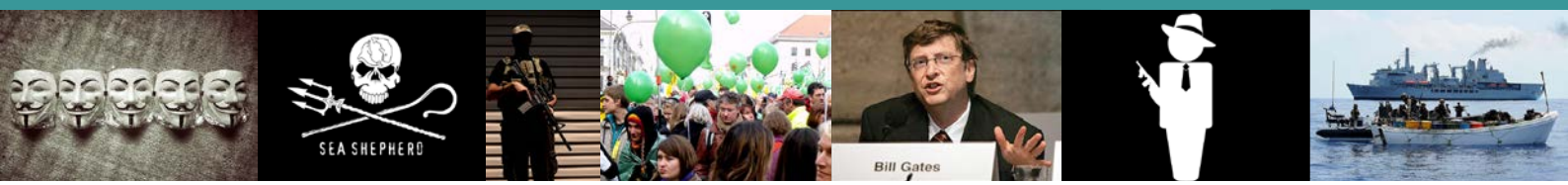
Zukunftsanalyse

Future Study 2012

Nichtstaatliche Konflikte in Räumen begrenzter Staatlichkeit



Planungsamt der Bundeswehr

Streitkräfte, Fähigkeiten und
Technologien im 21. Jahrhundert

Future Study 2012

Nichtstaatliche Konflikte in Räumen begrenzter Staatlichkeit

Impressum

Herausgeber
Planungsamt der Bundeswehr
Dezernat Zukunftsanalyse
Oberspreestraße 61L
12439 Berlin

E-Mail: plgabwdezzuka@bundeswehr.org

Layout und Druck
Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr
Druckerei Strausberg

Titelbilder
Von links nach rechts:

Bild 1: Anonymous, Foto von the|G|™,
http://www.flickr.com/photos/the-g-uk/7567312510/
(cc) BY-NC-ND 2.0; http://creativecommons.org/licenses/by-nc-nd/2.0/deed.de

Bild 2: Seashepherd, Foto von Velovotee,
http://www.flickr.com/photos/velovotee/4184871382/,
(cc) BY-NC-SA 2.0; http://creativecommons.org/licenses/by-nc-sa/2.0/deed.de

Bild 3: PMC, Foto von Rande Archer,
http://www.flickr.com/photos/randearcher/5795827234/
(cc) BY-ND 2.0; http://creativecommons.org/licenses/by-nd/2.0/deed.de

Bild 4: Anti AKW Demo, Foto von Lutz_ek,
http://www.flickr.com/photos/lutz_ek/5563299067/
(cc) BY-NC 2.0 ; http://creativecommons.org/licenses/by-nc/2.0/deed.de

Bild 5: Bill Gates world's most "spammed" person, Foto von IsaacMao,
http://www.flickr.com/photos/isaacmao/1568730/
(cc) BY 2.0; http://creativecommons.org/licenses/by/2.0/deed.de

Bild 6: La Cosa Nostra, Foto von leitza*,
http://www.flickr.com/photos/leitza/2586289000/
(cc) BY-NC-ND 2.0; http://creativecommons.org/licenses/by-nc-nd/2.0/deed.de

Bild 7: Personnel from RFA Fort Victoria Board a Boat Suspected of Use by Pirates Near Somalia, Foto von Defence Images,
http://www.flickr.com/photos/defenceimages/6460968023/
(cc) BY-NC 2.0 ; http://creativecommons.org/licenses/by-nc/2.0/deed.de

August 2013

© Planungsamt der Bundeswehr

Dieser Inhalt ist unter der Creative-Commons-Lizenz vom Typ Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 3.0 Deutschland lizenziert. Um eine Kopie dieser Lizenz einzusehen, besuchen Sie http://creativecommons.org/licenses/by-nc-sa/3.0/de/ oder schreiben Sie einen Brief an Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Vorwort

Das Planungsamt der Bundeswehr bündelt Aufgaben, Kompetenzen und Verantwortung im Planungsnetzwerk für die Bundeswehr auf der dem BMVg nachgeordneten Ebene. Es stellt unter anderem Methodenkompetenz und wissenschaftliche Werkzeuge für die Bundeswehr bereit und erarbeitet die Grundlagen für die zukünftige Ausrichtung der Bundeswehr.

In diesem Rahmen dient Sicherheitspolitische Zukunftsanalyse dem Zweck, frühzeitig und auf wissenschaftlicher Basis Erkenntnisse für die Fortschreibung konzeptioneller Vorgaben und Ziele zu gewinnen. Sie liefert ergebnisoffen und weisungsungebunden Ideen und Impulse für die zukünftige Ausrichtung der Bundeswehr und ist somit ein zentraler Bestandteil der Zielbildung.

Die Studien des Dezernats Zukunftsanalyse werden ressort-intern erstellt. Neben militärischer Expertise werden vor allem Erkenntnisse ziviler wissenschaftlicher Einrichtungen sowie verschiedener Ressorts des Bundes genutzt. Gleichwohl sind die Ergebnisse nicht mit anderen Ressorts und Forschungseinrichtungen abgestimmt und sollen auch keinen Eingriff in deren Verantwortlichkeiten darstellen. Die Studienarbeiten des Dezernats Zukunftsanalyse spiegeln keine offiziellen Positionen des BMVg wider.

Zusammenfassung

Die vorliegende *Future Study 2012* untersucht die bisher vernachlässigte Thematik, inwiefern die Sicherheit von Staaten – insbesondere jene Deutschlands und seiner Verbündeten –zukünftig von nichtstaatlichen Konflikten in Räumen begrenzter Staatlichkeit betroffen sein könnte.

Nichtstaatliche Konflikte sind Konflikte, die primär zwischen *transnationalen nichtstaatlichen Akteuren* (NSA) ausgetragen werden. Eine wichtige Rolle spielen dabei *transnationale Unternehmen* (TNU), *Nichtregierungsorganisationen* (NGOs), *transnationale kriminelle Netzwerke* (TKN), *private Militär- und Sicherheitsfirmen* (PMSF) sowie *Internetaktivisten*. Diese Akteure werden zukünftig über ein noch größeres Spektrum an Handlungsmitteln und -möglichkeiten verfügen.

Es ist davon auszugehen, dass sich nichtstaatliche Konflikte zukünftig häufig in Räumen entfalten, die sich staatlicher Souveränität, Regulierung und Durchgriffsmöglichkeiten weitgehend entziehen – in so genannten Räumen begrenzter Staatlichkeit: *Räume fragiler Staatlichkeit*, *maritime Räume*, der *Weltraum* und der *Cyberspace*. Diese Räume werden gleichzeitig immer wichtiger für moderne Gesellschaften.

Die *Future Study* skizziert potentielle nichtstaatliche Konfliktkonstellationen, die staatliche Sicherheit gefährden könnten. Im Cyberspace könnten Internetaktivisten in andauernde Konflikte mit Unternehmen treten, im Weltraum könnten TKN durch das Kapern von Satelliten Schutzgelder zu erpressen versuchen, um nur zwei Beispiele zu nennen.

Die möglichen sicherheitspolitischen Implikationen dieser und anderer nichtstaatlicher Konflikte in Räumen begrenzter Staatlichkeit sind vielfältig: Sollten die involvierten NSAs beispielsweise aus unterschiedlichen Ländern stammen, könnten sie zwischenstaatliche Krisen provozieren. Weiterhin könnten kritische Infrastrukturen wie Kommunikations- und Navigationssatelliten gefährdet werden, von denen moderne, hochvernetzte Gesellschaften abhängig sind.

Insbesondere der Cyberspace wird dabei, auch aufgrund der Wechselwirkungen mit den anderen Räumen, weiter an Bedeutung gewinnen. In fragilen Staaten werden nichtstaatliche Konflikte zukünftig weiterhin zur Destabilisierung und zur Verschlechterung der humanitären Lage beitragen und dabei verstärkt transnationalen Charakter annehmen.

Nichtstaatliche Konflikte werden zukünftig die Unübersichtlichkeit des ohnehin schon schwer zu überblickenden Umfeldes weiter erhöhen, dem sich die deutsche Sicherheitspolitik und die Bundeswehr gegenübersehen. Für die Früherkennung und die Erstellung von Lagebildern wird es daher zukünftig nicht mehr ausreichen, nur Bedrohungen durch andere Staaten, Rebellengruppen oder terroristische Organisationen im Blickfeld zu behalten. Vielmehr müssen auch andere NSA und deren Beziehungen untereinander systematisch berücksichtigt werden. Von besonderer

Bedeutung für die Bundeswehr sind dabei PMSF, die zukünftig vermehrt auch für NSAs wirken und die Handlungsmöglichkeiten von Streitkräften beeinträchtigen könnten. Ebenfalls von besonderer Relevanz sind NSA, die als Stellvertreter für Staaten agieren und so in vermeintlich nichtstaatlichen Konflikten bewusst staatliche Sicherheit gefährden könnten.

Die durch nichtstaatliche Konflikte und mögliche Stellvertreter-Konstellationen gesteigerte Unübersichtlichkeit erschwert es zusätzlich, Ereignisse und Handlungen sowie dahinter liegende Motivationslagen konkreten Akteuren zuordnen zu können (Attributionsproblematik). Daher wird es neben einer veränderten Bedrohungsanalyse immer wichtiger, das Augenmerk auch auf die eigenen Verwundbarkeiten zu legen.

Vor dem Hintergrund der Studienerkenntnisse gilt es nun zu reflektieren, wie die Bundeswehr ihren Beitrag in einen umfassenden Ansatz vernetzter Sicherheit einbringen kann, um die Widerstandsfähigkeit Deutschlands gegenüber Ereignissen in Räumen begrenzter Staatlichkeit zu stärken. Kompetenzen und Mechanismen der ressortübergreifenden Zusammenarbeit zum Schutz und zur Sicherstellung des freien Zugangs und der Nutzung der untersuchten Räume müssen geregelt, Abstimmungsprozesse für den Ernstfall des Ausfalls kritischer Infrastrukturen und Systemleistungen in und aus diesen Räumen auf den Weg gebracht werden. Weiterhin muss geklärt werden, welche Fähigkeiten es zu entwickeln gilt, um in Räumen begrenzter Staatlichkeit und im Kontext komplexer, nichtstaatlicher Konfliktkonstellationen handlungsfähig zu bleiben. Hierzu gehören beispielsweise auch eine Analyse eigener gegebenenfalls aufzubauender Fähigkeiten im Rahmen der nationalen Cyber-Strategie zur Prävention und Früherkennung von Angriffen für eine nur dann agile Verteidigung im Cyberspace, sowie die Untersuchung der Erweiterung des Weltraumlagezentrums, um ein umfassendes Lagebild der kritischen Infrastrukturen und ihrer möglichen Gefährdung im Weltraum zu erhalten.

Nur im Rahmen eines solchen ganzheitlichen Ansatzes wird Deutschland in diesen Räumen in der Lage sein, den potentiellen Bedrohungen und Risiken entgegenzuwirken und sich eröffnende Chancen zu nutzen.

Die Autoren

Kathrin Brockmann ist seit April 2010 wissenschaftliche Mitarbeiterin im Dezernat Zukunftsanalyse und für den Themenbereich Politik zuständig. Zu ihren beruflichen Stationen gehören die Deutsche Gesellschaft für Auswärtige Politik (DGAP), die Initiative „2° - Deutsche Unternehmer für Klimaschutz“ und das Institut für Europäische Politik (IEP) in Berlin. Seit Oktober 2011 ist sie Associate im Projekt „EU Security Foresight 2030“ der Stiftung Neue Verantwortung. Kathrin Brockmann studierte Politikwissenschaften, Geschichte und Rechtswissenschaften an der Universität Osnabrück (B.A. Europäische Studien) und European Public Affairs (M.A.) an der Universität Maastricht in den Niederlanden.

Jörn Richert war von September 2011 bis August 2013 wissenschaftlicher Mitarbeiter im Dezernat Zukunftsanalyse und verantwortlich für die Themenbereiche Wirtschaft und Energie. Er war Projektleiter der vorliegenden Studie. Er ist Mercator-IPC Fellow 2013/2014 am Istanbul Policy Center in Istanbul. Zu seinen beruflichen Stationen vor dem Dezernat Zukunftsanalyse gehören das Centre for Advanced Security Theory (CAST) an der Universität Kopenhagen, die Stiftung Wissenschaft und Politik (SWP) und das Institut für Weltwirtschaft in Kiel. Jörn Richert studierte Politikwissenschaft, Volkswirtschaftslehre und Psychologie (M.A.) in Kiel und Madrid und hat seit 2009 an der Bielefeld Graduate School in History and Sociology (BGHS) zur internationalen Energiepolitik promoviert.

Oberleutnant Sebastian Weise ist seit Januar 2012 als wissenschaftlicher Mitarbeiter im Dezernat Zukunftsanalyse unterstützend für den Bereich Politik tätig. Er studierte von 2006 bis 2010 an der Universität der Bundeswehr in München Staats- und Sozialwissenschaften mit der Vertiefungsrichtung Politik, Schwerpunkt Internationale Politik. Nach dem Ende seines Studiums war er unter anderem als Zugführer und S-4 Offizier in verschiedenen Truppenverwendungen eingesetzt.

Mithilfe bei der Erarbeitung einer globalen Trendlandschaft, die der vorliegenden Studie zugrunde liegt: Kristin Haase (Federführung Bereich Gesellschaft) und Dr. Annika Vergin (Federführung Bereich Technologie).

Organisatorische und technische Unterstützung der Studienarbeit: Oberfeldwebel Cabrera Garcia, Luis Ernesto und Oberfeldwebel Gronwald, Adrian.

Inhalt

1. Einleitung 1

1.1. Nichtstaatliche Konflikte heute und morgen 2

1.2. Analytische Herausforderung 3

1.3. Begriffliche Annäherung 3

1.4. Aufbau der Studie 4

2. Der Bedeutungsgewinn nichtstaatlicher Akteure 6

2.1. Die Entwicklung von nichtstaatlichen Akteuren bis heute 6

2.2. Die zukünftige Entwicklung nichtstaatlicher Akteure 13

2.3. Der Wandel der Form zukünftiger nichtstaatlicher Akteure 16

3. Transnationale nichtstaatliche Konflikte 18

3.1. Nichtstaatliche Konflikte in Räumen fragiler Staatlichkeit 18

3.2. Nichtstaatliche Konflikte in maritimen Räumen 24

3.3. Nichtstaatliche Konflikte im Weltraum 30

3.4. Nichtstaatliche Konflikte im Cyberspace 38

4. Sicherheitspolitische Relevanz nichtstaatlicher Konflikte in Räumen begrenzter Staatlichkeit 47

4.1. Sicherheitsinteressen Deutschlands und sicherheitspolitische Relevanz nichtstaatlicher Konflikte 47

4.2. Nichtstaatliche Akteure als Stellvertreter 52

4.3. Handlungsfelder 53

4.4. Zusammenfassung 56

Anlagen

A Die Entwicklung von fünf Gruppen nichtstaatlicher Akteure bis in die Gegenwart 59

A 1 Transnationale Unternehmen 59

A 2 Nichtregierungsorganisationen 62

A 3 Transnationale kriminelle Netzwerke 65

A 4 Private Militär- und Sicherheitsfirmen 68

A 5 Internetaktivisten 70
A 6 Schlussbemerkungen 73
B Treiber des Bedeutungsgewinns nichtstaatlicher Akteure 74

Abbildungsverzeichnis

Abbildung 1.1: Fünf Gruppen nichtstaatlicher Akteure 3
Abbildung 1.2: Vier Arten von Räumen begrenzter Staatlichkeit 4
Abbildung 2.1: Treiber des Bedeutungsgewinns nichtstaatlicher Akteure bis in die Gegenwart 12
Abbildung 3.1: Konfliktbild 1 – Das gefährliche Geschäft mit Ressourcen 23
Abbildung 3.2: Entwicklung der globalen Fischbestände seit 1974 25
Abbildung 3.3: Konfliktbild 2 – Die radikalen Retter der Natur 29
Abbildung 3.4: Ausbreitung menschengemachter Weltraumobjekte seit 1960 32
Abbildung 3.5: Konfliktbild 3 – Weltraumpiraterie 37
Abbildung 3.6: Zukünftige Entwicklung verschiedener Indikatoren für die Ausdehnung des Cyberspace 39
Abbildung 3.7: Globale Verteilung der Internetnutzer in den Jahren 1990 (oben) und 2007 (unten) 39
Abbildung 3.8: Konfliktbild 4 – Wertekonflikt im World Wide Web 46
Abbildung 4.1: Sicherheitspolitische Ziele und Sicherheitsinteressen Deutschlands 48
Abbildung A.1: Gesamtzahl transnationaler Unternehmen und relativer Anteil von Unternehmen aus entwickelten Staaten 60
Abbildung A.2: Anzahl der Nichtregierungsorganisationen 63
Abbildung B.1: Treiber des Trends Bedeutungsgewinn nichtstaatlicher Akteure 74

Abkürzungsverzeichnis

ACTA	Anti-Counterfeiting Trade Agreement
AGFA	Apple, Google, Facebook, Amazon
ARPANET	Advanced Research Projects Agency Network
BIP	Bruttoinlandsprodukt
CCC	Chaos Computer Club
CNAS	Center for a New American Security
COPUOS	United Nations Committee on the Peaceful Uses of Outer Space
DDoS	Distributed Denial of Service Attack
ESA	Europäische Weltraumbehörde
EU	Europäische Union
GPS	Global Positioning System
HIIK	Heidelberger Institut für Internationale Konfliktforschung
ICANN	Internet Corporation for Assigned Names and Numbers
IP	Internetprotokoll
ISS	International Space Station
LOIC	Low Orbit Ion Cannon
NASA	National Aeronautics and Space Administration
NASCO	National Association of Security Companies
NGO	Nichtregierungsorganisation
NSA	Transnationaler nichtstaatlicher Akteur
PMSF	Private Militär- und Sicherheitsfirma
RFC	Request for Comments
SSN	Space Surveillance Network
TKN	Transnationales kriminelles Netzwerk
TLD	Top-Level-Domains
TNI	Transnationalisierungsindex
TNU	Transnationales Unternehmen
UIA	Union of International Associations
UNCTAD	United Nations Conference on Trade and Development
UNHCR	Office of the United Nations High Commissioner for Refugees
USAF	US Air Force
VN	Vereinte Nationen
VPR	Verteidigungspolitische Richtlinien
WRV	Weltraumvertrag
WWF	World Wide Fund for Nature

1. Einleitung

Der Staat hat seine Rolle als Monopolist des Krieges eingebüßt.[1] An Schauplätzen wie Somalia, Ruanda und dem ehemaligen Jugoslawien wurde bereits kurz nach dem Ende des Kalten Krieges klar, dass nichtstaatliche Akteure für die Sicherheitspolitik an Bedeutung gewonnen haben. Spätestens mit den Terroranschlägen vom 11. September 2001 ist auch die transnationale Dimension der sicherheitspolitischen Herausforderung durch nichtstaatliche Akteure deutlich geworden.

Die wichtigsten strategischen Dokumente Deutschlands und seiner Verbündeten heben die gewachsene Bedeutung transnationaler nichtstaatlicher Akteure (NSA)[2] hervor.[3] Terroristen und transnationale kriminelle Netzwerke (TKN) zum Beispiel werden als Bedrohung beschrieben, Nichtregierungsorganisationen (*non-governmental organisations*, NGOs) als mögliche Partner betrachtet. Dennoch vernachlässigen diese Dokumente ein wichtiges Thema: *nichtstaatliche Konflikte in Räumen begrenzter Staatlichkeit*.

Solche Konflikte haben drei zentrale Merkmale:

Erstens beziehen sie ein breites Spektrum von NSA ein, darunter neben Rebellengruppen, TKN und terroristischen Organisationen auch transnationale Unternehmen (TNU), NGOs, private Militär- und Sicherheitsfirmen (PMSF) sowie Internetaktivisten.

Zweitens ist der Staat nicht direkt involviert. NSA sehen Staaten weniger als Konfliktparteien, sondern vielmehr als „Hindernisse, Störung oder Chance, die es zu überwinden, tolerieren oder ergreifen gilt“[4], wenn die eigentlichen Ziele in der Auseinandersetzung mit anderen NSA erreicht werden sollen.

Drittens sind es Konflikte, die in Räumen ausgetragen werden, in denen die Handlungsfähigkeit des Staates begrenzt ist, das heißt in Räumen begrenzter Staatlichkeit. Hierunter fallen in dieser *Future Study* Räume fragiler Staatlichkeit, maritime Räume, der Weltraum und der Cyberspace.

Nichtstaatliche Konflikte in Räumen begrenzter Staatlichkeit können zukünftig auch für Staaten verstärkt sicherheitspolitische Relevanz erlangen. Wie die *Future Study* zeigt, können sie sich zu größeren Krisen oder Konflikten ausweiten, die sicherheitspolitische Handlungsfähigkeit von Staaten beeinträchtigen, kritische Infrastrukturen und auf diesen basierende Systemleistungen gefährden sowie den freien und ungehinderten Welthandel und den freien Zugang zur Hohen See und zu natürlichen Ressourcen beeinträchtigen. Auch können in nichtstaatlichen Konflikten wichtige Normen wie die Menschenrechte verletzt werden.

Daher stellt diese *Future Study* folgende Frage: *Wie ist die Sicherheit von Staaten – insbesondere jene Deutschlands und seiner Verbündeten – von zukünftigen Konflikten zwischen NSA in Räumen begrenzter Staatlichkeit betroffen*?

Vor der Untersuchung dieser Fragestellung gilt es drei Punkte klarzustellen:

Erstens bedeutet die vorliegende Arbeit nicht, dass der Staat unwichtig geworden wäre. Staaten sind die wichtigsten Akteure der Sicherheitspolitik und werden dies wahrscheinlich auch in absehbarer Zukunft bleiben. Die Studie will stattdessen die Aufmerksamkeit auf eine zusätzliche, bisher jedoch unterbeleuchtete Dimension zukünftiger Sicherheitspolitik lenken.

Zweitens ist es nicht Ziel der Studie, NSA pauschal zu verurteilen. NGOs zum Beispiel leisten in vielen Politikbereichen wichtige Arbeit und auch TNU stellen heutzutage einen wichtigen Teil der globalen Ordnung dar. Die im Folgenden erarbeiteten Konstellationen nichtstaatlicher Konflikte betreffen daher nicht alle NSA, sondern versuchen zu ergründen, wie einzelne NSA in sicherheitspolitisch relevante Handlungen untereinander verwickelt werden könnten.

Drittens handelt es sich bei den folgenden Ausführungen nicht um Vorhersagen. Vielmehr geht es darum, auf wissenschaftliche und analytische Weise einen Raum möglicher Zukünfte zu eröffnen und so einen Orientierungsrahmen für politisches Handeln zu schaffen. Dieser erlaubt es Entscheidungsträgern, zukünftig ungewisse Entwicklungen in ihre strategischen Planungsprozesse einfließen zu lassen und Entscheidungen im Hinblick auf ihre Zukunftsrobustheit zu überprüfen.

1.1. Nichtstaatliche Konflikte heute und morgen

Vor fast zwanzig Jahren stritt die Umweltorganisation *Greenpeace* mit dem Energieunternehmen *Royal Dutch Shell* über die Versenkung der Ölplattform *Brent Spar*. Heute heuern Logistikunternehmen PMSF an, die Piraten bekämpfen. Auch zwischen Walfängern und der Organisation *Sea Shepherd* kam es in den letzten Jahren wiederholt zu teils dramatischen Auseinandersetzungen und die Internetgruppe *Anonymous* erklärte Ende 2011 dem Drogenkartell *Los Zetas* sogar „den Krieg“, da dieses ein Mitglied der Gruppe entführt hatte. All dies sind Beispiele für nichtstaatliche Konflikte.

Die sicherheitspolitische Relevanz solcher Konflikte war bisher jedoch verhältnismäßig gering. Warum sollte sich das ändern? Die *Future Study* führt zwei Gründe hierfür an: Erstens werden NSA zukünftig wahrscheinlich an Bedeutung und Handlungsmacht gewinnen. Nichtstaatliche Konflikte werden daher zukünftig potenziell mehr Schaden anrichten, als sie dies heute tun. Zweitens werden auch Räume begrenzter Staatlichkeit wichtiger, zum Beispiel als Handlungsräume von Streitkräften und weil sich dort zukünftig verstärkt Infrastrukturen finden werden, die für moderne Gesellschaften unentbehrlich sind. Der Schaden, den nichtstaatliche Konflikte in diesen Räumen anstellen, wird Gesellschaften damit zukünftig stärker treffen, als dies heute der Fall ist.

Abbildung 1.1: Fünf Gruppen nichtstaatlicher Akteure

Quelle: eigene Darstellung.

1.2. Analytische Herausforderung

In der Konfliktforschung ist schon heute häufig von NSA die Rede und teils wurden Begriffe wie postnationale Konflikte oder transnationale Konflikte verwendet.[5] Während dabei viele wichtige Aspekte angesprochen werden, werden die sicherheitspolitischen Implikationen nichtstaatlicher Konflikte in Räumen begrenzter Staatlichkeit bis heute wenig bis gar nicht diskutiert.

NSA gelten oft vorwiegend als direkte Bedrohung für Staaten, sei es in Form von Terrorismus[6], Organisierter Kriminalität[7] oder Cyberangriffen. Teils werden sie auch als Kooperationspartner von Staaten betrachtet (z.B. NGOs und PMSF).[8] In beiden Fällen spielt die Interaktion von NSA untereinander aber eine untergeordnete Rolle. Andere Arbeiten aus dem Bereich der Netzwerkforschung und zum Thema Weltgesellschaft deuten die Wichtigkeit nichtstaatlicher Konflikte in Räumen begrenzter Staatlichkeit hingegen an. Sie gehen jedoch zumeist nicht über theoretische Überlegungen hinaus.[9]

Konkreter beschäftigen sich Arbeiten im Bereich fragiler Staatlichkeit[10] und unter dem Stichwort „Neue Kriege“[11] mit nichtstaatlichen Konflikten. Sie legen ein stärkeres Augenmerk auf die Interaktion zwischen NSA. Dafür haben diese Arbeiten einen anderen Schwachpunkt: Sie beschränken sich vorwiegend mit Räumen fragiler Staatlichkeit. Maritime Räume spielen kaum eine Rolle, der Weltraum und der Cyberspace gar keine.

Auch zukunftsanalytisch ist das Thema der nichtstaatlichen Konflikte in Räumen begrenzter Staatlichkeit nicht erfasst. Zwar wird der Bedeutungsgewinn von NSA postuliert. Die Diskussion verbleibt jedoch wiederum innerhalb des analytischen Horizonts der gegenwärtigen Konfliktforschung.[12]

1.3. Begriffliche Annäherung

Schließlich gibt es zur begrifflichen Einordnung *nichtstaatlicher Konflikte in Räumen begrenzter Staatlichkeit* drei weitere Fragen zu klären: Was genau ist ein NSA? Was wird unter Konflikt verstanden? Was sind Räume begrenzter Staatlichkeit?

Als NSA werden in dieser *Future Study* Zusammenschlüsse von Individuen verstanden, die unter Einsatz eigener Mittel und Wege versuchen, ihre Ziele zu erreichen. Sie sind transnational

organisiert, das heißt aufgrund ihrer Mobilität oder Organisation nicht in einem einzigen Staats- und Rechtsraum zu verorten. Jene Akteure, die für die vorliegende Studie von besonderer Relevanz sind, besitzen darüber hinaus die Fähigkeit, ihr Umfeld mit ihrem Handeln substanziell zu beeinflussen. Die *Future Study* beschäftigt sich vorwiegend mit fünf Gruppen von NSA (vgl. Abb. 1.1).

Die bereits genannten Beispiele für NSA wie *Shell*, *Greenpeace*, *Anonymous* und *Los Zetas* lassen vermuten, dass sich Ziele, Wege und Mittel sehr unterschiedlich gestalten können. Wie im Verlauf der Studie gezeigt wird, gilt Gleiches auch für die Art des Zusammenschlusses. NSA können als hierarchisch organisierte Akteure oder als dynamische Netzwerke auftreten. Allen NSA gemeinsam ist hingegen, dass sie nicht den allgemeinen Regeln und Normen der Staatenwelt unterliegen.[13]

Um die Frage zu beantworten, was ein Konflikt ist, bedient sich die *Future Study* einer im Sinne der Fragestellung angepassten Version der Konfliktdefinition des Heidelberger Instituts für Internationale Konfliktforschung (HIIK). Demnach ist ein Konflikt eine Positionsdifferenz hinsichtlich relevanter Werte (Konfliktgegenstände) zwischen mindestens zwei maßgeblichen und direkt involvierten NSA, die durch beobachtbare und miteinander in Beziehung stehende Konflikthandlungen ausgetragen wird. Die Handlungen liegen außerhalb regulatorischer Verfahren und bedrohen Kernfunktionen der Akteure oder können dies in Zukunft tun.[14]

Abbildung 1.2: Vier Arten von Räumen begrenzter Staatlichkeit

Quelle: eigene Darstellung.

Begrenzte Staatlichkeit kann dem Begriffsverständnis dieser *Future Study* nach in zwei Formen auftreten: Entweder herrscht ein „Mangel an Können und Fähigkeiten“[15], staatliche Funktionen auszuüben. Dies ist in Räumen fragiler Staatlichkeit der Fall, in denen es zumindest theoretisch einen Staat gibt, dieser aber nicht in der Lage ist, seine Aufgaben (vgl. Kap. 3.1) zu erfüllen.

Oder es herrscht ein Mangel an Zuständigkeit, das heißt, es ist gar nicht beabsichtigt, dass ein Staat die entsprechenden Funktionen ausübt. Diese zweite Form begrenzter Staatlichkeit findet sich vor allem in den so genannten *global commons* oder globalen öffentlichen Gütern. Dies sind Räume, in denen keine ausschließlichen Eigentumsrechte bestehen und die außerhalb des Einflussbereiches einzelner Staaten liegen (vgl. Abb. 1.2).[16]

1.4. Aufbau der Studie

Die *Future Study* geht in drei Schritten vor: In Kapitel 2 wird der Trend „Bedeutungsgewinn von NSA“ hergeleitet. Dafür werden zuerst die genannten Akteursgruppen und ihre Entwicklung bis in die Gegenwart vorgestellt. Danach wird die zukünftige Entwicklung

des Trends beleuchtet. Abschließend wird ein Blick darauf geworfen, was dies für die Form konkreter NSA in der Zukunft heißen könnte.

Kapitel 3 beschäftigt sich daraufhin mit konkreten nichtstaatlichen Konflikten in den vier genannten Räumen. Die Räume werden beschrieben und wichtige Themen werden hinsichtlich ihrer heutigen Bedeutung und ihrer zukünftigen Entwicklung dargestellt. Gleichzeitig wird erörtert, welche NSA sich heute in den jeweiligen Räumen befinden und wie sich ihre Rolle verändern kann.

Sowohl hinsichtlich der zukünftige Entwicklung von NSA als auch bezüglich jener von Räumen begrenzter Staatlichkeit geht die *Future Study* von einem Zeithorizont bis 2040 aus.

Für jeden Raum werden anschließend Wege und Mittel dargestellt, die NSA zur Verfügung stehen, um Konflikte auszutragen. Auf dieser Grundlage findet dann eine systematische Einschätzung plausibler Konfliktkonstellationen zwischen NSA statt. Die Diskussion wird durch Konfliktbilder ergänzt, die in narrativer Form potenzielle Konfliktkonstellationen detaillierter betrachten.

Abschließend werden in Kapitel 4 die sicherheitspolitischen Implikationen nichtstaatlicher Konflikte in Räumen begrenzter Staatlichkeit für die Sicherheit von Staaten dargestellt und Handlungsfelder, um diesen Konflikten zu begegnen, werden aufgezeigt.

2. Der Bedeutungsgewinn nichtstaatlicher Akteure

NSA sind in den letzten Jahrzehnten zahlreicher, handlungsmächtiger und vielfältiger geworden, kurz: Sie haben an Bedeutung gewonnen. Ein Blick in die wichtigsten Dokumente der sicherheitspolitischen Zukunftsforschung[17] legt nahe, dass sich dieser Trend fortsetzen wird. Für ein besseres Verständnis zukünftiger nichtstaatlicher Konflikte wird der Bedeutungsgewinn von NSA im Folgenden eingehender betrachtet. Zuerst wird die bisherige Entwicklung verschiedener nichtstaatlicher Akteursgruppen verdeutlicht. Im zweiten Abschnitt wird der Trend mithilfe einer Treiberanalyse in die Zukunft fortgeschrieben. Der dritte Abschnitt geht darauf ein, was die betrachteten Entwicklungen für die Vielfalt und Form von NSA bedeutet, das heißt, wie NSA in der Zukunft aussehen könnten.

2.1. Die Entwicklung von nichtstaatlichen Akteuren bis heute

Das Hauptaugenmerk der folgenden Darstellung gilt fünf nichtstaatlichen Akteursgruppen: transnationalen Unternehmen (TNU), Nichtregierungsorganisationen (NGOs), transnationalen kriminellen Netzwerken (TKN), privaten Militär- und Sicherheitsfirmen (PMSF) sowie den Internetaktivisten. Anschließend werden weitere wichtige NSA diskutiert (für eine ausführliche Version des Abschnittes 2.1 vgl. Anl. A).[18]

Transnationale Unternehmen

TNU sind wirtschaftliche Einheiten, zu denen neben einem Mutterunternehmen auch Tochterunternehmen im Ausland gehören. Sie bewegen sich in sehr unterschiedlichen Branchen wie der Produktion von Nahrungsmitteln oder Kraftfahrzeugen, dem Vertreiben von Dienstleistungen, oder der Energiewirtschaft. Zentrales Handlungsmotiv aller TNU ist dabei das ökonomische Eigeninteresse.

Bereits in den 1960er- und 1970er-Jahren wurde verstärkt diskutiert, ob und wie TNU die unangefochtene Stellung des Staates in der internationalen Politik herausfordern. Seit dieser Zeit ist die weltweite Zahl von TNU stetig gestiegen. Allein in den letzten zwanzig Jahren hat sie sich auf über 80.000 mehr als verdoppelt. Auch der Grad ihrer Transnationalisierung hat in dieser Zeit zugenommen.[19] Weiterhin haben TNU aus Schwellenländern stetig an Bedeutung gewonnen.

TNU sind heutzutage Antreiber der Globalisierung und wichtige Pfeiler der Weltwirtschaft. Nach Schätzungen der *United Nations Conference on Trade and Development* (UNCTAD) tragen sie gut ein Viertel zum globalen Bruttoinlandsprodukt (BIP) bei. Damit sind sie für rund ebenso viel wirtschaftliche

Aktivität verantwortlich, wie alle Regierungen weltweit zusammen (24%).[20] Der Umsatz der größten TNU erreicht dabei die Höhe des BIPs einzelner Staaten. So entspricht der Umsatz von *Walmart* in etwa dem BIP von Österreich, die Umsätze von *Royal Dutch Shell* und *Exxon Mobil* wiederum jeweils dem der Vereinigten Arabischen Emirate. Wachsende finanzielle Mittel und Investitionstätigkeiten gehen mit zunehmenden politischen Gestaltungsmöglichkeiten einher.

Insbesondere NGOs kritisieren TNU. Sie argumentieren, dass TNU die Vorteile der transnationalen Produktion häufig zu Ungunsten von Sozial- und Umweltstandards ausschöpfen würden oder sogar zur Verfestigung von Konflikten in Räumen fragiler Staatlichkeit beitrügen. Die Maßnahmen von TNU im Bereich der *corporate social responsibility* werden vor diesem Hintergrund häufig als substanzlos abgetan.

Auch die Bereitstellung öffentlicher Güter durch TNU, zum Beispiel in den Bereichen Telekommunikation, Strom- und Wasserversorgung, wird mitunter kritisch gesehen, da deren Profitorientierung schwer mit der Idee der öffentlichen Daseinsvorsorge zu vereinbaren sei. Ein weiterer Streitpunkt betrifft die Frage nach staatlichen Beteiligungen bei TNU. Besonders in Bereichen wie der Energiewirtschaft wird kritisiert, dass vorgeblich privatwirtschaftliche Akteure lediglich die Agenda ihres Heimatstaates befördern würden.

Nichtregierungsorganisationen

NGOs sind auf ein bestimmtes Ziel ausgerichtete, nicht gewinnorientierte, zivilgesellschaftliche Organisationen.

In den 1970er- und 1990er-Jahren stieg die Zahl von NGOs deutlich an. Vor allem seit der Konferenz der Vereinten Nationen (VN) über Umwelt und Entwicklung, in Rio de Janeiro im Jahr 1992, haben sie kontinuierlich an Bedeutung und Akzeptanz gewonnen. Mit dieser Konferenz wurde die Idee der nachhaltigen Entwicklung zum Leitbild zahlreicher NGOs. In der Folgezeit wuchs das Themenspektrum kontinuierlich und umfasst heute neben Entwicklung, Menschenrechten, Umwelt und Konfliktbearbeitung auch zahlreiche Nischenthemen. Neben bekannten, großen und global agierenden NGOs wie *Amnesty International*, Ärzte ohne Grenzen, *Friends of the Earth* oder *Greenpeace* haben sich zunehmend auch kleinere NGOs gebildet.

Große NGOs finanzieren sich vorwiegend durch Spenden und Mitgliedsbeiträge. Verschiedene NGOs profitieren auch von staatlichen Zuwendungen.[21] Darüber hinaus haben sie ihre Ressourcen vermehrt in Netzwerken gebündelt oder sind Koalitionen mit staatlichen und wirtschaftlichen Akteuren eingegangen. Insbesondere für kleinere Organisationen spielen auch substanzielle Einzelspenden eine wichtige Rolle, da diese sie unabhängiger von breiter gesellschaftlicher Unterstützung machen und sich so ihr Handlungsspielraum vergrößert.

NGOs üben ihren Einfluss durch Tätigkeiten wie die Normsetzung und -überwachung, das Bereitstellen von Dienstleistungen und Expertise sowie durch öffentlichkeitswirksame Aktivitäten aus. Es sind jedoch auch strittige Praktiken zu beobachten, beispielsweise gezielte Täuschung und Fehlinformation. Einen Extremfall stellt die *Sea Shepherd Conservatory Society* dar. Die Umweltorganisation hat sich zum Ziel gemacht, illegalen Fisch- und Walfang zu verhindern. Sie greift dabei auf eine eigene Flotte hochseetauglicher Schiffe zurück und hat neben medienwirksamen Konfrontationen mit Walfängern bereits mehrfach Boote illegaler Fischer versenkt.

Letztgenannte Vorgehensweisen werden, beispielsweise von TNU, kritisiert. Auch wird bemängelt, dass NGOs in vielen Fällen kein Interesse an der Lösung der von Ihnen angeprangerten Probleme hätten, weil das Bestehen dieser Probleme auch ihre eigene Existenzberechtigung darstellt.

Weiterhin kann die Notwendigkeit finanzieller Zuwendungen ihre Unabhängigkeit von der Staatenwelt infrage stellen. Ein entsprechender Extremfall sind so genannte *astroturfs*, deren Name einem Kunstrasenprodukt entlehnt ist. Anders als zivilgesellschaftliche *grass-root* Bewegungen täuschen sie ihre basisdemokratischen Wurzeln nur vor, werden jedoch – sozusagen künstlich – von staatlicher Stelle initiiert oder gelenkt.

Auch die oft postulierte legitimierende Funktion, die NGOs in politischen Prozessen für sich reklamieren, wird nur bedingt anerkannt, denn weder sind sie durch demokratische Prozesse legitimiert, noch müssen sie selbst demokratisch verfasst sein. Zusätzlich herrschen beachtliche Ungleichgewichte in Bezug auf Anzahl, Ressourcen und Einfluss von NGOs sowohl zwischen Nord- und Südhalbkugel als auch zwischen thematisch unterschiedlich aufgestellten NGOs innerhalb der Industrieländer. Ein letzter Kritikpunkt ergibt sich hinsichtlich der Hilfeleistungen von NGOs in Entwicklungsländern und Räumen fragiler Staatlichkeit. Ähnlich wie die Tätigkeiten von TNU in solchen Räumen, können diese zur Verzerrung lokaler Machtstrukturen führen.

Transnationale kriminelle Netzwerke

Eine dritte bedeutende Gruppe von NSA sind TKN, das heißt auf Dauer organisierte, transnationale, profitorientierte Gruppen, die schwerwiegende kriminelle Aktivitäten verfolgen.

Insbesondere seit den 1990er-Jahren haben sich TKN wie die Albanische Mafia und Gruppen der italienischen Mafia global vernetzt. Heutzutage sind sie etablierter Bestandteil der internationalen (Un-)Ordnung, sei es in Industrieländern oder in Entwicklungsländern. Zentrale Betätigungsfelder von TKN sind Menschenschmuggel und Zwangsprostitution, Drogen- und Waffenhandel, Wirtschaftskriminalität, Geldwäsche aber auch die Piraterie. Darüber hinaus sind in den letzten Jahren neue Betätigungsfelder wie die Cyberkriminalität, der Schmuggel von Kulturgütern, Umweltverbrechen und der Organhandel entstanden. So setzen TKN schätzungsweise rund sieben bis zehn Prozent der weltweiten Wirtschaftsleistung um.[22]

Sie sind dabei oft sowohl mit lokalen wirtschaftlichen und gesellschaftlichen Strukturen als auch mit globalen Handelsströmen eng verwoben. Nur wenn eine (globale) Nachfrage besteht, lohnen sich die illegalen Aktivitäten von TKN beispielsweise beim Abbau von und Handel mit Ressourcen. Dabei können, wie teils beim Drogenanbau, durchaus Einkommensmöglichkeiten für die lokale Bevölkerung entstehen. In diesem Rahmen können die Aktivitäten von TKN in begrenztem Maße stabilisierend wirken. Generell sind auch sie auf ein Mindestmaß an gesellschaftlicher Ordnung und funktionierende Infrastrukturen (z.B. Häfen) angewiesen. Andererseits sind TKN nicht selten in Gewaltkonflikte verstrickt und finanzieren mitunter auch terroristische Organisationen.

Private Militär- und Sicherheitsfirmen

PMSF sind private Unternehmen, die Dienstleistungen in den Bereichen Beratung, Ausbildung, Unterstützung sowie der Bereitstellung von Sicherheit erbringen. In Konfliktzonen leisten sie unbewaffnete logistische Unterstützungen ebenso wie offensive und defensive militärische Dienste.

Besonders seit Ende des Kalten Krieges ist die Bedeutung von PMSF unter anderem aufgrund des zunehmenden Drucks auf staatliche Verteidigungsbudgets und eines gestiegenen Flexibilisierungsbedarfs von Streitkräften gestiegen. Ein Beispiel eines frühen Einsatzes bietet *Executive Outcomes*, das 1993 in Angola im Auftrag der Regierung von Rebellen besetzte Städte eingenommen und später das staatliche Militär mit aufgebaut hat.

Die heutige Bedeutung von PMSF lässt sich anhand folgender Zahlen verdeutlichen: Während sie von 1959 bis 1989 lediglich an 15 Konflikten beteiligt waren, war dies allein von 1990 bis 2000 achtzig Mal der Fall[23]; während 1996 lediglich zehn Prozent der einhundert umsatzstärksten Rüstungsunternehmen auf Sicherheitsdienstleistungen spezialisiert waren, hat sich dieser Wert bis 2010 verdoppelt; und während die Umsätze dieser Firmen 2002 bei 22,3 Milliarden US-Dollar lagen, waren es 2010 bereits 55 Milliarden.[24] Besonders deutlich wird die Bedeutung von PMSF in Analysen, welche darlegen, dass die US-Einsätze im Irak und Afghanistan ohne private Dienstleister nicht durchführbar gewesen wären.

Auch NSA fragen zunehmend die Dienste von PMSF nach. Beispielsweise engagieren Reedereien private Sicherheitsdienstleister, um ihre Schiffe mit Waffengewalt vor Übergriffen von Piraten zu schützen.

Etablierte PMSF setzen sich mittlerweile zunehmend für eine Regulierung des Marktes für Sicherheitsdienstleistungen ein, zum Beispiel durch die Registrierung von Firmen und die Überwachung der Ausbildung. Dennoch wird die durch PMSF sichtbare Privatisierung des Gutes Sicherheit auch kritisiert. So haben vor allem kleine und neue PMSF weiterhin die Möglichkeit, auch weniger akzeptierte und gegebenenfalls kontroverse Dienstleistungen anzubieten und eine strafrecht-

liche Verfolgung von PMSF und deren Angestellten ist oft schwierig.[25]

Internetaktivisten

Internetaktivisten sind oft lose organisierte, zivilgesellschaftliche Akteure, die den Cyberspace als ihren zentralen Handlungsraum ansehen. Im Mittelpunkt ihres Handelns steht zumeist das Ideal einer universellen und freien Verfügbarkeit von Informationen. Traditionelle Gesellschafts- und Herrschaftsstrukturen werden abgelehnt.

Vorgänger heutiger Internetaktivisten sorgten seit den 1980er-Jahren für Aufsehen. Damals brachen zum Beispiel Mitglieder des Chaos Computer Clubs (CCC) in Rechner von Banken sowie der US-amerikanischen *National Aeronautics and Space Administration* (NASA) ein. Neben Hackern entwickelten sich mit der Ausbreitung des Internets auch die so genannten *script kiddies*, das heißt zumeist Jugendliche, die – häufig ohne tiefgreifende Kenntnis der Materie – auf vorgefertigte Programme im Internet zurückgreifen, um zur eigenen Belustigung Schaden im Netz anzustellen. In diesem Milieu haben sich in den letzten Jahren auch politisch motivierte Gruppen, allen voran die Gruppe *Anonymous*, entwickelt. Schließlich kann die 2006 gegründeten Internetplattform *WikiLeaks* ebenfalls dem Bereich des Internetaktivismus zugeordnet werden.

