.[22] Deswegen offenbart sich oft nur spät und nicht eindeutig, um welche Operation es sich handelt(e).[23] Nur in bestimmten Fällen lassen die betroffenen Systeme plausible Schlüsse auf die Motivation der Angreifer zu. Das Ausforschen der Steuerung der Elektrizitätsversorgung verspricht z.B. weder Nachrichtendiensten noch der organisierten Kriminalität größeren Nutzen. Solche Operationen deuten vielmehr auf eine militärische Zielplanung hin. Deswegen wird vorgeschlagen, Computernetzwerkattacken (CNAs) auf solche kritischen Infrastrukturen rüstungskontrollpolitisch zu tabuisieren.[24]

Gravierender noch als die Unterscheidung legitimer und illegitimer Ziele ist die annähernde Unmöglichkeit verlässlicher Attribution komplexer CNAs. Kein staatlicher Angreifer ist bislang zweifelsfrei überführt worden. So kann der Tit-for-Tat-Mechanismus nicht greifen. Um die Attributionsproblematik zu umgehen, wurde insbesondere von US-amerikanischer Seite das Prinzip der Staatenverantwortung in die Diskussion eingebracht.[25] Demnach wäre jeder Staat verpflichtet, sämtliche CNAs aus seinem Souveränitätsbereich heraus zu unterbinden sowie zur Aufklärung solcher Vorfälle beizutragen. Ein entsprechendes Regime könnte auch Sanktionsmöglichkeiten, z.B. „Black-Listing" bestimmter Provider oder Exportbeschränkungen,[26] vorsehen, um die Kosten für eine Kooperationsverweigerung in die Höhe zu treiben.

Die Norm der Staatenverantwortung wurde inzwischen sowohl von der UN Group of Governmental Experts als auch in informellen US-chinesischen Konsultationen unterstützt.[27] Über das Monitoring sowie die Sanktionierung von Verstößen besteht indes noch kein Konsens. Weniger kontrovers sind eine Reihe vertrauensbildender Maßnahmen, deren Wirksamkeit keine unmittelbare Verifikation voraussetzt: Die Offenlegung von organisatorischen Kompetenzen und Verfahren, der Austausch militärischer Doktrinen, die Einrichtung von Routinen zum Informationsaustausch in Krisenfällen, die Notifikation von Cyberabwehrübungen oder gemeinsame Simulationen und Workshops.[28] Solche Maßnahmen sind u.a. von der UN Group of Governmental Experts und der OSZE vorgeschlagen worden.[29] Bilateral haben Russland und die USA 2013 u.a. Kontaktpunkte zwischen ihren jeweiligen Computer Emergency Response Teams (CERTs) sowie eine direkte Verbindung zwischen dem Weißen Haus und dem Kreml im Falle von größeren CNAs eingerichtet.[30]

Weniger gravierend ist die Frage der Gewinnverteilung. Während die USA (noch) über ungleich größere Budgets, einen technologischen Vorsprung sowie einen privilegierten Zugang zu global operierenden Internetkonzernen verfügen, werden China und Russland geringere legale Restriktionen sowie die Vereinnahmung von Forschungsinstituten, Staatskonzernen, der organisierten Kriminalität und sogenannten ‚patriotischen' Hackervereinigungen zugeschrieben.[31] Schließlich muss die Dimension der Verwundbarkeit mitberücksichtigt werden. Ihr zufolge würde die Wirtschaft der USA aufgrund ihrer starken Abhängigkeit vom Internet im Falle einer ungebremsten Militarisierung des Cyberspace den größten Schaden davontragen.[32]

Es gibt damit Machtasymmetrien, die aufgrund ihrer Implikationen für die jeweils zu erwartende Gewinnverteilung verschiedener institutioneller Designs ein Verteilungsproblem hervorrufen. Aber aufgrund der Multifunktionalität von Schadprogrammen und der Interdependenz von Nutzungschancen, insbesondere im Internet, lassen sich diverse Kopplungsgeschäfte mittels internationaler Regulierung denken. Beispielsweise könnten Normen, die die USA im Einsatz überlegener CNA-Fähigkeiten beschränken würden, mit einem Beitritt Russlands und Chinas zur Konvention gegen Cyberkriminalität des Europarates kombiniert werden.[33] Andere Varianten eines Paketgeschäftes wären hingegen aus demokratisch-normativer Perspektive inakzeptabel. Insbesondere sperren sich westliche Staaten gegen eine internationale Legitimierung und Durchsetzung politischer Zensur von Webinhalten im Austausch für Konzessionen Chinas, Russlands und anderer autoritärer Staaten.[34]