Strukturell unterscheiden sich diese Akteure stark. Während sich der CCC 1981 als Club jenseits der virtuellen Welt konstituierte und seit 1986 als eingetragener Verein geführt wird, gibt es bei *Anonymous* keine klare Mitgliedschaft und keine legitime Vertretung: die Anhänger treffen sich vorwiegend anonym im Cyberspace. *Anonymous* ist daher als eine Art Netzwerk zu begreifen, in dem handlungsfähige Gruppen spontan entstehen, ebenso schnell aber auch wieder zerfallen können. Generell gilt für solche netzwerkartigen Gruppen, dass die Berechenbarkeit hinsichtlich ihrer Ziele und ihres Handelns wesentlich geringer ist, als bei traditionell strukturierten Akteuren.

Internetaktivisten handeln durchaus unterschiedlich. Hacker beispielsweise können zur Sicherheit von Systemen beitragen, indem sie systematisch nach Schwachstellen suchen. Sie können solche Schwachstellen aber auch ausnutzen, um Informationen zu entwenden oder Schaden anzurichten. Gruppen wie *Anonymous* sind bisher hauptsächlich durch Attacken aufgefallen, bei denen eine Internetseite durch massenhafte Anfragen gezielt überfordert und zum Absturz gebracht worden ist, so genannte *Distributed Denial of Service* (DDoS). *WikiLeaks* wiederum hat für Aufsehen gesorgt, in dem es eine Vielzahl geheimer Dokumente veröffentlichte – darunter mehr als 100.000 Depeschen von US-Botschaften weltweit.

Internetaktivisten werden heute sehr unterschiedlich beurteilt. Während manche Kommentatoren sie lediglich als Ärgernis des Internetzeitalters verstehen, sehen andere sie als Bedrohung der nationalen Sicherheit. Generell sind sie teils heftiger Kritik ausgesetzt. Hauptkritiker sind dabei oft TNU, die versuchen, Urheberrechte auch in Zeiten des Internets durchzusetzen. Aber auch unter Internetaktivisten selbst sind Verwerfungen zu erkennen. So lehnt beispielsweise der

CCC die Verwendung von DDoS-Attacken vehement ab. Darüber hinaus kritisiert der Club *Anonymous* dafür, dass es der Gruppe nicht gelungen sei, ethische Verhaltensmaßstäbe aufzustellen.

Weitere nichtstaatliche Akteure

TNU, NGOs, TKN, PMSF und Internetaktivisten sind wichtige Beispiele für den Bedeutungsgewinn von NSA. Sie erschöpfen jedoch nicht die Vielfalt der nichtstaatlichen Welt. Weiterhin existieren zum Beispiel so genannte *super-empowered individuals*, Rebellengruppen und transnationale terroristische Organisationen.

Super-empowered individuals sind Individuen, die das Potenzial haben, das internationale Umfeld substanziell zu beeinflussen. Dabei fällt ihr Handeln aber häufig in das bisher besprochene Spektrum von Aktivitäten. So setzt sich zum Beispiel Bill Gates mit seinem Reichtum für die Entwicklungspolitik ein. Er tut dies über die Bill und Melinda Gates Stiftung, die im NGO-Bereich tätig ist. Eine weitere, als *super-empowered individual* bezeichnete Person, Julian Assange, kann durch die Gründung der Internetplattform *WikiLeaks* durchaus dem Bereich der Internetaktivisten zugeordnet werden.

Rebellen und andere lokale Gewaltakteure sowie transnationale terroristische Organisationen unterscheiden sich wiederum von den bisher diskutierten Akteuren insofern, als das sich ihr Handeln oft gegen eine bestehende politische und meist staatliche Ordnung wendet. Sie sind also weniger wirtschaftlich oder zivilgesellschaftlich, sondern politisch motiviert. Rebellen sind im Vergleich zu den bisher betrachteten NSA zumeist weniger transnational eingebunden und spielen in dieser Studie daher vorwiegend dann eine Rolle, wenn sich transnationale nichtstaatliche Konflikte mit lokalen Strukturen vermischen (vgl. Kap. 3.1 zu Räumen fragiler Staatlichkeit und Kap. 3.2 zu maritimen Räumen). Der Terrorismus wiederum wird in dieser *Future Study* weniger als Akteur begriffen, sondern als spezifischer Handlungsweg. Auch wenn dieser von den betrachteten NSA bisher nur bedingt eingesetzt wurde, steht er ihnen zumindest prinzipiell offen.

Abbildung 2.1: Treiber des Bedeutungsgewinns nichtstaatlicher Akteure bis in die Gegenwart

Übergreifende Kategorien	Treiber	Beschreibung	Folge
(A) technologische Entwicklung und Steigerung der Interaktionskapazität	(1) Transportwesen	Leistungssteigerung und Kostensenkung im globalen Transportwesen, z.B. Seetransport von Waren	TNU gewinnen Druckmittel durch potenzielle Produktionsverlagerungen; TKN nutzen globalisierte Handelsnetzwerke.
	(2) Kommunikationswesen	Verbreitung von Kommunikationsmedien, z.B. Fax, Telefon und Internet	Neuer, virtueller Handlungs- und Geschäftsraum für TNU und TKN und neue Vernetzungs- und Handlungsmöglichkeiten für NGOs entstehen; Internetaktivisten kommen auf.
	(3) Wirkmittel	gesteigerter Zugang zu Kleinwaffen und solchen mit immer größerer Reichweite und Wirkkraft; neue, leicht zugängliche Mittel im Bereich Cyberspace	TKN und andere illegale Akteure gewinnen an Handlungsmacht; PMSF etablieren sich und bieten auch anderen NSA Möglichkeiten, sicherheitsrelevante Dienste einzukaufen.
(B) gesellschaftlicher Wandel	(4) transnationale Netzwerke	Anstieg der Migration sowohl gut ausgebildeter Arbeitskräfte als auch ärmerer Menschen	Transnationale Eliten entstehen, auf die TNU und NGOs zurückgreifen können; TKN vernetzen sich zunehmend mit weltweit wachsenden Diaspora-Gemeinschaften.
	(5) Wertewandel	Verbreitung von Menschenrechten, Individualismus, Umweltschutz, Demokratie, politischer Partizipation und eines auf Konsum und Privatisierung aufbauenden Wirtschaftssystems	Nichtstaatliche Identifikationsmuster werden wichtiger; NGOs und Internetaktivisten werden zu einer ernsthaften Ausdrucksform politischen Engagements neben dem Staat.
	(6) Radikalisierung	ansteigende Radikalisierung (kombiniert mit größeren Wirkmitteln)	Der Terrorismus erlangt ein neues Ausmaß; Akteure mit radikaleren Vorstellungen gewinnen an Bedeutung – selbst im Bereich von NGOs.
(C) begrenzte Staatlichkeit	(7) Kompetenzabgabe an NSA	bewusste Abgabe von Kompetenzen durch den Staat an andere Akteure, z.B. durch Privatisierung	Große TNU entstehen, z.B. im Bereich Infrastrukturen; Nachfrage nach Sicherheitsdienstleistungen ermöglicht den Aufstieg von PMSF; NGOs werden aufgrund der Nachfrage nach ihrer Expertise wichtiger.
	(8) *governance*-Lücke	wachsende Lücke zwischen national begrenzten Regelungskompetenzen und zunehmend überstaatlichen/globalen Problemlagen	NGOs leisten wichtige Beiträge zum Regieren jenseits des Nationalstaates; TNU profitieren vom globalen Standortwettbewerb; TKN können zunehmend einer nationalen Strafverfolgung entgehen.

Quelle: eigene Darstellung.

2.2. Die zukünftige Entwicklung nichtstaatlicher Akteure

Um Aussagen über die Zukunft von NSA machen zu können, werden nun Faktoren betrachtet, die maßgeblichen Einfluss auf den Bedeutungsgewinn dieser Akteure ausüben – so genannte Treiber. Die insgesamt acht Treiber teilen sich auf drei übergreifende Kategorien auf: die technologische Entwicklung und die Steigerung der Interaktionskapazität, den gesellschaftlichen Wandel sowie die Begrenzung von Staatlichkeit. Die bisherige Entwicklung der Treiber ist in Abbildung 2.1 dargestellt (vgl. auch Anl. B). Im Folgenden werden ihre zukünftige Entwicklungen und die Folgen für NSA eingehender betrachtet. Die Nummerierung im Text stimmt dabei mit jener in der Abbildung überein.[26]

Technologische Entwicklungen und steigende Interaktionskapazitäten

Die Preise für technologische Entwicklungen werden zukünftig fallen und deren Zugänglichkeit steigen. So ist (1) mit einer weiter zunehmenden Verfügbarkeit von Transportmitteln zu rechnen. Selbst im Weltraum werden beispielsweise TNU zukünftig ihre Bewegungs- und Handlungsfähigkeit ausbauen (vgl. Kap. 3.3). Die Weiterentwicklung von (2) Kommunikationsmitteln ermöglicht immer mehr Menschen, sich über staatliche Grenzen hinweg zu informieren, ihre Meinung zu äußern und sich politisch zu engagieren. Hiervon profitieren zivilgesellschaftliche Akteure wie NGOs und Internetaktivisten. Mit einer Zunahme digitaler Kommunikation ergeben sich aber auch neue Möglichkeiten der Überwachung – nicht nur durch Staaten. Eine bedeutende Rolle spielt hier die Entwicklung des Cyberspace zu einem immer wichtigeren sozialen Raum (s.a. Kap. 3.4). So werden beispielsweise TNU zukünftig „auf Bergen von Daten sitzen und mehr Echtzeitinformationen als Regierungen in ihren Händen halten.“[27] Auch (3) im Bereich der Wirkmittel gilt Ähnliches: Im Cyberspace werden diese zukünftig weitläufig verfügbar sein – eine Monopolisierung durch den Staat ist unwahrscheinlich. Aber auch die Möglichkeiten des Erwerbs konventioneller Waffen, darunter nicht nur Kleinwaffen, sondern auch von (unbemannten) Systemen wie Drohnen werden voraussichtlich zunehmen.[28] Für NSA ergeben sich hieraus steigende Möglichkeiten, ihre Ziele auch gewaltsam zu verfolgen.

Gesellschaftlicher Wandel

(4) Transnationale gesellschaftliche Netzwerke werden sich wahrscheinlich weiter ausbilden. Neben der Entwicklung von Kommunikationsmitteln trägt hierzu auch Migration bei. Einerseits ist in diesem Zusammenhang eine steigende Mobilität gut ausgebildeter Arbeitskräfte zu erwarten; gefördert durch die Globalisierung sowie durch den steigenden Wettbewerb um Fachkräfte sowohl in alternden westlichen Gesellschaften als auch in aufstrebenden Schwellenländern. Für TNU und NGOs bieten global vernetzte Eliten neue Rekrutierungspotenziale. Andererseits wird die Migration von ärmeren in reichere Regionen wahrscheinlich ansteigen. Zumeist pflegen die so ent-

stehenden Diasporagemeinschaften ein friedliches Mit- und Beieinander mit den Gesellschaften der Länder, in denen sie sich niedergelassen haben. Gleichzeitig bieten sie aber entlang ethnischer oder kultureller Identitäten strukturierten TKN neue Möglichkeiten, sich transnational zu vernetzen.

Darüber hinaus werden sich (5) Werte wie Individualität und Konsum weiter ausbreiten und wandeln. So entstehen in wirtschaftlich aufsteigenden Staaten wie China und Indien neue Mittelschichten, die diese Werte aufnehmen und für sich neu interpretieren können. Dabei könnten zukünftig auch Werte entstehen, die nicht ohne Weiteres mit denen westlicher Gesellschaften zu vereinbaren sind. Neue Mittelschichten werden wahrscheinlich auch der Entwicklung neuer NGOs und Internetaktivisten Vorschub leisten beziehungsweise deren Bedeutung erhöhen.

In den Gesellschaften der Industriestaaten könnten post-moderne und post-materielle Werte wie der Umweltschutz noch weiter an Kraft gewinnen. Auch könnten alternde Gesellschaften, wie in Europa und Japan, zunehmend riskante Einsätze eigener Streitkräfte scheuen und verstärkt auf PMSF zurückgreifen.

Auch (6) die gesellschaftliche Radikalisierung könnte zukünftig zunehmen. Ein Grund hierfür liegt in wachsenden Wohlstandsgefällen, auf globaler, regionaler oder nationaler Ebene. Auch die steigende Frustration über mangelnde Fähigkeiten der internationalen Gemeinschaft, globalen Problemen aktiv zu begegnen (s.u.), könnte die Radikalisierung vorantreiben. Radikalisierung kann dabei auch zukünftig verschiedene, beispielsweise religiöse, nationalistische, aber auch auf zivilgesellschaftliche Werte fokussierte Formen annehmen und zu einer wachsenden Unterstützung radikaler NSA führen. Selbst wenn der Grad der Radikalisierung sich weltweit in den kommenden Jahrzehnten nicht wesentlich ändern sollte, würde die Bedeutung radikaler Akteure aufgrund steigender Wirkmittel wahrscheinlich steigen.

Begrenzung von Staatlichkeit

Inwiefern (7) Staaten weiterhin freiwillig, zum Beispiel durch die Privatisierung von Unternehmen, Kompetenzen an NSA abgeben werden, ist unklar. Im Zusammenhang mit der Finanz-, Wirtschafts- und Staatsschuldenkrise seit 2007 ist der *Washington Consensus*, das heißt das Ideal einer weitgehend privaten und deregulierten Wirtschaftsordnung, wiederholt kritisiert worden. Westliche Staaten haben zum Beispiel zahlreiche Banken verstaatlicht. Gleichzeitig bedienen sich viele neue Wirtschaftsmächte staatskapitalistisch geprägten Wirtschaftsmodellen, in denen Unternehmen oft eng mit dem Staat verbunden sind.

Eine klare Entwicklung hin zu einer Rückgewinnung staatlicher Kompetenzen gibt es dennoch nicht. So deuten zum Beispiel die in Europa zu beobachtenden Prozesse zur Staatsschuldenkonsolidierung darauf hin, dass der *Washington Consensus* durchaus noch eine einflussreiche Anhängerschaft hat. Im Kontext des Staatsschuldenabbaus könnte es zu weiteren Privatisierungen strategisch bedeutender Unternehmen kommen. Darüber hinaus könnte sich der *Washington Consensus* zunehmend

selbst zum Streitpunkt zwischen befürwortenden und ablehnenden NSA entwickeln.

Generell sind von staatlichen Versuchen, Kompetenzen von NSA zurückzuerlangen, vorwiegend TNU und PMSF betroffen. Während aber gezielte staatliche Rückkäufe strategisch wichtiger Unternehmen zukünftig durchaus plausibel sind, ist eine weitreichende Nationalisierung ganzer Wirtschaftszweige allein aufgrund ihrer Größe unwahrscheinlich. PMSF wiederum könnten durch Regulierung eingeschränkt und durch den Entzug von Aufträgen geschwächt werden.[29] Stark spezialisierte und daher nur bedingt auf große Märkte angewiesene PMSF könnten auf Staaten ausweichen, die sie weiterhin gewähren lassen.

Im Hinblick auf andere NSA wären die Rückgewinnung von Kompetenzen und die Beschränkung des Handlungsspielraumes durch den Staat noch schwieriger. NGOs wären – zumindest in Staaten, in denen demokratische Grundsätze gelten – voraussichtlich nur dann anfällig für entsprechende Versuche, wenn sie zu einem großen Teil auf staatliche Finanzierung angewiesen sind. Internetaktivisten könnten wiederum vorwiegend durch eine verschärfte Strafverfolgung betroffen sein. Zur nachhaltigen Eingrenzung der Aktivitäten dieser NSA wäre aber eine weitreichende und globale Regulierung ihrer Handlungsräume notwendig. Dies wird sich, wie im Folgenden zu sehen, jedoch weiterhin als schwierig erweisen. Am wenigsten betroffen von einer Rücknahme von Kompetenzen durch den Staat wären schließlich TKN, die von vornherein nicht durch eine freiwillige Kompetenzabgabe von Staaten profitieren konnten.

Von (8) der wachsenden Lücke zwischen globalen Herausforderungen und (staatlichen) Lösungsansätzen werden NSA hingegen wahrscheinlich weiter profitieren. Neben den Folgen des Klimawandels zeichnen sich auch Themen wie die Gentechnik, Nanotechnologie, Pandemien, die Entwicklungen der Finanzmärkte, der Verlust der Artenvielfalt durch ihre globalen Auswirkungen aus.[30]

Im Rahmen nationaler Politik sind diese Herausforderungen nicht zu lösen. Besonders groß ist der Mangel an adäquaten Problemlösungskapazitäten in Räumen begrenzter Staatlichkeit (vgl. Kap. 3). Schon heute bedarf es daher zunehmend globaler Koordination. In vielen Fällen gelingt diese jedoch nicht, wie beispielsweise in der Klimapolitik. Die zukünftige multipolare Weltordnung und die damit einhergehenden Interessensdifferenzen werden die notwendigen Koordinierungsbemühungen noch weiter erschweren.

Die wachsende Lücke zwischen globalen Problemen und deren Lösungsansätzen und das damit einhergehende Regulierungsdefizit werden die Handlungsfreiheiten von NSA zukünftig wahrscheinlich vergrößern. Neben internationalen Organisationen[31] könnten dabei besonders NGOs zu Anlaufstellen für jene werden, die von der mangelnden Problemlösungsfähigkeit der Staatenwelt enttäuscht sind.

Zusammenfassend führt die Treiberanalyse zu dem Ergebnis, dass sich der Bedeutungsgewinn von NSA auch zukünftig fortsetzen wird: Die Interaktionskapazitäten von NSA werden zukünftig aufgrund verschiedener Entwicklungen im technologischen Bereich weiter anwachsen. Durch den gesellschaftlichen Wandel gewinnen zivilgesellschaftliche NSA Unterstützer und Handlungsfelder. Gleichzeitig könnten sich einzelne NSA radikalisieren. Zwar ist unklar, inwiefern Staaten versuchen werden, zukünftig Kompetenzen von NSA zurückzuerlangen. Dennoch werden sich für NSA aufgrund einer weiter steigenden Inkongruenz zwischen politischen Herausforderungen und (staatlichen) Lösungsansätzen neue Handlungsräume ergeben.

2.3. Der Wandel der Form zukünftiger nichtstaatlicher Akteure

Die nachvollzogene Entwicklung der Treiber bestätigt nicht nur den zukünftigen Bedeutungsgewinn von NSA. Sie lässt auch Rückschlüsse auf deren zukünftige Form zu, die nun zum Abschluss dieses Kapitels angesprochen werden.

Konstante Motivationen

Die grundlegenden Motivationen von NSA werden sich zukünftig kaum ändern. Auch weiterhin kann ihr Handeln politisch motiviert sein, das heißt es würde sich auch künftig an der Kritik von beziehungsweise an der Konfrontation mit etablierten Herrschaftsstrukturen und -praktiken ausrichten – wie im Falle von Rebellen und terroristischen Organisationen. Andere Akteure werden hingegen wirtschaftliche Ziele verfolgen. Sie sind, wie TNU und PMSF, entweder *legal* oder, wie TKN, illegal profitorientiert. Zwischen diesen wirtschaftlichen Aktivitäten wird es auch zukünftig zu Überschneidungen kommen. TKN können heute und in Zukunft ebenso in legalen Geschäften engagiert sein, wie TNU in illegalen. NGOs und Internetaktivisten wiederum werden weiterhin vorwiegend nach der Verwirklichung zivilgesellschaftlicher Ideale wie der Informationsfreiheit oder dem Umweltschutz streben.

Neue Handlungs- und Themenfelder

Trotz konstanter Motivationen werden sich die Handlungs- und Themenfelder, in denen NSA ihre Ziele verfolgen werden, ausweiten. Für TNU, PMSF und TKN werden sich neue, gegebenenfalls auch gesellschaftlich umstrittene Geschäftsfelder auftun – beispielsweise im Bereich der Humangenetik oder beim Einsatz von Nanotechnologien. NGOs und Internetaktivisten wiederum werden auf neue gesellschaftliche und politische Entwicklungen, auch und gerade im Zusammenhang mit diesen neuen Geschäftsfeldern, reagieren und gegebenenfalls konträre Positionen vertreten und durchzusetzen suchen.

Neue Mittel und Wege

Wahrscheinlich werden NSA zukünftig neue Mittel und Wege zur Verfügung stehen, um ihre Ziele zu erreichen. Vor dem Hintergrund von Radikalisierungstendenzen und einer gesteigerten Verfügbarkeit von Wirkmitteln könnten sie zukünftig verstärkt zur Gewaltanwen-

dung bereit sein. So könnte zum Beispiel das vermehrte Auftauchen reicher Einzelspender das Entstehen kleinerer, ressourcenstarker, thematisch spezifischer NGOs erleichtern. Diese könnten neue Wege der Zieldurchsetzung beschreiten.[32]

Unterschiedliche Herkunft

Trotz des transnationalen Charakters von NSA ist ihr Handeln bisher zumeist an ethischen und wirtschaftlichen Maßstäben des Westens orientiert gewesen. Wie oben zeigt, bietet sich schon in diesem Rahmen viel Anlass für gegenseitige Kritik. Mit dem Bedeutungsgewinn von NSA aus anderen Teilen der Welt, könnten sich diese Differenzen noch vervielfältigen – sowohl hinsichtlich konkreter Handlungsfelder als auch hinsichtlich der eingesetzten Mittel und Wege.

Komplexe Akteurskonstellationen

Schließlich kann es zukünftig verstärkt zur Herausbildung komplexer Akteurskonstellationen kommen. Es könnten, wie heute schon im Bereich der Internetaktivisten sichtbar, zukünftig verstärkt netzwerkartig strukturierte Akteure entstehen. Die Zielbildung und Vorgehensweise solcher Netzwerke könnte verstärkt spontan geschehen und wäre daher schwerer zu verstehen und vorauszusehen.

Auch ist es wahrscheinlich, dass verstärkt Mischformen der hier betrachteten Akteursgruppen auftauchen. So könnten Akteure, die vermeintlich einer bestimmten Gruppe zuzuordnen sind, Ziele vertreten, die eigentlich von anderen Akteuren verfolgt werden (Proxy-NSA). Ein Beispiel bilden von TNU aufgesetzte *astroturfs*, bei denen sich die Durchsetzung unternehmerischer Ziele mit dem Erscheinungsbild von NGOs mischt. Solche Vermischungen müssen dabei nicht immer gewollt und bewusst vonstattengehen. So ergeben sich insbesondere im Bereich der weitgehend anonymen Interaktion von Internetaktivisten Möglichkeiten, dass diese von anderen NSA unterwandert werden. Auch Staaten könnten in solchen komplexen Akteurskonstellationen in Zukunft eine wichtige und veränderte Rolle spielen. Dieser letzte Aspekt wird in Kapitel 4 weiter erläutert. Vorher wird sich das nächste Kapitel aber eingehend mit Räumen begrenzter Staatlichkeit und nichtstaatlichen Konflikten in diesen Räumen befassen.

3. Transnationale nichtstaatliche Konflikte

Im Folgenden wird die Frage beantwortet, wie sich Konflikte zwischen NSA ausgestalten könnten. Dafür werden vier Räume – Räume fragiler Staatlichkeit, maritime Räume, der Weltraum und der Cyberspace – betrachtet. Diese Schwerpunktsetzung erfolgt aus zwei Gründen. Erstens ist besonders dort mit transnationalen nichtstaatlichen Konflikten zu rechnen, wo Staatlichkeit nur in begrenztem Maße vorkommt. In allen vier Räumen besitzen Staaten bereits heute nur beschränkte Regulierungs- oder sogar Handlungsmöglichkeiten. Zweitens zeichnen sich die Räume durch gesamtgesellschaftliche und sicherheitspolitische Relevanz aus, welche nach der folgenden Analyse in Kapitel 4 eingehender erläutert wird.

Für jeden Raum werden der gegenwärtige Zustand und die Entwicklung bis 2040 hinsichtlich folgender Fragen erarbeitet: Welche Akteure agieren in dem Raum? Welche Formen von *governance* und Herrschaftsstrukturen sind zu erkennen? Welche Nutzungsformen und Problemfelder existieren? Anschließend werden die Wege und Mittel aufgeführt, die den NSA zur Verfügung stehen, wenn sie miteinander in Konflikt geraten. Schließlich werden konkrete, zukünftig mögliche Konfliktkonstellationen zwischen NSA diskutiert.

In allen vier Räumen wird die Analyse durch „Konfliktbilder“ ergänzt, die mit mehr Detailschärfe die Dynamik potenzieller transnationaler nichtstaatlicher Konflikte aufzeigen. Obwohl sich diese Konfliktbilder jeweils auf konkrete Räume beziehen, sind die darin beschriebenen Konstellationen oft auch in anderen Räumen vorstellbar. Die Konfliktbilder sind nicht als konkrete Vorhersagen zu verstehen, sondern sollen den Gegenstand der Analyse greifbarer machen.

3.1. Nichtstaatliche Konflikte in Räumen fragiler Staatlichkeit

Räume fragiler Staatlichkeit sind Territorien in denen staatliche Institutionen keine oder nur noch sehr eingeschränkte Kontroll-, Steuerungs- und Handlungsfähigkeiten besitzen. Dies gilt insbesondere hinsichtlich der drei grundlegenden Funktionen des Staates – der Wahrung des Gewaltmonopols, der Aufrechterhaltung rechtsstaatlicher Institutionen und der Bereitstellung öffentlicher Güter.[33]

Governance und Akteure

Herrschaftsstrukturen in Räumen fragiler Staatlichkeit sind zumeist fragmentiert und unübersichtlich. Überreste staatlicher Institutionen, wie beispielsweise Teile der Streitkräfte, sind oft von Korruption und Klientelpolitik gezeichnet, genießen kein Vertrauen in der Bevölkerung[34] und werden rechtsstaatlichen Ansprüchen nicht gerecht.

Daneben existiert eine Fülle nichtstaatlicher Akteure, von denen einige als legitime lokale *power broker* wahrgenommen werden und sogar staatliche Kernaufgaben erfüllen.[35] Sie tun dies jedoch oftmals aus Eigeninteresse und nur lokal wie zeitlich begrenzt. Sicherheit wird in solchen Situation auch als Dienstleistung angeboten, zum Beispiel von Warlords und PMSF.[36]

Schon heute vermischen sich in Räumen fragiler Staatlichkeit die lokale und globale Dimension der Politik: Lokale Ethnien, Stämme, Dorfgemeinschaften oder Gangs können eng mit TKN verbunden sein. Auch Entwicklungsbehörden von Drittstaaten, NGOs und TNU sind vertreten und verändern, beabsichtigt oder unbeabsichtigt, mit ihrem Handeln lokale Machtgleichgewichte – beispielsweise im Rahmen von Entwicklungsprojekten.[37] Weiterhin haben die Vorkommnisse in Räumen fragiler Staatlichkeit auch Rückwirkungen auf andere Regionen. So können durch Auswanderung in anderen Gebieten Diasporagemeinschaften entstehen und TKN und TUN können sich in Räumen fragiler Staatlichkeit dem Zugriff internationaler Regeln entziehen.[38]

Problemfelder heute und morgen

Fragile Staaten sind ein zentrales ordnungs- und sicherheitspolitisches Problem. Neben der Organisierten Kriminalität werden innerstaatliche Kriege, unkontrollierte Migration und die Destabilisierung von Nachbarländern als Gründe hierfür genannt.[39] Zugleich haben aber externe Akteure Interesse an diesen Räumen, beispielsweise wenn dort Ressourcen vorkommen.[40] In der Ressourcengewinnung engagieren sich zusätzlich zu privatwirtschaftlichen Akteuren zunehmend auch aufstrebende Wirtschaftsmächte und deren oft staatsnahe Unternehmen. So hat China zum Beispiel in den vergangenen Jahren stark in Sub-Sahara Afrika investiert.[41]

Infrastrukturen, die zur Ressourcengewinnung notwendig sind, sind in diesen Räumen immer wieder gefährdet. Dies ist beispielsweise im Niger-Delta zu beobachten, wo Öl-Pipelines wiederholt Ziel von Sabotageaktionen und Diebstahl wurden.[42] Auch unklare Eigentums- beziehungsweise Abbaurechte können zum Problem werden, wenn verschiedene Parteien um die Gebietsherrschaft streiten und jeweils das Recht für sich beanspruchen, Fördergenehmigungen zu erteilen.

Zukünftig ist es trotz dieser Hemmnisse aufgrund zunehmender Knappheit sowohl fossiler als auch mineralischer Rohstoffe[43] wahrscheinlich, dass Räume fragiler Staatlichkeit noch stärker in globale Handels- und Warennetze eingebunden werden.[44]

Weiterhin sind die Räume durch die häufig schwierige humanitäre Lage geprägt. Staaten wie Somalia, der Tschad, die Demokratische Republik Kongo oder Sudan weisen hohe Analphabetenquoten, hohe Kindersterblichkeit und ein hohes Maß an Kriminalität und Gewalt im Alltag – insbesondere gegen Frauen, Kinder und religiöse oder ethnische Minderheiten – auf.[45]

Entwicklungsproblematik und Rohstoffabbau stehen dabei häufig im Wechselspiel: Einerseits ist es beispielsweise beim Abbau mineralischer Rohstoffe im Kongo wiederholt zu Konflikten zwischen lokalen Bergbauarbeitern, TNU, PMSF, Rebellen und Regierungstruppen gekommen.[46] Die systematische Verletzung von Umweltschutzbestimmungen und abbaubedingte Umweltverschmutzungen spielen hier eine wichtige Rolle. Wasserverschmutzung, die Zerstörung ganzer Ökosysteme oder der Verlust fruchtbarer Böden können Gesundheitsschäden nach sich ziehen oder gar Migration erzwingen.[47]

Auch kann der Rohstoffabbau für ein Land zum „Fluch“ werden.[48] Die Vergangenheit hat gezeigt, dass ein zu stark auf Ressourcen basiertes Wachstum oft nicht nachhaltig ist und der Stabilität staatlicher Strukturen sogar eher schadet.

Entwicklungschancen ergeben sich hingegen dadurch, dass das Rohstoffinteresse auch zum Aufbau nützlicher Infrastrukturen wie Straßen und Bildungseinrichtungen in den Förderländern führen kann. Dies zeigte sich in jüngerer Vergangenheit etwa im Zusammenhang mit chinesischen Investitionen.[49]

Zukünftig wird auch die zunehmende informationstechnische Vernetzung verstärkt Entwicklungschancen schaffen. Die Zahl an Mobiltelefonen ist beispielsweise selbst in Sub-Sahara Afrika enorm angestiegen.[50] Und die Zahl der Internetnutzer hat sich in Afrika von 4,5 Millionen im Jahr 2000 auf 139 Millionen im Jahr 2011 vervielfacht. Der Anstieg schließt zunehmend Regionen in Sub-Sahara Afrika mit ein.[51] Die Vernetzung führt dazu, dass lokale Märkte aufgrund neu zugänglicher (Preis-)Informationen wesentlich effizienter funktionieren.[52]

Trotz dieser Chancen werden auch zukünftig Räume fragiler Staatlichkeit existieren. Neben den genannten Problemen sprechen hierfür die zukünftigen Auswirkungen des Klimawandels[53] sowie eine gesteigerte Zugänglichkeit konventioneller (z.B. Kleinwaffen) und unkonventioneller Wirkmittel.

Zukünftige Herrschaftsstrukturen

Auch die Herrschaftsstrukturen werden sich weiter transnationalisieren. TNU werden sich zum Beispiel im Rohstoffsektor engagieren. Hilfsorganisationen und andere finanzstarke und gegebenenfalls wehrhafte NGOs werden vor Ort versuchen, der sich teils verschlechternden humanitären Lage und einem zunehmenden Verlust an Umweltgütern entgegenzuwirken. Bei Abwesenheit staatlicher Strukturen könnten sowohl TNU als auch NGOs verstärkt versuchen, Sicherheit bei PMSF einzukaufen, mittels eigener Sicherheitskräfte selbst zu produzieren oder lokale Strukturen hierfür einzubinden.

Durch eine steigende Vernetzung und den dadurch eintretenden Bedeutungsverlust räumlicher Distanzen, werden Räume fragiler Staatlichkeit auch für TKN als *safe havens* weiter an Bedeutung gewinnen (z. B. für Internetkriminalität, vgl. Kap. 3.4).

Zugleich erlaubt die zunehmende Vernetzung lokalen nichtstaatlichen Akteuren, sich besser zu koordinieren und zu organisieren. Sie könnten zukünftig noch stärker mit transnationalen Akteu-

ren interagieren, zum Beispiel bei einer stärkeren Kooperation lokaler Bürgerbewegungen und NGOs oder bei einer Vernetzung lokaler krimineller Strukturen mit TKN.

Konkrete Akteurskonstellationen werden wahrscheinlich noch unübersichtlicher werden und es könnte zu einer stärkeren Vermischung der Agenden verschiedener Akteursgruppen kommen. Eine langfristige Gewinnorientierung könnte zum Beispiel TNU zunehmend motivieren, zivilgesellschaftliche Strukturen und die Entwicklung vor Ort zu fördern. Sie würden damit an Legitimität gewinnen und gleichzeitig das Umfeld ihrer geschäftlichen Aktivitäten stabilisieren. Andererseits könnte es aber auch zu einer Zunahme privatwirtschaftlicher *astroturfs* kommen, die vorwiegend die Unternehmensinteressen vertreten.

Staaten werden zukünftig weiterhin Interesse an der Stabilisierung von Räumen fragiler Staatlichkeit Räume haben. Vor dem Hintergrund neuer aufstrebender Mächte und getrieben durch nationale Interessen (z.B. an Ressourcen) könnten sich aber sehr unterschiedliche Gestaltungsvorstellungen entwickeln, was einem global koordinierten Bestreben zur Stabilisierung solcher Räume im Wege stünde.

Konfliktmittel und -wege

Für die Austragung von Konflikten stehen NSA einerseits gewaltfreie Mittel zur Verfügung, zum Beispiel die politische Mobilisierung der lokalen Bevölkerung oder der internationalen Zivilgesellschaft. Solche Mittel sind insbesondere für NGOs und TNU interessant, weil ihr Handlungsspielraum oft durch die Notwendigkeit zivilgesellschaftlicher Unterstützung beziehungsweise wegen des drohenden Verlustes der Unternehmensreputation beschränkt ist. Allerdings gibt es auch TNU und NGOs, für die dies nur bedingt gilt. Bei TNU sind Reputationskosten gegebenenfalls sekundär, wenn das Unternehmen zum Beispiel als Rohstofflieferant von strategischer Bedeutung ist oder kritische Verhaltensweisen nur schwer zu entdecken sind. Bei NGOs könnte dies wiederum der Fall sein, wenn sie von einer kleinen Gruppe von Unterstützern abhängt, die eine radikale Agenda verfolgen.

Gleichzeitig gilt, dass die Gewaltanwendung in Räumen fragiler Staatlichkeit weitgehend unreguliert und die Eskalation von Konflikten daher immer möglich ist. Das Spektrum an gewaltsamen Mitteln reicht von kleinen Sabotageakten, der Provokation gewaltsamer Proteste lokaler sozialer Gruppen, dem gezielten Einsatz privater militärischer Kräfte bis hin zu selbstständigen systematischen Gewaltanwendungen. Letzteres ist im Falle von TKN am wahrscheinlichsten.

Generell besteht in Räumen fragiler Staatlichkeit das Potenzial, dass die eigentlichen Konfliktparteien die Kontrolle über die Auseinandersetzung verlieren und diese durch die Handlungen anderer Akteure weiter eskaliert. Die Einbeziehung oder Manipulation lokaler Gemeinschaften durch NSA kann beispielsweise Eigendynamiken

entwickeln und gegebenenfalls in großflächigeren, politischen Konflikten münden.

Nichtstaatliche Konfliktkonstellationen

Konflikte zwischen TNU, die aus sehr unterschiedlichen Regionen der Welt stammen können, könnten zukünftig im Rohstoffsektor auftreten (vgl. Abb. 3.1); vor allem dann, wenn die TNU über konkurrierende Abbaulizenzen verfügen, die von unterschiedlichen, das Lagergebiet der Ressourcen für sich beanspruchenden Machthabern ausgestellt wurden. Konflikte könnten sich auch schon vor der Rechtevergabe ergeben, wenn TNU aktiv versuchen, Auseinandersetzungen zwischen den Machthabern zugunsten jener Partei zu beeinflussen, von der sie sich die gewünschte Rechtevergabe versprechen.[54]

Konflikte zwischen TNU und TKN sind ebenfalls plausibel. Denkbar wäre, dass ein Unternehmen – unter Umständen unbewusst – in einem stark mit kriminellen Strukturen durchdrungenen Raum operieren will. Da TNU primär profitorientiert sind, wäre es möglich, dass sie sich mit Schutzgeldforderungen von TKN informell arrangieren, wenn dieses Verhalten wirtschaftliche Gewinne verspricht. Zu einer gewaltsamen Eskalation könnte es kommen, wenn ein entsprechender Konflikt erst auftritt, nachdem ein TNU bereits erhebliche Investitionen getätigt hat und sich anschließend genötigt sieht, diese auch – beispielsweise unter Beauftragung von PMSF – gegen TKN zu verteidigen. Auch ist es möglich, dass das TNU die verfügbaren Ressourcen für so wertvoll oder strategisch wichtig hält, dass ein Konflikt mit TKN rational erscheint.

Zwischen TKN könnten noch gewaltsamere Konflikte entstehen, wenn sich diese in lokale Machtkämpfe einmischen, begrenzte Landstriche – beispielsweise zum Anbau von Drogen oder zum Kontrollieren von Handelswegen – unter ihre Kontrolle bringen wollen oder grundlegend um die Vorherrschaft in einem Gebiet wetteifern.

In einer ähnlich gelagerten Konstellation gewinnt die transnationale Vernetzung von Räumen fragiler Staatlichkeit an Bedeutung: Lokale Terrorgruppen oder kriminelle Organisationen könnten nach Anschluss an größere, transnationale Netzwerke streben und dabei in einer Art Wettstreit versuchen, mit der Effizienz oder Brutalität ihres Vorgehens, um die Aufmerksamkeit der jeweiligen transnationalen Akteure zu werben.

Schlussendlich könnten auch NGOs in nichtstaatliche Konflikte verwickelt werden. Sie könnten sich gegen TNU aber auch gegen TKN wenden, deren Praktiken sie als ungerecht, menschenverachtend oder umweltzerstörend erachten. Eine gewaltsame Eskalation wäre nicht auszuschließen. Besonderes Eskalationspotenzial ergäbe sich, wenn es sich um radikale NGOs handeln würde, die auf Dienste von PMSF oder andere Sicherheitsdienstleister zurückgreifen, oder wenn sie globale Diasporagemeinden repräsentierten, die systematisch und resolut lokale Kräfte unterstützen oder schützen wollen.

Abbildung 3.1: Konfliktbild 1 – Das gefährliche Geschäft mit Ressourcen

Das gefährliche Geschäft mit Ressourcen

TNU (+ Stellvertreter-NGO) versus TNU

Heute, im Jahre 2031, ist *Global Resources* der Weltmarktführer im Bereich mineralischer Rohstoffe – ein Weltmarktführer in der Krise. Die wichtigste Mine des Unternehmens liegt in einer politisch instabilen Region. Lange war es gelungen, die Mine durch eine Mischung aus lokalen strukturbildenden Maßnahmen, den Einsatz von PMSF sowie gute Kontakte zur Regierung zu sichern. Kürzlich ist die Produktion jedoch faktisch zum Erliegen gekommen – Was ist passiert?

Die globale Rohstoffnachfrage hatte Unternehmen aus aller Welt immer stärker um Rohstoffvorkommen wetteifern lassen – auch in dem für *Global Resources* so wichtigen Gebiet. So begann das Konkurrenzunternehmen *Fair Resources* vor gut einem Jahr, die Regierung des Förderlandes dazu zu drängen, einen Teil der Abbaurechte umzuverteilen. Der Erfolg blieb jedoch aus.

Dann kam die landesweite Wahl im Herbst 2030: Globale NGOs berichteten, dass es der Opposition zum ersten Mal gelungen sei, die Mehrheit zu gewinnen. Dennoch stand nach offiziellem Wahlergebnis das alte Regime als Sieger dar. Die NGOs sprachen von Wahlbetrug.

Im Gebiet der *Global Resources*-Mine stachelte daraufhin die lokale NGO *Re-source-stainable*, getragen von angesehener Vertreter der regionalen Mehrheitsbevölkerung, ihre Mitbürger mit Flugblattaktionen gegen *Global Resources* auf. In den Blättern wurde vor allem die enge Zusammenarbeit zwischen Zentralregierung und dem Unternehmen angeprangert.

Im Land war es ein offenes Geheimnis, dass die Mehrheitsvertreter von *Fair Resources* bestochen worden waren, um mit dem Protest zu beginnen. „Astroturf Inc." titelte eine angesehene europäische Zeitschrift. Tatsächlich trat kurz nach der Flugblattaktion das *Fair Resources* selbst mit einer neuen Strategie auf den Plan. Es versprach der lokalen Mehrheit einen faireren Abbau der Rohstoffe, sollte diese sich für eine Neuvergabe der Abbaurechte einsetzen.

Global Resources lud daraufhin Vertreter von lokalen Minderheiten zu Gesprächen ein, die über gute Kontakte zur Zentralregierung verfügten. Das Wohlwollen dieser Vertreter, so hofften wohl die Unternehmenslenker, könnte ihren Einfluss sichern. *Fair Resources* reagierte mit verschärfter Rhetorik und warf *Global Resources* und den Minderheitsvertretern eine „Verschwörung gegen das Volk" vor.

Nur wenig später rief *Re-source-stainable* zu Protesten auf. Dabei kam es zu Auseinandersetzungen zwischen Minderheit und Mehrheit in der Minen-Region. Geschäfte und Wohnungen wurden geplündert und in Brand gesetzt. *Fair Resources* distanzierte sich von den *Re-source-stainable*-Aktionen und kündigte seinen Rückzug aus der Region an – die politische Lage ließe kein nachhaltiges Engagement zu.

Doch die Plünderungen gingen weiter. Von Tag zu Tag wurden die Auseinandersetzungen schlimmer. Die Regierung sah sich gezwungen, zum Schutz der ihr nahe stehenden Minderheit einzugreifen und verlegte Truppen in die Region. Im März 2031 kam es zu Kämpfen zwischen regionaler Mehrheit und dem Militär der Zentralregierung. Westliche Kommentatoren befürchten eine Destabilisierung des ganzen Landes. Eine Zeitschrift fragte sogar: „Wird das Pulverfass explodieren?"

Quelle: eigene Darstellung.

3.2. Nichtstaatliche Konflikte in maritimen Räumen

Unter maritimen Räumen werden im Folgenden die weltweit vorhandenen Meeresoberflächen, der jeweils darunterliegenden Meeresboden, die Wassersäule, sowie die Luft darüber verstanden.

Governance

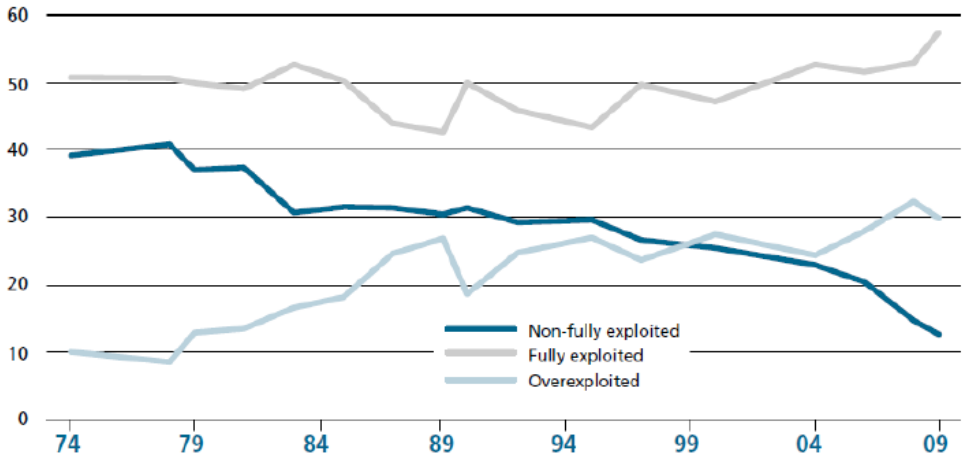
Nach dem Seerechtsübereinkommen der VN von 1982 gliedern sich maritime Räume in drei Kategorien: Die Zwölf-Seemeilen-Zone unterliegt der vollen Souveränität des jeweiligen Küstenstaates (Art. 3 und 4).[55] Hieran schließt sich eine zweihundert Seemeilen von der Küste ins Meer reichende ausschließliche Wirtschaftszone an (Art. 55–75). Jenseits dieser Zonen erstreckt sich, drittens, die Hohe See (Art. 86 und 87), die keiner nationalstaatlichen Souveränität unterworfen ist, teilweise aber durch Verträge und Institutionen mit VN-Mandat reguliert wird. Zu den wichtigsten Institutionen zählen die Internationale Meeresbodenbehörde, die Rohstoffvorkommen auf dem Meeresboden verwaltet, und die Internationale Seeschifffahrtsorganisation, welche sich zum Beispiel mit Sicherheitsstandards in der Schifffahrt und der Reduzierung der Meeresverschmutzung beschäftigt.

Nutzungsformen und Akteure heute und morgen

Neben Staaten haben traditionell Hochseefischer in maritimen Räumen agiert. Die Fischerei ist eine der wichtigsten Nutzungsformen maritimer Räume. Doch schon heute sind viele Bestände durch Überfischung gefährdet (vgl. Abb. 3.2).[56] In Zukunft wird diese Gefährdung durch den steigenden Fischkonsum wahrscheinlich weiter zunehmen.[57] Ursachen der Überfischung sind neben der Nachfragesteigerung der illegale Fischfang[58] und die Versäumnisse einiger Staaten, existierende Fangquoten durchzusetzen.[59] Die Situation hat dazu geführt, dass neue NSA sich in maritimen Räumen engagieren. Insbesondere NGOs versuchen, gegen die Überfischung vorzugehen und bedienen sich dabei sehr unterschiedlicher Mittel. Der WWF hat beispielsweise eine Software entwickelt, mit der eine verbesserte Überwachung illegaler Fischfangaktivitäten möglich sein soll.[60] Wesentlich kontroversere Reaktionen, nämlich unter anderem das Versenken illegaler Fischerboote und Walfänger, sind bei *Sea Shepherd* zu beobachten.