Grundsätzlich erschwert der Mangel an akteursübergreifendem Wissen die Identifikation von Interessengemeinsamkeiten und -gegensätzen. Allerdings bemühen sich etwa das China Institute of Contemporary International Relations (CICIR) und das US-amerikanische Center for Strategic and International Studies (CSIS) seit 2009 mittels regelmäßiger bilateraler Treffen („Sino-U.S. Cybersecurity Dialogue") unter Beteiligung von Regierungsvertretern um einen Abbau von Missverständnissen und Spannungen sowie die Identifizierung von Kooperationschancen.[35] In Europa wären beispielsweise die von UNIDIR koordinierten Aktivitäten (Cyber Index, Workshops) zu nennen.[36] Man kann diese und andere Foren durchaus als Nukleus einer entstehenden epistemischen Gemeinschaft

22 William A. Owens/Kenneth W. Dam/Herbert S. Lin, Technology, Policy, Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, Washington, DC 2009 (The National Academies Press), S. 20, 81, 315-317.
23 Lewis, Confidence-Building, S. 56-57
24 Götz Neuneck, Towards TCBMS in the Cybersphere, in: UNIDIR (Hrsg.), The Cyber Index. International Security Trends and Realities, New York/Genf 2010, S. 136-137; Andrew Rathmell, Controlling Computer Network Operations, in: Information and Security 7 (2001) 1, 212-144.
25 Siehe dazu Richard A. Clarke/Robert K. Knake, Cyberwar. The Next Threat to National Security and What to Do about It, New York 2010 (Harper/Collins), S. 249-255.
26 Clarke/Knake, Cyberwar, S. 249-255.
27 United Nations General Assembly, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/69, 24.06.2013, S. 8; Dong Qingling, Confidence Building for Cybersecurity between China and the United States, China Institute of International Studies, 23.09.2014, http://www.ciis.org.cn/english/2014-09/23/content_7254470.htm.
28 Neuneck, Towards TCBMS in the Cybersphere, S. 137; Lewis, Confidence-Building, S. 58-59; Katharina Ziolkowski, Confidence Building Measures for Cyberspace – Legal Implications, Talinn 2013 (NATO CCDCOE).
29 United Nations General Assembly, Report of the Group of Governmental Experts.
30 The White House, Fact Sheet. U.S.-Russian Cooperation on Information and Communications Technology Security, 17.06.2013, Washington DC, http://www.whitehouse.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol.
31 Alexander Klimburg, Mobilising Cyber Power, in: Survival 53 (2011) 1, S. 41-60.; Audrey K. Cronin, Cyber-Mobilization. The New Levée en Masse, in: Parameters 36 (2006) 2, S. 77-87
32 Clarke/Knake, Cyberwar, S. 144-149.
33 Es handelt sich um den bislang einzigen völkerrechtlichen Vertrag im Bereich der Cybersicherheit. Neben zahlreichen europäischen Staaten haben auch Australien, die Dominikanische Republik, Japan, Mauritius, Panama sowie die USA den Vertrag ratifiziert.
34 Alexander Klimburg, Roots Unknown: Cyberconflict Past, Present & Future, in: Sicherheit + Frieden 32 (2014) 1, S. 4.
35 CICIR/CSIS, Bilateral Discussions on Cooperation in Cybersecurity, June 2012, http://csis.org/files/attachments/120615_JointStatement_CICIR.pdf.
36 Siehe http://www.unidir.org/programmes/emerging-security-threats/perspectives-on-cyber-war-legal-frameworks-and-transparency-and-confidence-building und http://www.unidir.org/programmes/emerging-security-threats/the-cyber-index-tool.

deuten. Die wichtigste und vorderste Aufgabe wäre zunächst die Verständigung über gemeinsame Grundbegriffe.[37]