Nicht nur Fische, auch andere Teile maritimer Ökosysteme, wie Korallenriffe oder solche in der Arktis, sind heute schon gefährdet – beispielsweise durch Unglücke bei Tiefseebohrungen, wie bei der Ölkatastrophe im Golf von Mexiko 2010. Hinzu kommen Tankerunfälle und illegale Verschmutzungen durch eine weltweit anwachsende Containerflotte. Zukünftig werden mögliche negative Nebenfolgen beim Tiefseebergbau (s.u.) und auch der Klimawandel weitere maritime Ökosysteme zerstören.[61]

Abbildung 3.2: Entwicklung der globalen Fischbestände seit 1974



Als fully exploited werden jene Bestände bezeichnet, die bis an die Grenze der Nachhaltigkeit befischt werden. Overexploited verweist darauf, dass diese Schwelle überschritten ist. Abhängig von der konkreten Fischart gelten Bestände als überfischt, wenn mehr als 40 bis 60 Prozent des ursprünglichen Bestandes abgefischt werden und sich daher der Bestand dauerhaft nicht mehr regeneriert.

Quelle: FAO (2012: 56).

Andere NSA in maritimen Räumen sind Reedereien. Der Seehandel hat in den vergangenen Jahrzehnten starke Zuwächse verzeichnet und ist heute beispielsweise in der EU für rund neunzig Prozent des Außenhandels verantwortlich.[62] Hochrechnungen zufolge wird der Seehandel auch in Zukunft weiter wachsen. Allein bis 2015 werden die Kapazitäten der globalen Containerflotte um ungefähr 25 Prozent ansteigen.[63] Containerumschlag und -flotte wachsen damit gut doppelt so schnell wie das globale BIP.[64] Weiterhin könnten sich zukünftig durch die Folgen des Klimawandels neue und kürzere Transportwege in der Arktis auftun. Die Nutzung der an der russischen Nordküste entlangführenden Nordostpassage würde etwa die Transportzeit zwischen Hamburg und Yokohama um vierzig Prozent verkürzen.[65] Da diese jedoch durch das sensible Gebiet der Arktis führt, entstehen wiederum Gefahren für die Umwelt.

Ein zentrales Problemfeld im Zusammenhang mit dem Seehandel ist die Piraterie. Trotz des Engagements von Staaten, wie beispielsweise in der Operation *Atalanta* am Horn von Afrika, entstehen durch Piratenangriffe schätzungsweise Schäden von jährlich 4,9 bis 12 Milliarden US-Dollar,[66] und 40 Prozent des über Seewege transportierten Öls ist von Piratenangriffen bedroht.[67] Mittlerweile greifen immer mehr Reeder auf die Dienste von PMSF zurück,[68] die bei ihrer Arbeit teils auch robust vorgehen.[69]

Von besonderer Bedeutung für den Seehandel sind auch Engpässe, zum Beispiel die Straße von Malakka, die

Straße von Hormus und der Suezkanal sowie kritische Infrastrukturen, allen voran Häfen.[70] Weitere kritische Infrastrukturen in maritimen Räumen sind Öl- und Gaspipelines und die für Telekommunikation und das Internet unabdingbaren Unterseekabel. Der transozeanische Internet- und Telefonverkehr hängt heute beispielsweise zu 99 Prozent von diesen Kabeln ab. Nach einer Schätzung der *US Federal Reserve Bank* laufen über diese Leitungen pro Tag Transaktionen im Wert von zehn Billionen US-Dollar.[71]

Schließlich sind maritime Räume auch als Abbaugebiete von Rohstoffen wichtig. Rund achtzig Prozent der europäischen Erdöl- und Gasproduktion stammen beispielsweise aus Nordsee, Mittelmeer und der Adria.[72] Darüber hinaus befinden sich innerhalb der Zweihundert-Seemeilen-Zone weltweit eine Vielzahl von Öl- und Gasfeldern – beispielsweise im Golf von Mexiko, im Nigerdelta und in der Arktis. Auf Hoher See kommen weiterhin mineralische Rohstoffe vor, zum Beispiel polymetallische Knollen, Eisen-Mangan-Krusten und Massivsulfiden.[73] Bedeutende Vorkommen liegen zwischen Hawaii und Mexiko, im Perubecken und im zentralen Indischen Ozean. Sie werden von der Internationalen Meeresbodenbehörde verwaltet und bereits heute erkundet.[74] Zukünftig werden aufgrund steigender Preise und sinkender Reserven an Land wahrscheinlich sowohl die *offshore*-Förderung von Erdöl und -gas als auch neue Arten des Tiefseebergbaus vorangetrieben werden.

In Zukunft wird es somit zu einer Intensivierung der Nutzung maritimer Räume kommen und damit auch zu vermehrter Interaktion zwischen NSA. Die Handlungsspielräume von NSA werden besonders dort zunehmen, wo Staaten nicht gewillt oder fähig sein werden, ihre Macht zu projizieren und internationale Regelwerke durchzusetzen. NGOs könnten verstärkt versuchen, Normverletzungen entgegenzuwirken. Neben der Ausdehnung des Seehandels bergen auch Überfischung, Umweltrisiken, der Klimawandel und der Rohstoffabbau in Zukunft Konfliktpotenziale.

Nicht zuletzt gefährden solche Entwicklungen traditionelle Ernährungs- und Erwerbsmöglichkeiten in der lokalen Fischerei. Es ist daher damit zu rechnen, dass Piraten auch zukünftig ein Problem darstellen werden,[75] obwohl die Zahl der Piratenangriffe im Jahr 2012 zurückgegangen ist.[76] Zunehmend könnten sie sich dabei mit TKN oder politischen Kräften[77] verbinden. Durch neue Gefahren würden sich auch neue Geschäfte für PMSF ergeben. Die britische Firma *Typhon* plant beispielsweise den Aufbau einer privaten „Kriegsflotte“ zum Schutz von Transporten gegenüber illegalen Übergriffen auf der Hochsee.[78]

Konfliktmittel und -wege

Generell erleichtert sich durch die Verbreitung hochseetauglicher Schiffe für NSA der Zugang zur Hohen See. Denkbare gewaltfreie Mittel, die von NSA in Konflikten in maritimen Räumen verwendet werden könnten, sind Medienkampagnen, medial aufbereitete Proteste auf Hoher See und eine gezielte Diffamierung anderer NSA. Insbesondere für legale und auf ihre Reputation angewiesene Akteure sind diese attraktiv.

Weiterhin möglich ist zukünftig der verstärkte Einsatz nicht-letaler Wirkmittel, wie Lautstärkekanonen. Diese können aufgrund geringer physischer Schäden für Umwelt-NGOs interessant sein, wenn diese gegen illegale Fischer vorgehen.

Auch raumübergreifend Angriffe aus dem Cyberspace sind denkbar, etwa auf die Steuerungsanlagen von Bohrinseln oder auf Steuerungs-, Kommunikations- und Navigationssoftware von Schiffen. Eine Störung oder Manipulation der Navigation könnte auch durch gezieltes Stören von GPS-Signalen erfolgen (vgl. Kap. 3.3). Dies könnte insbesondere illegal operierenden Kräften neue Übergriffs- und Kaperungsmöglichkeiten eröffnen. Gegen eine Verwendung durch legale Akteure, zumindest innerhalb der Zwölf- und Zweihundert-Seemeilen Zone, sprechen hingegen Risiken, wie Schiffsunglücke und möglicherweise hieraus entstehende Umweltschäden.

Auch die Nutzung verschiedener physischer Gewaltmittel ist denkbar. So können Schiffe durch Rammen stark beschädigt oder versenkt werden. Eigene oder gegnerische havarierte Schiffe selbst könnten zur Sperrung von Engpässen und Fahrrinnen verwendet werden.

Ein Einsatz von Mitteln wie Handfeuerwaffen, relativ preiswerten und verfügbaren Seeminen, Aufklärungsdrohnen bis hin zu komplexen Waffensystemen ist außerdem denkbar. Bereits heute sind fernsteuerbare Raketensysteme mit einer Abschussvorrichtung aus einem modifizierten Frachtcontainer heraus erhältlich.[79] Solche Systeme sind in Zukunft eher finanzstarken Akteuren zuzurechnen.

Nichtstaatliche Konfliktkonstellationen

Konfliktkonstellationen innerhalb der Zwölf- und Zweihundert-Seemeilenzone könnten jenen in Räumen fragiler Staatlichkeit ähneln. TNU könnten auch in maritimen Räumen nahe der Küsten bei der Ausbeutung von Ressourcen – seien es fossile Energieträger oder Fischbestände – in Konflikt geraten, wenn sich Herrschaftsansprüche und damit Abbaulizenzen überschneiden. Zusätzlich besteht in maritimen Räumen jedoch eine erhöhte Wahrscheinlichkeit, dass es dort zu Streitigkeiten zwischen Unternehmen kommen könnte, wo Gebietsansprüche zwischen konsolidierten Staaten kollidieren. Dies könnte gegebenenfalls auch Konflikte zwischen den Staaten selbst provozieren.

Auch lokale Akteure oder radikalisierte NGOs könnten wie in Räumen fragiler Staatlichkeit, beispielsweise aus Umweltschutzgründen, mit TNU oder TKN in Konflikt geraten (vgl. Abb. 3.3). Sie könnten beispielsweise Infrastrukturen von Energieunternehmen vor der Küste virtuell oder physisch angreifen und so erheblichen Schaden anstellen.

Im Falle der Konstellation TNU versus TKN stellt sich die Situation ebenfalls ähnlich dar wie in Räumen fragiler Staatlichkeit. Zusätzlich bestehen hier jedoch Erpressungsmöglichkeiten, zum

Beispiel wenn ein TKN mit der Sperrung von Häfen oder Engpässen droht.[80] Durch eine solche Sperrung könnte die Nutzung maritimer Räume massiv gestört werden.[81] Einschränkend ist jedoch zu sagen, dass die Durchführung einer solchen Sperrung großer Fähigkeiten bedarf und dass eine solche Konstellation nicht mehr als rein nichtstaatlicher Konflikt angesehen werden kann. Statt allein gegen einzelne NSA, wäre eine solche Sperrung gegen eine Vielzahl von Akteuren – auch Staaten – gerichtet. Gerade als extremistische Tat mit Symbolcharakter ist sie dennoch zumindest denkbar.

Eine weitere Konfliktkonstellation wäre jene zwischen organisierten Menschenschmugglern auf See und PMSF, die als Grenzschützer maritimer Grenzverläufe – sei es für Staaten oder nichtstaatliche politische Kräfte – eingesetzt würden. Besondere Konfliktdynamiken könnten dann entstehen, wenn Diasporagemeinschaften Flüchtlingsbewegungen zusätzlich unterstützen.

Auf der Hohen See könnte es im Zusammenhang mit dem Abbau von Rohstoffen zu Konflikten kommen. Die Frage, wie der exklusive Zugang zu Tiefseebergbau-Gebieten von TNU effektiv gesichert werden kann, ist bis heute ungeklärt. Andere TNU aber auch TKN könnten die Überwachungsproblematik nutzen, um unautorisiert Ressourcen abzubauen und so einen Konflikt mit dem lizenzhaltenden Unternehmen provozieren. Angriffsziele sowohl für den illegal Abbauenden als auch für den sich verteidigenden Akteur könnten jeweils gegnerische Abbausysteme und Rohstofftransporte sein.

Eine gewaltsame Eskalation scheint möglich, wenn TNU versuchen, den Schutz der Abbaugebiete mittels PMSF sicherzustellen. Generell gilt aber auch hier, dass Reputationskosten gegebenenfalls eine Rolle spielen und die Konfliktaustragung nur dann plausibel ist, wenn das Unternehmen diese entweder nicht berücksichtigen muss oder wenn es gelingt, die eigenen Konflikthandlungen zu verschleiern – zum Beispiel durch die Nutzung von Proxy-Umweltaktivisten.

Zwischen TNU und NGOs könnte es auch auf Hoher See aufgrund der Bedrohung von Ökosystemen zu Konflikten kommen. Neben dem Fischfang könnten Letztere auch gegen den Tiefseebergbau vorgehen wollen. Der Gewalteinsatz durch wehrhafte NGOs wäre besonders in der Phase der Erkundung durch Rohstoffunternehmen plausibel, da in diesem Stadium, etwa durch die Zerstörung von Erkundungsschiffen, nur geringe Umweltschäden drohen würden. Weiterhin möglich sind Sabotageakte mit dem Ziel, den Betrieb zu stören und die Kosten für den Abbau so zu erhöhen, dass er unprofitabel wird. Ein reaktiver Einsatz von Gewaltmitteln seitens der TNU zum Schutz der Unternehmensinteressen wäre eine mögliche Konsequenz.

Schließlich ist auf die Piraterie zu verweisen, die zukünftig durch ein systematisches Engagement von TKN, die Zugänglichkeit neuer Wirkmittel und die Ausdehnung der Reichweite dieser Mittel trotz Gegenmaßnahmen eine neue Dimension annehmen könnte. Besser gerüstete und gegebenenfalls auch robuster vorgehende PMSF könnten in großräumige Konflikte mit TKN/Piraten verwickelt werden.

Abbildung 3.3: Konfliktbild 2 – Die radikalen Retter der Natur

Die radikalen Retter der Natur

NGO (+ PMSF) versus TKN

Im Jahre 2028 sind die Weltmeere überfischt und eine Vielzahl von Fischarten unterliegt weltweiten Handelsbeschränkungen. Dennoch werden die „verbotenen Meeresfrüchte“ auf dem Schwarzmarkt vertrieben.

Auch vor der Küste *Naturistans* kommen begehrte Fische vor – in einem maritimen Schutzgebiet, dass weit in die 200-Seemeilenzone hineinreicht. Die Pflege des Gebietes hat die Regierung wegen Kapazitätsmangels an die NGO *Green Conscience* übergeben. Bisher ist es dieser mit dem Einsatz von satellitengestütztem Monitoring, durch Verhandlungen mit internationalen Fangflotten und durch Patrouillen eigener Boote gelungen, das Fangverbot weitgehend durchzusetzen. Nur die lokale Bevölkerung darf im Schutzgebiet nachhaltigen Fischfang betreiben. Die Kontakte zur Bevölkerung sind gut. Der Wert der Fangbegrenzungen wird anerkannt.

Doch in den letzten Jahren sind die Schwarzmarktpreise für die im Schutzgebiet lebenden Fischarten schlagartig gestiegen – besonders der asiatische Raum hat die Fische als Delikatesse entdeckt. Vor der Küste *Naturistans* werden des Nachts zunehmend unbekannte Schiffe gesichtet. Viele verdächtigen eine Art *Fischmafia*, das Fangverbot systematisch zu verletzen. Schon einige Male hat *Green Conscience* die Küstenwache *Naturistans* um Hilfe gebeten. Die Regierung jedoch lehnte ab.

Ende 2028 wird die Lage unübersichtlich: Die internationale Gemeinschaft verurteilt zwar den illegalen Fischfang im Schutzgebiet, sieht sich aber nicht in der Lage, dagegen vorzugehen. In der lokalen Bevölkerung werden Rufe nach Gegenmaßnahmen immer lauter.

Gleichzeitig werden die Forderungen des zumeist aus westlichen Gesellschaften stammenden Unterstützerkreises von *Green Conscience* immer deutlicher – es könne nicht angehen, dass Kriminelle die Paradiese des Planeten zerstören. Man solle sie vertreiben! Anfang 2029 verkündet eine Splittergruppe von *Green Conscience* „endlich durchzugreifen“. Sie hätte dabei die „volle Unterstützung“ der lokalen Bevölkerung und mit Hilfe eines nicht genannten Großspenders sei es gelungen, einen robusten maritimen Wachdienst zu organisieren.

In der Folgezeit kommt es zu gewaltsamen Übergriffen zwischen Wachdienst und *Fischmafia*. Bei einer Schießerei kommen Angestellte der PMSF, die das Schutzgebiet bewachen soll, ums Leben und eines ihrer Schiffe wird stark beschädigt. In den nächsten beiden Monaten werden drei illegale Fischerboote versenkt. Nach Schätzungen europäischer Beobachter kommen dabei rund 40 Fischer ums Leben. Bei einer Versenkung nahe der Küste laufen große Mengen Altöl und Treibstoff aus. „Für die Küstenbevölkerung ist das ein Desaster“, so ein Sprecher von *Green Conscience*, „sie wird um ihre Lebensgrundlage gebracht. So gewinnt niemand.“

Dennoch richtet sich die Wut der Bevölkerung gegen *Green Conscience*, deren lokale Mitarbeiter angefeindet werden. Auch die Regierung schlägt auf diesen Kurs ein und nimmt europäische Aktivisten, darunter auch zwei Deutsche, fest. Auf einer Pressekonferenz erklärt sie: „Wir werden von kriminellen Banden und einer westlichen NGO bedroht und haben nicht die Mittel, uns dagegen zu wehren. Das kann nicht sein, wir verlangen Rechenschaft.“

Quelle: eigene Darstellung.

3.3. Nichtstaatliche Konflikte im Weltraum

Unter dem Weltraum wird im Folgenden der Raum jenseits der Erdatmosphäre inklusive aller der dort vorhandenen Objekte, wie Himmels- und Flugkörper, verstanden. Nach der international gebräuchlichsten Definition beginnt der Weltraum einhundert Kilometer über der Erdoberfläche mit der so genannten *Kármán*-Linie. Diese Definition der *Fédération Aéronautique Internationale* ist jedoch völkerrechtlich nicht verbindlich. Die NASA zum Beispiel sieht die Grenze bereits bei fünfzig Meilen beziehungsweise achtzig Kilometern über der Erdoberfläche.

Governance

Im Weltraum gelten das in Artikel 2 (4) der VN-Charta festgeschriebene Verbot bewaffneter Aggression und das dort in Artikel 51 verankerte Selbstverteidigungsrecht. Spezifischer regelt der Weltraumvertrag (WRV) von 1967 die Nutzung des Raumes.[82] Dieser beinhaltet das Gebot der friedlichen Nutzung für den Mond und andere Himmelskörper und verbietet Stützpunkte, Waffen und militärische Übungen auf diesen. Für den restlichen Weltraum gilt das Gebot nur teilweise, lediglich Kern- und Massenvernichtungswaffen sind dort explizit verboten. Ob Waffensysteme, die den Weltraum lediglich durchqueren, verboten sind, ist völkerrechtlich umstritten.[83]

Der WRV erklärt den Weltraum zur Allmende[84] und schließt so Eigentumsansprüche und Hoheitsrechte an Teilen des Weltraumes, am Mond und an anderen Himmelskörpern für Staaten aus (Art. II). Ob diese Regelung auch für NSA gilt, ist umstritten.[85] Auch über die Vermeidung von Verunreinigungen enthält der WRV Bestimmungen. Diese haben aber bisher kaum praktische Auswirkungen.[86]

Zum WRV gibt es noch einige Ergänzungsverträge.[87] Dennoch werden die bestehenden Verträge und Prinzipienkataloge nach Meinung vieler Beobachter der Bedeutung des Weltraumes und seiner Nutzung durch eine steigende Zahl von Akteuren nicht gerecht.[88] Obwohl es weitere Initiativen gegeben hat, um Verhaltensregeln aufzustellen,[89] unterscheiden sich die Vorstellungen von Staaten hinsichtlich der internationalen Verrechtlichung des Weltraumes nach wie vor deutlich.[90]

Akteure und Nutzungsformen

Die Kosten und technologischen Hürden, um im Weltraum zu agieren, sind im Vergleich zu anderen Räumen sehr hoch. Deshalb waren ursprünglich nur Staaten dort vertreten, die den Weltraum lange Zeit vorrangig zu militärischen Zwecken nutzten. Heute wird er für vielfältige Aktivitäten wie Wissenschaft und Forschung, Kommunikation, Navigation und Erdbeobachtung, sowie Aufklärung und Führung genutzt.

Auch die Akteure sind vielfältiger geworden. Zum einen gibt es mehr Raumfahrtnationen als früher. Insbesondere asiatische Staaten wie China, Japan und Indien bauen ihre Weltraumprogramme aus.[91] Manche Kommentatoren fürchten daher, dass eine Militarisierung die zukünftige Entwicklung des Weltraumes beeinflussen wird.[92]

Zum anderen drängen verstärkt Unternehmen in den Weltraum. Sie stellen

beispielsweise Trägersysteme und Satelliten her, verbringen diese in den Weltraum, betreiben sie und stellen satellitengestützte Dienstleistungen bereit, die aus modernen Gesellschaften nicht mehr wegzudenken sind. Unter Beobachtern herrscht weitgehend Einigkeit, dass die kommerzielle Nutzung des Weltraumes zukünftig deutlich ansteigen wird.[93] Besonders aufgrund absehbar angespannter Haushaltslagen vor allem in der westlichen Welt ist mit einer verstärkten Privatisierung der Raumfahrt zu rechnen.[94] Indiz für diesen Trend ist eine Mission im Mai 2012, in welcher der Nachschub für die internationale Weltraumstation (*International Space Station*, ISS) allein durch ein privates Raumschiff der Firma *SpaceX* bereitgestellt wurde – eine Aufgabe, die bis dahin nur durch staatliche Raumfahrtbehörden geleistet wurde und geleistet werden konnte.

Unternehmen spielen auch bei der touristischen Erschließung des Weltraumes eine wichtige Rolle.[95] Heutiger Marktführer ist *Space Adventures* aber auch andere Unternehmen wie *Blue Origin*, *SpaceX*, *Orbital* und *SpaceDev* wollen in diesem Geschäft Fuß fassen.[96] Selbst ein Weltraumhotel befindet sich bei der Firma *Bigelow Aerospace* bereits in der Entwicklung. Es ist anzunehmen, dass Firmen im Bereich Weltraumtourismus weiter investieren werden. Sinkende Kosten durch regelmäßigere Weltraumflüge könnten zu einer künftig steigenden Nachfrage nach Weltraumreisen führen.

Ein Handlungsfeld, zu dem bisher lediglich theoretische Konzepte existieren, ist das *asteroid mining,* bei dem es darum geht, mit bemannten und unbemannten Missionen Rohstoffe auf erdnahen Objekten, wie Asteroiden, Kometen und Meteoriten zu identifizieren, zu erforschen und abzubauen.[97] Es ist ungewiss, wann beziehungsweise ob *asteroid mining* in der Zukunft das Stadium theoretischer Konzepte verlassen wird und ob es überhaupt wirtschaftlich rentabel sein kann.[98] Sollte dies gegeben sein, könnte der Abbau von Rohstoffen perspektivisch einen weiteren wichtigen Aspekt in der Nutzung des Weltraumes darstellen.

Während TNU die Möglichkeit erlangt haben, direkt im Weltraum zu agieren, ist dies anderen NSA wegen der hohen technologischen und finanziellen Hürden bisher nicht gelungen. Allerdings werden Infrastrukturen und Systeme im Weltraum zumeist von der Erde aus „gesteuert“. Hierdurch können NSA prinzipiell auch auf diesen Raum zugreifen, wenn sie nicht direkt in ihm agieren können. Es bieten sich beispielsweise Möglichkeiten, weltraumbasierte Objekte – insbesondere Satelliten – direkt von der Erdoberfläche und über den Cyberspace zu beeinflussen (s.u.).

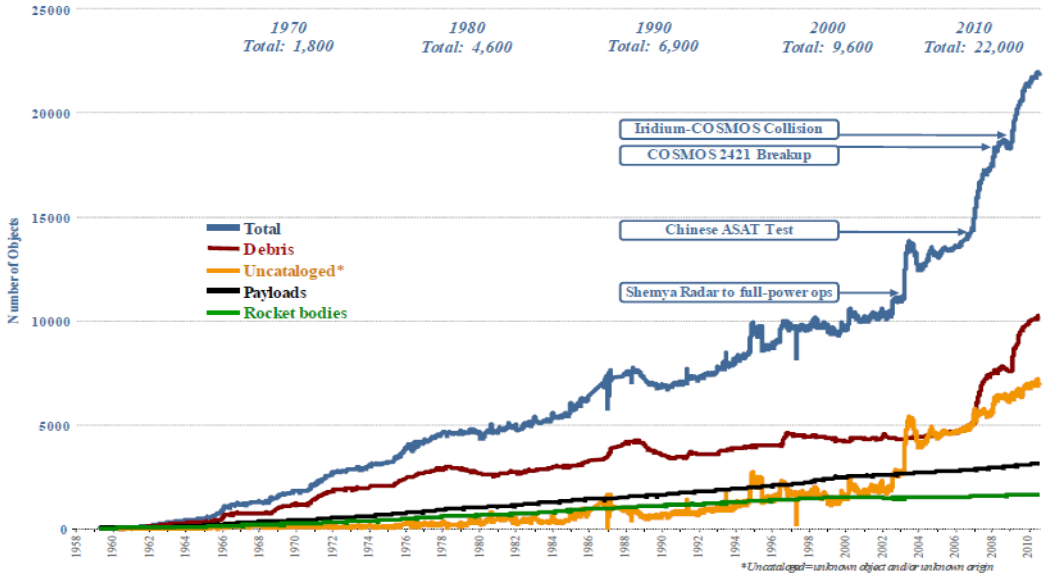
Problemaufriss

Mit einem größeren Aktivitäts- und Akteursspektrum wird es voller im Weltraum. Begehrte Satellitenpositionen werden stetig knapper. Schon heute befinden sich Satellitenbetreiber, wie *Intelsat* und *SES World*, in einem in-

tensiven Wettbewerb. Im Mai 2010 kam es beinahe zu einer Satelliten-Kollision, nachdem der *Intelsat*-Satellit *Galaxy 15* außer Kontrolle geraten war und sich gefährlich auf die Position eines *SES*-Fernsehsatelliten zubewegte.[99]

Doch nicht nur zwischen Satelliten besteht zunehmend Kollisionsgefahr, sondern auch zwischen diesen und anderen Himmelskörpern und Schrotteilen. Laut *U.S. Department of Defense* existieren etwa 22.000 menschengemachten Objekten im Weltall. Davon sind aber nur rund 1.100 funktionierende Satelliten. Der Rest, der Weltraumschrott oder *debris* genannt wird, besteht aus ausgebrannten Raketenstufen, stillgelegten Satelliten sowie Teilen davon (vgl. Abb. 3.4).[100] Hinzu kommen mehrere hunderttausend kleinere Schrottteile in der Größenordnung von über einem Zentimeter. In der Größenordnung von unter einem Zentimeter sind es Schätzungen zufolge weitere einhundert bis zweihundert Millionen Teile.[101]

Abbildung 3.4: Ausbreitung menschengemachter Weltraumobjekte seit 1960



Quelle: US National Security Space Strategy Summary (2011: 1).

Kollisionsgefahr und *debris* stehen in enger Wechselwirkung miteinander. Einerseits führen Kollisionen zur Ausbreitung von *debris*. So wurden beispielsweise bei der Kollision zwischen einem kommerziellen amerikanischen Satelliten und einem ausrangierten russischen Militärsatelliten im Februar 2009 hunderte Trümmerteile freigesetzt.[102] Auch Tests von Antisatelliten-Waffen tragen zum Problem bei. Im Jahr 2007 entstand beispielsweise durch den Abschuss eines inaktiven Wettersatelliten durch China die größte *debris*-Wolke, die jemals durch ein einzelnes Ereignis ausgelöst wurde.[103]

Andererseits gefährdet der *debris* das Agieren und die Infrastrukturen staatlicher und nichtstaatlicher Akteure. Bereits kleine Schrottteile können aufgrund ihrer Geschwindigkeit und der damit verbundenen kinetischen Energie erheblichen Schaden anrichten. Allein bei europäischen Satelliten entsteht durch Kollisionen mit anderen Himmelskörpern ein Schaden von über

330 Millionen Euro im Jahr. Schon heute müssen Satelliten und auch die ISS Ausweichmanöver fliegen, um einer Kollision mit Weltraumschrott zu entgehen. 2010 und 2011 soll die ISS-Besatzung wegen vorbeifliegender großer Schrottteile sogar evakuiert worden sein.[104]

Im schlimmsten Falle könnten Kollisionen oder der Einsatz von Antisatellitenwaffen zum, nach dem NASA-Berater Kessler benannten, Kessler-Effekt führen. In diesem *worst case*-Szenario kollidieren entstehende Schrottteile erneut, lösen Kaskadeneffekte aus und führen hierdurch zu einer so hohen Konzentration von *debris* im erdnahen Weltraum, dass die Raumfahrt langfristig unmöglich werden würde.

Vor dem Hintergrund dieser Entwicklungen wird eine zentrale zukünftige Herausforderung darin bestehen, den Überblick über die Vielzahl an Objekten, Akteuren und Aktivitäten im Weltraum zu behalten (Weltraumlage). Bisher gehören vor allem die USA zu den „Sehenden" im erdnahen Weltraum. Jedoch selbst deren *Space Surveillance Network* (SSN) erfasst nicht alle Vorgänge.[105]

Die Zukunft des Weltraumes wird oft mit den so genannten drei C – *congested*, *contested* und *competitive* – als zunehmend verstopft, umstritten und konkurrenzträchtig beschrieben.[106] Dies galt bisher in erster Linie für Staaten. Vor dem Hintergrund der beschriebenen Entwicklungen könnte es in Zukunft zunehmend aber auch NSA betreffen. Zwar haben manche NSA, zum Beispiel TNU, ein prinzipielles Interesse an einer nachhaltigen Nutzung des Weltraumes und könnten zur stärkeren Regulierung von Weltraumaktivitäten beitragen.[107] Dennoch könnte es zu unterschiedlichen nichtstaatlichen Konflikten kommen, die im folgenden Abschnitt näher beleuchtet werden.

Konfliktmittel und -wege

Die unterschiedlichen Wege, um andere NSA im Weltraum zu schädigen, reichen von der Täuschung und der Manipulation oder Fehlleitung von Informationen (*deception*), über die temporäre Beeinträchtigung und Ausschaltung von beziehungsweise die Zugriffsverweigerung auf Infrastrukturen und die Unterbrechung entsprechender Systemleistungen (*disruption* oder *denial*), bis hin zu deren dauerhaften Schädigung oder Zerstörung (*degradation* oder *destruction*).[108]

Um ihre Ziele zu erreichen, können Angreifer auf unterschiedliche Mittel zurückgreifen. Eine erste Möglichkeit, um Infrastrukturen wie Satelliten im Weltraum zu beeinflussen, sind Angriffe mit boden- oder luftgestützten Energiewaffen. Hierzu zählen Laser, Partikelstrom- und Ultraschallwaffen. Diese können Satelliten in unterschiedlicher Intensität schaden – von temporären (z.B. Blenden) zu nachhaltigen Schädigungen (z.B. von Satellitensensoren), bis hin zur Zerstörung.[109] Darüber hinaus gibt es unterschiedliche, beispielsweise boden- oder luftgestützte, kinetische Antisatellitenwaffen. Eine besonders

zerstörerische Angriffsvariante im Weltraum wäre schließlich eine nukleare Explosion. Durch diese würde ein intensiver elektromagnetischer Impuls generiert, der alle in Reichweite befindlichen Systeme zerstören würde.[110] Im schlimmsten Falle würde der Weltraum für Generationen unnutzbar.

Aufgrund der umfangreichen Fähigkeiten und der großen Finanzmittel, die für ein physisches, kinetisches oder gar nukleares Agieren im Weltraum notwendig sind, erscheint es plausibler, dass NSA auf einfachere Störmethoden zurückgreifen würden. Hierzu zählen erstens Angriffe auf Systemkomponenten am Boden. Zweitens bieten sich Möglichkeiten elektronischer Störung oder Manipulation von Satellitensignalen durch *jamming* oder *spoofing*.[111] Zum Beispiel gelang es angeblich einer Gruppe amerikanischer Forscher mit einem Einsatz von lediglich 1.000 US-Dollar eine nichtmilitärische Drohne durch die Manipulation von GPS-Signalen fernzusteuern.[112] Auch im Falle des Verlustes einer US-Drohne an den Iran im Jahr 2011 vermuteten einige Quellen den Einsatz von GPS-*spoofing*.[113]

Auch wäre es möglich, sich in die Steuerungs-, Kontroll- und Kommunikationsnetzwerke eines Satellitensystems einzuhacken (vgl. Kap. 3.4), dieses so zu übernehmen („Kapern“) und damit den Betrieb zu unterbrechen oder den Satelliten gar zu zerstören. Insgesamt stellt der Cyberspace einen vergleichsweise kostengünstigen, schwer nachvollziehbaren und damit attraktiven Angriffsvektor dar. Dort, wo Schnittstellen zwischen Cyberspace und Weltraum bestehen, eröffnen sich auch für eine Vielzahl von Akteuren mit geringeren Handlungsressourcen Spielräume, um schädigend im Weltraum zu wirken.

Das „Kapern“ von Satellitensystemen könnte nicht nur für finanziell motivierte Akteure interessant sein, sondern auch bei der Verbreitung politischer Botschaften. So gelang es beispielsweise den *Tamil Tigers* 2007, sich für einen begrenzten Zeitraum in einen Satelliten der Firma *Intelsat* einzuhacken und Propaganda zu verbreiten. *Intelsat* sprach damals von einer „unautorisierten Nutzung ihrer Satelliten durch eine terroristische Organisation“.[114] Ein ähnlicher Vorfall ereignete sich 2005, als die chinesische *Falungong*-Bewegung die Fernsehübertragung via eines Satelliten der Firma *Asia Satellite Telecommunications Co. Ltd.* (*AsiaSat*) in weiten Teilen Chinas unterbrach und in der entstandenen Übertragungspause eigenes Propagandamaterial sendete.[115]

Nichtstaatliche Konfliktkonstellationen

Zwischen TNU könnte es vor allem aufgrund des knapper werdenden Platzes, zum Beispiel von Satellitenpositionen, zu Konflikten kommen. Solche Konflikte werden durch die Abwesenheit rechtlich geregelter Besitzverhältnisse und Schlichtungsmechanismen sowie durch die Probleme geringer Sichtbarkeit und der schwierigen Analyse/Attribution von Störaktionen im Weltraum wahrscheinlicher. *Degradation* und *destruction*-Taktiken könnten dabei interessant erscheinen, um konkurrierende Systeme dauerhaft auszuschalten und damit die eigene Marktposition zu verbessern. Durch einen, bei solchen Aktionen ungewollt hervorgerufenen Anstieg des Welt-

raumschrotts könnten sich darüber hinaus auch größere Kollateralschäden ergeben.

Weitere potenzielle Spannungen zwischen TNU könnten entstehen, wenn sich das *asteroid mining* in der Zukunft als wirtschaftlich sinnvoll erweisen sollte und sich Konkurrenzdynamiken ähnlich denen im Rohstoffsektor auf der Erde ergäben.

Zweitens, könnte es in Zukunft verstärkt zu Konflikten zwischen TNU und NGOs kommen. Bei einer Realisierung des *asteroid mining* könnten NGOs versuchen, Aspekte wie Umweltschutz, Verteilungsgerechtigkeit und Nachhaltigkeit in den Weltraum verlängern. Somit würden sich neue Konfliktpotenziale ergeben. Es ist jedoch keinesfalls ausgemacht, dass NGOs Asteroiden, auf denen es nach heutigem Wissensstand keine Lebensformen gibt, als schützenswert erachten würden.[116]

Grundsätzlich könnten TNU und NGOs auch im Bereich Weltraumtourismus aufeinandertreffen. Eine „Liga für Weltraumschutz“ könnte sich für eine nachhaltige Nutzung dieses Raumes engagieren. Bei zunehmenden Platzproblemen könnte es zu Forderungen kommen, der Nutzung des Weltraumes für Wissenschaft, Forschung und den Erhalt der Lebensgrundlagen aller Menschen Vorrang vor kommerziellen

Jenseits dieser konkreten Konfliktkonstellation könnten TKN ein Interesse an der gesamten Bandbreite zur Verfügung stehender Taktiken zur Beeinträchtigung von Satellitensystemen haben, die der Aufklärung ihrer kriminellen Aktivitäten dienen. Ferner könnten sie die dauerhafte Beeinträchtigung oder Störung weltraumbasierter Infrastrukturen als Dienstleistung für Dritte anbieten.

und touristischen Aktivitäten zu gewähren.

Für NGOs wären je nach Eskalation alle Taktiken interessant. Neben der Kampagnenarbeit könnten sie versuchen, die Unternehmungen der Firmen zu sabotieren und zu verhindern. Während mit *deception*-Taktiken wie *spoofing* die eigene Agenda gezielt in Rundfunk- und Fernsehen platziert werden könnte, wäre es mittels *disruption* und *denial* von Infrastrukturen oder sogar der Androhung und Umsetzung von *degradation* und *destruction* gegen diese möglich, den eigenen Zielen Nachdruck zu verleihen.

TKN könnten – vor dem Hintergrund wachsender gesellschaftlicher und staatlicher Abhängigkeit von weltraumgestützten Leistungen und den großen Mengen an Kapital, welche TNU im Weltraum investieren – das „Kapern“ von Satelliten oder anderer systemrelevanter Infrastrukturen und das Erpressen von Lösegeld als lukratives Geschäftsmodell entdecken. Das Piraterie-Phänomen könnte sich so auf den Weltraum ausdehnen (vgl. Abb. 3.5). Vor allem *disruption* und *denial* bieten sich als Taktiken für Erpressungen an. Eine Zerstörung der Infrastrukturen erscheint im Kontext des Konfliktbildes „Weltraumpiraterie“ weniger plausibel.

Schließlich wird auch der Weltraumterrorismus von einigen Beobachtern als

mögliche Konfliktform der Zukunft diskutiert.[117] Dabei bleibt jedoch unklar, wie sich ein zentrales Wesensmerkmal von Terrorismus, nämlich die Verbreitung von Angst und Schrecken, im Weltraum entfalten würde. Zweitens, ist auch der internationale Terrorismus auf satellitenbasierte Systemleistungen vor allem für die Kommunikation angewiesen. Diese Abhängigkeit dürfte auch das Kalkül für Aktionen in diesem Raum beeinflussen, und spräche für zielgerichtete Angriffe, anstelle solcher mit unkontrollierbaren Folgewirkungen. Eine finale *Space 9/11*-Attacke mittels Kernwaffen erscheint vor allem aufgrund der notwendigen technischen Voraussetzungen wenig wahrscheinlich. Dennoch wäre es denkbar, dass terroristisch motivierten Akteuren über den Cyberspace eine solche umfassende Schädigung des Weltraumes gelingen könnte. Letztendlich kann wegen der großen auch militärischen Abhängigkeit von Staaten keinesfalls ausgeschlossen werden, dass terroristische Akteure künftig auch im Weltraum lohnenswerte Anschlagsziele finden könnten.

Zusammenfassend erscheinen für die nächsten Dekaden besonders kriminelle Aktivitäten sowie die Konkurrenz zwischen Unternehmen um Platz im Weltraum äußerst plausibel. Auch Interessensverlagerungen von NGOs in den Weltraum sind möglich, jedoch an die skizzierten Einschränkungen bezüglich Motivation und Handlungsfähigkeit in diesem Raum gebunden.

Abbildung 3.5: Konfliktbild 3 – Weltraumpiraterie

Weltraumpiraterie

TKN versus TNU

Die Kaperung von Satelliten ist zum beliebten Geschäftsfeld avanciert. 2026 drang diese neue Form der Organisierten Kriminalität sehr plastisch in das Bewusstsein und in die Wohnzimmer der Bürger weltweit. Während der Vorberichterstattung zum *Super Bowl* fiel die Übertragung aus. Wenige Minuten später bekannte sich eine Gruppe namens *Space Pirates* dazu, die Störung verursacht zu haben. Sie hätten die Satellitengruppe gekapert, über die das Sportereignis in alle Welt übertragen wurde. Gegenüber der Betreiberfirma der Satelliten forderten die Piraten ein Lösegeld in Millionenhöhe. „Kein Geld, kein *Super Bowl*" hieß es lapidar im Bekennerschreiben.

Nur acht Monate nach dem *Super Bowl*-Vorfall erreichte das Phänomen Weltraumpiraterie einen weiteren, weitaus traurigeren Höhepunkt. Ein Erdbeben hatte weite Teile des Landes *Tektonien* verwüstet. Millionen von Menschen hatten ihr Zuhause verloren. Tausenden wurden vermisst. Die Zahl der tot Geborgenen stieg stündlich.

Mit einem Hilferuf wandte sich *Tektoniens* Regierung an die internationale Gemeinschaft. Auch NGOs drängten auf schnelle Aktionen. Verwundete müssten versorgt, Heimatlose beherbergt werden. Schnell müsste man eingreifen, um die Verbreitung von Krankheiten zu verhindern und Trinkwasser zu verteilen. Und tatsächlich: Binnen kürzester Zeit machten sich eine Vielzahl von Akteuren, teils sehr unkoordiniert, daran zu helfen – darunter die Europäische Union, weite Teile der internationalen Staatengemeinschaft und eine Vielzahl von NGOs. Selbst TNU kündigten Nahrungsmittel- und Trinkwasserspenden an.

Doch bevor die Hilfe vor Ort aufgenommen war, brach der Großteil der Satellitendienste im schwer zugänglichen *Tektonien* und dessen Nachbarstaaten zusammen. Der Schock der internationalen Gemeinschaft war groß. An einen effizienten, eng getakteten Flugbetrieb, wie er zum Heranschaffen von Personal und Material notwendig war, war nicht zu denken. Die Aufklärung der Lage in der betroffenen Region war nahezu unmöglich. Und auch die bereits vor Ort stationierten Vorausteams konnten ohne die richtige Ausrüstung wenig ausrichten.

Nach einem Tag Unklarheit und Frustration meldeten sich, wie schon vor dem *Super Bowl*, die *Space Pirates* bei den Betreibern der Satelliten-Netzwerke. „Man habe absurde Lösegeldforderungen von den Erpressen erhalten", so verkündeten die Betreiber auf einer gemeinsamen Pressekonferenz, „die man nicht im Stande sei zu erfüllen." Man hätte sich jedoch darauf geeinigt, Sicherheitsfirmen zu beauftragen, um die Verursacher dieser „Grausamkeit schnellstmöglich auszuschalten."

Die internationale Gemeinschaft reagierte mit Entsetzen. Das Wohl der Menschen *Tektoniens* sei nun das Wichtigste; man müsse die Forderungen der Weltraumpiraten erfüllen. Doch wie? Eine hektische Debatte zwischen den engagierten Organisationen verlief im Sande. Schließlich vergingen zwei weitere Tage, bis die Blockade endete. Warum sie zu Ende ging, weiß niemand genau. Die Satelliten-Betreiber verkündeten lediglich, dass sie ihre Dienste nun wieder anbieten könnten. Das Leben wie vieler Menschen in den drei Tagen der Blockade hätte gerettet werden können, weiß niemand.

Quelle: eigene Darstellung.