4. Robotik/Drohnen

Vergleichsweise einfach scheint es hingegen im Bereich unbemannter, ferngesteuerter und autonomer Waffensysteme zu sein, vorausschauende Reglementierungen zu finden. Auf den ersten Blick werden hier tatsächlich physische Plattformen entwickelt, deren technologische Eigenschaften – wie etwa die Abwesenheit einer Besatzung, der Grad der Automatisierung, die Art der Bewaffnung usw. – charakteristisch genug erscheinen, um Ansatzpunkte für präventive Rüstungskontrolle, für Verbote und Beschränkungen zu liefern. Auf den zweiten Blick offenbaren sich Zweifel, ob die neue Qualität der Technologie durch ihren physischen Träger oder doch vielmehr durch die auf ihm ablaufenden Algorithmen zustande kommt.

Wer über Roboter-Rüstungskontrolle nachdenkt kommt nicht umhin, über die Einstiegsdroge[38] der militärischen Robotik, die Drohnen zu schreiben. Wie kaum eine andere Technologieplattform haben sich unbemannte, ferngesteuerte, fliegende Systeme in den letzten Jahren verbreitet. Nach einem Bericht des Government Accountability Office (GAO) aus dem Jahr 2012[39] verfügen rund 80 Staaten auf der Welt über unbemannte Flugsysteme (Unmanned Aerial Systems, UAS). Noch ist die Zahl der Länder klein, die diese auch bewaffnen können (USA, UK, Israel; vermutlich auch China und Russland). Der Trend zeigt aber nach oben. Im Bereich militärischer UAS zeichnen sich zudem zwei Entwicklungen ab: Erstens werden Plattformen und die Auswertung ihrer Sensordaten stärker automatisiert und führen zu einem höheren Autonomiegrad des Gesamtsystems. Zweitens bietet die zunehmende Miniaturisierung einzelner Systeme die Möglichkeit, ganze Schwärme von fliegenden Robotern einzusetzen, die untereinander vernetzt sind. Digitalisierung, Miniaturisierung und Autonomisierung überführen also heutige ferngesteuerte Systeme in zukünftig (teil-)autonom funktionierende Roboter.

Robotik hat das Potenzial, sowohl die Art der Kriegführung als auch den vorgelagerten Entscheidungsprozess zu beeinflussen. Im Hinblick auf die Kriegführung dominieren bei den technologisch führenden Staaten Szenarien, in denen robotische Systeme militärische und taktische Vorteile generieren. Die Distanzierung vom Gefechtsfeld und der damit einhergehende Schutz eigener Kräfte, Geschwindigkeitsvorteile durch maschinelle Reaktionen sowie das Vermeiden von Latenzzeiten bei Fernsteuerung, zählen zu den Hauptargumenten der Robotik-Befürworter.[40] Gleichzeitig eröffnet die Robotik auch strategische Optionen, z.B. den Konflikt in Regionen zu tragen oder auf sie auszuweiten, die bislang nicht erreichbar waren. Hierfür werden Drohnen bereits benutzt, z.B. im U.S.-amerikanischen Anti-Terror-Kampf. Neue militärische Planungen sehen vor, zukünftige Drohnengenerationen z.B. als radargetarnte, luftbetankbare, auf Flugzeugträgern stationierte Bomber einzusetzen.[41] Solche strategischen Optionen, generell aber die Möglichkeit militärische Gewalt ohne Risiko für das eigene Personal auszuüben, können die politische Hemmschwelle zum Einsatz von Gewalt beeinflussen.

Weder Drohnen noch Robotik allgemein unterliegen derzeit universellen rüstungskontrollpolitischen Beschränkungen.[42] Da es sich um eine ausgeprägte Dual-Use-Technologie handelt und weite Bereiche der Forschung und Technologieentwicklung durch die kommerzielle Industrie vorangetrieben werden, fallen generelle Technologieschranken, insbesondere plattform- und hardwarebasierte, aus. Dennoch erscheint ein Regime zur Regulierung und gegebenenfalls Beschränkung militärischer Robotik sinnvoll, da zwar die Technologienentwicklung schnell fortschreitet, serienreife Systeme aber rar sind und die Streitkräfte deshalb zögern, größere Beschaffungsvorhaben in die Tat umzusetzen. Vor allem die vertikale Proliferation, also die qualitative Weiterentwicklung der Robotik, in Staaten mit großen industriellen Kapazitäten und finanziellen Ressourcen, kann dabei regionale und globale Stabilität gefährden. Denn die neue Qualität der Art der Kriegführung mit Robotik wird militärische Gleichgewichte verschieben und einen Rüstungswettlauf in Gang setzen.