3.4. Nichtstaatliche Konflikte im Cyberspace

Der Cyberspace ist keine geografisch eingrenzbare Größe, sondern „der virtuelle Raum aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab“.[118] Er hat sowohl eine soziale sowohl eine soziale Dimension – die inhaltliche Ebene – als auch eine technische Dimension – bestehend aus physischen und logischen Elementen.[119]

Governance und Akteure

Der Cyberspace ist ein relativ neuer und sich dynamisch entwickelnder Raum,[120] dessen *governance* sich über die „Jahre hinweg von unten“ entwickelt hat.[121] Wichtige Funktionen werden von nichtstaatlichen Institutionen wahrgenommen.[122] Die für jede Kommunikation im Internet benötigen IP-Adressen werden beispielsweise von der in Kalifornien ansässigen *Internet Corporation for Assigned Names and Numbers* (ICANN) vergeben. Private *Internet Service Provider* ermöglichen ihren Kunden wiederum den Kontakt mit dem Internet und stellen die Netzinfrastruktur bereit.[123]

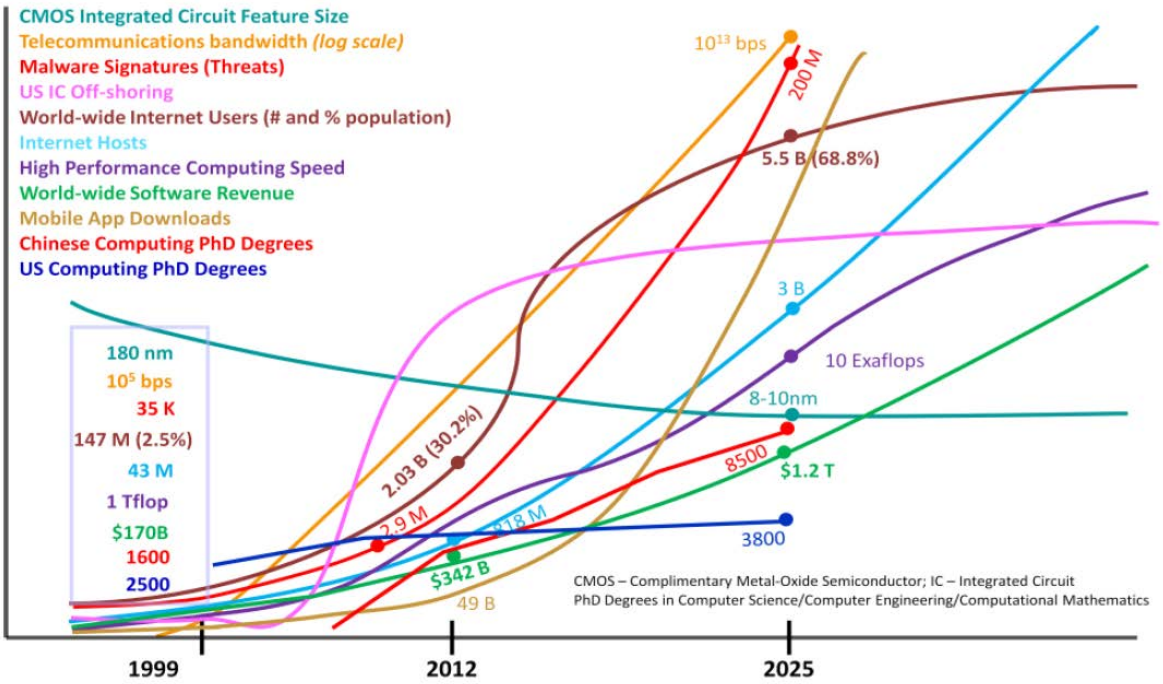
Auf der inhaltlichen Ebene engagiert sich mittlerweile beinahe jeder Akteur, der auch in anderen Räumen agiert. Dies gilt für Staaten genauso wie für NGOs, TNU, TKN und PMSF. Hinzu kommen NSA, für die das Internet den primären und unter Umständen auch einzigen Handlungsraum darstellt. Beispiele sind Unternehmen wie *eBay* und *Facebook* sowie die Internetaktivisten der Gruppe *Anonymous*.[124]

Im Rahmen der Weltgipfel zur Informationsgesellschaft seit 2003 und des *Internet Governance Forum* seit 2006 hat es von staatlicher Seite Versuche gegeben, das Internet stärker zu regulieren. Diese sind jedoch mit grundlegenden Problemen konfrontiert.[125] Die politischen Verhandlungen im *Internet Governance Forum* offenbaren schon heute „Risse im Gebälk der traditionellen wirtschaftlichen und politischen Machtstrukturen“.[126] Staaten, Unternehmen und Vertreter der Zivilgesellschaft agierten faktisch auf Augenhöhe. Das US-amerikanische *Center for a New American Security* (CNAS) bringt die Lage der heute bestehenden Cyber-*governance* auf den Punkt, wenn es feststellt, dass diese „ausreichend ist, damit der Cyberspace gedeihen kann, jedoch unzureichend, um ihn sicher zu machen.“[127]

Der Raum wächst weiter

Der Cyberspace wird sich weiterhin dynamisch entwickeln – hinsichtlich des Datenvolumens zum Beispiel wird er sich voraussichtlich weiter alle zwei Jahre verdoppeln.[128] Die steigende Nutzung mobiler Endgeräte[129] und die Entwicklung einer Vielzahl weiterer Indikatoren (vgl. Abb. 3.6) sprechen für die zukünftige Ausdehnung des Cyberspace und für eine immer stärkere Integration in den Alltag der Menschen. Der Cyberspace wächst dabei auch immer mehr über die traditionellen Industriestaaten hinaus (vgl. Abb. 3.7). Bereits bis 2025 könnten rund 5,5 Milliarden Menschen im Cyberspace aktiv sein.[130] Dennoch wird einer Vielzahl von Menschen der Zugang verwehrt bleiben (*digital divide*).[131]

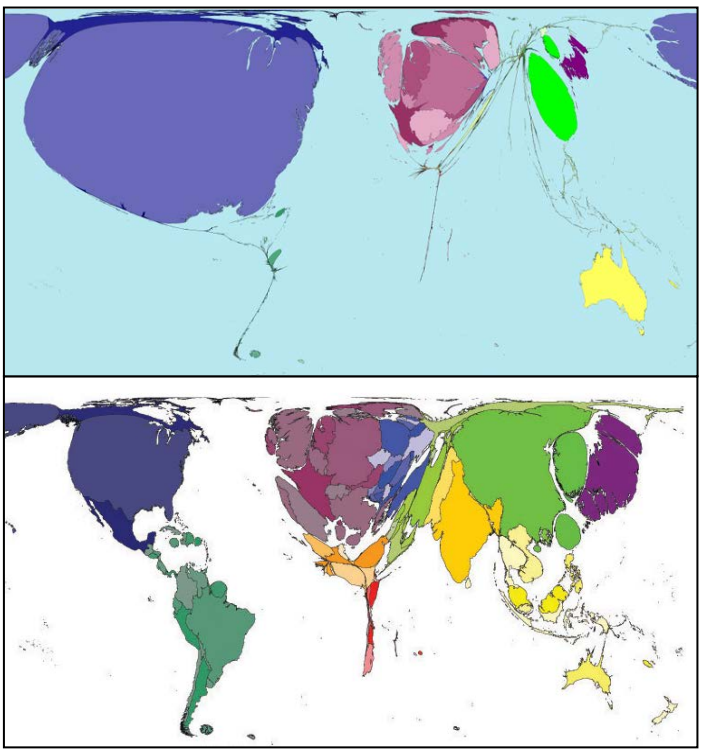
Abbildung 3.6: Zukünftige Entwicklung verschiedener Indikatoren für die Ausdehnung des Cyberspace



Quelle: USAF (2012: 9).

Abbildung 3.7: Globale Verteilung der Internetnutzer in den Jahren 1990 (oben) und 2007 (unten)

Die relative Größe der in den Karten gezeigten Länder repräsentiert den Anteil an den globalen Internetnutzern. Im Jahre 1990 war demnach der Großteil der Internetnutzer in den USA beheimatet, 2007 ist die Internetnutzung wesentlich stärker global verteilt.



Quelle: Worldmapper (2012a, b).

Aber nicht nur Menschen werden vernetzter. So verlagern sich die Speicherung von Informationen und die Verfügbarkeit von Software zunehmend von den Endgeräten ins Internet (*cloud computing*). Weiterhin wächst das „Internet der Dinge“ rasant, in dem sich Objekte und Infrastrukturen – egal ob mobile Endgeräte, Haushaltsgeräte oder gesellschaftlich relevante Infrastrukturen[132] – untereinander und mit den Anwendern vernetzen. Während 2011 noch ungefähr gleich viele Menschen und Geräte im Cyberspace verbunden waren, werden es bereits in weniger als fünf Jahren rund drei Mal so viele Geräte wie Menschen sein.[133]

Problemfelder

Eines der wichtigsten Problemfelder im Cyberspace ist die Internetkriminalität, durch die bereits heute erheblicher Schaden entsteht.[134] Sie wird auch zukünftig weiter wachsen. So rechnet beispielsweise die *US Air Force* (USAF) damit, dass die Menge krimineller Schadprogramme allein bis 2025 von gegenwärtig rund drei auf zweihundert Millionen ansteigen könnte (vgl. Abb. 3.6).[135]

Ein zweites wichtiges Problemfeld ist die andauernde Auseinandersetzung über die Informationsfreiheit. Dieses Feld untergliedert sich in verschiedene Bereiche. Erstens versuchen staatliche Organisationen durch Zensur und technische Barrieren den Zugang zum Cyberspace zu überwachen, einzuschränken oder zu blockieren. Einer der bekanntesten Konfrontationen ist dabei jene zwischen China und *Google*. Eine weitere Konfrontation um den freien Informationsfluss hat sich in Fällen ergeben, in denen geheime Informationen im Internet veröffentlicht wurden. Insbesondere die Plattform *WikiLeaks* ist dabei immer wieder in die Schlagzeilen geraten. Ein dritter Aspekt dieses Problembereiches ist, wie im Folgenden weiter ausgeführt wird, jener des Urheberrechtsschutzes.

Heutige Konflikte

Bereits heute ist der Cyberspace sowohl für staatliche Akteure als auch für NSA ein Konfliktaustragungsort.[136] Ein Beispiel aus dem Bereich Urheberrechte verdeutlicht mögliche Konfliktdynamiken.[137] 2010 versuchte eine Reihe indischer Filmstudios der Seite *The Pirate Bay* den Betrieb zu untersagen, da dort Inhalte der Studios verbreitet wurden. Als das nicht gelang, heuerten die Studios die Firma *Aiplex* an, um *The Pirate Bay* und andere *Filesharing*-Seiten mit Angriffen vom Netz zu holen. Daraufhin schaltete sich *Anonymous* ein und wollte die Internetpräsens von *Aiplex* angreifen. Die Gruppe musste aber feststellen, dass die Seite des Unternehmens nicht mehr abrufbar war. *Anonymous* griff daraufhin eine Vielzahl anderer Seiten an, darunter solche von Urheberrechtsverbänden und von Regierungsinstitutionen.[138]

Nur wenig später kam es zu weiteren Vorfällen. Die Enthüllungsplattform *WikiLeaks* hatte geheime Videos von Hubschrauberangriffen im Irak und Botschaftsdepeschen den USA veröffentlicht. Serveranbieter und Bezahldienste wie *Visa*, *Mastercard* und *PayPal* verweigerten *WikiLeaks* daraufhin ihre Dienste. Wieder griff *Anonymous* an.[139] Als das Hacker-

Magazin „2600“ die Aktion kritisierte, wurde auch dessen Internetseite angegriffen. Andere Hacker reagierten mit Angriffen auf den Server, von dem aus die Aktionen gegen die indischen Filmstudios koordiniert wurden. Letztendlich wurde dieser „Kleinkrieg“[140] nach Verhandlungen in einem neutralen Chatraum beigelegt.

Das Beispiel ist für nichtstaatliche Konflikte im Cyberspace in vielerlei Hinsicht repräsentativ: Den Medienunternehmen wurde klar, dass sie rechtlich nicht effektiv gegen *The Pirate Bay* vorgehen konnten. Sie griffen daraufhin zu radikaleren Mitteln, die sie extern einkauften. Ein zuerst unbeteiligter Akteur, *Anonymous*, schaltete sich ein und trug zur Eskalation bei. Daraufhin gerieten Institutionen, die primär nicht Ziel der Aktion sein sollten, in Mitleidenschaft – darunter auch staatlicher Institutionen. Letztendlich kam es auch zwischen Verfechtern des freien Internets selbst zum Streit. Insgesamt handelt es sich also um einen sehr dynamischen und unübersichtlichen Konflikt, dessen Verlauf durch die anfänglichen Parteien schon nach kurzer Zeit nicht mehr zu kontrollieren war.

Neue Themen

Mit dem generellen gesellschaftlichen, politischen und wirtschaftlichen Bedeutungsgewinn des Cyberspace ergeben sich weitere strittige Themen. Im Bereich der Informationsbeschränkung könnten zukünftig nicht nur Staaten, sondern noch stärker auch TNU in das Visier der Kritiker kommen; besonders wegen der zunehmenden Ausbildung von „Ökosystemen“[141] im Cyberspace. Ökosysteme sind abgegrenzte und teilgeschlossene Bereiche wie das soziale Netzwerk *Facebook*. Kennzeichnend für Ökosysteme ist, dass deren Betreiber über Zugang und interne Regeln bestimmen – sowohl für Nutzer als auch für Anbieter von Dienstleistungen. Auch die anderen Internetgrößen der so genannten AGFA[142] – also *Apple*, *Google, Facebook* und *Amazon* – treiben den Ausbau solcher Ökosysteme stark voran.

Weitere Streitpunkte könnten sich möglicherweise durch die Etablierung gesamtvolkswirtschaftlich wichtiger Internetwährungen[143] oder durch eine Virtualisierung von Wahlen in Internet-Ökosystemen,[144] oder klassischen politischen Einheiten ergeben. Auch durch potenzielle Einschränkung der Netzneutralität wäre der freie Fluss von Informationen im Cyberspace gestört.

Ein weiteres heftig diskutiertes Thema ist *big data.*[145] Hier geht es um die Verarbeitung großer Datenmengen, die in Institutionen, in Unternehmen (Ökosystemen) oder auch frei im Internet verfügbar sind – darunter E-Mails, Videos, Einträge in sozialen Netzwerken. Aus der Analyse solcher Daten, so die Befürworter, könnten neue wirtschaftliche Potenziale erwachsen und es könnten sich wissenschaftliche Entdeckungen oder sogar Vorhersagen machen lassen, beispielsweise über die Entwicklung von Aktienkursen oder die Bewegungsmuster von Individuen. Gegner befürchten hingegen verstärkte

Überwachung und einen Verlust der Privatsphäre.

Schließlich birgt der Cyberspace das Potenzial, dass zukünftig Interessensgegensätze zusammenstoßen, die zwar in der realen Welt latent vorhanden sind, denen bisher aber beispielsweise wegen fehlender Geldmittel oder der räumlichen Distanz der Konfliktparteien nicht nachgegangen werden konnte. Zu solchen Interessengegensätzen würden jene gehören, die durch einen fortwährenden *digital divide* erzeugt werden könnten. Auch kulturell oder nationalistisch motivierte Konfliktlinien sind denkbar. Ein Indiz hierfür sind die 2007 durchgeführten Angriffe vermutlich russischer Hacker auf verschiedene Ziele in Estland, nachdem dort ein sowjetisches Denkmal abgebaut wurde.[146]

Wegen der globalen Verbreitung, der eingeschränkten Kontrollierbarkeit und der verhältnismäßig geringen Handlungskosten wird der Cyberspace immer stärker zum primären Handlungsraum für viele NSA werden – auch um Ziele in anderen Räumen, wie dem Weltraum zu erreichen (vgl. Kap. 3.3). Eine wichtige Rolle wird dabei neben TNU, TKN, NGOs und Internetaktivisten auch PMSF zufallen, die Sicherheitslösungen anbieten, gleichzeitig aber auch als mögliches Angriffsziel für jene Kräfte attraktiv sind, die auf die Freiheit des Internets pochen. Für Staaten wird es hingegen schwer werden, zu weitreichenden Regulierungen des Cyberspace zu gelangen. Auch eine weitreichende Regulierung durch NSA ist, zumindest auf der inhaltlichen Ebene, wenig plausibel.[147]

Konfliktmittel und -wege

Der Cyberspace ermöglicht Akteuren einerseits die effektivere Nutzung bekannter Handlungswege, zum Beispiel den Verkauf von Dienstleistungen, die Mobilisierung von Mitstreitern und das Sammeln von Spenden. Auch für Informationszwecke ist er äußerst gut geeignet – im Positiven ebenso wie im Negativen, das heißt im Sinne von Desinformation, Propaganda und Rufmord.

Akteuren stehen jedoch auch andere Mittel zur Verfügung. Hierzu zählt die gezielte Blockade von Angeboten im Cyberspace, beispielsweise durch DDoS-Attacken. Hierbei werden Internetseiten und Server systematisch überfordert und zum Absturz gebracht, indem mit Hilfe möglichst vieler Computer möglichst viele Anfragen an sie gesendet werden. Die Wirkung solcher Attacken kann durch das Herunterladen und Aktivieren von Programmen aus dem Internet – wie der *Low Orbit Ion Cannon* (LOIC), die automatisiert Anfragen an einen bestimmten Empfänger absendet – potenziert werden. Insbesondere Internetaktivisten haben sich dieses Mittels vielfach bedient. Auch durch *botnets* wird die Wirkung solcher DDoS-Attacken potenziert. Diese wurden bereits von TKN genutzt, beispielsweise zum Zwecke der Erpressung von TNU.[148]

Auch können Angreifer in fremde Computersysteme eindringen (Hacking) und so Informationen entwenden; beispielsweise Kundendaten, Passwörter, interne E-Mails, Protokolle, oder sogar Konstruktionspläne. Durch personenspezifische Daten können Online-Identitäten „gekapert“ und unter falschem Namen beispiels-

weise schädliche Inhalte kommuniziert oder Transaktionen abgewickelt werden.

Durch Hacking ist schließlich auch die Fremdsteuerung von Systemen möglich und es könnte Hacking zur Sabotage oder Zerstörung von mit dem Internet verbundenen Infrastrukturen genutzt werden. Wie ein Sprecher von *Shell* beispielsweise unlängst feststellte, seien solche Angriffe auf physische Elemente in der Ölförderung „nicht nur möglich, sondern schon jetzt real".[149]

Generell gibt es bei der Beurteilung von Konfliktmitteln- und wegen im Cyberspace drei Sachverhalte zu beachten: Erstens ist die Verfügbarkeit von Konfliktmitteln in diesem Raum vergleichsweise hoch. Viele Mittel, wie die LOIC, erfordern keine großen Kenntnisse und sind kostenfrei verfügbar. Gleichzeitig ist zu beobachten, dass die Hemmschwelle von Individuen, an schadhaften Aktionen – besonders bei der Blockade von Internetseiten – teilzunehmen, im Cyberspace geringer ist als im realen öffentlichen Raum. Komplexere Mittel können darüber hinaus mit Hilfe von PMSF oder auch TKN relativ leicht erworben werden.

Zweitens verändert sich der Raum rasant. Es ist daher schwer abzusehen, welche Art von Handlungsmittel zukünftig zur Verfügung stehen werden – ob zum Beispiel DDoS-Attacken langfristig eine effektive Strategie zum Blockieren von Internetseiten bleiben werden. Jedoch ist der Cyberspace, drittens, dadurch gekennzeichnet, dass offensive Aktionen systematisch Vorteile vor defensivem Verhalten haben. Angriffe finden im Cyberspace in einem großen, weitgehend offenen Netzwerk statt. Sie sind schwer nachzuvollziehen und keineswegs immer einer konkreten Quelle zuzuordnen. Während sich ein Angreifer gezielt und unentdeckt ganz konkret systemische Schwachstellen suchen kann, steht der Verteidiger vor der Herausforderung ständig das gesamte und zumeist sehr komplexe System bewachen zu müssen.[150]

Nichtstaatliche Konfliktkonstellationen

Konflikte zwischen TNU werden schon heute diskutiert. Dabei stehen besonders Spannungen der AGFA-Internetgrößen im Mittelpunkt. Zwar sind solche Konflikte prinzipiell denkbar. Ein „Endspiel um das Internet"[151] zwischen den AGFA-Unternehmen mit sicherheitspolitischen Folgen ist jedoch unwahrscheinlich. Die Unternehmen werden wahrscheinlich auch zukünftig, zum Beispiel mit Patentklagen, gegeneinander vorgehen. Trotz ihrer jeweils sehr starken Marktmacht, bleiben sie jedoch auf das Wohlwollen ihrer Kunden angewiesen. Drastischere Operationen gegen einen Konkurrenten könnten den eigenen Börsenkurs negativ beeinträchtigen und den Ruf bei potenziellen Kunden verschlechtern. Sie sind damit eher unattraktiv.

Plausibler ist die Konfliktkonstellation TNU versus TNU im Falle kleinerer, spezialisierter und weniger in der Öffentlichkeit agierender Unternehmen, zum Beispiel auch im Bereich der Sicherheitsdienstleistungen. Diese sind weniger auf ihre Reputation in der brei-

ten Öffentlichkeit angewiesen und könnten sich gegebenenfalls eigene Expertise im Bereich der Verschleierung von Handlungen im Cyberspace zunutze machen, um unbemerkt gegen Konkurrenten vorzugehen, zum Beispiel auch mit Hilfe von Proxy-Internetaktivisten. Jedoch auch PMSF sind genau wie TNU primär profitorientiert. Einer entsprechenden Konfrontation müsste daher eine Kalkulation zugrunde liegen, bei welcher der Nutzen der Diffamierung des Konkurrenten die Risiken der Enttarnung überwiegt.

In einem letzten Fall könnte die Konfrontation zwischen PMSF sehr akut werden, nämlich dann, wenn diese jeweils von anderen Akteuren dazu beauftragt wurden, entsprechende Aktionen durchzuführen. In diesem Falle würden aber andere Motivationen vorliegen, die nicht auf die PMSF zu beschränken sind. PMSF wären eher Mittel als tatsächliche Treiber eines Konfliktes.

Eine wahrscheinliche Konfliktkonstellation ist jene zwischen TNU und TKN. Vorwiegend geht es in dieser Konstellation (schon heute) um die Erpressung von Schutzgeldern (s.a. Abb. 3.5). Auch der systematische Diebstahl von Unternehmensgeheimnissen durch TKN oder andere TNU ist zukünftig wahrscheinlich.

Mit Blick auf die Konstellation TNU versus Internetaktivisten könnten insbesondere durch die weitläufige Anwendung von *big data* Konflikte entstehen. Ein weiterer Konfliktpunkt könnte sich ergeben, wenn Aktivisten auf eine Demokratisierung virtueller Ökosysteme drängen, während TNU ihre eigenen Kompetenzen nicht an die Nutzer abgeben wollen. Konfliktwege könnten bis zu Versuchen reichen, durch Hacking die Serversysteme von *big data*-Anwendungen oder Ökosystemen zu zerstören.

Weiterhin ist es wahrscheinlich, dass Aktivisten im Cyberspace versuchen, gegen Unternehmen auf die Verwirklichung von Zielen aus der nichtvirtuellen Welt hinzuwirken – wie zum Beispiel Entwicklung oder Umweltschutz. Auch TNU können Angriffe gegen NGOs in den Cyberspace verlagern, beispielsweise wenn eine NGO versucht, durch Transparenzkampagnen die Praktiken nicht vollständig legal arbeitender Unternehmen offenzulegen.

Neben Öffentlichkeitskampagnen im Cyberspace bieten sich auf beiden Seiten verschiedene Handlungswege, zum Beispiel Angriffe auf die Internetauftritte des Kontrahenten, das Hacken sensibler Informationen über diesen, das Löschen sensibler Daten auf deren Servern oder Angriffe auf mit dem Cyberspace vernetzte Infrastrukturen.

Zu einer Eskalation könnte es zwischen TNU und NGOs/Internetaktivisten insbesondere dann kommen, wenn sich die Verfolgung gesellschaftlicher Normen mit kulturellen Unterschieden oder nationalistischen Tendenzen mischt. Auch hinsichtlich der Konstellation NGO/Internetaktivisten vs. NGO/Internetaktivisten sind solche nationalistisch oder kulturell aufgeladenen Situationen wahrscheinlich am konfliktträchtigsten. Ein Beispiel für darin involvierte Akteure wären „nichtstaatliche Cybernationalisten“, also gesellschaftliche Akteure, die in Eigenregie und ohne Koordinierung mit

staatlichen Institutionen eine (Cyber-Außen-)Politik verfolgen, die aus ihrer Perspektive im Interesse ihres Heimatstaates ist. Sowohl zwischen TNU und Internetaktivisten als auch zwischen Internetaktivisten selbst könnten solche Konstellationen gezielt oder unbeabsichtigt Krisen zwischen Staaten provozieren (vgl. Abb. 3.8).

Andere Konflikte zwischen NGOs beziehungsweise Internetaktivisten könnten sich an entgegengesetzten gesellschaftlichen Normen entzünden – sowohl innerhalb einer Gesellschaft als auch über Gesellschaften, Nationen oder Kulturen hinweg.[152] Schlussendlich bleiben auch weniger klar angelegte Konfliktkonstellationen denkbar, in denen Internetaktivisten, zum Beispiel aufgrund von Entführungen (wie im Falle *Anonymous* vs. *Los Zetas*),[153] verbalen Androhungen (wie im Falle *Anonymous* vs. *HBGary*)[154] oder ähnlichen Vorfällen mit anderen NSA in Konflikt geraten.

Zusammenfassend ist festzuhalten, dass Konflikte zwischen TNU im Allgemeinen eher unwahrscheinlich, in wenigen aber sicherheitspolitisch sehr relevanten Fällen – zum Beispiel zwischen Cybersecurity-Firmen – jedoch durchaus denkbar erscheinen. Die Erpressung von TNU durch TKN ist eine wahrscheinliche Konstellation, die insbesondere, wenn Infrastrukturen im Visier der Angreifer sind, durchaus signifikanten Schaden anrichten könnte. Darüber hinaus bietet der Cyberspace vielen Akteuren einen neuen Betätigungsraum. Teils unberechenbare Aktivisten können durch Hacking Schaden anrichten und die Austragung von Konflikten, die vorher aufgrund räumlicher Distanz nur latent vorhanden waren, wird eine neue Herausforderung darstellen.

Abbildung 3.8: Konfliktbild 4 – Wertekonflikt im World Wide Web

Wertekonflikt im World Wide Web

Internetaktivisten versus TNU (+ PMSF)

Nachdem westlich geprägte TNU lange den Cyberspace dominiert hatten, hat sich die Situation seit Anfang der 2020er Jahre entscheidend geändert. Unternehmen aus verschiedenen aufstrebenden Wirtschaftsnationen haben ihre Expansion in andere Regionen und Sprachräume vorangetrieben und bieten konkurrenzfähige Produkte auch in Europa und den Vereinigten Staaten an.

Gleichzeitig gibt es auf der Welt jedoch immer noch bedeutende Unterschiede im Verständnis von Presse- und Informationsfreiheit. Insbesondere in Nordamerika und den europäischen Staaten haben sich Gruppen von Internetaktivisten zusammengefunden, die immer stärker auf eine absolute Freiheit von Informationen drängen. In andere Staaten, die teilweise noch inmitten schwieriger gesellschaftlicher Transformationsprozesse stecken, beherrschen hingegen eine selektive Informationspolitik und die Zensur der Medien das Bild.

2025 eskaliert der Streit zwischen Internetaktivisten von *FreeInfoSec* und dem mittlerweile auch in westlichen Staaten populären sozialen Ökosystem *MyLife*, dass neben einem sozialen Netzwerk und Suchmaschinenfunktionen auch zahlreiche *Cloud Computing* Dienste anbietet. *FreeInfoSec* unterstellt *MyLife* aktiv Falschinformationen zu verbreiten, Zensur zu praktizieren, und die Daten seiner Kunden unrechtmäßig weiterzuverwenden.

In einer Welle von Cyberangriffen geht die Seite des Unternehmens über Monate hinweg in verschiedenen westlichen Staaten, teilweise sogar im Heimatmarkt, immer wieder vom Netz. Auch werden Rechenzentren des Unternehmens angegriffen. Durch Überlastung der Infrastruktur entstehen Millionenschäden. Gezielte (Des-)Informationskampagnen von *FreeInfoSec* provozieren einen Absturz des *MyLife*-Aktienkurses.

MyLife beauftragt daraufhin die Firma *YourCyberSecurity* aus ihrem Heimatland, um Gegenattacken zu fahren und die eigene Sicherheit zu gewährleisten. Die Internetaktivisten weiten ihre Aktionen darauf auch auf *YourCyberSecurity* aus. Von den Servern der Firma entwenden die Aktivisten Beweise über schwere Menschenrechtsverletzungen im Heimatland von *MyLife* und veröffentlichen diese.

An dieser Stelle schreitet die Regierung des *MyLife*-Heimatlandes ein. Statt jedoch *FreeInfoSec* zu konfrontieren, droht sie den vermeintlichen Heimatländern der *FreeInfoSec*-Aktivisten mit ernsthaften Konsequenzen. Deren Regierungen sehen sich in einer problematischen Situation. Nicht nur werden sie außenpolitisch vom *MyLife*-Heimatland unter Druck gesetzt. Auch innenpolitisch hat der Vorfall Konsequenzen: Die nationale Gesellschaften beäugen den Aufstieg des *MyLife*-Heimatlandes schon seit Jahren sehr kritisch. Der Großteil der Bürger steht hinter den Werten, die von den Aktivisten vertreten werden. Nicht wenige Stimmen fordern ein hartes Vorgehen gegen die Menschenrechtsverletzer.

Quelle: eigene Darstellung.

4. Sicherheitspolitische Relevanz nichtstaatlicher Konflikte in Räumen begrenzter Staatlichkeit

Die vorliegende *Future Study* hat gezeigt, dass sowohl NSA als auch Räume begrenzter Staatlichkeit zukünftig wahrscheinlich an Bedeutung gewinnen werden. Hierdurch steigt auch die Relevanz nichtstaatlicher Konflikte in diesen Räumen. Im Folgenden wird zuerst für jeden der untersuchten Räume gezeigt, auf welchem Wege nichtstaatliche Konflikte sicherheitspolitisch relevant werden könnten. Anschließend wird die Rolle, die Staaten selbst in solchen, zunächst nichtstaatlichen Konfliktkonstellationen spielen könnten, näher beleuchtet. Was zunächst nach einem NSA oder einem nichtstaatlichen Konflikt aussehen mag, könnte durchaus durch Staaten motiviert, initiiert, unterstützt oder orchestriert sein. Nichtstaatliche Konflikte könnten demnach auch als neue Stellvertreterkonflikte zwischen Staaten oder zwischen Staaten und NSA entstehen. Abschließend werden Handlungsfelder für Deutschland und die Bundeswehr aufgezeigt, um den sicherheitspolitischen Implikationen nichtstaatlicher Konflikte zu begegnen.

4.1. Sicherheitsinteressen Deutschlands und sicherheitspolitische Relevanz nichtstaatlicher Konflikte

Die sicherheitspolitischen Ziele Deutschlands sowie die deutschen Sicherheitsinteressen sind in den Verteidigungspolitischen Richtlinien von 2011 festgehalten (vgl. Abb. 4.1).

Vor dem Hintergrund der VPR, den deutschen Sicherheitsinteressen, und den Ergebnissen dieser Future Study, lässt sich die potenzielle sicherheitspolitische Relevanz nichtstaatlicher Konflikte in Räumen begrenzter Staatlichkeit in fünf Punkte untergliedern.

Abbildung 4.1: Sicherheitspolitische Ziele und Sicherheitsinteressen Deutschlands

„Die sicherheitspolitischen Ziele Deutschlands sind:

- **Sicherheit und Schutz der Bürgerinnen und Bürger Deutschlands;**
- **territoriale Integrität und Souveränität Deutschlands und seiner Verbündeten;**
- **Wahrnehmung internationaler Verantwortung.**

Zu den deutschen Sicherheitsinteressen gehören:

- **Krisen und Konflikte zu verhindern, vorbeugend einzudämmen und zu bewältigen, die die Sicherheit Deutschlands und seiner Verbündeten beeinträchtigen;**
- **außen- und sicherheitspolitische Positionen nachhaltig und glaubwürdig zu vertreten und einzulösen;**
- **die transatlantische und europäische Sicherheit und Partnerschaft zu stärken;**
- **für die internationale Geltung der Menschenrechte und der demokratischen Grundsätze einzutreten, das weltweite Respektieren des Völkerrechts zu fördern und die Kluft zwischen armen und reichen Weltregionen zu reduzieren;**
- **einen freien und ungehinderten Welthandel sowie den freien Zugang zur Hohen See und zu natürlichen Ressourcen zu ermöglichen.“**

Quelle: VPR (2011: 4–5).

Demnach werden diese Konflikte sicherheitspolitisch relevant, wenn

(1) sie sich zu größeren Krisen und Konflikte ausweiten (können);

(2) sie die Handlungsfähigkeit Deutschlands und der Bundeswehr in Räumen begrenzter Staatlichkeit einschränken, so dass außen- und sicherheitspolitische Positionen nicht mehr nachhaltig und glaubwürdig vertreten werden können;

(3) sie kritische Infrastrukturen und auf diesen basierende Systemleistungen in Räumen begrenzter Staatlichkeit gefährden;

(4) sie den freien und ungehinderten Welthandel sowie den freien Zugang zur Hohen See und zu natürlichen Ressourcen einschränken;

(5) sie Menschenrechte, demokratische Grundsätze oder das Völkerrecht verletzen, beziehungsweise zu einer Stärkung der Kluft zwischen armen und reichen Weltregionen führen.

In den verschiedenen Räumen spiegeln sich diese Punkte wie folgt wider.

Räume fragiler Staatlichkeit

(1) Bereits heute sind nichtstaatliche Konflikte häufig Verstärker fragiler und schwacher Staatlichkeit. Auch in Zukunft werden sie destabilisierend auf staatliche Strukturen wirken und könnten damit auch weitläufigere Krisen und Konflikte auslösen, verschärfen

und verlängern. Eine solche Situation könnte je nach Intensität auch regionale Migrationsbewegungen zur Folge haben. Migration und zunehmende Vernetzung befördert dabei eine Entgrenzung nichtstaatlicher Konflikte mit Auswirkungen weit über die direkt betroffenen Länder und Regionen hinaus.

(2) Staaten müssen diese Konstellationen berücksichtigen, wollen sie ihre sicherheitspolitische Handlungsfähigkeit in Räumen fragiler Staatlichkeit sicherstellen. Insbesondere wird zukünftig die Zahl von Eingriffen durch NSA – seien dies TKN, PMSF, TNU oder NGOs – in Räumen fragiler Staatlichkeit wahrscheinlich zunehmen. Herrschaftsstrukturen gestalten sich hierdurch zunehmend komplexer und sind immer weniger auf ein einziges Staatsgebiet eingrenzbar.

(3) In einer Vielzahl von Konstellationen nichtstaatlicher Konflikte können wichtige Infrastrukturen, wie Pipelines, beispielsweise durch Sabotageakte, beschädigt oder zerstört werden.

(4) Der Export wichtiger Güter könnte durch Infrastrukturschädigungen belastet werden.

(5) Konflikte, zum Beispiel zwischen TKN, aber auch durch Infrastrukturschädigungen hervorgerufene Umweltschäden, können die humanitäre Lage in Räumen fragiler Staatlichkeit verschlechtern.

Maritime Räume

(1) Weitläufigere Krisen und Konflikte könnten provoziert werden, wenn NSA aus unterschiedlichen Staaten in Gewässern, die zwischen diesen Staaten umstritten sind, in Konflikt geraten – beispielsweise wegen des Abbaus von Ressourcen oder des Fischfangs.

(2) Die zukünftig höhere Anzahl von Akteuren wie PMSF und Piraten wird die sicherheitspolitische Handlungsfähigkeit beeinflussen. Gleichzeitig könnte die verstärkte Nutzung von maritimen Räumen für Handel (und unter Umständen den Tiefseebergbau) neue Ansprüche an das Handeln von Streitkräften, zum Beispiel bei Schutzaufgaben, nach sich ziehen.

(3) Auch maritime Räume beherbergen eine Vielzahl kritischer Infrastrukturen, die in Folge nichtstaatlicher Konflikte gezielt oder unintendiert in Mitleidenschaft gezogen werden können. Hierzu zählen Unterseekabel, Gas- und Ölpipelines sowie *offshore*-Bohranlagen und Stromleitungen von Windkraftanlagen. Eine Störung transozeanischer Kommunikationsmöglichkeiten bei einer Beschädigung von Unterseekabeln könnte beispielsweise ernstzunehmende Folgewirkungen im Finanzsystem erzeugen, das über diese Kabel eine Vielzahl von Transaktionen abwickelt.

(4) Zukünftig kann der freie und ungehinderte Welthandel sowie der freie Zugang zur Hohen See zunehmend bedroht werden; insbesondere durch Konflikte bei denen Piraten, PMSF und in geringerem Umfang auch radikalisierte Umwelt-NGOs beteiligt sind. Unwahrscheinlich aber dennoch möglich sind temporäre Blockaden von Engpässen, wie der Straße von Hormus, welche die Versorgungssicherheit

von Staaten einschränken würden.[155] Eine auch nur kurze Blockade würde beispielsweise den Öltransport massiv behindern und könnte zu kurzzeitigen Preisschocks führen. Auch eine mögliche Blockade bedeutender Häfen ist zwar unwahrscheinlich jedoch nicht auszuschließen.

(5) Die humanitäre Lage in Küstengebieten könnte durch nichtstaatliche Konflikte beeinträchtigt werden, wenn diese durch die Beschädigung von Förderanlagen, Gas- oder Ölpipelines oder durch Schiffshavarien zu großflächigen Umweltverschmutzungen führen und so die Lebensgrundlagen lokaler Gemeinschaften stark einschränken würden. Weiterhin kann die Ausdehnung nichtstaatlicher Aktivitäten und Konflikte den bestehenden Rechtsrahmen auf Hoher See überfordern. Bereits heute stellt sich die Frage, wer die Einhaltung von Rechtsnormen bei der Bekämpfung von Piraten durch PMSF auf Hoher See überwacht.

Weltraum

(1) Während die Wahrscheinlichkeit der Ausweitung nichtstaatlicher Konflikte im Weltraum auf andere Akteure eher gering ist, könnten sich Situationen ergeben, in denen Staaten Konflikthandlungen zwischen NSA als aggressive Handlungen gegen sich selbst verstehen und gegebenenfalls auch andere Staaten für diese Handlungen verantwortlich machen. Eine besondere Rolle spielt hier die Attributionsproblematik von Handlungen im Weltraum.

(2) Konfliktkonstellationen zwischen NSA im Weltraum bergen bei einer Eskalation die Gefahr einer schwerwiegenden Beeinträchtigung der sicherheitspolitischen Handlungsfähigkeit von Staaten. Dies gilt für militärische Anwendungen, wie bei der weltraumgestützten Aufklärung und Beobachtung sicherheitspolitisch relevanter Entwicklungen (z.B. Rüstungskontrolle) sowie bei der militärischen Führung und Kommunikation, ebenso wie für Aufgaben der humanitären Hilfe, des zivilen Krisenmanagements und der langfristigen Beobachtung von Umweltveränderungen.

(3) Nichtstaatliche Konflikte könnten, beispielsweise durch die Kollision oder Zerstörung von Satelliten oder durch eine massiven Steigerung der *debris*-Mengen, vitale, auch sicherheitsrelevante Infrastrukturen gefährden. Im Falle einer zunehmenden Stationierung militärisch relevanter Systeme im Weltraum, könnte es hier zu besonders weitreichenden Folgen kommen, sollten Angriffe auf diese Systeme trotz erhöhter Sicherheitsstandards gelingen oder diese von unintendierten Schädigungen betroffen sein.

Vor dem Hintergrund der enormen Einschränkung, die Staaten in ihrer Handlungsfähigkeit erfahren könnten, ist es aus sicherheitspolitischer Perspektive bis 2040 bedeutsam, wie in einem solch schwer zu überblickenden Raum, auf der Grundlage eines verbesserten Lageverständnisses, die Prävention unintendierter Schädigungen und die Abschreckung, Attribution und Verfolgung intendierter Angriffe von vitalen Infrastrukturen erreicht werden können. Da diese Aspekte Staaten im Weltraum auch perspektivisch vor große Herausforderungen stellen dürften und sich im Falle von Konflikten zwischen NSA noch schwie-

riger gestalten, stellen der noch bessere Schutz ziviler und militärischer Infrastrukturen und die fokussierte Verbesserung der eigenen Widerstandsfähigkeit und Redundanz ein prioritäres Handlungsfeld dar.

(4) Für einen freien und ungehinderten Welthandel ist der Weltraum wichtig, weil durch ihn essenzielle Kommunikations- und Navigationsleistungen angeboten werden können. Eine Störung der Aktivitäten im Weltraum durch nichtstaatliche Konflikte hätte damit auch mittelbare Auswirkungen auf den Welthandel, beispielsweise im Bereich der Finanztransaktionen und beim Zugang zur Hohen See.

(5) Die Weiterentwicklung des Völkerrechts, beziehungsweise der *governance* für die Nutzung des Weltraums wird bis 2040 eine der zentralen Herausforderungen internationaler Politik darstellen.[156] NSA werden hier mit einbezogen werden müssen, um die friedliche, freie und faire Nutzung des Weltraums zum Wohle aller Menschen sicherzustellen. Nichtstaatliche Konflikte könnten entsprechende Bemühungen erschweren.

Cyberspace

(1) Nichtstaatliche Konflikte im Cyberspace könnten zwischenstaatliche Krisen heraufbeschwören, sollten sie über Staaten und Regionen beziehungsweise Gesellschaften und Kulturen hinweg reichen. Solche Konflikte erscheinen aufgrund der durch den Cyberspace geschaffenen Nähe und Unmittelbarkeit wahrscheinlich. So könnten Staaten andere Staaten dafür verantwortlich machen, dass ein NSA von deren Territorium aus Schaden angerichtet hat.

(2) Die Sicherstellung der Handlungsfähigkeit von Streitkräften im Cyberspace stellt allein aufgrund der Anzahl von NSA, der Komplexität und Unübersichtlichkeit nichtstaatlicher Konflikte und dem Problem der Attribution von Handlungen eine große Herausforderung dar. Der Diebstahl oder die Veröffentlichung sensibler Informationen könnte die staatliche Handlungsfähigkeit weit über den Cyberspace hinaus einschränken. Die Bedrohung, die dem Staat direkt durch die Entwendung solcher Informationen durch NSA entsteht, wird durch nichtstaatliche Konflikte noch vergrößert. Dies gilt sowohl bei Konflikten zwischen spezialisierten Sicherheitsfirmen, als auch bei solchen zwischen PMSF und Internetaktivisten.

(3) Kritische Infrastrukturen, die mit dem Cyberspace verbunden sind, sind durch nichtstaatliche Konflikte gefährdet, beispielsweise aufgrund von Erpressungsaktionen von TKN oder auch durch Aktivisten, die einem Unternehmen schaden wollen, dass zum Beispiel Umwelt- oder Sozialstandards drastisch verletzt. Bei der Bedrohung von Infrastrukturen zeigt sich ganz besonders, dass der Cyberspace als Raum viele Anknüpfungspunkte an andere Räume hat. So könnten Infrastrukturen, die sich in anderen Räumen befinden – Satelliten im Weltraum oder Ölbohrinseln in maritimen Räu-

men – in Mitleidenschaft gezogen werden.

(4) Eine Einschränkung des Zugangs zum Cyberspace beziehungsweise die systematische Verhinderung von Handelstransaktionen durch nichtstaatliche Konflikte ist in Fällen einzelner Akteure möglich, in einem umfassenderen Maßstab jedoch unwahrscheinlich.[157]

(5) Die Weiterentwicklung der internationalen *governance* für den Cyberspace stellt eine wichtige Herausforderung für die Zukunft dar. Aufgrund der wachsenden Bedeutung und der weitreichenden Vernetzung des Cyberspace wird dieses Handlungsfeld zunehmend an Priorität gewinnen.

4.2. Nichtstaatliche Akteure als Stellvertreter

Nachdem die sicherheitspolitischen Implikationen nichtstaatlicher Konflikte skizziert wurden, muss eine weitere Frage gestellt werden: Sind NSA tatsächlich immer *nicht*staatliche Akteure? Bisher wurde davon ausgegangen und in vielen Fällen wird dies in Zukunft auch so sein. Dennoch wurde auch darauf verwiesen, dass Unternehmen in Staatsbesitz sind oder Staaten (Quasi-)NGOs gegründet haben. Dies deutet darauf hin, dass nichtstaatliche Konflikte in Zukunft auch zu einer neuen Art Stellvertreter-Konflikte werden könnten.

Die Wege und Mittel, mit denen solche Konflikte durchgeführt werden, als auch ihr Erscheinungsbild wären grundsätzlich mit tatsächlichen nichtstaatlichen Konflikten vergleichbar. Hinsichtlich der Ziele von Konflikthandlungen könnten sich hingegen Änderungen ergeben. So wären Staaten vermutlich interessierter daran, genau solche Ziele ins Visier zu nehmen, die von besonderer strategischer Bedeutung sind – seien dies Konstruktionspläne aus dem Rüstungsbereich oder Kommunikations- und Überwachungsinfrastrukturen. Vier Ausprägungen, bei denen der Staat in unterschiedlicher Intensität zu nichtstaatlichen Konflikten beiträgt, können unterschieden werden.

Erstens besteht die Möglichkeit, dass der Staat unintendiert zu nichtstaatlichen Konflikten beiträgt oder in diese hineingezogen wird, wenn er durch Aufträge oder Zuwendungen NSA finanziell oder materiell unterstützt, welche anschließend mit anderen NSA in Konflikt geraten. So könnte sich der Staat als zahlungskräftigster Kunde einer PMSF erweisen, die an anderer Stelle in Konflikte mit anderen NSA gerät oder diese sogar provoziert.

Zweitens ist auch in Zukunft zu erwarten, dass manche NSA enge Verbindungen zu Staaten haben werden, beziehungsweise von diesen instruiert werden. Der Staat wäre so bewusst an den Aktionen der NSA beteiligt und bestimmt diese gegebenenfalls maßgeblich mit. Besonders sichtbar ist diese Konstellation schon heute im Bereich von Rohstoffunternehmen oder bei instrumentalisierten NGOs in (semi-)autokratischen Staaten.

Drittens könnten Staaten NSA infiltrieren. Diese Möglichkeit besteht insbesondere bei Internetaktivisten. Diese finden weitgehend anonym zusammen und können daher die Herkunft und Motivation einzelner Teilnehmer nicht ohne Weiteres nachvollziehen. So bestehen Möglichkeiten, dass staatlich

instruierte Teilnehmer Aktivistengruppen unterwandern.[158] In Zukunft könnten staatliche Stellen dabei nicht nur versuchen, NSA zu überwachen oder deren Aktivitäten zu behindern, sondern ebenso Aktionen zu provozieren, welche den Zielen des jeweiligen Staates zuträglich sind.

Eine vierte Möglichkeit für den Staat, sich nichtstaatliche Konflikte zunutze zu machen, besteht darin, eigenes Handeln auf solche Situationen zu konzentrieren, in denen die öffentliche Aufmerksamkeit auf nichtstaatliche Konflikte gerichtet ist. So könnten Staaten versuchen, im „Nebel des nichtstaatlichen Krieges“, zum Beispiel bei einer Welle nichtstaatlicher Cyberattacken, unbemerkt eigene Angriffe auf strategisch relevante Systeme durchzuführen.

4.3. Handlungsfelder

Um den sicherheitspolitischen Implikationen nichtstaatlicher Konflikte entgegenzuwirken, ergeben sich für Deutschland und die Bundeswehr folgende Handlungsfelder.

Früherkennung und ganzheitliches Lagebild neu denken

Klassische, akteurszentrierte Bedrohungsanalysen (Akteur, Intention, Fähigkeit) verlieren an Aussagekraft, denn nichtstaatliche Konflikte, Stellvertreter-Konstellationen, komplexe und dynamische Akteursnetzwerke und vielfache Möglichkeiten des verdeckten Agierens machen es zukünftig immer schwerer, Konfliktakteure sowie deren Intentionen und Handlungsmittel klar zu identifizieren (Attributionsproblematik). Nichtstaatliche Konflikte zeigen, dass Gefährdungen sogar dann entstehen können, wenn es keinen dem Staat geltenden Angriff gibt. Die klassische Bedrohungsanalyse muss daher angepasst und um neue Ansätze ergänzt werden.

Dies beinhaltet die Berücksichtigung eines breiteren Spektrums an Akteuren und Akteurskonstellationen. Neben NSA selbst müssen auch deren Beziehungen und Konflikte untereinander sowie die Möglichkeit der Nutzung von NSA als Stellvertreter durch Staaten berücksichtigt werden. Weiterhin gilt es, einen stärkeren Fokus auf die besprochenen Räume begrenzter Staatlichkeit, die darin perspektivisch zur Verfügung stehenden Wege und Mittel sowie auf die Verbindungen der Räume untereinander (*inter-domain vulnerabilities*) zu legen.

Weiterhin können Früherkennung und Erstellung eines ganzheitlichen Lagebildes nur gelingen, wenn ein breites Spektrum an Kooperationspartnern eingebunden wird. Ein wirklich tiefgreifendes Verständnis kann nur in ressortübergreifendem und multinationalem Austausch erreicht werden. Auch die Einbeziehung von Kompetenzen aus Wissenschaft, Wirtschaft und Zivilgesellschaft ist unabdingbar.

Selbst mit elaborierten sowie ressort- und sektorübergreifenden Instrumenten für eine ganzheitliche Analyse kann jedoch nicht jede Gefährdung durch nichtstaatliche Konflikte frühzeitig erkannt werden. Daher muss der Blick

verstärkt auch auf eigene Abhängigkeiten und Vulnerabilitäten gerichtet werden. Auch hier gilt es, Dynamiken und Vernetzungen zwischen den Räumen und in ihnen vorkommende Infrastrukturen und Fähigkeiten einzubeziehen. Eventualfallplanungen, auch für weniger wahrscheinliche Großschadensereignisse, und die Stärkung der eigenen Widerstandsfähigkeit (Resilienz) gewinnen an Bedeutung und müssen gezielt vorangetrieben werden.

Schließlich müssen Konzepte, die die eigenen Gegenmaßnahmen anleiten, überdacht werden. Wer agiert überhaupt? Und gegen wen? Wessen Handeln soll unterbunden werden? Und wie kann das gelingen, wenn der Angriff in erster Linie gar nicht gegen den Staat gerichtet ist? Traditionelle sicherheitspolitische Konzepte wie „Abschreckung“ gelangen hier an ihre Grenzen, und es müssen gegenüber NSA und deren Konflikte untereinander neue Ansätze entwickelt werden.

Koordinierter Umgang mit nichtstaatlichen Akteuren

Nichtstaatliche Konflikte stellen jedoch nicht nur eine analytische Herausforderung dar. Vielmehr muss auch mit ihnen umgegangen werden. Hierzu ist ein Risikomanagement notwendig, dass die Bereiche der Bedrohungsabwehr in Räumen begrenzter Staatlichkeit sowie die Steigerung der Resilienz vernetzter Gesellschaften verknüpft.[159] In Verbindung stehen diese Bereiche insbesondere durch Infrastrukturen, die von entscheidender Bedeutung für Gesellschaften sind und sich dabei teils oder vollständig in Räumen begrenzter Staatlichkeit befinden.

Ob und wie die Bundeswehr im Rahmen des Risikomanagements sinnvoll eingesetzt werden kann, kann nur auf Grundlage des zuvor thematisierten ganzheitlichen Lageverständnisses beantwortet werden. Generell muss sich die Bundeswehr dabei auf neue Handlungsräume wie den Cyberspace einstellen, um auch dort flexibel mit neuen handlungsmächtigen Akteuren umgehen zu können und um in der Lage zu sein, auch dort sicherheitsrelevanter Systeme zu schützen.

Vor diesem Hintergrund bedarf es jenseits von Lippenbekenntnissen einer konsequenten praktischen Umsetzung der Zusammenarbeit relevanter Akteure in den diskutierten Räumen. Hierzu müssen auf politischer Ebene klare Kompetenzen festgelegt werden, welche Exekutivkräfte für die Abwehr von Bedrohungen und Gefährdungen aus und in den Räumen begrenzter Staatlichkeit sowie für die Verbesserung der Resilienz verantwortlich sein werden.

Schließlich hat sich im Laufe der Studie ergeben, dass PMSF in vielen Fällen eine Sonderrolle einnehmen. Sie können Fähigkeiten für staatliche Streitkräfte bereitstellen, aber zukünftig auch NSA unterstützen. Die Kooperation mit PMSF verlangt in vielen Fällen die Weitergabe sensibler Informationen und schafft so neue Verwundbarkeiten. Zukünftig könnte eine Vielzahl neuer PMSF in anderen Weltregionen entstehen. Insgesamt sind PMSF somit einen Schlüsselfaktor in der zukünftigen Entwicklung auch nichtstaatlicher Konflikte, welchen es weiter zu untersuchen gilt.

Dialog über die Verantwortlichkeit von Staaten für das Handeln von nichtstaatlichen Akteuren

Um zu verhindern, dass nichtstaatliche Konflikte Krisen zwischen Staaten provozieren, gilt es im internationalen Kontext die Frage zu klären, wer für das Handeln von NSA mit bekannter Herkunft verantwortlich ist.

Welche Verantwortung hat beispielsweise eine Regierung für den Schaden, den Hackergruppen von ihrem Territorium aus in anderen Ländern anrichten? Diese Frage hat schon in der Vergangenheit im Kontext der Hackerangriffe auf Estland und Georgien eine wichtige Rolle gespielt. Der vom *Cooperative Cyber Defence Centre of Excellence* der NATO erarbeitete Vorschlag eines so genannten „Territorialprinzips“ würde implizieren, dass Staaten für alle von ihrem Hoheitsgebiet ausgehenden Cyberangriffe die Verantwortung tragen.[160] Dieser Vorschlag wird jedoch kontrovers diskutiert. Die Fragen nach der Verantwortung für das Handeln von NSA sowie nach der grundlegenden Rolle von NSA in den einzelnen Räumen bleiben damit ungelöst und bedürfen eines erhöhten Abstimmungsbedarfs nicht nur zwischen Bündnispartnern innerhalb der NATO, sondern auch mit weiteren Staaten über die Allianz hinaus. Dieser Dialog ist auch mit aufstrebenden Staaten zu führen, deren Ordnungsvorstellungen des Cyberspace teils stark divergieren.

Verrechtlichung der nichtstaatlichen Politik

Schließlich ist das Vorgehen gegen nichtstaatliche Konflikte immer nur der zweitbeste Ansatz. Sinnvoller ist die Prävention. Eine nachhaltige Verrechtlichung des Handelns von NSA und deren Beziehungen untereinander kann dazu beitragen, nichtstaatliche Konflikte zu vermeiden.

Generell herrscht in Räumen begrenzter Staatlichkeit ein eher geringes Regelungsniveau. Zusätzlich gilt, dass das Völkerrecht für Staaten verbindlich ist, für NSA jedoch in vielen Fällen nicht – ein Beispiel hierfür ist der in Kapitel 3.3 angesprochene Weltraumvertrag. Auch viele Verhaltenskodizes, beispielsweise für den Weltraum oder den Cyberspace, integrieren NSA nicht oder nur unzureichend.

Eine Regulierung und Verrechtlichung mit Augenmaß kann Anreize für NSA schaffen, sich friedfertig zu verhalten. Es sollten dabei nicht nur Verhaltensregeln geschaffen werden. Auch sollten klare Verantwortlichkeiten und Sanktionen für nicht regelkonformes Handeln etabliert und Mechanismen geschaffen werden, um diese Sanktionen auch durchzusetzen. Ein weiterer lohnenswerter Ansatz wäre die Etablierung von Streitschlichtungsmechanismen zur Konfliktlösung zwischen NSA.[161]

Zur Durchsetzung dieser Maßnahmen für die *governance* in Räumen begrenzter Staatlichkeit ergeben sich vier Vorgehensweisen. Eine erste wichtige Option wäre es, bestehende zwischen-

staatliche Regelungen, wie beispielsweise die Nutzung des Weltraumes als Allmende, rechtlich zweifelsfrei auf NSA auszudehnen. Zweitens sollten in Fällen, in denen solche Regulierungen nicht bestehen, wie im Cyberspace, NSA bei der Verrechtlichung von Beginn an berücksichtigt werden.

Diese beiden Vorgehensweisen sind jedoch aufgrund der Kooperationsprobleme zwischen Staaten oft nur schwer durchführbar. Auch wenn allgemein akzeptierte, globale Regelungen die effektivste Grundlage zur Verrechtlichung nichtstaatlicher Politik darstellen, ergeben sich darüber hinaus mindestens zwei weitere Ansätze, eine Verrechtlichung der Aktivitäten von NSA und ihrer Beziehungen untereinander zu bewirken:

So können NSA teils auch national oder regional reguliert und dabei eine Wirkung erzielt werden, die über die eigenen Grenzen hinausgeht. Ein Beispiel hierfür ist der 2010 in den USA verabschiedete *Dodd-Frank Act*, der Transparenzvorschriften für Rohstoffunternehmen enthält, die an US-Börsen notiert sind.[162] Da auch viele ausländische Unternehmen über US-Börsennotierungen verfügen, wirkt die Vorschrift weit über die Grenzen der USA hinaus.

Schließlich erscheint es erstrebenswert, die sich bereits heute zwischen NSA entwickelnden Regelwerke zu unterstützen. Oft haben solche Regeln das Potenzial, Beiträge zu einer friedlichen (nichtstaatlichen) Politik zu leisten, die durch staatliche Regulierungen alleine nicht erreicht werden könnten. Ein Beispiel ist hierbei die Überwachung und Zertifizierung der Aktivitäten von TNU durch NGOs. NGOs können dabei, zum Beispiel in Räumen fragiler Staatlichkeit, oft auf Kompetenzen und Expertise zurückgreifen, die Staaten nur begrenzt zur Verfügung stehen.

4.4. Zusammenfassung

Nichtstaatliche Konflikte in Räumen begrenzter Staatlichkeit können zukünftig bedeutende sicherheitspolitische Implikationen für Staaten haben. In fragilen Staaten tragen nichtstaatliche Konflikte schon heute zur Ausweitung von Krisen und Konflikten und zur Verschlechterung der humanitären Lage bei und werden dies auch in Zukunft tun.

Als besonders bedeutsam haben sich darüber hinaus die potenziellen Auswirkungen nichtstaatlicher Konflikte auf Infrastrukturen herausgestellt. Gerade durch diese sind moderne, hochvernetzte Gesellschaften eng mit Räumen begrenzter Staatlichkeit verbunden. Schließlich wirken sich nichtstaatliche Konflikte auch auf die Handlungsfähigkeit von und das Verhältnis zwischen Staaten aus.

Nichtstaatliche Konflikte werden zukünftig ein ohnehin schon schwer zu überblickendes Umfeld noch komplexer machen, dem sich die deutsche Sicherheitspolitik und die Bundeswehr gegenübersehen. Die Studie hat gezeigt, dass es hinsichtlich der Instrumente der Früherkennung und der Erstellung von Lagebildern zukünftig nicht mehr ausreichen wird, nur konkrete Bedrohungen des Staates durch andere Staaten oder NSA im Blickfeld zu behalten. Stattdessen müssen darüber hinaus auch die Beziehungen von NSA untereinander stetig berücksichtigt werden. Generell wird es neben

der Abwehr von Bedrohungen immer wichtiger, das Augenmerk auch auf die eigenen Verwundbarkeiten zu legen und die eigene Widerstandsfähigkeit gegen die Auswirkungen nichtstaatlicher Konflikte zu stärken.

Sowohl die Bedrohungsabwehr als auch die Steigerung der Resilienz vernetzter Gesellschaften, kurz das Risikomanagement, sind keine Aufgaben, die klar nur einem Ressort zugeordnet werden können. Umso wichtiger ist es, dass die Entwicklung politischer Leitlinien vorangetrieben wird, die die Kompetenzen und Mechanismen der Zusammenarbeit bei diesen Aufgaben regelt und die notwendigen Fähigkeiten möglichst klar definiert. Nur im Rahmen eines solchen gesamtstaatlichen Ansatzes kann konkretisiert werden, ob und wie die Bundeswehr im Rahmen nichtstaatlicher Konflikte und der Ausgestaltung der in dieser Studie dargestellten Handlungsfelder zum Einsatz kommen kann.

Anlagen

A Die Entwicklung von fünf Gruppen nichtstaatlicher Akteure bis in die Gegenwart

Diese Anlage stellt eine ausführlichere Version des in Kapitel 2.1 behandelten Bedeutungsgewinns verschiedener NSA-Gruppen dar. Als Ausgangspunkt der Betrachtung dieser Entwicklungen wurde vorwiegend die Zeit des Kalten Krieges gewählt, also eine Zeit, in der Staaten die Geschicke der internationalen Politik dominierten.[163] Der staatszentrierte Ansatz des sicherheitspolitischen Denkens und der sicherheitspolitischen Analyse, der in dieser Zeit entstanden ist, prägt nach wie vor unser Bild der internationalen Politik in besonderer Weise. Wie in der Einleitung dieser *Future Study* dargestellt, werden heutzutage zwar auch NSA in der Sicherheitspolitik wahr- und ernstgenommen. Die Vielfältigkeit der nichtstaatlichen Politik – und damit auch die mögliche Relevanz nichtstaatlicher Konflikte – sind jedoch nur bedingt erkannt worden. Deswegen wird im Folgenden aufgezeigt, wie sich die internationale Politik in den letzten Jahrzehnten stetig von einer allein staatenzentrierten Welt entfernt hat.

Schon während des Kalten Krieges gewannen NSA kontinuierlich an Bedeutung. Seit den 1970er-Jahren wurde verstärkt darüber diskutiert, ob und wie zum Beispiel TNU die unangefochtene Stellung des Staates herausforderten.[164] In den 1980er-Jahren gewannen darüber hinaus NGOs an Bedeutung.[165] In der Folgezeit ist das Spektrum von NSA noch breiter geworden. So gewannen beispielsweise TKN immer mehr an Bedeutung. Spätestens seit der Jahrtausendwende sind darüber hinaus auch PMSF verstärkt in den Blickpunkt geraten. Eine letzte hier näher betrachtete Gruppe sind Internetaktivisten, die besonders in den vergangenen Jahren für Aufsehen gesorgt haben.

Die Definition und Abgrenzung der im Folgenden vorgestellten Gruppen ist keineswegs einfach und nicht immer trennscharf. Auch innerhalb der jeweiligen Gruppen findet sich nicht selten eine Vielfalt verschiedener Akteure. Trotz notwendiger Vereinfachungen in der Kategorisierung geben die folgenden Beschreibungen einen Überblick über die Welt der NSAs, ihre Handlungsmotivationen und Ziele, ihre Entwicklung, ihrer Bedeutung für das internationale System und die Kritik, die an der Rolle einzelner Gruppen geäußert wird.

A 1 Transnationale Unternehmen

TNU sind wirtschaftliche Einheiten, zu denen neben einem Mutterunternehmen auch Tochterunternehmen im Ausland gehören.[166] Sie bewegen sich in sehr unterschiedlichen Branchen wie der Produktion von Nahrungsmitteln oder Kraftfahrzeugen, dem Vertreiben von Dienstleistungen, oder der Energiewirtschaft.

Ziele und Motivationen

Zentrales Handlungsmotiv von TNU ist das ökonomische Eigeninteresse, also

die Gewinnmaximierung und Steigerung von Marktanteilen. Dies schließt jedoch nicht aus, dass TNU teils auch gemeinwohlorientiert agieren.[167] Solche Tätigkeiten können sowohl normativ als auch ökonomisch motiviert sein, das heißt sie sind häufig auch mit entsprechenden wirtschaftlichen Anreizen verbunden und „rechnen sich“ (Reputationsnutzen).

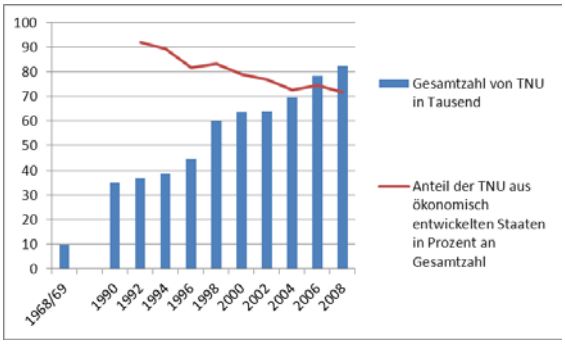
Entwicklung und Bedeutung

TNU gehören zu den einflussreichsten NSA auf der weltpolitischen Bühne. Nach Schätzungen der UNCTAD trägt die Aktivität von TNU heutzutage gut ein Viertel zum globalen BIP bei. Das ist etwas mehr als die globalen öffentlichen Ausgaben (24%).[168] Die größten TNU – wie zum Beispiel *Walmart* mit 421,8 Milliarden US-Dollar Umsatz im Geschäftsjahr 2010, *Royal Dutch Shell* mit 378,1 Milliarden US-Dollar Umsatz oder *Exxon Mobil* mit 354,6 Milliarden US-Dollar Umsatz – vereinen eine beachtliche Wirtschaftskraft auf sich. Die Zahl der Beschäftigten der größten TNU geht dabei in die Hunderttausende. *Walmart* beschäftigt weltweit sogar über zwei Millionen Menschen.[169]

Häufig wird die Größe einzelner Unternehmen mit dem BIP von Staaten verglichen. So entspricht der Umsatz von *Walmart* in etwa dem BIP von Österreich mit 418 Milliarden US-Dollar und die Umsätze von *Royal Dutch Shell* und *Exxon Mobil* jeweils in etwa dem BIP der Vereinigten Arabischen Emirate mit rund 360 Milliarden US-Dollar.[170] Obwohl TNUs keine direkten Konkurrenten für Staaten darstellen und bei einem solchen Vergleich entsprechende Vorsicht geboten ist, illustriert er gleichwohl die Größe und Bedeutung dieser Akteursgruppe.[171]

Die Zahl der TNU ist über die letzten Jahrzehnte kontinuierlich gestiegen (vgl. Abb. A.1).

Abbildung A.1: Gesamtzahl transnationaler Unternehmen und relativer Anteil von Unternehmen aus entwickelten Staaten



Quelle: BpB (2010).

Neben dem Bedeutungsgewinn von TNU allgemein lassen sich zwei Trends erkennen: Ein steigender Transnationalisierungsgrad und und ein relativer Bedeutungsverlust von TNU aus Industrieländern im Vergleich zu jenen, die aus Schwellenländern stammen. Die Transnationalisierung kann am Transnationalisierungsindex (TNI) der UNCTAD abgelesen werden, der Vermögenswerte, Umsatz und die Beschäftigten im Heimatland in Relation zu denen der ausländischen Tochtergesellschaften setzt. Der Transnationalisierungsgrad der weltweit 100 größten TNU hat sich dabei von 51,5 Prozent im Jahre 1995 auf 63,4 Prozent im Jahre 2008 erhöht (BpB 2010).[172]

Gleichzeitig ist der relative Anteil von TNU aus so genannten Industriestaaten stetig gesunken. Besonders im Zusammenhang mit der globalen Finanz- und Wirtschaftskrise haben sich diese Tendenzen gegenseitig verstärk:[173]

Zurückgehende Einnahmen zwangen die Unternehmen verstärkt, sich zusammenzuschließen. Wegen des Drucks auf den Heimatmärkten drängten TNU aus Industriestaaten dabei stärker in die Märkte der Schwellenländer. Unternehmen aus diesen Ländern nutzten wiederum die Chancen, die ihnen die Krise bei ihren hauptsächlich westlichen Konkurrenten bot und expandierten ins Ausland.

TNU haben eine große Bedeutung für die Weltwirtschaft und sind Treiber der Globalisierung. Ihr ökonomischer Einfluss, die großen finanziellen Handlungsressourcen und ihre Investitionstätigkeiten gehen dabei zunehmend mit politischen Gestaltungsmöglichkeiten einher.[174] Dabei lassen sich unterschiedliche Arten politikrelevanter Tätigkeiten von TNUs erkennen. Diese reichen von normensetzenden und -überwachenden Tätigkeiten (z.B. ICANN), über Dienstleistungstätigkeiten und die Bereitstellung von Expertise (z.B. im Rahmen von *Public Private Partnerships*) bis hin zu einer direkten Beeinflussung von Politikgestaltung (Lobbyismus).[175]

Kritik

Aufgrund ihrer Rolle im Prozess der Globalisierung werden TNU häufig von Globalisierungskritikern, wie zum Beispiel *Attac* oder *Human Rights Watch*, kritisiert. Die Art der Kritik ist dabei vielfältig und reicht von konstruktiven Vorschlägen zur Lösung konkreter Probleme bis hin zu pauschaler Verteufelung.[176]

Ein Hauptpunkt der Kritik ist die Ausnutzung unterschiedlicher Umwelt- und Sozialstandards. Nicht selten siedeln TNU ihre Produktion in Ländern an, in denen solche Standards nicht oder nur unzureichend verankert sind. So werden die ökonomischen Vorteile der transnationalen Produktion häufig auf Kosten von Menschenrechten, Sozial- und Umweltstandards ausgeschöpft.[177]

Die *corporate social responsibility* Maßnahmen von TNU werden zudem häufig als Augenwischerei abgetan.[178] Das vorrangige Ziel, Gewinn und Marktanteile zu maximieren, setze den gemeinwohlorientierten Aktivitäten der Unternehmen deutliche Grenzen und schränke ihre Glaubwürdigkeit ein.[179]

Auch die Erbringung von öffentlichen Gütern und Dienstleistungen, zum Beispiel im Bereich der Telekommunikation, Strom- oder Wasserversorgung, durch private Akteure wird mitunter kritisch gesehen. Die Profitorientierung von Unternehmen, so das Hauptargument, sei mit der Idee der öffentlichen Daseinsvorsorge nicht oder nur schwer zu vereinbaren. Außerdem würden bei Privatisierungen teils lediglich staatliche Monopole durch privatwirtschaftliche Monopole ersetzt. Die mit einer Privatisierung angestrebten Effizienzgewinne würden damit konterkariert.[180]

Im Kontext transnationaler Politikgestaltung sind TNU in den Augen zahlreicher NGO bereits überrepräsentiert.

Ein weiterer Streitpunkt betrifft die Frage nach staatlichen Beteiligungen an TNU. Besonders in Bereichen wie der Energiewirtschaft wird immer wieder

kritisiert, dass vorgeblich transnationale privatwirtschaftliche Akteure durch ihr Handeln lediglich die Agenda ihres Heimatstaates befördern würden.

Auch die Rolle von TNU in Ländern, die von fragiler Staatlichkeit und bewaffneten Konflikten betroffen sind, ist Gegenstand umfangreicher Kritik. Zwar haben TNU grundsätzlich ein Interesse an stabilen Umfeldbedingungen in Ländern, in denen sie investieren und beteiligen sich dort daher teilweise auch an konstruktiven Konfliktlösungen. Doch die (auch nur mittelbare) Zusammenarbeit mit teils korrupten, klientelistischen Eliten oder Gewaltakteuren kann illegitime Regime unterstützen und Kriegsökonomien befördern. TNU trügen so unter Umständen dazu bei, Gewaltkonflikte zu festigen und zu verlängern. Besonders häufig betrifft dieser Vorwurf TNU, die am Abbau und Handel mit Rohstoffen beteiligt sind.[181]

A 2 Nichtregierungsorganisationen

Für die vorliegende Studie werden NGOs als nichtstaatliche, nicht gewinnorientierte und auf ein bestimmtes Ziel ausgerichtete Organisationen definiert.[182] Dabei sind vor dem Hintergrund der Fragestellung besonders nicht profitorientierte, *transnationale* Akteure von Interesse.

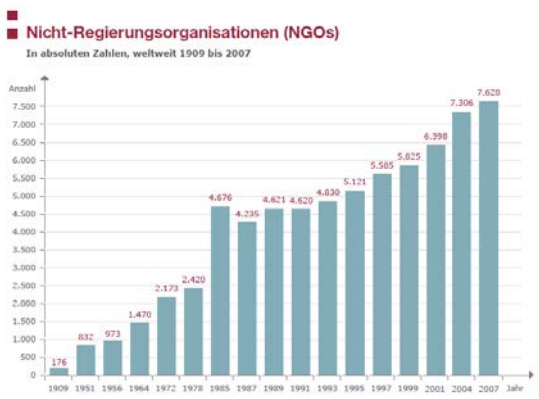
Ziele und Motivationen

NGOs sind ihrem Anspruch nach Vertreter universeller zivilgesellschaftlicher Interessen. Die Idee der nachhaltigen Entwicklung, also eines angestrebten Einklangs von ökologischem Gleichgewicht, sozialer Gerechtigkeit und ökonomischem Wachstum, wurde in den 1990er-Jahren in besonderer Weise zum Leitbild zahlreicher NGOs. Viele dieser NGOs stehen in ihren Zielen und Handlungsmotivationen daher den Auswirkungen der Globalisierung sowie multinationalen Unternehmen kritisch gegenüber.[183] In der Folgezeit wuchs das Themenspektrum kontinuierlich und umfasst heute neben Entwicklung, Menschenrechten, Umwelt und Konfliktbearbeitung auch zahlreiche Nischenthemen. Gemein haben die NGOs hinsichtlich ihrer Handlungsmotivation eine prinzipielle Gemeinwohlorientierung. In der Realität sind jedoch auch NGOs nicht frei von Partikular- und Eigeninteressen (siehe Kritik).

Entwicklung und Bedeutung

Bekannte Vorläufer von NGOs aus dem 19. Jahrhundert sind die Menschenrechtsorganisation *Foreign Anti-Slavery Society* (Anti-Sklaverei-Gesellschaft) und das Rote Kreuz. Erst nach dem zweiten Weltkrieg wurde der Begriff NGO im Kontext der VN eingeführt. Unterschiedliche private Akteure wirkten in der Gründungsphase der VN mit, so zum Beispiel bei der Ausarbeitung der Charter. Ausgehend von diesen Bemühungen wurden mit Artikel 71 der Charter Konsultationsprinzipien von „non-governmental organisations“ mit den VN festgeschrieben.[184] Seither hat sich die Begrifflichkeit NGO verbreitet und auch ihre Anzahl ist deutlich gestiegen (vgl. Abb. A.2).

Abbildung A.2: Anzahl der Nichtregierungsorganisationen



Quelle: BpB (2010).

Vor allem in den 1970er- und 1990er-Jahren waren drastische Wachstumsschübe zu verzeichnen. Die VN-Weltkonferenzen hatten hierauf maßgeblichen Einfluss. Insbesondere seit dem VN-Gipfel über Umwelt und Entwicklung in Rio de Janeiro im Jahr 1992 haben NGOs als Vertreter zivilgesellschaftlicher Interessen kontinuierlich an Bedeutung und Akzeptanz gewonnen. Verbunden damit wurden neue Partizipationsmöglichkeiten, effizientere Formen für die Lösung transnationaler Probleme und eine Demokratisierung des internationalen Systems. Ihnen wird eine legitimierende und kontrollierende Funktion für politische Prozesse zugesprochen. Das Phänomen der Globalisierung befördert seither eine zunehmend grenzüberschreitende Organisation dieser Akteure.

Heute müssen sich Staatenvertreter in der Festlegung von internationalen Normen, Standards und Regelwerken in zunehmendem Maße mit Vertretern einer wachsenden Anzahl von NGOs auseinandersetzen.[185] Transnational vernetzte NGOs nehmen Einfluss auf die Willensbildung und Gestaltung zahlreicher Politikbereiche und Regelwerke.

Mit der Anzahl von NGOs wuchs auch das Spektrum an Themen, welches diese mit ihrer Arbeit abdecken. Neben den großen Themenlinien Entwicklung, Menschenrechte, Umwelt und Konfliktbearbeitung und den bekanntesten großen und global agierenden NGOs wie beispielsweise *Amnesty International*, Ärzte ohne Grenzen, *Friends of the Earth*, *Greenpeace* oder *World Wide Fund for Nature* (WWF) gibt es zunehmend auch kleinere NGOs, die sich jenseits dieses „Mainstreams“ bewegen und thematische Nischen besetzen.

Diese Spezialisierung bedeutet auch, dass sich solche NGOs nicht um das Wohl Aller bemühen, beispielsweise um Menschenrechte allgemein, sondern die Interessen spezifischer Gruppen vertreten, sich beispielsweise um die Situation von Kindersoldaten kümmern.[186]

Neben Einfluss, Größe und Thema lassen sich – wie für TNU – unterschiedliche politikrelevante Tätigkeiten von NGOs identifizieren. Diese reichen von normensetzenden und überwachenden Tätigkeiten (z.B. *Forest Stewardship Council*), über Dienstleistungen und die Bereitstellung von Expertise (z.B. Ärzte ohne Grenzen) bis hin zu einer direkten Beeinflussung von Politikgestaltung durch öffentlichkeitswirksame Aktivitäten (*Advocacy*).[187] Die Grenzen sind häu-

fig fließend und Organisationen decken oft mehrere Tätigkeiten ab.[188]

Zwar sind die finanziellen Ressourcen der meisten NGOs verglichen mit denen von Nationalstaaten und TNU eher gering. Größere NGOs verfügen jedoch über beachtliche Jahresbudgets von teils mehreren Millionen Euro, die ihnen signifikante Handlungsspielräume eröffnen. Die Ressourcen setzen sich vor allem aus Spenden, Mitgliedsbeiträgen, sowie Gewinnen aus dem Verkauf von Waren und Dienstleistungen zusammen. Aber auch staatliche Zuwendungen spielen eine Rolle für die Finanzierung.[189] Auch agieren NGOs häufig nicht für sich allein, sondern bündeln ihre Ressourcen auf unterschiedlichen Ebenen in Netzwerken untereinander oder in Koalition mit staatlichen und wirtschaftlichen Akteuren.[190]

Die beschriebenen Ressourcen stehen in unmittelbarer Wechselwirkung zu den Maßnahmen und Prozessen, mit denen NGOs ihre Ziele zu erreichen suchen. Wegen ihrer meist eingeschränkten finanziellen Möglichkeiten sind NGOs auf andere Mittel der Einflussnahme angewiesen. Hierzu gehören vor allem Mechanismen, die ihnen erlauben, Anreize für betroffene Akteure zu setzen oder Druck auf diese auszuüben. Das heißt gezielt Kosten-Nutzen-Kalküle dieser Akteure (z.B. Reputationsgewinne und -verluste) auszunutzen. Hinzu kommen Aktivitäten, welche NGOs aufgrund der Dienstleistungen und Expertise, die sie bereitstellen „unverzichtbar“ machen und ihnen so den entsprechenden Einfluss auf Politikgestaltung ermöglichen.[191]

Kritik

Trotz der skizzierten demokratisierenden und legitimierenden Funktionen, die NGOs zugesprochen werden, sind deren Strukturen und Aktivitäten auch Gegenstand umfangreicher Kritik. Vor allem ihre Spendenabhängigkeit kann in Kombination mit den jeweiligen politischen Agenden ihre Unabhängigkeit und Glaubwürdigkeit deutlich einschränken. Die klare Trennung von NGOs und Staat ist auch nicht immer gegeben.

So illustriert der Begriff *astroturf*, also Kunstrasen, in Abgrenzung zum Begriff *grass-roots* die kritische Sicht auf Initiativen, die vortäuschen, eine Graswurzelbewegung zu sein, jedoch nicht von Privatpersonen oder NGOs sondern von staatlichen Akteuren ausgehen. Auch können NGOs aufgrund finanzieller Abhängigkeiten ihre Distanz zu staatlichen Akteuren nicht immer wahren. Solche Fälle werden auch *quasi-non-governmental organizations* (Quasi-NGOs) genannt.

Auch wird bemängelt, dass NGOs in vielen Fällen kein Interesse an der Lösung der von Ihnen angeprangerten Probleme hätten, weil das Bestehen dieser Probleme auch ihre eigene Existenzberechtigung darstellt. Tatsächlich bewegen sich NGOs nicht selten im Spannungsfeld von Selbsterhalt und Festigung ihrer Existenzberechtigung einerseits und der tatsächlichen Durchsetzung der postulierten Ziele andererseits. Auch die Praktiken einiger NGOs sind teils umstritten. Kritisiert werden beispielsweise gezielte Täuschung und Fehlinformation, die den Agenden der NGOs dienen und militante Aktionen einiger Organisationen, wie zum Bei-

spiel der *Seashepherd Conservation Society*, einer Umweltorganisation, die sich berechtigt fühlt, illegal fischende Schiffe zu versenken.

Auch kann die fehlende Legitimation transnationaler Politik nicht durch NGOs ausgeglichen werden. NGOs sind nicht demokratisch legitimiert und müssen auch hinsichtlich ihrer internen Struktur nicht notwendigerweise demokratisch verfasst sein. Darüber hinaus herrschen enorme Ungleichgewichte in Bezug auf Anzahl, Ressourcen und Einfluss der NGOs zwischen der Nord- und der Südhalbkugel. Die meisten NGOs haben ihren Sitz nach wie vor in Europa und Nordamerika. Auch innerhalb der Industrieländer herrschen Ungleichgewichte. Einige NGOs vertreten Minderheiten oder Nischenthemen und verfügen dennoch über beachtliche Ressourcen, während andere, die vielleicht eine größere Interessensgruppe vertreten über geringere Handlungsressourcen verfügen und weniger artikulationsstark sind. Besonders deutlich wird diese Problematik der ungleichen Repräsentation im Zusammenhang mit sogenannten „Politikunternehmern", die sich entlang ihrer spezifischen Interessen, und mit erheblichen finanziellen Mitteln eine eigene NGO „leisten" können. Diese Aspekte schränken die zugeschriebene Funktion von NGOs, die Input- oder Prozesslegitimität transnationalen Regierens zu erhöhen, deutlich ein.

Neben den positiven Beiträgen, die sie zu Konfliktbearbeitung und humanitärer Hilfe leisten, werden Aktivitäten von NGOs in Entwicklungsländern, fragilen oder von Bürgerkriegen betroffenen Staaten mitunter auch kritisch gesehen. Kritikpunkte sind eine mögliche Verzerrung lokaler Marktstrukturen durch Hilfslieferungen sowie der in der Vergangenheit (z.B. im Sudan) aufgetretene, selbstbereichernde Missbrauch dieser Hilfen und Mittel durch Konfliktakteure. NGOs würden so dazu beitragen, Kriegsökonomien zu festigen und Gewaltkonflikte zu verlängern.[192]

A 3 Transnationale kriminelle Netzwerke

Unter dem Begriff TKN werden hier auf Dauer organisierte Gruppen verstanden, die profitorientierte, schwerwiegende kriminelle Aktivitäten verfolgen, welche sich im Gegensatz zu anderen Formen der Kriminalität durch ihre Häufigkeit und ihre transnationale Dimension auszeichnen. Diese sogenannten „dunklen Netzwerke" stellen die Schattenseite nichtstaatlicher Politik dar.[193]

Ziele und Motivationen

TKN sind primär von ökonomischen Interessen getrieben, so dass man sie vereinfacht als Fortführung der Wirtschaft mit kriminellen (insbesondere gewalttätigen) Mitteln bezeichnen kann.[194] Für ihre Handlungsfähigkeit benötigen sie sichere Rückzugsmöglichkeiten (*safe havens*) vor Strafverfolgungsbehörden. Sie haben Interesse am Erhalt rechtsfreier Räume mit eingeschränktem staatlichem

Gewaltmonopol, gleich ob diese in fragilen Staaten oder strukturschwachen Gebieten in Industriestaaten und deren Metropolen zu finden sind. Gleichzeitig sind sie aber auch auf vorhandene und funktionierende Infrastrukturen für ihre Aktivitäten angewiesen. So zeigen etwa Studien zu dem Phänomen der Piraterie, dass diese insbesondere dort floriert, wo Staaten schwach sind, nicht aber an Orten, an denen keinerlei staatliche Strukturen mehr vorhanden sind.[195]

Entwicklung und Bedeutung

Während des Kalten Krieges wurden existierende TKN durch die Blockkonfrontation weitgehend überdeckt.[196] Ihre heutige Bedeutung und Erscheinung haben sie erst durch das Ende der Blockkonfrontation und die Globalisierung erhalten.[197] Im Laufe der 1990er-Jahre haben sich Akteure wie die Albanische Mafia oder verschiedene Gruppen der italienischen Mafia global vernetzt und transnationalisiert und sind heutzutage etablierter Bestandteil der internationalen (Un-)Ordnung – in Industrieländern (z.B. in Form von Wirtschaftskriminalität) und in Entwicklungsländern (z.B. Piraterie).[198]

Unterschiedliche Aspekte spielten für diese Entwicklungen eine Rolle: Erstens lässt sich die Ausweitung von TKN und ihrer Aktivitäten auf die eingeschränkte Fähigkeit von Staaten zurückführen, transnationalen Problemen effektiv zu begegnen. Verstärkt wird dies insbesondere durch das Phänomen schwacher Staatlichkeit. In schwachen oder fragilen Staaten konnten und können sich kriminelle Akteure Verfolgungsbehörden entziehen.

Zweitens wurde die globale Kommunikation und Organisation von TKN stark durch die zunehmende globale Vernetzung der Kommunikationswege und -infrastrukturen vereinfacht. Mit dieser Entwicklung ging auch eine stärkere transnationale Vernetzung von ethnischen Gruppen und Diasporagemeinschaften auf der ganzen Welt einher. Auf Basis solch sozialer, transnationaler Netzwerke konnten sich auch TKN, wie beispielsweise die albanische Mafia, herausbilden oder ihre Aktivitäten auf neue Gebiete ausweiten.

Drittens profitieren auch TKN von der Globalisierung von Wirtschaftskreisläufen, die auch für den Handel mit illegalen Gütern nutzbar sind. Darüber hinaus konnten TKN in Folge der Deregulierung und Digitalisierung des Finanzmarktes leichter Geld waschen und ihre Gewinne leichter in legalen Bereichen reinvestieren.

Schließlich beförderten auch die in Folge der Globalisierung entstehenden globalen Unterschiede in der Wohlstandsverteilung die Entwicklung und Ausweitung von TKN.

Vor dem Hintergrund dieser Entwicklungen haben TKN in den letzten Jahren erheblich an Bedeutung gewonnen. Heute werden circa sieben bis zehn Prozent des weltweiten BIP auf illegalen Märkten durch die TKN umgesetzt.[199] So betrug in Deutschland der geschätzte Schaden durch Organisierte Kriminalität von 2001 bis 2010 laut Zahlen des Bundeskriminalamtes knapp zwölf Milliarden. Euro.[200] Im Jahr 2010 lag die direkte Schadenssumme in Deutschland bei etwa 1,65 Milliarden Euro,[201] was Folgekosten, zum Beispiel im Gesundheitswesen durch Drogenkonsumenten, nicht

einbezieht. In Italien wird der Umsatz der Organisierten Kriminalität auf jährlich rund 138 Milliarden Euro geschätzt. Damit hat sie einen fast doppelt so großen Umsatz wie das größte legale Unternehmen des Landes, der Erdölkonzern ENI mit 83 Milliarden Euro.[202]

Die etablierten Betätigungsfelder von TKN umfassen den Drogen-, Waffen und Menschenhandel (inkl. Zwangsprostitution) sowie die Wirtschaftskriminalität, Geldwäsche und die Piraterie. Darüber hinaus sind insbesondere in den letzten Jahren Betätigungsfelder wie die Cyberkriminalität, identitätsbezogene Kriminalität, der Schmuggel von Kulturgütern, Umweltverbrechen und der Organhandel hinzugekommen.[203]

Die Beispiele Drogenhandel und Piraterie illustrieren das Ausmaß dieser Tätigkeiten. Allein auf dem illegalen Drogenmarkt in Europa werden pro Jahr schätzungsweise 124 Tonnen Kokain und 87 Tonnen Heroin mit einem Gesamtwert von rund 54 Milliarden US-Dollar umgesetzt.[204]

Ein weiteres internationales Problem, dem zunehmende Aufmerksamkeit gewidmet wird, ist die Piraterie. Allein in der ersten Jahreshälfte 2012 wurden 168 Piraterieangriffe sowie 19 Geiselnahmen von Schiffen registriert.[205] Der jährliche Schaden durch Piraten vor der Küste Somalias beträgt nach Schätzungen etwa sieben Milliarden US-Dollar. Weltweit sind 40 Prozent des globalen über Seewege transportierten Öls von Piratenangriffen bedroht.[206]

Die genannten Zahlen und Beispiele verdeutlichen, dass Akteure und Aktivitäten Organisierter Kriminalität längst kein innerstaatliches Ordnungsproblem mehr sind. Vielmehr stellen sie ein zentrales transnationales Problem dar, mit Implikationen für unterschiedliche Politikbereiche, auch die Sicherheitspolitik.[207]

Kritik

TKN nehmen durch ihre Aktivitäten Einfluss auf die Stabilität von Staaten und stehen in teils enger Wechselwirkung mit dem internationalen Terrorismus. Das Beispiel Liberia unter dem ehemaligen Präsidenten Charles Taylor illustriert diese Verflechtungen. Taylor machte das Land zu einem Hort für Gewaltakteure unterschiedlicher Art. Er verfügte über zutiefst korrupte staatliche Strukturen und kriminelle Akteure. Diese bereicherten sich einerseits massiv selbst. Andererseits schafften sie einen *safe haven* unter anderem für russische und ukrainische kriminelle Netzwerke, die mit Edelhölzern und Blutdiamanten handelten. Im Jahr 2000 stiegen Teile von Al-Qaida in den Diamantenschmuggel ein. Hierbei griffen sie für den Transport wiederum auf Netzwerke der Hisbollah zurück.[208]

Solche Netzwerke können ohnehin schwache oder fragile Staaten überfordern und Destabilisierungs- und Zerfallsprozesse weiter vorantreiben.[209] Auch die Entstehung und Verstetigung innerstaatlicher Konflikte werden durch Strukturen Organisierter Kriminalität, vor allem durch den Export illegaler

Güter als zugleich zentrale Konfliktressourcen, gefördert.[210]

Trotz der hier skizzierten, in der Mehrheit destabilisierenden Aktivitäten von TKN, können sie in Zonen fragiler oder gescheiterter Staatlichkeit auch eine – wenngleich begrenzte – Ordnungsfunktion erfüllen, kleinere Inseln von Stabilität herstellen oder Einkommensmöglichkeiten für zumindest Teile der Bevölkerung generieren.

A 4 Private Militär- und Sicherheitsfirmen

PMSF sind private Unternehmen, die Sicherheitsdienstleistungen anbieten. Zu diesen Leistungen zählen neben der Beratung auch unbewaffnete logistische Unterstützungen und das Bereitstellen bewaffneter Sicherheitskräfte.[211] Weiterhin umfasst die Begrifflichkeit alle Firmen, welche in militärische oder sicherheitsbezogene Tätigkeiten, seien sie offensiv oder defensiv, in Konfliktzonen oder Postkonfliktsituationen involviert sind.[212] Ein Großteil der PMSF ist primär im unterstützenden Bereich tätig.[213]

Ziele und Motivationen

PMSF richten ihr Handeln nach ökonomischen Interessen aus, das heißt sie sind profitorientiert. Etablierte PMSF zielen zunehmend auf eine Konsolidierung und Normalisierung des Marktes ab. Ziel ist es, sich als legitime profitorientierte Akteure darzustellen.[214] Hierzu organisieren sie sich in Verbänden, wie der amerikanischen *National Association of Security Companies*, und befürworten eine weitere Regulierung und Kontrolle, etwa bei der Registrierung von Firmen und Überwachung der Ausbildung.[215] Insbesondere kleine und neue Marktakteure können jedoch aufgrund fehlender Regulierung und Kontrolle auch kurzfristig gewinnmaximierend operieren und kein Interesse an einer internationalen Verrechtlichung haben.

Entwicklung und Bedeutung

Die heutigen speziell militärisch orientierten PMSF haben ihren Ursprung zumeist in den 1970er-Jahren in Großbritannien.[216] Ihre heutige Bedeutung verdanken sie einer historisch einmaligen Dynamik, die nach dem Ende des Kalten Krieges einsetzte. Treiber dieser Dynamik war unter anderem eine stetig steigende staatliche Nachfrage aufgrund des zunehmenden Drucks auf das Verteidigungsbudget und einen gestiegenen Flexibilisierungsbedarf von Streitkräften.

Auch NSA fragten die Leistungen von PMSF nach, zum Beispiel um Gebäude schützen zu lassen. In schwachen und fragilen Staaten, in denen effektive staatliche Strukturen fehlten, wurden auch robustere Dienstleistungen nachgefragt.[217]

Durch diese Dynamiken sowie durch die Globalisierung begünstigt entstand ein umfassender Markt für Sicherheitsdienstleistungen, sowohl militärischer als auch nicht-militärischer Natur.[218]

Die heutige Bedeutung von PMSF lässt sich anhand folgender Zahlen verdeutlichen: Während sie von 1959 bis 1989 lediglich an 15 Konflikten beteiligt waren, war dies allein von 1990 bis 2000 achtzig Mal der Fall[219]; während 1996 lediglich zehn Prozent der einhundert umsatzstärksten Rüstungsunternehmen auf Sicherheitsdienstleistungen spezialisiert waren, hat sich dieser Wert bis 2010 verdoppelt; und

während die Umsätze dieser Firmen 2002 bei 22,3 Milliarden US-Dollar lagen, waren es 2010 bereits 55 Milliarden.[220] Besonders deutlich wird die Bedeutung von PMSF in Analysen, welche darlegen, dass die US-Einsätze im Irak und Afghanistan ohne private Dienstleister nicht durchführbar gewesen wären.

Zwar bleibt die Letztverantwortung von Staaten zum Einsatz militärischer Gewalt in dem Sinne bestehen, dass sie die größten Auftraggeber sind und potenziell auch den rechtlichen Rahmen setzen können. Dennoch ist bereits heute eine Vielzahl verschiedener Bereiche des Militärhandwerks in der Praxis an PMSF ausgelagert. So hat *Executive Outcomes* bereits 1993 in Angola im Regierungsauftrag von Rebellen besetzte Städte wieder eingenommen und später das staatliche Militär mit aufgebaut. Ein weiteres Beispiel für die umfangreichen Aktivitäten von PMSF ist der Einsatz von ehemaligen US-Generalen in der Firma *Military Professional Resources Incorporated*, die 1995 auf taktisch-operativer Ebene einen Feldzug für die kroatischen Truppen in den Balkankriegen unterstützten. PMSF werden heute von nahezu allen westlichen Armeen eingesetzt.