Derzeit spricht allerdings in der politischen Entwicklung um die militärische Robotik nicht viel für das Installieren präventiver Rüstungskontrolle. Technologisch führende Nationen im Bereich der Robotik, wie die USA, sehen in ihrem Vorsprung einen militärischen Vorteil. Staaten wie China und Russland streben danach, diesen aufzuholen. Im Rahmen der CCW Arbeitsgruppe zu Lethal Autonomous Weapons (LAW) haben die USA und Kanada im Mai 2013 in Genf deutlich gemacht, dass sie selbst an einer Einsatzbeschränkung zweifeln und das Konzept der Mindestvoraussetzung „bedeutender menschlicher Kontrolle“ („meaningful human control“) kritisch sehen.[43] Während sich hier europäische Staaten, insbesondere Frankreich und Deutschland, mit einiger Unterstützung aus Mittel- und Südamerika als Befürworter einer Einsatzbeschränkung im Rahmen des CCW hervorgetan haben, blieben China, Russland und andere bedeutende Wirtschaftsnationen im Hintergrund. Dieser Vorstoß im Rahmen des CCW krankt zudem an der Tatsache, dass sich der CCW,[44] anders als in der Präambel des Vertrages vermerkt, bislang ausschließlich auf Einsatzverbote, nicht aber auf Technologiebeschränkung bezieht. Gleichzeitig erscheint es wegen der vielfältigen technischen Gestalten der

37 Neuneck, Towards TCBMs in the Cybersphere, S. 133.

38 In Anlehnung an den Aufsatz von Frank Sauer, Einstiegsdrohnen. Zur deutschen Diskussion um bewaffnete unbemannte Luftfahrzeuge, in: Zeitschrift für Außen- und Sicherheitspolitik 7 (2014) 3, S. 343-363.

39 GAO, Nonproliferation. Agencies Could Improve Information Sharing and End-Use Monitoring on Unmanned Aerial Vehicle Exports, Washington, DC, http://www.gao.gov/products/GAO-12-536, S. 9.

40 André Haider, Remotely Piloted Aircraft Systems in Contested Environments – A Vulnerability Analysis, JAPCC Report, Kalkar 2014 (The Joint Air Power Competence Centre), http://www.japcc.org/publications/report/Report/JAPCC_RPAS_In_Contested%20_Environements.pdf, S. 101.

41 Siehe z.B. Niklas Schörnig, Unmanned Military Systems and the New Western Way of War, Vortrag gehalten auf der Unmanned Military Systems Conference, Berlin, Stiftung Wissenschaft und Politik, 23. 05. 2013.

42 Eine gute Übersicht bietet Wolfgang Richter, Rüstungskontrolle für Kampfdrohnen, *SWP Aktuell* 2013/A 29 , Berlin, http://www.swp-berlin.org/fileadmin/contents/products/aktuell/2013A29_rrw.pdf.

43 Ein guten Überblick gibt United Nations, Lethal Autonomous Weapons, The CCW Meeting of Experts on Lethal Autonomous Weapons Systems (LAWS), Geneva, 13-16 May 2014 (CCW/MSP/2014/3) Genf, http://www.unog.ch/80256EE600585943/(httpPages)/6CE049BE22EC75A2C1257C8D00513E26.

44 Siehe United Nations, Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects as amended on 21 December 2001, o. J., http://www.unog.ch/80256EDD006B8954/%28httpAssets%29/40BDE99D98467348C12571DE0060141E/$file/CCW+text.pdf.

Robotik nahezu unmöglich, einzelne Systeme oder Plattformen für Verbote zu definieren. Diese Definitionsproblematik hat den Ansatz hervorgebracht, Funktionsweisen robotischer Systeme, insbesondere das maschinelle Entscheiden zum (taktischen) Gewalteinsatz (im Feld) zu ächten. Wie die Diskussionen im Rahmen der Genfer Gespräche zeigen, ist diese Vorgehensweise aber umstritten.