Die große Bandbreite militärischer Mittel und Fähigkeiten von PMSF ist als käufliche Dienstleistung aber auch NSA zugänglich. Dies zeigt sich anschaulich beim Piraterieproblem, bei dem Reedereien private Sicherheitsdienstleister engagieren, um ihre Schiffe auch mit Waffengewalt vor Übergriffen zu schützen. Trotz der hauptsächlichen Beauftragung durch Staaten kommen einige Autoren zu dem Schluss, von einem Ende des Gewaltmonopols des Staates zu sprechen.[221]

Kritik

Die Kritik an PMSF ist sehr vielfältig und umfassend, teils aber auch von Vorurteilen getragen.[222] Eingangs wurde beispielsweise die Profitorientierung von PMSF als zentrale Handlungsmotivation herausgestellt. Diese bedeutet jedoch nicht, dass PMSF von apolitischer Natur im Sinne eines neutralen Instruments der Staaten oder transnationaler Unternehmen sind. Vielmehr haben sie sich als eigenständige Akteure auch mit politischem Einfluss etabliert.[223] Beispielsweise erarbeiten PMSF als Sicherheitsexperten Analysen sicherheitspolitischer Problemlagen. Hierdurch erlangen sie eine Deutungsmacht und können Einfluss auf die Wahrnehmung von Ereignissen, auf Interessenbildungsprozesse wichtiger Akteure und damit auch auf die Sicherheitsagenda eines Landes haben.[224]

Ein weiterer zentraler Punkt ist die grundlegende Kritik an der Privatisierung des Gutes Sicherheit. Hierdurch werde sukzessive das staatliche Monopol auf militärische Machtmittel und deren Kontrolle untergraben. Dies umfasst etwa die schwierige und ungenügende Kontrolle von PMSF und deren Praktiken durch die internationale Gemeinschaft. In der Wirklichkeit von Einsätzen in Krisenregionen gestaltet

sich die strafrechtliche Verfolgung von Straftaten beziehungsweise Kriegsverbrechen durch PMSF problematisch. Neben praktischen Problemen, wie der Beweisführung, ist das Kernproblem die Kollision verschiedener Rechtsebenen. Da nach dem Humanitären Völkerrecht Angehörige von PMSF Kombattanten darstellen, wenn sie einer Konfliktpartei zuzuordnen sind,[225] gilt für sie folglich auch das Kriegsvölkerrecht. Gleichzeitig jedoch schließen Armeen oftmals sogenannte *Status of Forces Agreements*, wodurch sichergestellt werden soll, dass beispielsweise amerikanische Soldaten auch nur von amerikanischen Gerichten verurteilt werden dürfen. Durch die Eingliederung in reguläre Streitkräfte und auf vertraglicher Basis überträgt sich dies auch auf Angehörige von PMSF. Damit ist die Verfolgung von Kriegsverbrechen privater Sicherheitsdienstleister sehr stark vom politischen Willen des Entsendestaates abhängig.

Weiterhin ist grundlegend umstritten, ob PMSF tatsächlich zu einer Kostenreduzierung. Ein weiterer Kritikpunkt ist stärker innenpolitischer Natur: Beim Einsatz von PMSF durch die Exekutive wird die Kontrolle nationaler Parlamente eingeschränkt.

Neben diesen rechtlichen und politischen Aspekten, wirkt sich die fehlende Kontrolle auch auf die Operationsführung aus. Denn PMSF gehen im Gegensatz zu Soldaten nur eine vertragliche Bindung mit dem Staat ein und leisten keinen Eid. Folglich ist die Vertragstreue nicht garantiert und kann durch eine Veränderung der Situation und eine neue Abwägung von Kosten und Nutzen durch die PMSF in Extremfällen potenziell aufgekündigt werden. So könnten im Ernstfall operativ notwendige und eingeplante Fähigkeiten wegfallen. Weiterhin problematisch ist, dass ein umfassendes Lagebild über im Einsatzraum operierende PMSF fehlt und es hierdurch zu *friendly-fire* zwischen staatlichen Streitkräften und Angehörigen von PMSF kommen kann. Abschließend wird von militärischer Seite kritisiert, dass PMSF militärisches Fachpersonal und besonders Spezialkräfte abwerben, ohne für deren Ausbildung aufkommen zu müssen.

A 5 Internetaktivisten

Internetaktivisten werden hier als zivilgesellschaftliche Akteure definiert, die den Cyberspace als ihren zentralen Handlungsraum ansehen und deren Ziele eng mit dem Informationsfluss im Internet verknüpft sind. Besonders neue Internetaktivisten zeichnen sich des Weiteren dadurch aus, dass sie eher dynamischen Netzwerken als klar strukturierten Organisationen ähneln. Damit unterscheiden sie sich zum Beispiel von NGOs und Akteuren der Finanzwelt, die zwar auch im Internet agieren, dabei aber zumeist weiterhin auf hergebrachte Motivationen und Organisationsstrukturen vertrauen.[226]

Ziele und Motivationen

Die grundlegende Motivation vieler Internetaktivisten ist aus der sogenannten Hackerethik abzulesen, der sich zum Beispiel der CCC schon früh verschrieb. Der universelle Informationszugang steht hier im Mittelpunkt. Traditionelle Gesellschafts- und Herrschaftsstrukturen werden abgelehnt.[227]

Während der Ruf nach der Freiheit des Internets die Internetaktivisten eint,

steht oft auch der Spaß an erster Stelle (siehe unten: *script kiddies*). In den letzten Jahren haben sich aber auch in diesen Milieus politische Ziele entwickelt. Die Grenzen zwischen Spaß und politischem Aktivismus sind häufig fließend und die netzwerkartige Struktur neuerer Gruppierungen lässt die Zielformulierung oft sehr intransparent und teilweise willkürlich erscheinen.[228]

Entwicklung und Bedeutung

Internetaktivisten sind eine verhältnismäßig neue Gruppe in der Welt der NSA. Ihr Bedeutungsgewinn ist eng mit jenem des Mediums Internet gekoppelt. Für erstes Aufsehen sorgten bereits in den 1980ern die Hacker des CCC, als sie in Rechner der Hamburger Sparkasse sowie der NASA und anderer wissenschaftlicher Institutionen einbrachen.[229] Die Erfolge wurden häufig von den Aktivisten selbst veröffentlicht, was nicht unwesentlich zum Erkennen von Sicherheitslücken in den sich entwickelnden Netztechnologien beitrug.[230]

Mit der Weiterentwicklung des Internets gewannen die sogenannten *script kiddies* an Bedeutung, das sind zumeist Jugendliche, die – häufig ohne tiefgreifende Kenntnis der Materie – auf vorgefertigte Programme im Internet zurückgreifen, um zur eigenen Belustigung Schaden im Netz anzustellen.[231] Nicht zuletzt aus dieser Kategorie hat sich um das Jahr 2003 *Anonymous* entwickelt.[232]

Während sich der CCC 1981 in Hamburg als Club jenseits der virtuellen Welt konstituierte und seit 1986 als eingetragener Verein geführt wird, gibt es bei *Anonymous* keine klare Mitgliedschaft und keine legitime Vertretung: die Anhänger treffen sich vorwievorwiegend im Internet und anonym.[233] *Anonymous* ist daher als eine Art Netzwerk zu begreifen, in dem handlungsfähige Gruppen spontan entstehen, ebenso schnell aber auch wieder zerfallen können. Der Akteur *Anonymous* entsteht dabei nicht nur durch Identifikation von Individuen mit den Symbolen der Gruppe – zum Beispiel die *Guy Fawkes*-Maske. Auch die Bezeichnung „als Akteur“ durch Beobachter, Befürworter und Kritiker ist ein wichtiges Element der Gruppenbildung.

Die Anzahl der *Anonymous*-Aktionen ist in den letzten Jahren stark gestiegen. Anstelle des Hackings wurde dabei häufiger auf DDoS-Attacken zurückgegriffen.[234] Während zuerst vor allem „Internetstreiche“ zu den Aktivitäten der Gruppe zählten, bildeten sich im Laufe der Zeit explizit politische Ziele heraus – die meisten dabei im Bereich der Informationsfreiheit.

So wurden 2009, nach der Verurteilung der Betreiber der Downloadseite *The Pirate Bay*, und 2012, nach dem Abschalten der Seite *Megaupload*, eine Vielzahl von DDoS-Attacken durchgeführt, um die Internetseiten von Medienunternehmen, Urheberrechts-Verbänden und Regierungsinstitutionen lahmzulegen.

2011 hackte Anonymous sich in die Systeme verschiedener Unternehmen, darunter die US-Sicherheitsfirmen

Stratfor und *HB Gary*. [235] Ende desselben Jahres konfrontierte die Gruppe einen weiteren NSA: Auf *YouTube* erschien ein Video, in dem die Internetaktivisten bekanntgaben, dass das mexikanische Drogenkartell *Los Zetas* eines ihrer Mitglieder gefangen genommen hatte. Die Gruppe forderte die Freilassung des Mitgliedes und drohte mit „Krieg“ und damit, Identitäten von *Zetas*-Kollaborateuren, unter anderem im mexikanischen Staatsdienst, zu enthüllen. Es kam jedoch nicht dazu. Am 5. November 2011 veröffentlichte *Anonymous* eine weitere Botschaft, nachdem die entführte Person freigelassen worden war.

Als erste jenseits der virtuellen Welt ausgetragene Aktion gilt das gegen Scientology gerichtete *Project Canology* (seit 2008), in dem *Anonymous* nicht nur die Internetpräsenz der Sekte angriff, sondern das Internet unter anderem auch dazu nutzte, anhaltende Proteste gegen die Sekte zu organisieren.

Eine andere Art von Internetaktivisten, die in der jüngeren Vergangenheit für Aufsehen gesorgt hat ist die Internetplattform *WikiLeaks*, die geheime Dokumente veröffentlichte – darunter mehr als 100.000 Depeschen von US-Botschaften weltweit.

Allgemein finden die Handlungen von Internetaktivisten vorwiegend im Cyberspace statt, entfalten ihre Wirkung aber häufig auch darüber hinaus.[236] Die in der jüngeren Vergangenheit am meisten diskutierten Vorgehensweisen sind die bereits erwähnten DDoS-Attacken[237] und die Veröffentlichung geheimer Dokumente. Bei der Veröffentlichung geheimer Informationen ist die Informationsbeschaffung von Bedeutung. Diese kann sowohl durch das Hacken von Systemen als in der realen Welt geschehen. Beide Handlungsformen können empfindlichen Schaden verursachen, besonders für Akteure, die ihr Geschäft hauptsächlich im Internet betreiben oder für die die Geheimhaltung der Information einen entscheidenden Wettbewerbsvorteil bietet.

Kritik

Von Beginn ihres Wirkens an nahmen Internetaktivisten eine gesellschaftlich ambivalente Rolle ein. Das Aufspüren von Sicherheitslücken stieß neben anfänglich vorwiegend kritischen Stimmen schnell auch auf positive Resonanz in Politik und Gesellschaft. Mittlerweile stellen Institutionen sogenannte *White Hacker* ein, um Sicherheitslücken gezielt aufzudecken und zu beheben.

Gleichzeitig wurden Internetaktivisten von Telekommunikationsunternehmen wegen ihres Vorgehens stark kritisiert. In jüngerer Vergangenheit wurden diese Akteursgruppe und ihre Aktivitäten immer wieder als Sicherheitsbedrohung bezeichnet, wobei über die tatsächliche Gefährdung, die von ihnen ausgeht, heftig gestritten wird.[238] Hauptkritiker sind dabei Staaten und besonders Unternehmen, die versuchen, Urheberrechte auch in Zeiten des Cyberspace durchzusetzen.

Auch innerhalb der Reihen der Internetaktivisten sind Verwerfungen zu erkennen. So lehnt beispielsweise der CCC die Verwendung von DDoS-Attacken vehement ab.[239] Darüber hinaus kritisiert der CCC *Anonymous* dafür, dass es ihnen nicht gelungen sei, ethische Codes für das eigene

Verhalten aufzustellen.[240] Generell gilt, dass die Berechenbarkeit von netzwerkartig strukturierten Akteuren wesentlich geringer ist als bei traditionell strukturierten Akteuren. Andere Kritiker wiederum sehen selbst in neuen Formen des Internetaktivismus zu viel der eigentlich abgelehnten Machtstrukturen reproduziert und bemängeln die fehlende Gleichheit aufgrund von Unterschieden im Zugang zum Internet und den Kompetenzen hinsichtlich dessen Nutzung.[241]

A 6 Schlussbemerkungen

Die uneingeschränkte Vormachtstellung des Staates in der internationalen Politik, wie sie in der Zeit des Kalten Krieges oft als gegeben angesehen wurde, existiert heute nicht mehr. NSA sind über die letzten Jahrzehnte zu wichtigen Akteuren in der internationalen Politik geworden. Dabei erschöpfen die besprochenen Akteursgruppen – TNU, NGOs, TKN, PMSF und Internetaktivisten – nicht die Vielfalt der nichtstaatlichen Welt. Weiterhin existieren zum Beispiel so genannte *super-empowered individuals*, Rebellengruppen und transnationale terroristische Organisationen.

Super-empowered individuals sind Individuen, die das Potenzial haben, das internationale Umfeld substanziell zu beeinflussen. Dabei fällt ihr Handeln aber häufig in das bisher besprochene Spektrum von Aktivitäten. So setzt sich zum Beispiel Bill Gates mit seinem Reichtum für die Entwicklungspolitik ein. Er tut dies über die Bill und Melinda Gates Stiftung, die im NGO-Bereich tätig ist. Eine weitere, als *super-empowered individual* bezeichnete Person, Julian Assange, kann durch die Gründung der Internetplattform *WikiLeaks* durchaus dem Bereich der Internetaktivisten zugeordnet werden.

Rebellen und andere lokale Gewaltakteure sowie transnationale terroristische Organisationen unterscheiden sich wiederum von den bisher diskutierten Akteuren insofern, als das sich ihr Handeln oft gegen eine bestehende politische und meist staatliche Ordnung wendet. Sie sind also weniger wirtschaftlich oder zivilgesellschaftlich, sondern politisch motiviert. Rebellen sind im Vergleich zu den bisher betrachteten NSA zumeist weniger transnational eingebunden und spielen in dieser Studie daher vorwiegend dann eine Rolle, wenn sich transnationale nichtstaatliche Konflikte mit lokalen Strukturen vermischen (vgl. Kap. 3.1 zu Räumen fragiler Staatlichkeit und Kap. 3.2 zu maritimen Räumen). Der Terrorismus wiederum wird in dieser *Future Study* weniger als Akteur begriffen, sondern als spezifischer Handlungsweg. Auch wenn dieser von den betrachteten NSA bisher nur bedingt eingesetzt wurde, steht er ihnen zumindest prinzipiell offen.

B Treiber des Bedeutungsgewinns nichtstaatlicher Akteure

In dieser Anlage werden die Treiber des Bedeutungsgewinns von NSA sowie die Aussagen, die in Kapitel 2, Abbildung 2.1, getroffen werden, hergeleitet.

Neun Treiber werden diskutiert (vgl. Abb. A 2.1). Diese teilen sich auf drei übergreifende Kategorien auf – technologische Entwicklung und Steigerung der Interaktionskapazität, gesellschaftlicher Wandel sowie die Begrenzung von Staatlichkeit. Für jeden Treiber wird zuerst die Entwicklung beschrieben und dann erläutert, wie diese Entwicklung zum Bedeutungsgewinn von NSA beigetragen hat.

Abbildung B.1: Treiber des Trends Bedeutungsgewinn nichtstaatlicher Akteure

Übergreifende Kategorien	Treiber
(A) technologische Entwicklung	(1) Transportwesen
	(2) Kommunikationswesen
	(3) Wirkmittel
(B) gesellschaftlicher Wandel	(4) transnationale Netzwerke
	(5) Wertewandel
	(6) Radikalisierung
(C) begrenzte Staatlichkeit	(7) Kompetenzabgabe an NSA
	(8) *governance*-Lücke

Quelle: eigene Darstellung.

Technologische Entwicklung und Steigerung der Interaktionskapazität

Besonders die Bereiche des Transport- und Kommunikationswesens sowie jener der Wirkmittel haben sich über die letzten Jahrzehnte bedeutend verändert. In allen drei Bereichen gilt, dass Mittel nicht nur effizienter, sondern in den meisten Fällen auch leichter zugänglich geworden sind. Für NSA bedeutet dies eine Steigerung ihrer Handlungsfähigkeit, beziehungsweise ihrer Interaktionskapazität.[242]

(1) Im *Transportwesen* ist es in den letzten Jahrzehnten zu bedeutenden Vergünstigungen von Land-, See- und Lufttransport gekommen. Der Einsatz des 1956 erfundenen standardisierten

Containers und die Entstehung moderner Handelsflotten mit immer größeren Schiffen schufen die Möglichkeit, große Warenmengen günstig und verhältnismäßig schnell über weite Strecken zu transportieren. Gleichzeitig wurde es durch die Ausweitung des Luftverkehrs für eine immer größere Zahl von Individuen möglich, in nur wenigen Stunden um die Welt zu reisen.

Für TNU ergaben immer größere Möglichkeiten, die Produktion ihrer Güter über die ganze Welt zu verteilen und so Staaten mit angedrohten Produktionsverlagerungen unter Druck zu setzen. Gleichzeitig boten neue Transport- und Handelsrouten für TKN die Möglichkeit, neue und teils Kontinente übergreifende Schmuggelrouten, zum Beispiel für Waffen aber auch für Menschen, zu etablieren.[243]

(2) Noch stärker als die Entwicklung des Transportwesens haben neue *Kommunikationstechnologien* – das Fax, transkontinentale Telefonie und schließlich auch die sogenannten IT-Revolution mit ihren Kommunikationsmöglichkeiten im Cyberspace – in den letzten Dekaden die interaktionshemmende Wirkung räumlicher Distanz vermindert.

TNU ist es heute möglich, ortsungebunden und in Echtzeit im Cyberspace Geschäfte zu tätigen. Für TKN haben sich Geschäftsfelder wie die Internetkriminalität ergeben. Gesellschaftlichen Akteuren wiederum erlaubten die neuen Kommunikationsmittel, sich effizienter und über größere Entfernungen hinweg zu organisieren. Auch haben diese Akteure Möglichkeiten gewonnen, neue Unterstützerkreise zu mobilisieren und so den eigenen Einfluss zu mehren. Während dies klassisch für NGOs gilt, ist diese Tendenz im Falle von Internetaktivisten noch wesentlich ausgeprägter.

(3) Schließlich hat sich die Welt auch hinsichtlich der den Akteuren zugänglichen Wirkmittel verändert. Besonders in den 1990er-Jahren kam es zu einer starken Proliferation von Kleinwaffen. Generell sind konventionelle Waffen, auch mit zunehmender Reichweite und Wirkkraft, heute längst nicht mehr nur Staaten zugänglich.[244] Weiterhin sind mit dem Aufkommen neuer Handlungsräume wie dem Cyberspace neue Möglichkeiten der Schädigung entstanden, die noch wesentlich einfacher zugänglich sind, als dies beispielsweise bei konventionellen Waffen der Fall ist.

Heute besitzen viele NSA die Möglichkeit, sich durch Gewaltanwendung Gehör zu verschaffen. Insbesondere TKN haben bedeutende Fähigkeiten entwickelt. Aber auch für andere NSA sind Wirkmittel heute einfacher zugänglich. Eine besondere Rolle spielen dabei PMSF, die heute selbst komplexe Leistungen, also nicht allein Wirkmittel, sondern auch Personal und Expertise, zeitnah und bedarfsgerecht anbieten.[245]

Gesellschaftlicher Wandel

Im Bereich des gesellschaftlichen Wandels sind eine zunehmend grenzüberschreitende Vernetzung gesellschaftlicher Gruppen, ein

kontinuierlicher Wertewandel und Tendenzen gesellschaftlicher Radikalisierung zu beachten. Diese Entwicklungen haben NSA erlaubt, ihren Handlungsraum und ihre Netzwerke auszudehnen sowie neu entstandene Themenfelder als legitime Akteure zu besetzen.

(4) Die *transnationale Vernetzung*[246] wurde nicht nur durch Entwicklungen Transport- und Kommunikationsmitteln, sondern ebenso durch verschiedene Formen von Migration vorangetrieben. Eine steigende Migration gut ausgebildeter Arbeitskräfte, die besonders zwischen wirtschaftlich starken Ländern auftritt, hat beispielsweise zum Entstehen globaler Netzwerke im Bereich der internationalen Wirtschaft geführt.[247] Ähnliche Tendenzen sind heute auch im Bereich der Zivilgesellschaft zu erkennen.

Sowohl TNU als auch NGOs ermöglichten diese neuen Netzwerke, kompetentes, gut vernetztes und daher auch einflussreiches Personal zu gewinnen und so ihre eigenen Handlungsressourcen auszubauen.

Migrationsbewegungen zwischen wirtschaftlich unterschiedlich entwickelten Regionen führten zur Entstehung gut vernetzter Diasporagemeinschaften.[248] In vielen Fällen pflegen solche Gemeinschaften ein friedliches Mit- und Beieinander mit den Gesellschaften der Länder, in denen sie sich niedergelassen haben. Gleichzeitig boten sie aber auch TKN die Möglichkeit, sich transnational zu vernetzen, da diese Akteure oft nach ähnlichen, zum Beispiel ethnischen, Mustern strukturiert sind. Ein Beispiel hierfür ist die albanische Mafia.

(5) Der *Wandel gesellschaftlicher Werte* hat Folgen für die Politikfelder, die von einer Gesellschaft als relevant erachtet werden und für die politischen Akteure, mit denen sich Menschen identifizieren.

Besonders seit dem Ende des Kalten Krieges ist es zu einer starken Ausbreitung von Werten gekommen, die historisch zumeist mit der Moderne, geografisch wiederum mit westlichen Industriestaaten verbunden werden: die Idee universeller Menschenrechte, demokratische Werte, die Idee eines auf Konsum und Privatisierung aufbauenden Wirtschaftssystems (*Washington Consensus*).[249] Hiermit einher gingen ein steigender Grad an Individualisierung sowie der Anspruch des Bürgers an der Konsumgesellschaft zu partizipieren. Bereits seit den 1970er-Jahren haben sich vor allem in westlichen Industriestaaten darüber hinaus post-materieller oder spätmoderne Werte, insbesondere der Umweltschutz, herausgebildet.[250] Der Wertewandel schlägt sich auch in der Entwicklung neuer politischer Partizipations- und Identifikationsformen nieder.[251]

Aufgrund dieser Entwicklungen sind wichtige neue politische Handlungsfelder entstanden, die besonders Internetaktivisten und NGOs zugutekommen, da solche Akteure die entsprechenden Themen meist direkter vertreten können als Staaten. Sie sind daher für viele Menschen zu einer ernsthaften alternativen Ausdrucksform politischen Engagements geworden.[252] NGOs haben dabei neben dem Gewinn potenzieller Mitstreiter auch durch steigende finanzielle Zuwendungen profitiert.

(6) Der letzte Aspekt des gesellschaftlichen Wandels ist die *Radikalisierung*. Besonders in den 1990er-Jahren wurde viel über einen globalen „Kampf der Kulturen“[253] oder das Duell „Dschihad vs. *McWorld*“[254] diskutiert. Auch wenn sich solche Thesen nur bedingt bestätigt haben, so sind in vielen Bereichen Radikalisierungstendenzen zu erkennen. Dies gilt für Teile religiöser Gemeinschaften ebenso wie im westlichen Kontext für Globalisierungsgegner oder sogar Umweltschützer.

Radikalisierungstendenzen haben insbesondere zusammen mit der höheren Verfügbarkeit von Wirkmitteln an Bedeutung gewonnen. Radikalisierte Islamisten waren so beispielsweise in der Lage, am 11. September 2001 das *World Trade Center* zum Einsturz zu bringen und das *Pentagon* stark zu beschädigen.

Begrenzte Staatlichkeit

Die dritte Kategorie von Treibern lässt sich unter dem in Kapitel 1 eingeführten Begriff der begrenzten von Staatlichkeit fassen. Zwei Aspekte müssen hier beachtet werden: Die freiwillige Kompetenzabgabe des Staates an NSA sowie die wachsende Lücke zwischen globalen politischen Herausforderungen und staatlichen Lösungsansätzen. Diese Aspekte haben zu einer steigenden Legitimität von NSA beigetragen. Sie haben aber auch dafür gesorgt, dass NSA zunehmend staatlichen Regulierungen und staatlicher Rechtsprechung entgehen konnten.

(7) Über die letzten Jahrzehnte hat der Staat, oft bewusst und gewollt, Kompetenzen an andere Akteure – sei es an internationale Organisationen oder NSA – abgegeben.[255] Im Zuge von Privatisierungsbemühungen wurde zum Beispiel die Bereitstellung von Infrastrukturen an Unternehmen übergeben. Getrieben wurde dies nicht zuletzt durch den Wertewandel im Zuge des *Washington Consensus*.

PMSF haben durch die Nachfrage des Staates nach spezifischen Dienstleistungen an Bedeutung gewonnen. Auch NGOs haben von der Kompetenzabgabe des Staates profitiert, weil Staaten sich auf deren Leistungen, beispielsweise die Bereitstellung von Informationen, Daten und Expertise in Bereichen wie der Entwicklungs- und Umweltpolitik, eingelassen haben.

(8) Durch die wachsende *Lücke zwischen globalen politischen Herausforderungen und staatlichen Lösungsansätzen* (*Governance*-Lücke) verliert der Staat hingegen unfreiwillig an Einfluss. Symptomatisch für die wachsende *Governance*-Lücke sind Umweltphänomene wie das Ozonloch und besonders der Klimawandel.[256] Es handelt sich um Herausforderungen, die nicht auf das Gebiet eines Nationalstaates zu begrenzen sind und somit die Rechtsprechungs- und Handlungskompetenzen einzelner Staaten überschreiten.

Um die Lücke zu schließen, wurden und werden Problemlösungen im Bereich *global governance*, das heißt dem Regieren jenseits des Nationalstaates,[257] gesucht. In der Praxis ste-

hen entsprechende Bemühungen jedoch zumeist vor dem Problem, sehr unterschiedliche staatliche Interessen vereinbaren zu müssen.

NSA treten in verschiedener Form an der Schnittstelle zwischen globalen Herausforderungen und nationaler Politik auf. NGOs gewinnen zum Beispiel Einfluss dadurch, dass sie aktiv am Regieren jenseits des Nationalstaates mitwirken. Andere NSA nutzen die Lücke hingegen für ihr eigenes Handel aus: TNU machten sich den globalen Standortwettbewerb zunutze, um optimale Investitionsbedingungen zu erreichen. Für TKN wiederum wurde es einfacher, der Strafverfolgung zu entgehen.

Endnoten

[1] (Geis 2006: 11).

[2] Das Hauptaugenmerk in dieser *Future Study* wird auf *transnationalen* nichtstaatlichen Akteuren liegen. Dennoch sollen diese, aus Gründen der Lesbarkeit, nicht mit TNSA sondern mit NSA abgekürzt werden.

[3] BMVg (2006, 2011); Europäischer Rat (2003, 2008); Vereinigte Staaten von Amerika (2002, 2006, 2010); NATO (2010).

[4] Rosenau (1990: 249–251).

[5] Beide dieser Begriffe legen nahe, dass der Staat die Souveränität über Konflikte verliert. Ulrich Beck (2005) verwendet den Begriff des postnationalen Konflikts um aufzuzeigen, wie militärische Einsätze nicht mehr zwangsweise durch Staatsmänner und nicht mehr nur aufgrund nationaler Interessen geführt werden, sondern immer mehr auf Grundlage globaler Normen – allen voran den Menschenrechten – und auf Wunsch, beziehungsweise Druck der eigenen Bevölkerung. Weller und Bösch (2011: 2) wiederum definieren transnationale Konflikte als solche Konflikte, bei denen es sich „um grenzüberschreitende Konfliktkonstellationen handelt und mindestens eine der Konfliktparteien ein nichtstaatlicher Akteur ist." Diese Kategorie umfasst sowohl die hier betrachteten nichtstaatlichen Konflikte als auch Konflikte zwischen NSA und Staaten. Letztere sind in der sicherheitspolitischen Analyse bereits weitgehend als Themenfeld etabliert. Um ein Abgleiten in diese wichtige, aber weitgehend bekannte Problematik zu vermeiden und den Fokus dieser *Future Study* auf ein tatsächlich neues Phänomen zu legen, wird im Folgenden der Begriff *nichtstaatliche Konflikte* verwendet. Auch dieser Begriff ist in gewisser Weise eine rhetorische Vereinfachung. Genauer als das hier verwendete Attribut „nichtstaatlich" würde das von Rosenau (1990) verwendete „nichtsouverän" das Besondere dieser Konflikte beschreiben. Während „nichtstaatlich" lediglich hervorhebt, *dass* die in dieser *Future Study* betrachteten Konflikte etwas anderes sind als staatliche Konflikte, beschreibt „nichtsouverän" einen primären Grund dafür, *warum* sie anders sind: Anders als Staaten sind NSA keine souveränen Akteure im Sinne des Völkerrechts. Sie genießen dementsprechend weder die Rechte der Souveränität, wie beispielsweise eine Vollmitgliedschaft bei den Vereinten Nationen. Andererseits sind sie jedoch ebenso wenig ohne weiteres durch internationale Verträge und Konventionen gebunden, denen souveräne Staaten unterliegen.

[6] Schneckener (2006a).

[7] Williams (2008).

[8] Hierunter insbesondere solche, die ihr Hauptaugenmerk auf komplexe Akteursnetzwerke in der Sicherheitspolitik oder die *security governance* legen. *Governance* ist als Regieren jenseits des Nationalstaates zu verstehen (vgl. Zürn 1998). Mit *security governance* ist das Regieren jenseits des Nationalstaates im Politikbereich Sicherheit gemeint. Zum Thema *security governance* siehe Krahmann (2003, 2005). Zu sicherheitsgefährdenden Netzwerken siehe Arquilla und Ronfeldt (2001); Eilstrup-Sangiovanni und Jones (2008) sowie Raab und Milward (2003). Zu sicherheitsproduzierenden Netzwerken siehe Dupont (2004).

[9] In der Netzwerkforschung thematisiert z.B. Gerlach (2001) Konflikte von radikalen Umweltgruppen und Kapitalismusgegnern mit TNU und internationalen Banken. In der Forschung zur Weltgesellschaft beschäftigen sich Herkenrath und Bornschier (2006) mit dem Konflikt zwischen TNU und NGOs im Konflikt um ein Investitionsregime. Siehe zur Weltgesellschaft auch Albert und Stetter (2006), Bonacker (2007), Bonacker und Weller (2006a, 2006b), Take (2006) sowie Weller und Bösch (2011).

[10] Chojnacki (2006: 60); s.a. Chojnacki (2004); Hansen (2011); Lemke (2008); Schneckener (2006b).

[11] Kaldor (1999), Münkler (2002). Neue Kriege können demnach nur unter der Berücksichtigung der Globalisierung verstanden werden. So führe z.B. die Ausbeutung lokaler Rohstoffe dazu, dass sich Konfliktparteien über den Weltmarkt refinanzieren könnten. Auch erleichtere die Globalisierung den Zugang zu Konfliktmitteln, insbesondere Kleinwaffen. Insbesondere TKN und Rebellengruppen hätten Interesse an einem schwachen Staat, um dieses „Geschäftsmodell" aufrechtzuerhalten.

[12] Vgl. DCDC (2010); EDA (2011); EUISS (2006); HCSS (2011); Ministry of Defence of the Netherlands (2010); NATO (2009); NIC (2008, 2010, 2012); USJFCOM (2010).

[13] Vgl. auch Endnote 5 zur Bedeutung von „nichtstaatlich" und „nichtsouverän".

[14] Die originale Definition lautet: "[A] political conflict is a positional difference, regarding values relevant to a society (the conflict items), between at least two decisive and directly involved actors, which is being carried out using observable and interrelated conflict measures that lie outside established regulatory procedures and threaten core state functions, the international order or hold out the prospect to do so." (HIIK 2011: 108).

[15] Risse und Lehmkuhl (2007: 15). Der Begriff „Räume begrenzter Staatlichkeit" wurde durch den von der Deutschen Forschungsgemeinschaft finanzierten Sonderforschungsbereich 700 „Governance in Räumen begrenzter Staatlichkeit" geprägt. Die hier gewählte Definition geht jedoch über die vom Sonderforschungsbereich vorgeschlagene Definition hinweg. Während sich der erste der o.g. Formen (Mangel an Können und Fähigkeiten) dessen Arbeiten anschließt, so geht die zweite Form (Mangel an Zuständigkeiten) über diese hinaus.

[16] Vgl. UNEP (2012). Laut Völkerrecht zählen hierzu die Hohe See, die Atmosphäre, die Antarktis und der Weltraum. Zusätzlich wird häufig der Cyberspace als *global common* genannt (z.B. Denmark/Mulvenon 2010). Dieser wird auch in die Betrachtungen dieser *Future Study* miteinbezogen. Zwei andere Räume – die Antarktis und die Atmosphäre – werden hingegen nicht berücksichtigt. Während insbesondere die Atmosphäre (bzw. der Luftraum) auch von sicherheitspolitischer Bedeutung ist, wird er hier aus folgenden Gründen nicht berücksichtigt: Der Luftraum über Staatsgebieten ist Teil des Souveränitätsgebietes dieser Staaten und fällt damit nicht in den Bereich begrenzter Staatlichkeit (Kraska 2010: 57–58). Der Luftraum über der Hohen See wiederum wird in die Definition maritimer Räume mit eingeschlossen. Zwar werden Konflikte im Luftraum hier nicht prioritär abgedeckt. Wichtige Konfliktkonstellationen werden aber im *Future Topic – Geoengineering* (Planungsamt der Bundeswehr 2013) diskutiert.

[17] Vgl. DCDC (2010: 15–18); EDA (2011: 6, 62–68); EUISS (2006: 194, 197); HCSS (2011: 146–147); Ministry of Defence of the Netherlands (2010: 104–107); NATO (2009: 28, 46, 52, 54); NIC (2008: IV, VI, 2010: 10, 2012: 48); USJFCOM (2010: 52–53).

[18] Dort wird auch die Literatur angegeben, auf der der Abschnitt 2.1 basiert. Im Folgenden wird diese Literatur nur dann zitiert, wenn es um die Nennung konkreter Zahlen geht.

[19] Laut Transnationalisierungsindex (TNI) der UNCTAD, welcher Vermögenswerte, Umsatz und Beschäftigte im Heimatland in Relation zu denen der ausländischen Tochtergesellschaften setzt, hat sich der Transnationalisierungsgrad der weltweit 100 größten TNU von 51,5% im Jahre 1995 auf 63,4% im Jahre 2008 erhöht. Dabei sind branchenspezifische Unterschiede zu erkennen: Die Transnationalisierung in den Bereichen Pharma, Telekommunikation, Ernährung und Getränke ist wesentlich höher als jene zum Beispiel in den Bereichen Fahrzeuge, Erdöl und Energie (BpB 2012a, b).

[20] WIR (2011: 24).

[21] So bestand beispielsweise das Budget der Nothilfe- und Entwicklungsorganisation Oxfam im Geschäftsjahr 2010–2011 zu einem Viertel aus staatlichen Mitteln (vorwiegend aus dem Vereinigten Königreich). Weitere 11,3% der Gesamteinnahmen kamen von supranationalen Institutionen wie der Europäischen Union und den VN (Oxfam 2012: 42).

[22] Hansen (2011: 2).

[23] Isenberg (2009: 13).

[24] Sipri (2012). Diese Zahlen bilden aber nur einen Teil der realen Ausgaben ab, da sie sich nur auf spezialisierte Firmen beziehen und z.B. Subunternehmen von Rüstungsfirmen und deren Gewinn im Service Bereich nicht einbeziehen. So hat etwa allein *BAE Systems* 48% des Umsatzes, also 15,8 Mrd. US-Dollar, im Services-Markt erwirtschaftet.

[25] Insbesondere aus staatlicher Sicht ergeben sich weitere Kritikpunkte an PMSF in den Bereichen Kosteneffizienz, Rekrutierung von Fachpersonal, demokratische Legitimation, Vertragstreue und Erstellung von Lagebildern im Einsatzraum (vgl. Anl. A).

[26] Die Ausführungen dieses Abschnittes basieren grundlegend auf zwei Arten von Quellen: Erstens der Anl. B und der darin zitierten Literatur. Zweitens einer globalen Trendlandschaft, das heißt einer systematischen Auswertung zentraler Dokumente der internationalen sicherheitspolitischen Zukunftsforschung hinsichtlich der wichtigsten Trends. Für eine Nennung dieser Dokumente vgl. Fn. 17.

[27] NIC (2012:19).

[28] Eine darüber hinaus zukünftig wachsende Gefahr wird nach nahezu einhelliger Meinung der wichtigsten *Foresight*-Dokumente von der möglichen Verwendung von Massenvernichtungswaffen durch NSA ausgehen.

[29] Andere Faktoren sprechen hingegen gegen einen weitreichenden Einfluss einzelner Staaten auf PMSF. Wenn PMSF beispielsweise auch im Bereich sicherheitspolitischer Analyse zurate gezogen werden, besteht die Gefahr, dass eben diese Analysen den Einsatz von PMSF unverzichtbar und damit unumkehrbar erscheinen lassen. Weiterhin könnten PMSF verstärkt nach nichtstaatlichen Kunden suchen, sollten weniger staatliche Aufträge an sie vergeben werden.

[30] Vgl. hierzu insbesondere die Arbeiten zur „Weltrisikogesellschaft“ (Beck 2007).

[31] Zürn et al. (2007).

[32] Hierdurch könnte es auch verstärkt innerhalb von Akteursgruppen zu Konfliktpotenzialen kommen. Sollten sich beispielsweise gleichzeitig zur Entwicklung kleiner und gegebenenfalls radikaler NGOs verstärkt basisdemokratische Bewegungen im Bereich der Massen-NGOs ausprägen, würden diametral entgegengesetzte NGO-Modelle entstehen, die miteinander in Konkurrenz und gegebenenfalls auch in Konflikt geraten könnten.

[33] Planungsamt der Bundeswehr (2012: 127); Schneckener (2007: 1). Abhängig vom konkreten Grad der Leistungserbringung wird zwischen geschwächter, schwacher und fragiler Staatlichkeit unterschieden. Räume fragiler Staatlichkeit müssen dabei nicht zwangsläufig mit ganzen Staatsgebieten deckungsgleich sein. Sie können auch in Form von *failed cities*, wie z.B. Johannesburg und Rio de Janeiro (Greve 2010; Norton 2003), oder einzelnen Stadtbezirken, z.B. den Pariser *Banlieus*, innerhalb grundlegend funktionierender Staaten auftreten (Muccielli 2010).

[34] BMZ (2007: 9–10).

[35] Risse (2012: 9–12).

[36] Insbesondere in Afghanistan haben Warlords in ihren Herrschaftsgebieten die Aufgaben des Staates übernommen (Chojnacki/Branovic 2011). Im Niger-Delta hingegen hat *Shell* mit eigenen Sicherheitskräften und teils gar mit staatlicher Billigung parallele, das Unternehmen begünstigende Ordnungsstrukturen geschaffen (Zimmer 2010). Vgl. für eine Entwicklung von Sicherheitsmärkten durch NSA in Somalia auch Chojnacki et al. (2009).

[37] Börzel und Hönke (2011: 26–28); Risse (2012: 9–24).

[38] Zu TKN und deren Nutzung von Räumen fragiler Staatlichkeit als sichere Rückzugsräume vgl. Rabasa et al. (2007); zu TNU und deren Nutzung solcher Räume zum Umgehen von Umweltregulierungen vgl. Neumayer (2001).

[39] Schneckener (2004: 6–7).

[40] HWWI (2010: 14); Stürmer (2008). Im Kongo haben sich zum Beispiel trotz der angespannten Sicherheitslage eine Vielzahl von Unternehmen angesiedelt, um Kupfer abzubauen (Westerkampf et al. 2010: 12f.).

[41] Lag der Anteil der chinesischen Direktinvestitionen am Gesamtvolumen der ausländischen Direktinvestitionen in Sub-Sahara Afrika 2003 noch bei ca. 1%, so sind diese allein bis 2008 auf 15% gestiegen. Allein ungefähr ein Drittel der Investitionen in Sub-Sahara und Nordafrika entfallen auf den Bereich Ressourcen (IMF 2011: 48–52).

[42] Kappel (2010).

[43] IEA (2012).

[44] So wird etwa der Handel zwischen China und Afrika in den nächsten Jahrzehnten im globalen Vergleich voraussichtlich mit am schnellsten wachsen (PWC 2011: 8).

[45] BMZ (2007: 9); Chojnacki (2006: 60); Debiel et al. (2007: 8–11); KfW (2011: 2); Risse (2012: 7); Stewart und Brown (2010: 8–11).

[46] Vgl. hierzu Aust und Japsers (2006); Global Witness (2005, 2009).

[47] Westerkampf et al. (2010: 14–15).

[48] Vgl. Müller (2004).

[49] So hat allein China bei Verträgen mit dem Kongo Infrastrukturmaßnahmen garantiert in denen 3.500 km Straßen und Bahngleise, 31 Krankenhäuser, 145 Polikliniken, Universitäten und Schulen gebaut werden sollen (Westerkampf et al. 2010: 17).

[50] So lag 1989 die Zahl von Mobilfunkgeräten noch bei 4.000, überstieg im Jahr 2006 die 100-Millionen-Grenze und lag 2010 bereits bei 330 Millionen (GIZ 2010).

[51] Aker und Mbiti (2010: 207–209); Internet World Stats (2011).

[52] Aker und Mbiti (2010).

[53] WBGU (2007).

[54] Insbesondere in Räumen fragiler Staatlichkeit sind Abbaulizenzen und deren Rechtmäßigkeit komplexe Streitfragen, da eine staatlich gelenkte Verwaltung der Ressourcen fehlt. Solche Tendenzen waren beispielsweise schon Ende der 1990er Jahre im Kongo zu erkennen, als vor Ort Unternehmen mit Milizen und andere Unternehmen mit Fraktionen der Armee kooperiert haben (Aust/Jaspers 2006).

[55] Gemessen wird diese von der so genannten normalen Basislinie, d.h. der Niedrigwasserlinie.

[56] Abhängig von der konkreten Fischart gelten Bestände als überfischt, wenn mehr als 40 bis 60% des ursprünglichen Bestandes abgefischt werden und sich daher der Bestand dauerhaft nicht mehr regeneriert (FAO 2011: 345).

[57] Allein bis 2021 wird der globale Fischkonsum um rund 16% steigen (FAO 2012b: 189–192). Treiber dieser Entwicklung sind das globale Bevölkerungswachstum, steigende Einkommen in Schwellenländern und die damit verbundenen Veränderungen der Ernährungsgewohnheiten sowie eine zunehmende Urbanisierung in Küstenregionen.

[58] Es fällt jede Fischerei unter diese Kategorie, wenn der Fang undokumentiert und unreguliert im Sinne der Meldung des gefangenen Fisches zur Registrierung und Einhaltung der Fangquoten ist. Schätzungsweise wird weltweit rund jeder fünfte Fisch illegal gefangen und der illegale Fang beläuft sich jährlichen auf 11–26 Mio. Tonnen (Agnew et al. 2009; WWF 2012).

[59] Dabei dienen oft Entwicklungsländer als Flaggen- und Hafenstaaten. Für die illegalen Fischer sind sie damit nicht nur im übertragenen Sinne *safe havens* vor internationalen Normen (vgl. hierzu Agnew et al. 2009; FAO 2012a).

[60] Sie greift dabei auf ein weltweit eingesetztes, satellitengestütztes System, das *Automatic Identification System* (AIS), zurück, mit dem Kollisionen von Schiffen vermieden werden sollen (WWF 2012).

[61] Letzterer wird zu einer Erwärmung und Versauerung der Weltmeere sowie zu einem weiteren Anstieg des Meeresspiegels führen (Umweltbundesamt 2009).

[62] Tsetsos (2012: 6).

[63] Statista (2012); vgl. auch HWWI (2006, 2009: 33).

[64] Während etwa 2013 von einer Steigerung des globalen BIP von 3,1% ausgegangen wird, prognostizieren Analysten einen Zuwachs des Containerumschlags um 8,3% (MPC 2012).

[65] Humrich und Wolf (2011: 3).

[66] Bowden et al. (2010) und Geopolicity (2011). Für einen Überblick über verschiedene Studien siehe Endler et al. (2012).

[67] Reuters (2011).

[68] 2012 waren laut einer Umfrage von *Price Waterhouse Coopers* unter 100 deutschen Reedereien bereits auf 58% der Schiffe bewaffnete Sicherheitskräfte an Bord, wenn diese in von Piraterie bedrohten Gewässern gefahren sind (PWC 2012).

[69] So hat etwa im April 2012 ein Video für Aufsehen gesorgt, bei dem zu sehen ist, wie Angestellte einer PMSF Piraten erschießen (Spiegel Online 2012).

[70] Emmerson und Stevens (2012); Rodrigue (2004). Aufgrund hoher Investitionssummen und natürlicher Anforderungen für Infrastrukturen im maritimen Raum ist auch zukünftig zwar von einem weiteren Ausbau von Häfen und Umschlagsorten auszugehen, eine Reduzierung ihrer Kritikalität durch Neubauten und Schaffung redundanter Strukturen, die über das generelle Wachstum des Seetransportes hinausgeht, ist aber nicht zu erwarten.

[71] Sechrist (2012: 8).

[72] Tsetsos (2012: 6).

[73] Diese enthalten neben einer hohen Konzentration von Mangan, Eisen, Kupfer oder Cobalt auch Seltene Erden, welche für Photovoltaikanlagen, Computerchips und neue Batterietechnologien benötigt werden. Vgl. hierzu Hein et al. (2010); Wiedicke-Hombach und Reichert (2012).

[74] Die BGR erkundet in diesem Zusammenhang bereits ein deutsches Lizenzgebiet, welches sich im zentralen Nordostpazifik vor der Küste Mexikos befindet (Wiedicke-Hombach und Reichert 2012). Für einen Überblick über den zukünftigen Energiebedarf siehe Exxon (2012), und für eine Studie in Bezug auf den in Zukunft erwartbaren Bedarf an Kupfer siehe Fraunhofer (2010).

[75] Mair (2010: 7).

[76] Dem *International Maritime Bureau* der *International Chamber of Commerce* folgend gab es in den Jahren 2009 bis 2011 jeweils mehr als 400 Piratenangriffe (ICC-International Maritime Bureau 2012a), im Jahre 2012 waren es 233 (ICC-International Maritime Bureau 2012b).