Ein Ausweg könnte sein, Kombinationen von Fähigkeiten zu beschränken, wenn sie in einem Waffensystem, nicht notwendigerweise auf einer Plattform, vereint werden. Mit Hilfe eines Kriterienkatalogs könnten dann Schwellenwerte definiert werden, bei deren kumulativer Überschreitung ein Waffensystem verboten werden könnte. Solche Kriterien könnten z.B. die Art, Anzahl und Wirkungsweise der Waffen des „Roboters", die Art, Anzahl und Fähigkeit autonomer Funktionen, die Umsetzung von menschlicher Steuerung und Kontrolle sowie die Art und der Umfang sensorischer Wahrnehmung der Umwelt darstellen. Solch ein Ansatz könnte das Vertrauensproblem, insbesondere die Frage der Definition und Notifikationen, abschwächen. Es ist klar, dass das Verifikationsproblem wegen der software-basierten Grundlage autonomer Funktionen durch diese technische Klassifizierung nicht komplett gelöst werden kann. Allerdings könnten entlang unterschiedlicher Autonomie- und Bewaffnungsklassen abgestufte Verifikationsmechanismen, z.B. Vor-Ort-Inspektionen für bewaffnete Systeme, definiert werden, von denen nicht alle hohe Eindringtiefe und Souveränitätseinschränkungen aufweisen müssten.[45]

Auch wenn sich partielle Lösungen für prozedurale und technische Fragen finden lassen, bleibt der Unwillen technologisch führender Staaten wie den USA, überhaupt über Begrenzungen zu verhandeln. Derzeit fehlt eine staatenübergreifende, internationale Wahrnehmung gemeinsamer Interessen zur Initiierung Präventiver Rüstungskontrolle. An Anreizen dafür mangelt es sicher nicht. Die Robotik befördert Abhängigkeiten von digitaler Kommunikation. Noch stärker als bisher wird dadurch zivile und militärische Kommunikationsinfrastruktur zum Ziel von potenziellen Gegenmaßnahmen beim zukünftigen Einsatz von Robotik. Gleichzeitig planen westliche Streitkräfte schon jetzt den Einsatz von Robotern gegen diese selbst ein.[46] Eine qualitative Rüstungsspirale ist vor allem dort erkennbar, wo Geschwindigkeitsvorteile robotischer Systeme durch noch schnellere eigene, zwangsläufig autonome Systeme gekontert werden müssen. Eine Begrenzung dieser absehbaren Rüstungsdynamiken liegt auch im Interesse der USA, zumal Staaten wie China technologisch rasant aufholen. Dies schwächt das Verteilungsproblem deutlich ab. Auf dieses Bewusstsein aufbauend könnten internationale Verhandlungen beginnen und durch wechselseitige Moratorien zur Stationierung und zum Einsatz von LAW flankiert werden. Der technologische Fortschritt, allein in der zivilen Entwicklung, wird in den kommenden Jahren ausreichend Erfahrungsbasis liefern, um Definitionen, Verbotstatbestände und Einsatzbeschränkungen weiterzuentwickeln. Die besondere Herausforderung an die Präventive Rüstungskontrolle besteht bei der (teil-)autonomen Robotik darin, die Logik des militärischen Wettrüstens zu durchbrechen und dabei zivile Technologieentwicklung nicht unnötigerweise einzuschränken.