[77] Ein Beispiel für Letzteres bietet die *Free Aceh*-Bewegung aus Indonesien, die im Jahr 2001 nicht nur für Lösegeld Handelsschiffe überfallen, sondern explizit versucht hat, sich als souveräne Macht über das Seegebiet zu konstituieren, mit dem Anspruch Schiffspassagen zu genehmigen und ihr eigenes politisches Handeln zu finanzieren (Erhart et al. 2010: 27).

[78] Wirminghaus (2013).

[79] Homeland Security News Wire (2010).

[80] Dies ist insbesondere auch daher plausibel, da jenseits der Verfügbarkeit der Waffensysteme auch zukünftig Zonen schwacher bis fragiler Staatlichkeit als sichere Häfen nutzbar sein können.

[81] Zwar könnten zeitnah alternative Routen oder Häfen genutzt werden, allerding wären bei längeren Wegstrecken erhöhte Transportkosten, ein logistischer Mehraufwand die Folgen und selbst kurzfristige Versorgungsengpässe in Extremfällen nicht auszuschließen.

[82] Die volle Bezeichnung dieses Vertrages lautet Vertrag über die Grundsätze zur Regelung der Aktivitäten von Staaten zur Erforschung und Nutzung des Weltraumes einschließlich des Mondes und anderer Himmelskörper (UNOOSA 1967).

[83] Auswärtiges Amt (2011).

[84] Als Allmende werden die so genannten Allgemeingüter bezeichnet, oder Güter gemeinschaftlichen Eigentums, die rechtlich allen Menschen der Erde gehören.

[85] Diese Gruppen wären, wenngleich auch nur indirekt, durch einen anderen Vertrag, den Mondvertrag, eindeutiger abgedeckt worden (Art. 11). Da diesen Vertrag jedoch bisher nur 13 Staaten ratifiziert haben – darunter keine bedeutende Raumfahrtnation – gilt er als gescheitert. Darüber hinaus sind NSA im Weltraum nicht direkt durch das Völkerrecht gebunden. Eine solche Bindung müsste über den Umweg der Staaten, also die nationale Gesetzgebung erfolgen. Vgl. Auswärtiges Amt (2011) und UNOOSA (1979).

[86] Der 1959 eingerichtete Weltraumausschuss (COPUOS) der VN hat daher Richtlinien zur Vermeidung von Weltraumschrott erarbeitet, die im Jahr 2007 von der Generalversammlung verabschiedet wurden. Diese sind jedoch rechtlich nicht verbindlich (UN 2009; UNOOSA 2007).

[87] Hierzu gehören neben dem Mondvertrag, das Weltraumrettungsübereinkommen (1968), das Weltraumhaftungsübereinkommen (1972) und das Weltraumregistrierungsübereinkommen (1975). Vgl. Auswärtiges Amt (2011).

[88] Sterner (2010: 107).

[89] Hierzu gehören ein 2008 erstellter und 2010 überarbeiteter EU-Entwurf eines Verhaltenskodex für Weltraumaktivitäten (EU 2008) und die Initiative der EU für einen internationalen Verhaltenskodex auch unter Berücksichtigung nichtstaatlicher Akteure (EU 2012), sowie ein Entwurf, den das US-amerikanische *Stimson Center* in Zusammenarbeit mit mehreren nichtstaatlichen Partnern unterschiedlicher Nationen erstellt hat (Stimson Center 2007).

[90] Mutschler (2012: 3).

[91] Robinson (2012).

[92] „Während der Weltraumvertrag (1967) zwar das Stationieren von Atomwaffen und anderen Massenvernichtungswaffen im Weltraum verbietet, gibt es kein spezifisches Verbot der Stationierung und Nutzung konventioneller Waffen im Weltraum. Daher wurden bei den Vereinten Nationen wiederholt Verhandlungen über weitere Vereinbarungen eingefordert, die ein Wettrüsten im Weltraum verhindern sollen.“ (PNND 2007) Zwar wäre eine Militarisierung wahrscheinlich eine staatliche Angelegenheit, aber auch für NSA und ihre Weltraumaktivitäten könnte eine solche Entwicklung Wirkung entfalten. In jedem Fall würden sich mit mehr militärischer Infrastruktur im Weltraum das Platzproblem und gegebenenfalls entsprechende Konkurrenzdynamiken verschärfen. Weiterhin könnten sich die Wirkmittel von NSA sogar noch erhöhen, sollte es ihnen gelingen, militärische Infrastrukturen beispielsweise über den Cyberspace unter ihre Kontrolle zu bringen.

[93] Dickow (2010); Mutschler (2012).

[94] Mutschler (2012: 1).

[95] Seit über zehn Jahren fliegen vereinzelt Privatpersonen ins All. Die erste Privatperson besuchte bereits 2001die ISS. Das Ticket kostete 20 Mio. US-Dollar (Zeit Online 2011).

[96] Weiterhin arbeitet EADS Astrium an einem Raumschiff, welches einen Piloten und vier Passagiere für 90-minütige Flüge in 100 km Höhe bringen kann. Dabei kalkuliert der Konzern

mit Kosten von derzeit 150.000 bis 200.000 Euro pro Ticket und einem Markt von jährlich 15.000 Passagieren.

[97] Das *Keck Institute for Space Studies* (2011) untersuchte das Potenzial, die Durchführbarkeit und Erfordernisse von *asteroid mining* in einer Machbarkeitsstudie. Im *Advanced Space Transportation Program* der NASA werden ebenfalls fortgeschrittene Raumfahrtsysteme und Antriebstechnologien entwickelt, die u.a. für *asteroid mining* genutzt werden könnten (NASA 2003). Ein weiteres Programm der NASA und der Firma *Caterpillar* beschäftigt sich mit zukünftigen Bergbau-Technologien, die auf dem Erdmond eingesetzt werden könnten (NASA 2009).

[98] Miller (2012). So hängt die Wirtschaftlichkeit sowohl von der Art der Rohstoffe und ihrer Seltenheit als auch vom technologischen Fortschritt in der Raumfahrt sowie der Entwicklung von Nachfrage und Reserven auf der Erde ab.

[99] Financial Times Deutschland (2010).

[100] Mutschler (2012: 2).

[101] NASA (2012).

[102] Deutscher Bundestag (2009); New York Times (2009).

[103] Die Menge der Schrottteile von 1 cm Größe in seiner Flughöhe von 850 km stieg nach Berechnungen der TU Braunschweig um 28% (TU Braunschweig 2007). Andere Schätzungen gehen von einer Erhöhung des Weltraumschrotts um insgesamt rund 10% im erdnahen Orbit aus (Zissis 2007).

[104] Welt Online (2012).

[105] Die Europäer sind bisher in der Weltraumlage stark auf Informationen aus den USA angewiesen, die diese Informationen jedoch nur begrenzt teilen. Ein umfassendes Weltraumaufklärungssystem existiert derzeit weder auf nationaler noch auf europäischer Ebene. Jedoch wurde 2008 im Rahmen der Europäischen Weltraumbehörde (*European Space Agency*, ESA) mit der Vorbereitung des für 2012–2019 geplanten Aufbaus eines eigenständigen Weltraumlagesystems begonnen (Dürr 2012). Deutschland hat außerdem mit dem Aufbau des Weltraumlagezentrums in Kalkar einen wichtigen institutionellen Schritt gemacht, um dazu beizutragen, erdnahe Objekte systematisch zu überwachen, aufzuklären und den Schutz weltraumgestützter Systeme, unter anderem der Bundeswehr (SATCOMBw-2 und SAR-Lupe), zu gewährleisten (Weltraumlagezentrum 2012).

[106] US-DoD (2011: 1).

[107] Mutschler (2012: 4).

[108] Sterner (2010: 117).

[109] Grego (2012: 6); Sterner (2010: 117).

[110] Remuß (2009: 5); Sterner (2010: 117).

[111] *Jamming* bezeichnet das gezielte Aussenden von Störsignalen, um den Empfang eines ursprünglichen Signals schwierig oder unmöglich zu machen. Das *jamming* kann auf derselben oder auf benachbarten Frequenzen des ursprünglichen Signals erfolgen. Unter *spoofing* versteht man das Aussenden von Störsignalen, welche ein ursprüngliches Signal auf derselben Frequenz imitieren beziehungsweise überlagern. Ziel hierbei ist es, den Empfang von Signalen nicht nur zu stören, wie beim *jamming*, sondern den Empfänger mit formal gültigen, aber falschen Daten zu täuschen. *Spoofing* ist technisch wesentlich aufwändiger als *jamming* jedoch ebenfalls nicht besonders kostenintensiv.

[112] BBC (2012).

[113] Danger Room (2011).

[114] Daly (2007).

[115] Chan (2005).

[116] Der Ressourcenabbau auf Asteroiden könnte sogar Vorteile gegenüber dem auf der Erde haben, da so für den Menschen und andere Lebewesen lebenswichtige Ökosysteme geschont werden würden. Motivationen von NGOs wären daher eher sehr abstrakter Natur und könnten sich beispielsweise darauf richten, dem Gesellschaftsmodell moderner Staaten und der damit verbundenen Ausbeutung gemeinschaftlicher Räume Einhalt zu gebieten.

[117] Remuß (2009).

[118] BMI (2011: 14).

[119] Der Begriff Cyberspace wurde ursprünglich geprägt vom Science Fiction Autor William Gibson (Thill 2009). Zu der physischen Ebene zählt die Netzinfrastruktur mit ihren Glasfaserkabeln und Endgeräten. Die logische Ebene besteht zum Beispiel aus der von Endgeräten verwendeten Software und verwendeten Internet-Protokollen (Benkler 2000: 562).

[120] Diese Entwicklung begann mit dem Aufbau militärisch-universitärer Computernetzwerken in den 1960er- und 1970er-Jahren – allen voran des *Advanced Research Projects Agency Network* (ARPANET) in den USA. Der Begriff Internet wurde erstmalig 1974 im Zusammenhang mit Bestrebungen gebraucht, diese Netze in einem „Netz der Netze" zusammenzufügen. Das Internet liegt dem Cyberspace als „universelles und öffentlich zugängliches Verbindungs- und Transportnetz" zugrunde, „welches [im Cyberspace] durch beliebige andere Datennetze ergänzt und erweitert werden kann" (BMI 2011: 14). Erst in den letzten zwei Dekaden hat sich aus diesen Bestrebungen kontinuierlich der heutige Cyberspace entwickelt. Die Entwicklung ging dabei auf allen Ebenen voran. So werden Endgeräte kontinuierlich leistungsstärker und mobiler. Auf der logischen Ebene kommt es zur Umstellung von Internet-Protokollen von der Version 4 (IPv4) auf die Version 6 (IPv6) und die inhaltliche Ebene verändert sich zum Beispiel durch die immer stärkere Verbreitung sozialer Medien wie *Facebook* und *Twitter* und der dadurch gesteigerten Aktivität und Teilhabe von immer mehr Individuen.

[121] Kleinwächter (2006).

[122] S.a. Denmark und Mulvenon 2010 (2010: 150).

[123] Generell gilt, dass die Infrastruktur des Cyberspace zum größten Teil vom privaten Sektor besessen und kontrolliert wird (Denmark/Mulvenon 2010: 150).

[124] *Anonymous* ist ein Beispiel dafür, dass der Cyberspace die Entstehung von Gruppen über realweltliche Interaktionskontexte, nationalstaatliche Grenzen und auch Kulturen hinweg erleichtert, die ohne diesen Raum nie zusammengefunden hätten (vgl. auch Sassen 2011). Der Anlass solcher Gruppenbildung kann vielfältig sein und sowohl kommerziellen als auch gesellschaftspolitischen Interessen folgen.

[125] Zwar kann ein Staat den Zugang zum Cyberspace durch nationale Gesetzgebung beeinflussen. Sehr unterschiedliche Vorgehensweisen sind beispielsweise in den USA und China zu beobachten (Denmark/Mulvenon 2010: 151). Auch können Staaten Taten, die im Internet begangen werden, in vielen Fällen strafrechtlich verfolgen. Dies ist beispielsweise im Zusammenhang mit einer Reihe von DDoS-Attacken passiert, die *Anonymous* in den letzten Jahren durchgeführt hat (z.B. Reißmann et al. 2012: 152–156). Dennoch überfordern die für den Raum typischen Schwierigkeiten der Attribution von Handlungen sowie der virtuelle und transnationale Charakter der Handlungs- und Problemzusammenhänge in vielen Fällen die Rechtssetzungskompetenzen von Staaten. Zusätzlich zeigen sich zwischen Staaten Interessensgegensätze hinsichtlich der Vorstellungen, den Cyberspace weiter zu regulieren; nicht nur in den bereits genannten Foren (Kleinwächter 2010). Auch bei anderen Gelegenheiten, wie dem auf der Münchener Sicherheitskonferenz 2011 angestoßenen „Londoner Prozess", ergeben sich ähnliche Schwierigkeiten (Kleinwächter 2012). Darüber hinaus gibt es eine starke Opposition sowohl gesellschaftlicher Kräfte, als auch von NSA im Cyberspace gegenüber staatlichen Regulierungsversuchen. Dies wurde besonders im Zusammenhang mit der Unterzeichnung und Ratifizierung des *Anti-Counterfeiting Trade Agreement* (ACTA) deutlich,

das unter anderem für einen besseren Schutz von Urheberrechten im Internet sorgen sollte. Europaweite Proteste und Internetaktionen führten letztendlich dazu, dass das Abkommen in vielen Ländern des Kontinents nicht ratifiziert wurde.

[126] Kleinwächter (2010).

[127] Denmark/Mulvenon (2010: 150, eigene Übersetzung). In einer ausführlicheren Beschreibung vergleicht das CNAS den Cyberspace sogar mit dem Wilden Westen: „In many respects, governance in cyberspace resembles the American Wild West of the 1870s and 1880s, with limited governmental authority and engagement. Users – whether organizations or individuals – must typically provide for their own security. Much of cyberspace operates outside the strict controls of any hierarchical organizations. No one individual or entity is in charge. Internet traffic is routed through peer arrangements between Internet Service Providers, without central authority or control. The resolution of domain names fundamental to web browsing and e-mail is strictly based on an agreed set of protocols, loosely coordinated by a nongovernmental organization referred to as the Internet Corporation for Assigned Names and Numbers (ICANN)" (Denmark/Mulvenon 2010: 149).

[128] USAF (2012: 17); Das Unternehmen *Cisco* wiederum erwartet in den nächsten fünf Jahren eine Verdreifachung des globalen Datentransfers (Cisco 2012).

[129] Cisco (2012); vgl. hierzu wiederum auch Abb. 3.6, Downloads mobiler *Apps*.

[130] USAF (2012:11). Besonders in Asien wird die Nutzung des Internets stark ansteigen (Cisco 2012).

[131] Dieses Phänomen manifestiert sich sowohl innerstaatlich als auch auf internationaler Ebene und könnte unter anderem auf sozioökonomische Unterschiede zurückgeführt werden (Ruggie/Dossal 2000; Zickuhr und Smith 2012).

[132] Das CNAS (Denmark/Mulvenon 2010: 139) schreibt hierzu: "the cyber commons enables private and public institutions to provide essential services such as energy, food and water. Banks and asset traders use the Internet to shift billions of dollars within seconds. Modern militaries – especially the U.S. military – employ the cyber commons as a key enabler of military operations, using commercial and private networks for everything from command and control to logistics support." Es fährt fort: "the increasing use of the Internet and other aspects of the cyber commons by advanced states to manage domestic infrastructure creates new strategic vulnerabilities that adversaries cannot ignore" (Denmark/Mulvenon 2010: 148).

[133] Cisco (2012). Die USAF weist daraufhin, dass weitere Gefahren entstehen könnten, wenn insbesondere alternden Gesellschaften immer stärker darauf drängen, in möglichst viele Lebensbereichen menschliche Arbeit durch Roboter zu ersetzen – zum Beispiel im Gesundheitswesen könnte dies der Fall sein (USAF 2012: 9).

[134] Schätzungen zufolge entstanden allein in Deutschland im Jahren 2011 über 70 Mio. Euro Schaden durch Internetkriminalität (BKA 2011: 8), in den USA waren es im gleichen Zeitraum rund 485 Mio. US-Dollar (ICCC 2011: 10). Diese Zahlen sind jedoch mit Vorsicht zu behandeln. Sie werden dem Problem unter Umständen nicht gerecht, denn viele Tatbestände bleiben unentdeckt oder werden nicht gemeldet. Insbesondere Unternehmen haben ein Interesse daran, ihre Kunden nicht durch das Offenlegen von Sicherheitslecks im Cyberspace zu verunsichern.

[135] Cyber-Kriminelle machen sich bei ihren Aktivitäten häufig die Regulierungsschwäche von Staaten zunutze. So werden ganz gezielt jene *top-level-domains* (TLD) – das heißt Bezeichnungen wie „.de" oder „.com" – für kriminelle Aktivitäten missbraucht, bei denen Kriminelle mit möglichst wenig Regulierung konfrontiert sind. In den letzten Jahren war dies besonders bei Kameruns TLD „.cm" der Fall (McAfee 2009b).

[136] Denmark/Mulvenon (2010: 139).

[137] Zum Folgenden vgl. Reißmann et al. (2012: 132–149).

[138] Es blieb dabei nicht beim Einsatz von DDoS-Attacken. So hackten sich Aktivisten in das System des portugiesischen Branchenverbandes und entwendeten und veröffentlichten interne E-Mails. Insgesamt wurden in der *Operation Payback* über 7 Wochen hinweg mehr als 20 Ziele für insgesamt mehr als 500 Stunden außer Gefecht gesetzt (Reißmann 2012: 132).

[139] Reißmann (2012: 135–138).

[140] Reißmann (2012: 149).

[141] Zum Begriff der Ökosysteme siehe Dobusch et al. (2012).

[142] LFM (2012).

[143] Unter der Herausbildung einer Internetwährung ist dabei nicht lediglich ein Virtualisierung des Zahlungsverkehrs mit bestehenden Währungen zu verstehen, wie sie heute schon durch das Online-Banking oder Dienste wie *PayPal* geleistet wird. Es handelt sich dabei, wie im Falle *Bitcoin*, um eigenständige, geschlossene Währungssysteme mit flexiblen Wechselkursen zu anderen Währungen, wie dem US-Dollar oder dem Euro. Die Umsätze solcher Währungen sind schwer zu beziffern, betragen allerdings schon heute schätzungsweise mehrere Milliarden Euro jährlich (Menn 2011). Die Etablierung entsprechender Währungen könnte weitreichende, teils problematische Folgen haben. Sie bieten unter anderem TKN Möglichkeiten zur Geldwäsche. Langfristig gedacht, könnten sie unter Umständen sogar zur Destabilisierung nationaler Geldmärkte führen (Menn 2011).

[144] Die Abschaffung eben dieses Wahlrechts, z.B. über Änderungen im Bereich des Datenschutzes, im Falle von *Facebook* (Heise Online 2012), muss nicht das generelle Aus für solche Abstimmungsmechanismen bedeuten. Vielmehr wurde diese Abschaffung auch mit starker Kritik bedacht und *Facebook* ein eklatantes Demokratiedefizit vorgeworfen (Kreye 2012).

[145] Vgl. Lohr (2012).

[146] Denmark/Mulvenon (2010: 144, 149).

[147] Auf der logischen Ebene werden hingegen schon heute durch NSA vielerlei Regeln festgelegt, vor allem mithilfe der so genannten *requests for comments* (RFCs).

[148] So drohten Unbekannte zum Beispiel gegenüber *eBay*, *Yahoo* und *Amazon* sowie kurz vor wichtigen Sportübertragungen auch gegenüber Online-Wettbüros, deren Internetseiten außer Gefecht zu setzen, sollte nicht ein Schutzgeld bezahlt werden (Rötzer 2004).

[149] BBC (2011). Für eine eingehende Analyse der Bedrohungen kritischer Infrastruktur durch Cyberangriffe vgl. McAfee (2009b).

[150] Vgl. hierzu insbesondere die Arbeit des CNAS (Denmark/Mulvenon 2010: 141). Selbst eine Automatisierung von Verteidigungsmaßnahmen ist nur bedingt erfolgsversprechend und kann sich sogar kontraproduktiv auswirken: „The requirement for rapid response in cyberspace can mean higher levels of automated decisions for states and other entities. […] Unfortunately, cyberspace presents myriad opportunities for adversaries to subvert automated systems and turn them against their operators, or against third parties" (Denmark/Mulvenon 2010: 145).

[151] Schmidt (2011).

[152] Ein plausibles Beispiel ist hier der Einsatz von biotechnologischen Maßnahmen, zum Beispiel im Bereich der Genmanipulation, zur „Vervollkommnung" des Menschen. Während ein solches Projekt von gewissen gesellschaftlichen Akteuren vorangetrieben werden könnte, könnten sich ebenso Gegner formieren und dagegen angehen. Der Cyberspace bietet hier nicht den einzigen, jedoch einen möglichen Aktionsraum.

[153] Ein weiteres Beispiel für Konflikte zwischen NGOs und TKN wäre Folgendes: Eine kleine, radikalisierte NGO – „Die Wächter des Rechts" – nehmen sich zum Ziel, die strafrechtlichen Versäumnisse der Staatenwelt dadurch zu kompensieren, dass sie systematisch im Cyberspace (und ggf. darüber hinaus) die Verfolgung der Organisierten Kriminalität betreiben.

[153] Für Folgendes siehe Reißmann (2012: 172–180).

[154] *Anonymous* griff die Sicherheitsfirma *HBGary* an, weil ein Manager des Unternehmens 2010 erklärt hatte, dass er die Identitäten der wichtigsten *Anonymous*-Aktivisten kenne. Kurz darauf wurde als Antwort auf diese Behauptung die Internetseite des Unternehmens gehackt und zahlreiche Daten entwendet. Neben internen E-Mails und Passwörtern zählten hierzu auch Informationen über Cyber-Offensivkapazitäten, wie beispielsweise Spionageprogramme, die der Öffentlichkeit vorher nicht bekannt gewesen waren (Reißmann 2012: 172–180).

[155] Die Straße von Hormus kann, im Gegensatz etwa zum Suezkanal oder der Strasse von Malakka, nicht auf maritimen Wegen umfahren werden, da sie die einzige „Ausfahrt" aus dem Persischen Golf darstellt. Ihre strategische Bedeutung zeigt sich, bedenkt man, dass nach offiziellen Angaben im Jahr 2011 ca. 17 Mio. Barrel Öl und Ölprodukte durch diese Meerenge transportiert worden sind (US Energy Information Administration 2012).

[156] Sterner (2010: 125–127).

[157] Dabei sind Angriffe „gegen das Internet selbst" zumindest nicht auszuschließen – beispielsweise als Protest jener, die durch den *digital divide* ausgeschlossen sind oder als Aktion radikaler Modernisierungskritiker, die den Cyberspace als Bedrohung für gesellschaftliche Wertesysteme verstehen. Es ist jedoch davon auszugehen, dass die Infrastrukturen des Internets zukünftig durch zunehmende Redundanzen eher Widerstandsfähiger werden, was solche Angriffe erschweren dürfte. Gegebenenfalls erfolgsversprechender, zumindest für eine zeitweise und regional Störung des Internets, wären unter Umständen Angriffe, die sich auf die physische Infrastruktur des Cyberspace richten. Gleichzeitig bieten die Vermehrung von Redundanzen jedoch auch eine erweiterte Grundlage für Angriffe, da zum Beispiel größere Mengen an Rechnern für DDoS-Attacken zusammengeschaltet werden könnten (*botnets*).

[158] Indizien hierfür liefert beispielsweise die Unterwanderung von *Anonymous* durch amerikanische Geheimdienste und die US Bundespolizei (Pilkington 2011).

[159] Die Forderung nach einer Steigerung der Resilienz ist dabei nicht ausschließlich aus der Bedrohung durch nichtstaatliche Konflikte herzuleiten. Vielmehr stellt sie einen breiteren Impetus der heutigen vernetzten Welt dar. Auch viele andere Gegebenheiten – von den Auswirkungen des Klimawandels, über Finanzkrisen bis hin zur terroristischen Bedrohung – verlangen nach einer gesteigerten Resilienz. Vgl. beispielsweise Planungsamt der Bundeswehr (2012).

[160] Tikk (2011).

[161] Ein solcher Mechanismus besteht für zwischenstaatliche Dispute beispielsweise bereits bei der Welthandelsorganisation. Teils beziehen sich diese Streitigkeiten aber auch konkret auf die Beziehungen zwischen TNU, wie beispielsweise zwischen *Airbus* und *Boeing*. Eine zentrale Herausforderung bei der Übertragung bei solchen Mechanismen auf Beziehungen zwischen NSA besteht darin, dass dort andere Interessenskonstellationen vorherrschen. Während Staaten zum Beispiel über konkrete Zölle in Streit geraten können, eint sie zumeist dennoch die Motivation, den Handel möglichst profitabel zu gestalten. Ähnliches gilt auch für TNU. Die Motivationen von NGOs und Internetaktivisten sind jedoch nicht durch Profitmaximierung getrieben. Wenn dementsprechend ein TNU auf eine an Normdurchsetzung interessierte NGO trifft, fehlt das grundlegende Verständnis, dass die beiden Parteien, wie im Falle zwischenstaatlicher Dispute in der Handelspolitik, verbindet.

[162] Das Gesetz verpflichtet diese Unternehmen offenzulegen, ob ihre Produkte mineralische Rohstoffe beinhalten, die aus dem Kongo stammen. Öl- und Gasunternehmen müssen darüber hinaus ihre Zahlungen an Regierungen offenlegen. Die Regelungen treffen rund „90 Prozent der weltweit größten international agierenden Ölfirmen und acht von zehn der weltgrößten Bergbauunternehmen." (Lauster et al. 2010) Das Gesetz soll so mehr Transparenz in den Handel mit Gütern bringen, die in der Abbauregion nicht selten als Konfliktressourcen

fungieren. Zwar sind mit der Umsetzung des Gesetzes auch Probleme verbunden. Dennoch zeigt es, wie NSA in beinahe globalem Maßstab auch ohne internationalen Konsens reguliert werden können.

[163] Nimmt man eine langfristigere Perspektive ein, so wird klar, dass nichtstaatliche Akteure in vielerlei Hinsicht eine wichtige Rolle in der Weltgeschichte gespielt haben. Der Städtebund der Hanse, zum Beispiel, war seit dem zwölften Jahrhundert eine wichtige Macht in Nordeuropa und die *British East India Company* hatte während des 17. und 18. Jahrhunderts großen Einfluss in Südasien. Die Gründung des Roten Kreuzes, als eine der ersten NGOs, wiederum geht auf das 19. Jahrhundert zurück (Spruyt 1994; The Economist 2011). Geschichtlich betrachtet bildete sich die Vormachstellung des Staates in der internationalen Politik erst im Laufe der Jahrhunderte heraus.

[164] Keohane und Nye (1977).

[165] Risse-Kappen (1995).

[166] Für Definitionen siehe UNCTAD, Transnational Corporations Statistics, sowie Rittberger et al. (2010: 239).

[167] Dies gilt beispielsweise für Bemühungen im Bereich Umweltschutz und Sozialstandards, denen auch unter dem Begriff Corporate Social Responsibility eine wachsende Bedeutung beigemessen wird.

[168] WIR (2011: 24).

[169] Fortune Global 500 Liste (2012).

[170] Weltbank (2012).

[171] Eine Studie aus dem Jahr 2000 schließt demnach sogar, dass in ihrem Erscheinungsjahr 51 der 100 weltweit größten Ökonomien Unternehmen waren (Anderson und Cavanagh 2000: 3).

[172] Dabei sind branchenspezifische Unterschiede zu erkennen: Die Transnationalisierung in den Bereichen Pharmazie, Telekommunikation, Ernährung und Getränke ist wesentlich höher als jene zum Beispiel in den Bereichen Fahrzeuge, Erdöl und Energie (BpB 2010).

[173] WIR (2011: 25).

[174] Rittberger et al. (2010: 263f).

[175] Rittberger et al. (2010: 245).

[176] Benner/Witte (2006: 1–7).

[177] Informationsplattform humanrights.ch (2012).

[178] Im Bereich der Umweltstandards wird dies häufig mit dem Begriff „Greenwashing“ in Verbindung gebracht.

[179] Rittberger et al. (2010: 271).

[180] Rittberger et al. (2010: 249).

[181] Benner/Witte (2006: 1–7).

[182] Für weitere Definitionen vgl. Frantz und Martens (2006: 23–30); Gordenker und Weiss (1996: 20); Rittberger et al. (2010: 241). Die Union of International Associations (UIA) hat einen anspruchsvollen Kriterienkatalog für die Definition von NGOs formuliert, vgl. Brunnengräber et al. (2005: 14).

[183] Brunnengräber et al. (2005: 27).

[184] Martens (2002: 29).

[185] Brunnengräber et al. (2005: 12–13).

[186] Lochbihler (2010).

[187] Rittberger et al. (2010: 245).

[188] Rittberger et al. (2010: 245).

[189] So bestand beispielsweise das Budget der Nothilfe- und Entwicklungsorganisation Oxfam im Geschäftsjahr 2010–2011 zu einem Viertel aus staatlichen Mitteln (vorwiegend GBR). Weitere 11,3% der Gesamteinnahmen kamen von supranationalen Institutionen wie der Europäischen Union und den Vereinten Nationen (Oxfam 2012: 42).

[190] Brunnengräber et al. (2005: 16).

[191] Rittberger et al. (2010: 247).

[192] Rittberger et al. (2010: 253).

[193] Für weiterführende Definitionen vgl. Council of Europe (2005: 18); Lampe (2012a); UNODC (2012a).

[194] Brombacher (2010: 22–24); Williams und O´Hayon (2002: 129).

[195] De Groot et al. (2011); Hastings (2009). “Sophisticated” criminal activities involving the production or acquisition of goods that cannot be directly and immediately consumed – for example piracy and drug production – are not viable at the bottom end of the governance spectrum (anarchy). First, criminals need protection from other criminals who may attempt to steal their loot or extort their profits Gambetta (1993). Second, criminals need a basic transport infrastructure and functioning markets to convert loot into consumables. During periods of anarchy (for example during civil conflict) the state cannot provide the security and law enforcement necessary to support market activity” (De Groot et al. 2011: 2).

[196] Williams und O´Hayon (2002: 130).

[197] Für eine detailliertere Darstellung der Ursachen siehe Council of Europe (2005: 22–27); Hansen (2011: 1–2); Williams (1997: 316–320); Williams und O´Hayon (2002: 129–134).

[198] Brombacher (2010: 20); Mair (2010); UNODC (2010: 2).

[199] Hansen (2011: 2).

[200] BKA (2010: 12).

[201] BKA (2010).

[202] UNODC (2011: 28). Dabei ist jedoch die strikte Trennung zwischen illegalen und legalen Märkten insofern irreführend, als TKN teils legale Zweige besitzen, u.a. etwa um ihr Geld zu waschen oder zu re-investieren (Inkster und Comolli 2012: 27–28).

[203] UNODC (2012b); Europol (2011).

[204] UNODC (2012: 6f).

[205] IMBPRC (2012).

[206] Reuters (2011).

[207] vgl. hierzu Brombacher (2010). In einem 2004 erschienenen Artikel bilanziert Makarenko als Ergebnis des Bedeutungsgewinns von TKN „As a result, non-state actors, in the guise of transnational organised crime and terrorism are directly challenging the security of the state – arguably for the first time in history“ (Makarenko 2004: 141).

[208] Farah (2010).

[209] vgl. hierzu Farah (2010); Hansen (2011); Makarenko (2004).

[210] vgl. hierzu Collier (2006); Collier und Hoeffler (1998); Fearon (2004).

[211] Perlo-Freeman und Sköns (2008: 4–7).

[212] UNHCR doc. A/HRC/7/7: 4, zit. nach Berndtsson (2009: 51). Für eine kritische Auseinandersetzung mit der Definition und den Tätigkeitsfeldern von PMSF vgl. Berndtsson (2009: 42–52); und Avant (2005: 17); Deittelhoff und Geis (2012: 140); Heck (2010: Kap. 2); Schreier und Caparini (2005: 23–25, 31–33).

[213] Deittelhoff und Geis (2012: 140).

[214] Vgl. hierzu Singer (2008: 80–87).

[215] So hat die US-amerikanische NASCO zum Ziel „to advocate for raising standards at the federal, state and local level for the licensing of private security firms and the registration, screening and training of security officers increase public awareness of the important role and function of private security" (NASCO 2012).

[216] O´Brien (2000: 60–61.); Logistische Unterstützungsleistungen werden dabei bereits seit den 1960er Jahren von Rüstungskonzernen angeboten (Perlo-Freeman und Sköns 2008: 1).

[217] vgl. hierzu Mandel (2002); Singer (2008: 40).

[218] Für die Ursachen des Aufschwungs vgl. Baker (2011); Berndtsson (2009: 111–136); Heinecken und Motzouris (2011: 78–81); und Singer (2008: 48–72) .

[219] Isenberg (2009: 13).

[220] Sipri (2012). Diese Zahlen bilden aber nur einen Teil der realen Ausgaben ab, da sie sich nur auf spezialisierte Firmen beziehen und z.B. Subunternehmen von Rüstungsfirmen und deren Gewinn im Service Bereich nicht einbeziehen. So hat etwa allein *BAE Systems* 48% des Umsatzes, also 15,8 Mrd. US-Dollar, im Services-Markt erwirtschaftet.

[221]z.B. Mandel (2002: 1); O´Brien (2007: 60); Singer (2008: 18, 39). "The state's hold over violence is broken" (Singer 2008: 18) und „thus, in the future, we should not expect that organized violence would only be located in the public realm" (Singer 2008: 39).

[222] Für einen allgemeinen Überblick über verschiedene Kritikpunkte und teils deren Diskussion siehe u.a. Feichtinger et al. (2008); Singer (2007, 2008: Abschnitt III); Avant (2005); Avant/Nevers (2011); oder den amerikanischen Kongressbericht von Schwartz (2011). Für die vertiefende innenpolitische Diskussion z.B. Deittelhoff und Geis (2010); für operationelle Hürden Urey (2005) sowie Butkus und Howes (2006) und die Kostendiskussion, z.B. Isenberg (2009: 23–30).

[223] vgl. hierzu Leander (2005, 2010).

[224] vgl. hierzu Leander (2005).

[225] Heck (2010: 51–72).

[226] Sassen (2011).

[227] CCC (2012).

[228] Reißmann et al. (2011).

[229] Sen (2001) und Ward (2011).

[230] Wichtig ist dabei zwischen Hackern und sogenannten Crackern zu unterscheiden, denen es darum geht, Schaden anzurichten oder sich zu bereichern. Sie rücken damit in die Nähe der (Organisierten) Kriminalität (Janowicz 2007: 8–10). Natürlich gibt es zwischen diesen Polen allerlei Zwischenformen (Betz und Stevens 2011:25).

[231] Janowicz (2007:10).

[232] Reißmann et al. (2011).

[233] Wiedemann (2012). Dies heißt jedoch nicht, dass dieser Handlungsraum vollkommen losgelöst von anderen Räumen betrachtet werden kann. Stattdessen ist der Cyberspace auf vielfältige Weise mit anderen Räumen verwoben (Sassen 2011), wie nicht zuletzt die Festnahmen von mit Anonymous in Verbindung gebrachten Personen nach sogenannten Distributed Denial of Service Attacken (DDoS) auf Internetseiten verschiedener Unternehmen und Regierungsorganisationen zeigte.

[234] Bei DDoS Attacken werden Internetseiten durch die Überfrachtung mit Anfragen außer Gefecht gesetzt.

[235] Ball (2012); Beiersmann und Espiner (2011); Kling und Meyer (2011).

[236] Zum Folgenden vgl. Re:publika (2012); Janowicz (2007).

[237] Für eine allgemeine Übersicht verschiedener technischer Arten von Attacken im Internet siehe BSI-Register aktueller Cybergefährdungen und Angriffsformen, www.datenschutzbeauftragter-info.de.

[238] vgl. Baudzus (2012); Betz und Stevens (2011).

[239] Re:publica (2012).

[240] Re:publica (2012).

[241] Wiedemann (2012).

[242] Vgl. Held und McGrew (2007); Kessler und Steiner (2009). Für Interaktionskapazitäten vgl. Buzan und Little (2000).

[243] Barrett et al. (2011).

[244] Williams (2008:7); USJFCOM (2010).

[245] Zwar sind heute die vorwiegenden Nachfrager auf diesem Markt immer noch Staaten. Aber schon heute nehmen, wie das Beispiel der Logistikfirmen in von Piraterie bedrohten Gebieten im vorangegangenen Kapitel gezeigt hat, auch NSAs die Angebote von PMSFs wahr.

[246] Mau (2006).

[247] Strange (1996).

[248] Dies sind ethnisch, kulturell oder religiös definierte Gemeinschaften, die sich in fremden Ländern niedergelassen haben, sich aber weiterhin stark mit der Heimat verbunden fühlen.

[249] Boli und Thomas (1999); Held (2007).

[250] Beck (1999); Giddens (1996); Inglehart (1977).

[251] Während die Ausbreitung moderner Werte generell das politische Selbstvertrauen vieler Menschen steigerte – sie waren nun bereit, für ihre Werte einzustehen – ist besonders in den letzten zwei Jahrzehnten zu beobachten, dass Bürger dieses Selbstvertrauen nicht mehr nur durch politische Partizipation im Staat äußern, sondern vielmehr begonnen haben, eine Vielzahl von Partizipationsformen zu nutzen, die von der lokalen Gemeinschaften bis hin zu globalen Netzwerken reichen.

[252] Beck (1999).

[253] Huntington (1993).

[254] Barber (1996).

[255] Genschel und Zangl (2007); Hurrelmann et al. (2008). Genschel und Zangl spezifizieren die Bereiche, in denen der Staat Kompetenzen abgeben kann wie folgt: „Staatlichkeit umfasst drei für die effektive Herrschaftsausübung unerlässliche Kompetenzen: - Entscheidungskompetenz, das heißt die Macht, kollektiv-verbindliche Entscheidungen zu treffen; - Organisationskompetenz, also das Vermögen, kollektiv-verbindliche Entscheidungen verlässlich umzusetzen; - Letztverantwortung, das heißt die Fähigkeit, faktische Anerkennung als höchste politische Autorität zu finden, in deren Namen Herrschaft ausgeübt wird, und die die Folgen einer mangelhaften Kollektivgutproduktion zu verantworten hat“ (Genschel/Zangl 2007).

[256] Planungsamt der Bundeswehr (2012).

[257] Zürn (1998).

Literaturverzeichnis

Agnew, D.J. /Pearce, J./Pramod, G./Peatman, T./Watson, R./Beddington, J.R./ Pitcher, T.J. 2009: Estimating the Worldwide Extent of Illegal Fishing, in: http://www.plosone.org/article/info:doi/10.1371/journal.pone.0004570; 30.08. 2013.

Aker, J.C./Mbiti, I.M. 2010: Mobile Phones and Economic Development in Africa, in: Journal of Economic Perspectives 24: 3, 207–232.

Albert, M./Stetter, S. 2006: Viele Weltgesellschaften, viele Konflikte? Zur Rolle von Konflikt in Weltgesellschaftstheorien, in: Bonacker, T./Weller, C. (Hrsg.): Konflikte der Weltgesellschaft, Frankfurt a.M., 49-79.

Anderson, S./Cavanagh, J. 2000: Top 200: The Rise of Global Corporate Power (Institute for Policy Studies, Washington), Washington D.C.

Arquilla, J./Ronfeldt, D. (Hrsg.) 2001: Networks and Netwars: The Future of Terror, Crime, and Militancy, Santa Monica, CA.

Aust, B./Jaspers, W. 2006: From Resource War to ”Violent Peace”: Transition in the Democratic Republic of the Congo (Paper Nr. 50 des Bonner International Center for Conversion, Bonn), in: http://www.bicc.de/uploads/tx_bicctools/ paper50.pdf; 30.08.2013.

Auswärtiges Amt 2011: Weltraumrecht, in: http://www.auswaertiges-amt.de/DE/Aussenpolitik/InternatRecht/Einzelfragen/Weltraumrecht/Uebersicht_node.html; 30.08.2013.

Avant, D.D. 2005: Market of Force: The Consequences of Privatizing Security, Cambridge.

Avant, D.D./Nerves, R. de 2011: Military Contractors & the American Way of War, Daedalus 140: 3, 88-99.

Baker, D.-P. 2011: Will Global Demand for Private Military Services in Major Conflicts Continue?, in: Gumedze, S. (Hrsg.): Merchants of African Conflict: More than just a Pound of Flesh, Pretoria, 1-18.

Ball, J. 2012: WikiLeaks Published Stratfor Emails Linked to Anonymous Attack, Guardian Online vom 27.02.2012, in: http://www.guardian.co.uk/media/2012 /feb/27/wikileaks-publishes-stratfor-emails-anonymous; 30.08.2013.

Barber, B. 1996: Jihad vs. McWorld: Terrorism's Challenge to Democracy: How Globalism and Tribalism Are Re-Shaping the World, New York, NY.

Barrett, M./Bedford, D./Skinner, E./Vergles, E. 2011: Assured Access to the Global Commons, in: http://meerverstehen.net/2012/05/13/von-den-global-commons/; 30.08.2013.

Baudzus, T. 2012: Ein Blick hinter die Maske von Anonymous, Welt Online vom 16.04.2012, in: http://www.welt.de/regionales/duesseldorf/article106182090/ Ein-Blick-hinter-die-Maske-von-Anonymous.html; 30.08.2013.

BBC 2011: Oil Cyber-Attacks Could Cost Lives, Shell Warns, BBC Online vom 12.12.2011, in: http://www.bbc.co.uk/news/technology-16137573; 30.08.2013.

BBC 2012: Researchers Use Spoofing to 'Hack' into a Flying Drone, BBC Online vom 29.06.2012, in: http://www.bbc.co.uk/news/technology-18643134; 30.08.2013.

Beck, U. 1999: World Risk Society, New York, NY.

Beck, U. 2005: War Is Peace: On Post-National War, in: Security Dialogue 36: 1, 5-26.

Beck, U. 2007: Weltrisikogesellschaft: Auf der Suche nach der verlorenen Sicherheit, 1. Auflage, Frankfurt a.M..

Beiersmann, S./Espiner, T. 2011:“Anonymous” hackt Sicherheitsfirma, ZDNet News vom 08.02.2011, in: http://www.zdnet.de/41548071/bericht-anonymous-hackt-sicherheitsfirma/; 30.08.2013.

Benkler, Y. 2000: From Consumers to Users: Shifting the Deeper Structures of Regulation towards Sustainable Commons and User Access, in: Federal Communications Law Journal 52: 3, 561-579.

Benner, T./Witte, J.M. 2006: Keine Macht den Multis? Die Rolle transnationaler Konzerne in Entwicklungsländern, in: Internationale Politik 2006: 9, 1-7.

Berndtsson, J. 2009: The Privatisation of Security and State Control of Force: Changes, Challenges and the Case of Iraq (Dissertation an der Universität von Göteborg), Göteborg.

Betz, D.J./Stevens, T. 2011: Cyberspace and the State: Toward a Strategy for Cyber-Power, New York, NY.

Boli, J./Thomas, G.M. (Hrsg) *1999:* Constructing World Culture: International Non-Governmental Organizations Since 1875, Palo Alto, CA.

Bonacker, T. 2007: Der Kampf der Interpretationen: Zur Konflikthaftigkeit der politischen Moderne, in: Bonacker, T./Reckwitz, A. (Hrsg.): Kulturen der Moderne: Soziologische Perspektiven der Gegenwart, Frankfurt a. M., 199-218.

Bonacker, T./Weller, C. (Hrsg.) 2006a: Konflikte der Weltgesellschaft: Akteure - Strukturen – Dynamiken, 1. Auflage, Frankfurt am Main.

Bonacker, T./Weller, C. 2006b: Konflikte in der Weltgesellschaft: Aktuelle Theorie- und Forschungsperspektiven, in: Bonacker, T./Weller, C. (Hrsg.): Konflikte der Weltgesellschaft: Akteure - Strukturen – Dynamiken, 1. Auflage, Frankfurt a. M., 9-48.

Börzel, T.A./Hönke, J. 2011: From Compliance to Practice: Mining Companies and the Voluntary Principles on Security and Human Rights in the Democratic Republic of Congo (SFB-Governance Working Paper Series Nr. 25), Berlin.

Bowden, A./Hurlburt, K./ Marts, C./ Lee, A./ Aloyo, E. 2010: The Economic Costs of Maritime Piracy (Working Paper der One Earth Future), in: http://oneearthfuture.org/images/imagefiles/The%20Economic%20Cost%20of%20Piracy%20Full%20Report.pdf; 30.08.2013.

Brombacher, D. 2010: Nicht nur ein Problem innerer Sicherheit: Folgen der organisierten Kriminalität für das internationale System, in: Internationale Politik 2010: 6, 20-25.

Brunnengräber, A./ Klein, A./ Walk, H. (Hrsg.) 2005: NGOs im Prozess der Globalisierung: Mächtige Zwerge – umstrittene Riesen (Schriftenreiher der Bundeszentrale für Politische Bildung), Wiesbaden.

Bundeskriminalamt (BKA) 2010: Organisierte Kriminalität: Bundeslagebild 2010, Wiesbaden.

Bundeskriminalamt (BKA) (Hrsg.) 2011*:* Bundeslagebild Cybercrime 2011, Wiesbaden.

Bundesministerium des Inneren (BMI) (Hrsg.) 2011: Cybersicherheitsstrategie für Deutschland, Berlin.

Bundesministerium der Verteidigung (BMVg) (Hrsg.) 2006: Weißbuch 2006: Zur Sicherheitspolitik Deutschlands und der Zukunft der Bundeswehr, Berlin.

Bundesministerium der Verteidigung (BMVg) (Hrsg.) 2011: Verteidigungspolitische Richtlinien 2011, Berlin.

Bundesministerium für wirtschaftliche Zusammenarbeit und Entwicklung (BMZ) (Hrsg.) 2007: Entwicklungsorientierte Transformation bei fragiler Staatlichkeit und schlechter Regierungsführung (BMZ Konzepte 149), Berlin.