5. Schlussfolgerungen

Die Untersuchung der beiden Technologiefelder „Cyber" und „Robotik" hat gezeigt, dass es sinnvoll ist, die Instrumente und Erfahrungen aus der Geschichte der Rüstungskontrolle auch auf solche neuen, sich rasant entwickelnden Technologiebereiche anzuwenden. Allerdings sind auch die Probleme und Grenzen präventiver Rüstungskontrolle deutlich geworden. Dies illustriert insbesondere der Cyber-Fall. Hier ist es vor allem das Vertrauensproblem, das infolge der Schwierigkeiten bei der Definition von „Cyberwaffen" und den eingeschränkten Verifikationsmöglichkeiten das zentrale Kooperationshindernis darstellt. Selbst wenn es also gelingen sollte, die potenziell bestehende Deadlock-Situation („Wettrüsten im Cyberspace ist besser als Rüstungskontrolle") zu überwinden und zu einer Situation des Gefangenendilemmas zu kommen („Rüstungskontrolle im Cyberspace ist besser als ein Wettrüsten"), wäre es wohl für alle beteiligten Akteure schwierig, ein ausreichendes Maß an Vertrauen in die tatsächliche Zurückhaltung der anderen Akteure zu entwickeln, um sich auf die Bildung eines Regimes einzulassen. Eine sinnvolle Alternative für sicherheitspolitische Kooperation ist in diesem Fall die Etablierung von Normen und Regeln, nicht für die Begrenzung und Kontrolle bestimmter Technologien, sondern für deren Einsatz. So könnte beispielsweise eine Tabuisierung von CNAs auf kritische Infrastrukturen in Kombination mit einer Reihe von Transparenz- und Vertrauensbildenden Maßnahmen, wie etwa der Austausch über militärische Doktrinen oder die Einrichtung von Routinen zum Informationsaustausch in Krisenfällen, dazu beitragen, das Sicherheitsdilemma zumindest etwas zu entschärfen.

Daraus jedoch den Schluss zu ziehen, dass präventive Rüstungskontrolle, verstanden als die Kontrolle und Beschränkung bestimmter technologischer Entwicklungen, nicht machbar und daher auch irrelevant sei, wäre falsch. Dies zeigt die Untersuchung des Robotik-Falls.[47] Hier stehen die Chancen für präventive Rüstungskontrolle deutlich besser als im Cyber-Bereich. Sowohl das Vertrauens-, wie auch das Verteilungsproblem erscheinen hier nicht als unüberwindbare Hindernisse. So könnten bestimmte Fähigkeiten nur in den Fällen verboten werden, in denen sie in einem Waffensystem vereint werden. Mit der technologischen Aufholjagd von China und anderen Staaten schrumpft das Verteilungsproblem. Damit fällt der Blick vor allem auf die Präferenzen der wichtigsten Staaten und die daraus resultierenden Spielsituationen. Maßgebliches Kooperationshindernis ist eine Deadlock-Situation, die sich vor allem daraus ergibt, dass die zentralen Akteure in erster Linie die militärische Nützlichkeit der Robotik und die dadurch zu erreichende Erhöhung der eigenen Fähigkeiten sehen, allerdings die Gefahren und negativen Folgen für die eigene Sicherheit, die

45 Einige Überlegungen, insbesondere zu Kontroll-Schnittstellen („glass box") der software-basierten Autonomie-Funktionen von Robotern beschreiben Mark Gubrud und Jürgen Altmann, Compliance Measures for an Autonomous Weapons Convention, ICRAC Working Paper Series, Nr. 2 (2013), http://icrac.net/wp-content/uploads/2013/05/Gubrud-Altmann_Compliance-Measures-AWC_ICRAC-WP2.pdf.

46 Dies trifft auch auf die Bundeswehr zu.

47 Ähnlich sieht es für den Fall der Bewaffnung des Weltraums aus, siehe dazu Mutschler, Arms Control in Space.

aus einem Rüstungswettlauf entstehen, zu wenig berücksichtigen. Eine staatenübergreifende, internationale Wahrnehmung gemeinsamer Interessen zur Initiierung Präventiver Rüstungskontrolle fehlt. Dass sich dies jedoch auch ändern kann, hat das historische Beispiel des ABM-Falles gezeigt. Auch im Fall der Robotik sind staatenübergreifende Lernprozesse denkbar, die zu einer verstärkten Wahrnehmung der negativen Folgen eines ungehinderten Rüstungswettlaufs für die Sicherheit aller Beteiligten ins Zentrum rücken.

Die Fragen nach der Definition der zu verbietenden technologischen Optionen, der Gewinnverteilung und den Verifikationsmöglichkeiten sind zwar wichtig, um die Erfolgsaussichten der Regimebildung im Bereich der präventiven Rüstungskontrolle bewerten zu können. Die Analyse jedoch nur darauf zu konzentrieren, genügt nicht. Vielmehr müssen gerade auch die dominierenden Denkmuster und deren Alternativen wieder verstärkt in den Blick genommen werden, um die oben genannten Lernprozesse zu initiieren.

The Role of Civil Society in the Control of New Weapon Technologies: The Case of 'Less Lethal' Weapons

Abi Dymond and Brian Rappert*

Abstract: This article sets out some of the difficulties involved in attempting to control technologies – in particular, those weapons sometimes termed 'less lethal' – and argues that, faced with such challenges, civil society can support regulatory efforts in five distinct, yet inter-linked, ways. Yet, the act of fulfilling such roles, whilst valuable in many ways, can also bring with it inherent tensions and ambiguities that we ignore at our peril.

Keywords: Less lethal weapons, Science and Technology Studies, civil society, governance
Schlagworte: Weniger tödliche Waffen, Wissenschafts- und Technologiestudien, Zivilgesellschaft, Steuerung

1. Introduction

The end of the Cold War has seen a marked increase in the production, use and transfer of so-called 'less lethal' weapons, in law enforcement and military contexts alike. Yet comparatively little attention has been given to the thorny issue of their governance, and in particular what role the civil society can and should play within this. This article tackles this issue, outlining some general difficulties in regulating weaponry, before arguing that civil society stakeholders have an important role to play. Five distinct, yet inter-linked, facets of this role are elaborated. Yet, civil society involvement is not a panacea, and is not without its challenges. Ultimately it is argued that the responsibility lies with state actors to ensure that the weapons they select for use are adequately tested, controlled, and evaluated.

Before elaborating on these points, some definitions are necessary. First, we use the term 'less lethal' weapons to refer to a class of weapons which, in general, have as their stated aim to "subdue or incapacitate" rather than to cause "serious harm or death".[1] As we are at pains to underscore later on in the article, while this term is now well established, we do not accept it as an unproblematic reflection of the intent or outcome of such weapons in practice. We focus predominantly (albeit not exclusively) on this class of weapons – drawing our examples from technologies as varied as chemical irritants, electric-shock weapons and acoustic devices – for several reasons.

First, there is a growing demand for such weaponry – with the global less lethal weapons market estimated at $1.4 billion in 2011[2], and expected to treble by 2020[3] – which brings to the fore issues around the trade, use, monitoring and evaluation of such technologies. However, standard setting efforts have rarely kept pace with technological developments. Indeed, whilst standards for the use of lethal forces are relatively well understood, standards for the use of less lethal weapons are much more ambiguous. In practice their use can prove highly controversial. For example, whilst Article 3 of the UN Basic Principles on the Use of Force and Firearms states that less lethal weapons should be 'carefully evaluated' and 'carefully controlled', what this might mean in practice is not clearly spelt out. This is perhaps not surprising in light of the vast range of less lethal technologies now available; the differing claims that are made for, and about, their relevance, utility and lethality; and the undone science around their functioning and effects.

* Abi Dymond is a PhD Candidate at the Department of Sociology, Philosophy and Anthropology, University of Exeter, and the School of Law, University of Bristol, Bristol, UK. This work was supported by an Economic and Social Research Council South West Doctoral Training Centre Studentship. She is also a serving member of the Metropolitan Police's Taser Reference Group and works part-time for the UK NGO the Omega Research Foundation. Brian Rappert is a Professor of Science, Technology and Public Affairs in the Department of Sociology and Philosophy at the University of Exeter.

1 W. P. Bozeman and J. E. Winslow (2005), 'Medical aspects of less lethal weapons.' *International Journal of Rescue and Disaster Medicine,* 5(1), 37–47.

2 Business Wire (2012), *Homeland Security Research Corp.'s New Market Research: Non-Lethal Weapon Technologies to Transform 21st Century Conflicts* available online at http://www.businesswire.com/news/home/ 20120405005511/en/Homeland-Security-Research-Corp.%E2%80%99s-Market-Research-Non-Lethal (accessed 15th January 2015).

3 Summary of Homeland Security Research Publication Non-Lethal Weapons: Technologies & Global Market – 2012-2020 in Report Linker (2011), *Non-Lethal Weapons: Technologies & Global Market – 2012-2020,* http://www.reportlinker.com/p0799475-summary/Non-Lethal-Weapons-Technologies-Global-Market-.html (accessed 26th September 2012).