Bundeszentrale für Politische Bildung (BpB) 2010: Zahlen und Fakten: Globalisierung, NGOs in: http://www.bpb.de/nachschlagen/zahlen-und-fakten/globalisierung/52808/ngos; 30.08.2013.

Bundeszentrale für politische Bildung (BpB) 2012a: Zahlen und Fakten: Globalisierung, Transnationale Unternehmen, in: http://www.bpb.de/nachschlagen/zahlen-und-fakten/globalisierung/52629/transnationale-unternehmen; 30.08.2013.

Bundeszentrale für politische Bildung (BpB) 2012b: Zahlen und Fakten. Globalisierung, Die größten TNU, in: http://www.bpb.de/nachschlagen/zahlen-und-fakten/globalisierung/52633/die-groessten-tnu; 30.08.2013.

Butkus, J.J./Howes, M.F. 2006: A Critical Analysis of the Coordination, Command and Control of Contractors in Iraq, Monterey, CA.

Buzan, B./Little, R. 2000: International Systems In World History: Remaking the Study of International Relations, Oxford.

Chan, F. 2005: Falungong Sabotages Chinese Satellite TV, Asia Times Online vom 26.03.2005, in: http://www.atimes.com/atimes/China/GC26Ad04.html; 30.08.2013.

Chaos Computer Club (CCC) 2012: Hackerethik, in: http://www.ccc.de/de/hackerethik; 30.08.2013.

Chojnacki, S. 2004: Gewaltakteure und Gewaltmärkte: Wandel der Kriegsformen?, in: Frech, S./Trummer, P. (Hrsg.): Neue Kriege: Akteure, Gewaltmärkte, Ökonomie, Schwalbach, 73-99.

Chojnacki, S./Branovic, Z. 2011: New Modes of Security: The Violent Making and Unmaking of Governance in War-Torn Areas of Limited Statehood, in: Risse, T. (Hrsg.): Governance without a State? Policies and Politics in Areas of Limited Statehood, New York, NY, 89-114.

Chojnacki, S./Grömping, M./Spies, M. 2009: Armed Conflict Beyond the State: Spatial and Temporal Patterns of Non-State Violence in Somalia 1990-2007 (Paper for the Joint CSCW WG3/GROW-Net Workshop: Environmental Conflicts and Conflict Environments), Oslo.

CISCO (Hrsg.) 2012: Cisco Visual Networking Index: Forecast and Methodology 2011-2016, San Jose, CA.

Collier, P./Hoeffler, A. 1998: On Economic Causes of Civil War, in: Oxford Economic Papers 50: 4, 563-573.

Collier, P. 2006: Economic Causes of Civil Conflict and their Implications for Policy (Department of Economics der Weltbank), Washington, DC.

Council of Europe (Hrsg.) 2005: Organised Crime Situation Report 2005: Focus on the Threat of Economic Crime, in: http://www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Report2005E.pdf; 30.08.2013.

Daly, J.K. 2007: LTTE: Technologically Innovative Rebels, in: http://isn.ch/isn/Digital-Library/Articles/Detail/?ots783=4888caa0-b3db-146198b9e20e7b9c13d4&lng=en&id=53217; 30.08.2013.

Danger Room 2011: Iran's Alleged Drone Hack: Tough, but Possible, Danger Room vom 16.12.2011, in: http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps/; 30.08.2013.

Development, Concepts and Doctrine Centre (DCDC) (Hrsg.) 2010: Global Strategic Trends: Out to 2040, 4. Auflage, London.

Debiel, T./Lambach, D./Reinhardt, D. 2007: „Stay Engaged" statt „Let Them Fail": Ein Literaturbericht über entwicklungspolitische Debatten in Zeiten fragiler Staatlichkeit (INEF Report 90/2007), Duisburg-Essen.

De Groot, O. J./Rablen, M.D./Shortland, A. 2011: "Gov-aargh-nance": Even Criminals Need Law and Order'" (Economics of Security Working Paper 46, Berlin), in: http://www.economics-of-security.eu/sites/default/files/WP46_%20Criminals_need_law_and_order.pdf; 30.08.2013.

Deittelhoff, N./Geis, A. 2010: Entkernt sich der Leviathan? Die organisatorische und funktionelle Umrüstung der Militär- und Verteidigungspolitik westlicher Demokratien, in: Leviathan 38: 3, 389-410.

Deitelhoff, N./Geis, A. 2012: Die Privatisierung des Militärs, in: Militärsoziologie: Eine Einführung, Wiesbaden, 139-157.

Denmark, A.M./Mulvenon, J. (Hrsg.) 2010: Contested Commons: The Future of American Power in a Multipolar World, Washington, D.C.

Deutscher Bundestag 2009: Aktueller Begriff: Weltraummüll, Wissenschaftliche Dienste des Deutschen Bundestages, in: http://www.bundestag.de/dokumente/analysen/2009/weltraummuell.pdf;30.08.2013.

Dickow, M. 2010: Führung statt Dominanz: Die neue US-Raumfahrtpolitik sucht internationale Partner (SWP-Aktuell 2010/A 59, August 2010), Berlin.

Dobusch, L./Bahr, F./Dapp, T.F./Grzegorzek, M./Kerst, V./Meinberg, R./Rehse, M./ Saenger, J./Schauf, T./Tillmann, H. 2012: Schönes neues Internet? Chancen und Risiken für Innovation in digitalen Ökosystemen (Policy Brief, Stiftung Neue Verantwortung 2012), Berlin.

Dupont, B. 2004: Security in the Age of Networks, in: Policing and Society 14: 1, 76-91.

Dürr, W. 2010: Weltraumlage als Voraussetzung für den sicheren Betrieb von Raumfahrt-systemen, Hardthöhen Kurier Online Archiv, in: http://www.hardthoehenkurier.de/index.php?option=com_content&view=article&id=585%3Aweltraumlage-als-voraussetzung-fur-den-sicheren-betrieb-von raumfahrtsystemen&Itemid=152; 30.08.2013.

Ehrhart, H.-G./Petretto, K./Schneider, P. 2010: Security Governance als Rahmenkonzept für die Analyse von Piraterie und maritimem Terrorismus: Konzeptionelle und Empirische Grundlagen (PiraT-Arbeitspapiere zur Maritimen Sicherheit Nr. 1, November 2010), Berlin.

Eilstrup-Sangiovanni M./Jones, C. 2008: Assessing the Dangers of Illicit Networks: Why Al-Qaida May Be less Threatening than many Think, in: International Security 33: 2, 7–44.

Emmerson, C./Stevens, P. 2012: Maritime Choke Points and the Global Energy System: Charting a Way Forward, London.

Endler, J./Engerer, H./ Gössler, M./Pfeiffer, P. 2012: Ökonomische Aspekte von Piraterie und maritimem Terrorismus: Literatursurvey (PiraT-Arbeitspapiere zur Maritimen Sicherheit Nr. 16, Mai 2012), Berlin.

European Defence Agency (EDA) (Hrsg.) 2011: Future Global Context Study, Brüssel.

European Union Institute for Security Studies (EUISS) (Hrsg.) 2006: The New Global Puzzle: What World for the EU 2025, Paris.

Europäischer Rat 2003: Europäische Sicherheitsstrategie: Ein sicheres Europa in einer besseren Welt, Brüssel.

Europäischer Rat 2008: Bericht über die Umsetzung der Europäischen Sicherheitsstrategie: Sicherheit schaffen in einer Welt im Wandel, Brüssel.

Europäische Union (EU) 2008: Draft Council Conclusions on the Draft Code of Conduct for Outer Space Activities, in: http://www.eu2008.fr/webdav/site/PFUE/shared/import/1209_CAGRE_resultats/Code%20of%20Conduct%20for%20outer%20space%20activities_EN.pdf; 30.08.2013.

Europäische Union (EU) 2012: EU Launches Negotiations on an International Code of Conduct for Outer Space Activities, in: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/EN/foraff/130649.pdf; 30.08.2013.

Europäisches Polizeiamt (Europol) 2011: The Future of Organised Crime: Challenges and Recommended Actions, in: https://www.europol.europa.eu/content/press/european-police-chiefs-convention-draws-conclusions-tackling-future-organised-crime-an; 30.08.2013.

Exxon (Hrsg.) 2012: The Outlook for Energy: A View to 2040, in: http://www.exxonmobil.com/corporate/files/news_pub_eo2012.pdf; 30.08.2013.

Farah, D. 2010: Warum Kriminelle und Terroristen zuweilen kooperieren, in: Internationale Politik 2010: 6, 32-39.

Fearon, J. 2004: Why Do some Civil Wars Last so much longer than Others?, in: Journal of Peace Research 41: 3, 275–301.

Feichtinger, W./Braumandl, W./Kautny, N.-E. (Hrsg.) 2008: Private Sicherheits- und Militärfirmen: Konkurrenten - Partner – Totengräber?, Böhlau.

Financial Times Deutschland 2010: Kollisionsgefahr: SES-Satellit macht für Konkurrenten Platz im All, Financial Times Deutschland Online vom 23.05.2010, in: http://www.ftd.de/wissen/technik/:kollisionsgefahr-ses-satellit-macht-fuer-konkurrenten-platz-im-all/50117714.html; 30.08.2013.

Fortune 2012: Global 500: List 2011, in: http://money.cnn.com/magazines/fortune/global500/2011/full_list/; 30.08.2013.

Frantz, C./Martens, K. 2006: Nichtregierungsorganisationen (NGOs): Elemente der Politik, Wiesbaden.

Geis, A. 2006: Den Krieg überdenken: Kriegsbegriffe und Kriegstheorien in der Kontroverse, in: Geis, Anna (Hrsg.): Den Krieg überdenken: Kriegsbegriffe und Kriegstheorien in der Kontroverse (Schriftenreihe der DVPW-Sektion Politische Theorien und Ideengeschichte), Baden-Baden, 9-43.

*Genschel, P./Zangl, B.*2007: Die Zerfaserung von Staatlichkeit und die Zentralität des Staates, in: Aus Politik und Zeitgeschichte 2007: 20-21, 10-16.

Geopolicity 2011: The Economics of Piracy, in: http://www.geopolicity.com/upload/content/pub_1305229189_regular.pdf; 30.08.2013.

Gerlach, L.P. 2001: The Structure of Social Movements: Environmental Activism and its Opponents, in: Arquilla, J./Ronfeldt, D. (Hrsg.): Networks and Netwars: The Future of Terror, Crime, and Militancy, Santa Monica, CA, 289-310.

Gesellschaft für Internationale Zusammenarbeit (GIZ) 2010: Handynutzung in Afrika, in: https://www.giz.de/Themen/de/SID-D50C96C1-25A90146/34567.htm; 30.08.2013.

Giddens, A. 1996: Konsequenzen der Moderne, Frankfurt a.M.

Global Witness 2005: Under-Mining Peace: Tin - the Explosive Trade in Cassiterite in Eastern DRC, in: http://www.globalwitness.org/sites/default/files/pdfs/Under-Mining%20Peace.pdf; 30.08.2013.

Global Witness 2009: Faced with a Gun, what Can you Do: War and the Militarisation of Mining in Eastern Congo, in: http://www.globalwitness.org/site/default/files /pdfs/report_en_final_0.pdf; 30.08.2013.

Gordenker, L./ Weiss, T.G. (Hrsg.) 1996: NGOs, the UN and Global Governance, Boulder, CO.

Grego, L. 2012: A History of Anti-Satellite Programs (Union of Concerned Scientists, Januar 2012), in: http://www.ucsusa.org/assets/documents/nwgs/a-history-of-ASAT-programs_lo-res.pdf; 30.08.2013.

Greve, Janna 2010: Failing Cities? Die Krise der Megastädte - Von Johannesburg bis Rio de Janeiro, in: Blätter für deutsche und internationale Politik 55: 4, 99-106.

Hein, J.R./Conrad, T.A./Staudigel, H. 2010: Seamount Mineral Deposits: A Source of Rare Metals for High-Technology Industries, in: Oceanography 23: 1, 184-190.

Humrich, C./Wolf, K.D. 2011: Vom Meltdown zum Showdown? Herausforderungen und Optionen für Governance in der Arktis (HSFK-Report Nr. 4/2011), Frankfurt a.M.

Hague Center for Strategic Studies (HCSS) (Hrsg.) 2011: Contours of Conflicts in the 21st Century: A Cross-Language Analysis of Arabic, Chinese, English and Russian Perspectives on the Future Nature of Conflict, Den Haag.

Hamburgisches Weltwirtschaftsinstitut (HWWI) 2006: Maritime Wirtschaft und Transportlogistik: Perspektiven für maritime Wirtschaft und Transportlogistik – Strategieansätze aus Unternehmens- und Investorensicht, in: http://www.hwwi.org/fileadmin/hwwi/Publikationen/Partnerpublikationen/Berenberg/Strategie2030_Maritim_B.pdf; 30.08.2013.

Hamburgisches Weltwirtschaftsinstitut (HWWI) 2009: Langfristige Perspektiven von Anlagen in Sachwerten (Report Nr. 11 des HWWI-Kompetenzbereiches Wirtschaftliche Trends), in: http://www.hwwi.org/fileadmin/hwwi/Publikationen/Policy/HWWI_Policy_Report_Nr._11.pdf; 30.08.2013.

Hamburgisches Weltwirtschaftsinstitut (HWWI) 2010: Afrika: Strategie 2030, Hamburg.

Hansen, W. 2011: The Failed State – Organized Crime – Terrorism Nexus (SWP Comments 40/2011), Berlin.

Hastings, J. V. 2009: Geographies of State Failure and Sophistication in Maritime Piracy Hijackings, in: Political Geography, 28: 4, 213-223.

Heck, D. 2010: Grenzen der Privatisierung militärischer Aufgaben, Baden-Baden.

Heidelberger Instituts für Internationale Konfliktforschung (HIIK) 2011: Conflict Barometer, in: http://www.hiik.de/de/konfliktbarometer/pdf/ConflictBarometer011.pdf; 30.08.2013.

Heinecken, L./Motzouris, M. 2011: The Effect of Private Security on National Armed Forces' Capacity and Capabilities, in: Gumedze, S. (Hrsg.): Merchants of African conflict: More than just a Pound of Flesh, Pretoria, 78-81.

Heise Online (Hrsg.) 2012: Facebook: Eine letzte Abstimmung über Abstimmungen, in:http://www.heise.de/newsticker/meldung/Facebook-Eine-letzte-Abstimmung-ueber-Abstimmungen-1761618.html; 30.08.2013.

Held, D. 2007: Mythen der Globalisierung, in: Beck, U. (Hrsg.): Generation global: Ein Crashkurs, Frankfurt a.M., 12-26.

Held, D./McGrew, A. 2007: Globalization Theory: Approaches and Controversies, Oxford.

Herkenrath, M./Bornschier, V. 2006: Konfliktakteure der Weltgesellschaft, Transnationale Konzerne und ihre zivilgesellschaftlichen Opponenten im Konflikt um ein globales Investitionsregime: Weltgesellschaftliche Akteure im Widerstreit, in: Bonacker, T./Weller, C. (Hrsg.): Konflikte der Weltgesellschaft: Akteure - Strukturen – Dynamiken, 1. Auflage, Frankfurt a. M., 81 – 102.

Homeland Security News Wire 2010: New Russian Weapon System Hides Missiles in Shipping Container, in http://www.homelandsecuritynewswire.com/new-russian-weapon-system-hides-missiles-shipping-container; 04.02.2013.

Huntington, S.P. 1993: The Clash of Civilizations, in: Foreign Affairs 72: 3, 22-49.

Hurrelmann, A./Leibfried, S./Martens, K./Mayer, P. (Hrsg.) 2008: Zerfasert der Nationalstaat? Die Internationalisierung politischer Verantwortung (Reihe: Staatlichkeit im Wandel), Frankfurt a.M.

Inkster, N./Comolli, V. 2012: Drugs, Insecurity and Failed States: The Problems of Prohibition (The International Institute for Strategic Studies (IISS), Adelphi Series 428), Oxon.

International Energy Agency 2012: World Energy Outlook 2012, Paris.

International Maritime Bureau of the International Chamber of Commerce (*ICC)* (Hrsg.) 2012a: Piracy and Armed Robbery Against Ships: Report for the Period of 1st of January to 31 December 2011, London.

International Maritime Bureau of the International Chamber of Commerce (ICC) (Hrsg.) 2012b: Piracy & Armed Robbery News & Figures, in: http://www.icc-ccs.org/piracy-reporting-centre/piracynewsafigures; 30.08.2013.

International Monetary Fund (IMF) (Hrsg.) 2011: Regional Economic Outlook: Sub-Saharan Africa Sustaining the Expansion, Washington, D.C.

Internet Crime Complaint Center (ICCC) (Hrsg.) 2011: Internet Crime Report 2011, Washington, D.C.

Informationsplattform Humanrights.ch (Hrsg.) 2012: Transnationale Unternehmen: Begriff und Bedeutung, in: http://www.humanrights.ch/de/Themendossiers/TNC/Uebersicht/idart_3493-content.html; 30.08.2013.

Inglehart, R. 1977: The Silent Revolution: Changing Values and Political Styles among Western Publics, Princeton, NJ.

International Monetary Fund *(IMF)* 2011: Regional Economic Outlook - Sub-Saharan Africa: Recovery and New Risks, in: http://www.imf.org/external/pubs/ft/reo/2011/afr/eng/sreo0411.pdf; 30.08.2013.

Internet World Stats 2011: Internet World Stats-Usage and Population Statistics: Africa Stats, in: http://www.internetworldstats.com/stats1.htm; 30.08.2013.

Isenberg, D. 2009: Private Military Contractors and U.S. Grand Strategy, Oslo.

Janowicz, K. 2007: Sicherheit im Internet, 3. Auflage, Köln.

Kaldor, M. 1999: New and Old Wars: Organized Violence in a Global Era, Stanford, CA.

Kappel, Robert 2010: Nigeria: Die Instabilität wächst (German Institute of Global and Area Studies Focus 2/2010), in: http://www.giga-hamburg.de/dl/download.php?d=/content/publikationen/pdf/gf_afrika_1002.pdf; 30.08.2013.

Keck Institute for Space Studies 2011: Asteroid Retrieval Misson Study, in: http://kiss.caltech.edu/workshops/asteroid2011/index.html; 30.08.2013.

Keohane, R.O./Nye, J.S. 1977: Power and Interdependence: World Politics in Transition, Boston, MA.

Kessler, J./Steiner, C. 2009: Facetten der Globalisierung: Zwischen Ökonomie, Politik und Kultur, Wiesbaden.

Kleinwächter, W. 2006: Kurze Rede, langer Sinn, in: http://www.heise.de/tp/artikel/22/22774/1.html; 30.08.2013.

Kleinwächter, W. 2010: Minenfeld Internet Governance: Wo geht die Machtverschiebung hin?, in: http://www.heise.de/tp/artikel/34/34042/5.html; 30.08.2013.

Kleinwächter, W. 2012: Universelle Prinzipien für das Internet, in: http://www.heise.de/tp/artikel/37/37814/1.html; 30.08.2013.

Kling, B./Meyer, M. 2011: Anonymus-Angriff auf Stratfor: Details durchgesickert, ZDNet News vom 28.12.2011, in: http://www.zdnet.de/41559055/anonymous-angriff-auf-stratfor-details-durchgesickert/; 30.08.2013.

Krahmann, E. 2003: Conceptualising Security Governance, in: Cooperation and Conflict 38: 1, 5-26.

Krahmann, E. 2005: Security Governance and Networks: New Theoretical Perspectives in Transatlantic Security, in: Cambridge Review of International Affairs 18: 1, 19-34.

*Kraska, J.*2010: Indistinct Legal Regimes, in: Jasper, Scott (Hrsg.): Securing Freedom in the Global Commons, Stanford, CA, 49-63.

Kreditanstalt für Wiederaufbau (KfW) 2011: Entwicklung in fragilen Staaten: Krisen bewältigen, Perspektiven schaffen (Jahresbericht über die Zusammenarbeit mit Entwickungsländern), Frankfurt a.M.

Kreye, A. 2012: Facebook-Demokratie: Eine Frechheit, in: http://www.sueddeutsche.de/digital/abstimmung-ueber-nutzungsbedingungen-facebook-demokratie-eine-frechheit-1.1373411; 30.08.2013.

Lampe, K. von 2012: Definitions of Organized Crime, in: http://www.organized-crime.de/organizedcrimedefinitions.htm; 30.08.2013.

Landesanstalt für Medien Nordrhein-Westfalen (LFM) (Hrsg.) 2012: Apple. Google. Facebook. Amazon: Strategien und Geschäftsmodelle einfach auf den Punkt gebracht, Düsseldorf.

Lauster, G./Mildner, S.-A./Wodni, W. 2010: Transparenz im Rohstoffhandel: US-Finanzgesetz soll Handel mit Konfliktressourcen eindämmen (SWP-Aktuell 76, November 2010), Berlin.

Leander, A. 2005: The Power to Construct International Security: On the Significance of Private Military Companies, in: Journal of International Studies 33: 3, 803-825.

Leander, A. 2010 The Paradoxical Impunity of Private Military Companies: Authority and the Limits to Legal Accountability, in: Security Dialogue 41: 5, 467-490.

Lemke, D. 2008: Power Politics and Wars without States, in: American Journal of Political Science 52: 4, 774-786.

Lochbihler, B. 2010: Welche Interessen vertreten NGOs? „Spiegel der Zivilgesellschaft“, in: Kulturaustausch Online 2010: 4, in: http://www.ifa.de/pub/kulturaustausch/archiv/ausgaben-2010/das-deutsche-in-der-welt/welche-interessen-vertreten-ngos/spiegel-der-zivilgesellschaft/; 30.08.2013.

Lohr, S. 2012: New U.S. Research Will Aim at Flood of Digital Data, New York Times Online vom 29.03.2012, in: http://www.nytimes.com/2012/03/29/technology/new-us-research-will-aim-at-flood-of-digital-data.html?_r=0; 30.08.2013.

Mair, S. (Hrsg.) 2010: Piraterie und Maritime Sicherheit (Stiftung Wissenschaft und Politik Studie 2010), in: http://www.swp-berlin.org/de/publikationen/swp-studien-de/swp-studien-detail/article/piraterie_und_maritime_sicherheit.html; 30.08.2013.

Makarenko, Tamara 2004: The Crime-Terror Continuum: Tracing the Interplay between Transnational Organised Crime and Terrorism, in: Global Crime 6: 1, 129-145.

Mandel, R. 2002 Armies without States: The Privatization of Security, Boulder, Co.

Martens, K. 2002 : Alte und Neue Players: Eine Begriffsklärung, in: Frantz, C./Zimmer, A. (Hrsg.): Zivilgesellschaft international: Alte und neue NGOs, Opladen, 25-49.

Mau, S. 2006: Transnationale Vergesellschaftung: Die Entgrenzung sozialer Lebenswelten (Aus der Reihe Staatlichkeit im Wandel), Frankfurt, a.M.

McAfee (Hrsg.) 2009a: In the Crossfire: Critical Infrastructure in the Age of Cyber War, in: http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf; 01.02.2013.

McAfee (Hrsg.) 2009b: Mapping the Mal Web: Die gefährlichsten Domänen weltweit, in: http://de.mcafee.com/de/local/docs/Mapping_Mal_Web.pdf; 30.08.2013.

Menn, A. 2011: Warum Internetwährungen Staaten nervös machen, Wirtschaftswoche Online vom 14.07.2011, in: http://www.wiwo.de/technologie/cyber-geld-warum-internetwaehrungen-staaten-nervoes-machen/5155564.html; 30.08.2013.

Miller, J.W. 2012: Weltall oder Meeresboden: Woher kommen die Rohstoffe der Zukunft?, The Wall Street Journal Online vom 10. Juni 2012, http://www.wallstreetjournal.de/article/SB10001424052702303753904577454450510799814.html#articleTabs%3Darticle; 30.08.2013.

Ministry of Defence of the Netherlands (Hrsg.) 2010: Future Policy Survey: A New Foundation for the Armed Forces of Tomorrow, Den Haag.

MPC (Hrsg.) 2012: Marktbericht Schifffahrt H1/2012, in: http://www.mpc-capital.de/contell/forward/Marktbericht%20Schifffahrt.pdf?realURL=/contell/cms/data/Downloads_Public/Produktdownloads/Zusammenstellungen/Allgemeine_Informationen/Intranet/Marktberichte/Schiffe/Marktbericht_Schiffe_2012_H1/datei; 01.02.2013.

Mucchielli, *L.* 2010: Urbane Aufstände im heutigen Frankreich, in: Sozial.Geschichte Online 2010: 2, 64–115.

Mutschler, M.M. 2012: Stoppschilder im Weltraum: Die Privatisierung der Raumfahrt als Herausforderung und Chance für die transatlantische Kooperation (SWP-Aktuell 33, Juni 2012), Berlin.

Müller, F. 2004: Der Ressourcenfluch: Rohstoffexporte als Konfliktfaktor (SWP Diskussionspapier der Forschungsgruppe Globale Fragen), in: http://www.swpberlin.org/fileadmin/contents/products/arbeitspapiere/DiskP2004_01_mlr_sicher.pdf; 30.08.2013.

Münkler, H. 2002: Die neuen Kriege, Reinbek.

National Aeronautics and Space Administration (NASA) 2003: Advanced Space Transportation Program, in: http://www.nasa.gov/audience/forstudents/postsecondary/features/F_Adv_Space_Transportation_prt.htm; 30.08.2013.

National Aeronautics and Space Administration (NASA) 2009: NASA and Caterpillar Inc.: Partner for Lunar Excavation and Construction, in: http://www.nasa.gov/offices/ipp/centers/jsc/news/Nasa_Caterpillar.html; 30.08.2013.

National Aeronautics and Space Administration (NASA) 2012: Orbital Debris Frequently Asked Questions, in: http://www.orbitaldebris.jsc.nasa.gov/faqs.html; 30.08.2013.

National Association of Security Companies (NASCO) 2012: Our Mission, in: http://www.nasco.org/; 30.08.2013.

National Intelligence Council (NIC) (Hrsg.) 2008: Global Trends 2025: A Transformed World, Washington, DC.

National Intelligence Council (NIC) (Hrsg.) 2010: Global Governance 2025: A Critical Juncture, Washington, DC.

National Intelligence Council (NIC) (Hrsg.) 2012: Global Trends 2030: Alternative Worlds, Washington, DC.

Neumayer, E. 2001: Pollution Havens: An Analysis of Policy Options for Dealing with an Elusive Phenomenon, in: Journal of Environment & Development 10: 2, 147-177.

New York Times 2009: Debris Spews Into Space After Satellites Collide, New York Times vom 11.02.2009, in: http://www.nytimes.com/2009/02/12/science/space/12satellite.html?_r=0; 30.08.2013.

North Atlantic Treaty Organization - Allied Command Transformation (NATO-ACT) (Hrsg.) 2009: Multiple Futures: Navigating towards 2030, in: http://www.act.nato.int/subpages/nato-multiple-futures-project-documents; 30.08.2013.

North Atlantic Treaty Organization (NATO) 2010: Active Engagement, Modern Defence: Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, in: http://www.nato.int/cps/en/natolive/official_texts_68580.htm; 30.08.2013.

Norton, R. 2003: Feral Cities: The New Strategic Environment, in: Naval War College Review 56: 4, 97-106.

O´Brien, K.A. 2000: PMCs, Myths and Mercenaries: The Debate on Private Military Companies, in: The RUSI Journal 145: 1, 59-64.

O'Brien, K.A. 2007: What Future, Privatized Military and Security Activities? in: The RUSI Journal 152: 2, 54 – 61.

Oxfam (Hrsg.) 2012: Oxfam Annual Report 2010-2011, in: http://www.oxfam.org/sites/www.oxfam.org/files/oxfam-annual-report-2010-2011.pdf; 30.08.2013.

Parlamentarisches Netzwerk für nukleare Abrüstung und Nichtverbreitung (PNND) 2007: Test der chinesischen Anti-Satellitenrakete macht auf die Militarisierung des Weltraumes aufmerksam (PNND Update 16 - Februar 2007), in: http://www.pnnd.de/index.php?id=148; *30.08.2013*.

Perlo-Freeman, S./Sköns, E. 2008: The Private Military Services Industry (SIPRI Insights on Peace and Security, Nr. 2008/1), in: http://books.sipri.org /files/insight/SIPRIInsight0801.pdf; 30.08.2013.

Pilkington, E. 2011: One in Four US Hackers 'Is an FBI Informer', Guardian Online vom 06.06.2011, in: http://www.theguardian.com/technology/2011/jun/06/us-hackers-fbi-informer; 30.08.2013.

Planungsamt der Bundeswehr (Hrsg.) 2012: Klimafolgen im Kontext: Implikationen für Sicherheit und Stabilität im Nahen Osten und Nordafrika (Future Study des Dezernats Zukunftsanalyse, Reihe Umweltdimensionen von Sicherheit, Teilstudie 2), Berlin.

Planungsamt der Bundeswehr (Hrsg.) 2013: Geoengineering (Future Topic des Dezernats für Zukunftsanalyse) Berlin.

PricewaterhouseCoopers (PWC) 2011: Future of World Trade: Top 25 Sea and Air Freight Routes in 2030, in: http://www.pwc.com/gr/en/publications/future-of-world-trade.jhtml; 30.08.2013.

PricewaterhouseCoopers (PWC) 2012: Sturmtief voraus: Deutsche Reeder suchen Kurs aus der Krise in: http://www.pwc.de/de/pressemitteilungen/2012/sturmtief-voraus-deutsche-reeder-suchen-kurs-aus-der-krise.jhtml; 30.08.2013.

Raab, J./Milward, B. 2003: Dark Networks as Problems, in: Journal of Public Administration and Theory 13: 4, 413-439.

Rabasa, A./Boraz, S./Chalk, P./Cragin, K./Karasik, T.W./Moroney J.D.P./O'Brien, K.A./Peters J.E. 2007: Ungoverned Territories: Understanding and Reducing Terrorism Risks (RAND Corporation Monographies Volume 561), Santa Monica, CA.

Remuß, N.L. 2009: The Need to Counter Space Terrorism: A European Perspective (European Space Policy Institute (ESPI), ESPI Perspectives No. 17, January 2009), in: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=124638; 30.08.2013.

Reißmann, O./Stöcker, C./Lischka, K. 2012: We are Anonymous: Die Maske des Protests - Wer sie sind, was sie antreibt, was sie wollen, München.

Reuters 2011: Oil Cargoes at Risk from Somali pirates, in: http://af.reuters.com/article/topNews/idAFJOE70O0MT20110125?pageNumber=2&virtualBrandChannel=0&sp=true; 30.08.2013.

Re:publika 2012: „Phänomen Anonymous" (Diskussion auf der Re:publika mit Frank Rieger, Carolin Wiedemann, Jacob Appelbaum unter Moderation von Ole Reißmann in Berlin am 04.05.2012), in: http://www.spiegel.de/video/anonymous-auf-re-publica-internetkonferenz-thematisiert-hackergruppe-video-1194191.html; 30.08.2013.

Risse, T. 2012: Governance Configurations in Areas of Limited Statehood: Actors, Modes, Institutions, and Resources (SFB-Governance Working Paper Series Nummer 32, April 2012), Berlin.

*Risse, T./Lehmkuhl, U.*2007: Regieren ohne Staat? Governance in Räumen begrenzter Staatlichkeit (Schriften zur Governance-Forschung), Baden-Baden.

*Risse-Kappen, T.*1995: Bringing Transnational Relations Back in: Non-State Actors, Domestic Structures and International Institutions (Cambridge Studies in International Relations, Band 42), Cambridge.

Rittberger, V.r/Kruck, A./Romund, A. 2010: Grundzüge der Weltpolitik: Theorie und Empirie des Weltregierens, Wiesbaden.

Robinson, J. 2012: Status of Europe's Space Cooperation with Asia (ESPI Perspectives No. 61, Juli 2012), in: http://www.espi.or.at/images/stories/dokumente/Perspectives/ESPI_Perspectives_61.pdf; 30.08.2013.

Rosenau, J. 1990: Turbulence in World Politics: A Theory of Change and Continuity, Princeton, NJ.

Rötzer, F. 2004: Schutzgelderpressung mit Drohung von DoS-Attacken, Heise Online vom 01.02.2004, in: http://www.heise.de/tp/artikel/16/16663/1.html; 30.08.2013.

Ruggie, J./Dossal, A. 2000: Towards Bridging the Digital Divide, in: http://www.un.org/partnerships/Docs/Towards_Bridging_the_Digital_Divide_by_JR-AAD.pdf; 30.08.2013.

Sassen, S. 2011: Die Macht des Digitalen: Ambivalenzen des Internet, in: Blätter für deutsche und internationale Politik 2011: 2, 93-104.

*Schmidt, H.*2011: Endspiel um das Internet, Frankfurter Allgemeine Zeitung Online vom 09.12.2011, in: http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/die-herrscher-im-netz-endspiel-um-das-internet-11556556.html; 04.02.2013).

Schneckener, U. 2004: States at Risks: Fragile Staaten als Sicherheits- und Entwicklungsproblem (SWP-Studien 2004/S 43), Berlin.

Schneckener, U. 2006a: Transnationaler Terrorismus: Charakter und Hintergründe des "neuen" Terrorismus, Berlin.

Schneckener , U. 2006b: Fragile Staatlichkeit: "States at Risk" zwischen Stabilität und Scheitern, Baden-Baden.

Schneckener, U. 2007: Ranking und Indizes: Welche Staaten gelten als fragil? (SWP Diskussionspapier FG 8, 2007), Berlin.

Schreier, F./Caparini, M. 2005: Privatising Security: Law, Practice and Governance of Private Military and Security Companies (Occasional Paper Nummer 6, des Genfer Zentrums für demokratische Kontrolle von Streitkräften (DCAF)), Genf.

Schwartz, M. 2011: The Department of Defense's Use of Private Security Contractors in Afghanistan and Iraq: Background, Analysis, and Options for Congress, Washington D.C.

Sechrist, M. 2012: New Threats, Old Technology: Vulnerabilities in Undersea Communication Cable Network Management Systems (Discussion Paper 2012-03, des Science, Technology, and Public Policy Programms des Belfer Center for Science and International Affairs an der Harvard Kennedy School), in:http://belfercenter.hks.harvard.edu/publication/21745/new_threats_old_technology.html; 30.08.2013.

Sen, W.E. 2001: Wau Holland - Der Tod eines Hackers, Hackertales Online Archiv von 12.2001, in: http://www.hackerland.de/hackertales/arc_aos_wauholland.htm;30.08.2013.

Singer, P.W. 2008: Corporate Warriors: The Rise of the Privatized Military Industry, 2. Auflage, Ithaca, NY.

Sterner, E. 2010: Beyond the Stalemate in the Commons, in: Denmark, A.M./Mulvenon, J. (Hrsg.): Contested Commons: The Future of American Power in a Multipolar World, 105-136.

Stockholm International Peace Research Institute (SIPRI) 2012: Business as Usual for Top Arms Producers (Sipri Press Release vom 27.02.2012), in: http://www.sipri.org/research/armaments/production/researchissues/pmsc/media/pressreleases/27-feb-2012-Business-as-usual-for-top-arms-producers; 30.08.2013.

Spiegel Online 2012: Umstrittener Einsatz: Wie Söldner somalische Piraten jagen, in: http://www.spiegel.de/panorama/piraten-vor-somalia-bundesregierung-plant-gesetz-fuer-privatarmee-a-827202.html; 30.08.2013.

Spruyt, H. 1994: Institutional Selection in International Relations: State Anarchy as Order, in: International Organization 48: 4, 527-557.

Statista (Hrsg.) 2012: Kapazität der weltweiten Containerschiffflotte im Vergleich der Jahre 2011 und 2015, in http://de.statista.com/statistik/daten/studie/223181/umfrage/kapazitaet-der-weltweiten-containerschiffflotte/; 30.08.2013.

Stewart, F./Brown, G. 2010: Fragile States (Überblick Nummer 3 des Centre for Research on Inequality, Human Security and Ethnicity (CRISE)), in: http://www.qeh.ox.ac.uk/pdf/pdf-research/crise-ov3; 30.08.2013.

Strange, S. 1996: The Retreat of the State: The Diffusion of Power in the World Economy, 9. Auflage, Cambridge.

Stürmer, M. 2008: Staatseinnahmen aus dem Rohstoffsektor in Subsahara-Afrika (Serie Entwicklungsfinanzierung des Deutschen Instituts für Entwicklungspolitik), Bonn.

Take, I. 2006: Die Schattenseite der Weltgesellschaft: Die transnationale Vernetzung von Gewaltakteuren als weltgesellschaftliche Herausforderung, in: Bonacker, T./Weller, C. (Hrsg): Konflikte der Weltgesellschaft: Akteure - Strukturen – Dynamiken, 1. Auflage, Frankfurt a. M., 103-126.

The Economist 2011: East India Company: The Company that Ruled the Waves, The Economist Online vom 17.12.2011, in: http://www.economist.com/node/21541753; 30.08.2013.

Thill, S. 2009: William Gibson: Father of Cyberspace, in: http://www.wired.com/science/discoveries/news/2009/03/dayintech_0317; 30.08.2013.

Tikk, E. 2011: Ten Rules for Cyber Security, in: Survival 53: 3, 119-132.

Tsetsos, K. 2012: Die maritime Dimension der Sicherheits- und Verteidigungspolitik der Europäischen Union und Deutschlands im 21. Jahrhundert: Maritime Sicherheit der Europäischen Union, München.

TU Braunschweig 2007: Erhöhtes Kollisionsrisiko von Satelliten durch chinesischen Anti-Satelliten-Test: TU Braunschweig berechnet den Zuwachs von Weltraummüll, in: https://www.tu-braunschweig.de/presse/medien/presseinformationen?year=2007&pinr=33; 30.08.2013.

Umweltbundesamt (Hrsg.), 2009: Klimawandel und marine Ökosysteme: Meeresschutz ist Klimaschutz, Dessau-Roßlau.

Union of International Associations (UIA) 2012: Multinational Enterprises, in: http://www.uia.be/23-multinational-enterprises; 30.08.2013.

United Nations Conference on Trade and Development (UNCTAD) 2012: Transnational Corporations Statistics, in: http://unctad.org/en/Pages/DIAE/Transnational-Corporations-Statistics.aspx; 30.08.2013.

United Nations (UN) 2009: Space Debris, in: http://www.un.org/en/events/tenstories/08/spacedebris.shtml; 30.08.2013.

United Nations Environmental Programme (UNEP) 2013: IEG of the Global Commons: Background, in: http://www.unep.org/delc/GlobalCommons/tabid/54404/Default.aspx; 30.08.2013.

United Nations Food and Agriculutre Organization (UN-FAO) (Hrsg.) 2011: Review of the State of World Marine Fishery Resources (FAO Fisheries and Aquaculture Technical Paper 569).

United Nations Food and Agriculutre Organization (UN-FAO) (Hrsg.) 2012a: Report of the FAO/APFIC: FAO Fisheries and Aquaculture Report R1008 (Workshop on Implementing the 2009 FAO Agreement on Port State Measures to Combat Illegal, Unreported and Unregulated Fishing, 23. bis 27. April 2012 in Rom), Rom.

United Nations Food and Agriculutre Organization (UN-FAO) (Hrsg.) 2012b: The State of the World Fisheries and Aquaculture 2012, Rom.

United Nations Office for Outer Space Affairs (UNOOSA) 1967: Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, in: http://www.oosa.unvienna.org/oosa/SpaceLaw/outerspt.html; 30.08.2013.

United Nations Office for Outer Space Affairs (UNOOSA) 1979: Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, in: http://www.oosa.unvienna.org/oosa/SpaceLaw/moon.html; 30.08.2013.

United Nations Office for Outer Space Affairs (UNOOSA) 2007: Space Debris Mitigation Guidelines of the Commitee on the Peaceful Use of Outer Space, in: http://orbitaldebris.jsc.nasa.gov/library/Space%20Debris%20Mitigation%20Guidelines_COPUOS.pdf; 30.08.2013.

United Nations Office on Drugs and Crime (UNODC) 2010: The Globalization of Crime: A Transnational Organized Crime Threat Assessment, Wien.

United Nations Office on Drugs and Crime (UNODC) 2012a: Organized Crime, in: http://www.unodc.org/unodc/en/organized-crime/index.html#what_organized_crime; 30.08.2013.

United Nations Office on Drugs and Crime (UNODC) 2012b: Emerging Crimes, in: http://www.unodc.org/unodc/en/organized-crime/emerging-crimes.html; 30.08.2013.

United States Air Force (USAF) (Hrsg.) 2012: Cyber Vision 2025: Cyberspace Science and Technology Vision 2012-2025, Washington, D.C.

United States Joint Forces Command (USJFCOM) (Hrsg.) 2010: Joint Operating Environment 2010, Suffolk, VA, in: www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf; 30.08.2013.

United States Department of Defense (USDoD) 2011: National Security Space Strategy, Washington, D.C.

Urey, R.G. 2005: Civilian Contractors on the Battlefield (USAWC Strategy Research Project des US Army War College), Carlisle Barracks, PA.

Vereinigte Staaten von Amerika 2002: National Security Strategy of 2002, Washington, D.C.

Vereinigte Staaten von Amerika 2006: National Security Strategy of 2006, Washington, D.C.

Vereinigte Staaten von Amerika 2010: National Security Strategy of 2010 Washington D.C.

Ward, M. 2011: A Brief History of Hacking, BBC Nachrichten Technologie vom 09.06.2011, in: http://www.bbc.co.uk/news/technology-13686141; 30.08.2013.

*Westerkamp, M./ Feil M./Tänzler, D.*2011: Rohstoffkonflikte nachhaltig vermeiden: Fallstudie und Szenarien zu Kupfer und Kobalt in der Demokratischen Republik Kongo (Teilbericht 3.2 des Forschungsprojektes FKZ), in: http://www.adelphi.de/files/uploads/andere/pdf/application/pdf/rohkon_bericht_3-2_kongo.pdf; 30.08.2013.

Weller, C./Bösch, R. 2011: Globalisierung und transnationale Konflikte: Frieden aus einer Global-Governance-Perspektive, Bonn.

Welt Online 2012: Allianz-Versicherung fordert Aufräumen im All, Welt Online Nachrichten vom 12.07.2012, in: http://www.welt.de/wissenschaft/weltraum/article108273328/Allianz-Versicherung-fordert-Aufraeumen-im-All.html; 30.08.2013.

Weltbank 2012: Bruttoinlandsprodukt 2011, in: http://databank.worldbank.org/databank/download/GDP.pdf; 29.11.2012.

Weltraumlagezentrum 2012: Weltraumlagezentrum – Der Auftrag, http://www.luftwaffe.de/portal/a/luftwaffe/!ut/p/c4/NYvBCsIwEET_aLe5lOBNEYsXPRWtt9ikIZhmw7KxFz_eBHEGhgePwQfWJvMO3kigZCLecZrD7rlB3IDYw1JcpZel_CNTFry1l3UwU3LSVlySUNezEWLIxBKbKczVQLA4dep46PruH_XR_TjoQWl9vpyumNd1_wXwne9r/; 30.08.2013.

Wiedemann, C. 2012: Irrepresentable Collectivity: Anonymous and the Technologies of the Common, in: Cox, G./Andersen, C.U. (Hrsg.): World of the News - The World`s Greatest Peer-reviewed Newspaper of in/compatible 1: 2, 25.

Wiedicke-Hombach, M./Reichert, C. 2012: Tiefseebergbau, in: http://www.bgr.bund.de/DE/Themen/MarineRohstoffforschung/Meeresforschung/Tiefseebergbau/tiefseebergbau_node.html; 30.08.2013.

Williams, P. 1997: Transnational Criminal Organisations and International Security, in: Survival 36: 1, 96–113.

Williams, P. 2008: Violent Non-State Actors and National and International Security, in: http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?id=93880&lng=en; 30.08.2013.

Williams, P./O´Hayon, G. 2002: Global Governance, Transnational Organized Crime and Money Laundering, in: McGrew, A./Held, D. (Hrsg.): Governing Globalization: Power, Authority and Global Governance, Cambridge, 127 -144.

Wirminghaus, N. 2013: Britische Geschäftsidee: Mächtige Söldnerflotte soll Piraten abschrecken, Spiegel Online vom 19.01.2013, in: http://www.spiegel.de/wirtschaft/aufruestung-gegen-piraten-private-kriegsflotte-sollschiffe-schuetzen-a-877976.html; 30.08.2013.

Wissenschaftlicher Beirat Globale Umweltveränderungen (WBGU) 2007: Sicherheitsrisiko Klimawandel: Hauptgutachten 2007, Berlin.

World Wide Fund For Nature (WWF) (Hrsg.) 2012: Satellitentechnik im Kampf gegen illegale und unregulierte Fischerei, in: http://www.wwf.de/2012/september/satellitentechnik-im-kampf-gegen-illegale-und-unregulierte-fischerei/; 30.08.2013.

Zeit 2011: Ticket ins All – für 35 Millionen Dollar, Zeit Online vom 28.04.2011, in: http://www.zeit.de/wissen/geschichte/2011-04/weltraumtourismus-all; 30.08.2011.

Zickuhr, K./Smith, A. 2012: Digital Differences (Report des PEW Research Center, Washington), in: http://www.pewinternet.org/~/media//Files/Reports/2012/PIP_Digital_differences_041312.pdf; 30.08.2013.

Zimmer, M. 2010: Oil Companies in Nigeria: Emerging Good Practice or Still Fuelling Conflict?, in: Deitelhoff, N./Wolf, K.D. (Hrsg.): Corporate Security Responsibility: Corporate Governance Contributions to Peace and Security in Zones of Conflict, Houndmills, 58-84.

Zissis, C. 2007: China's Anti-Satellite Test (Hintergrundinformationen des Council on Foreign Relations), in: http://www.cfr.org/china/chinas-anti-satellite-test/p12684; 30.08.2013.

Zürn, M. 1998: Regieren jenseits des Nationalstaates, Frankfurt a.M.

Zürn, M./Binder, M./Ecker-Erhardt, M./Radtke, K. 2007: Politische Ordnungsbildung wider Willen, in: Zeitschrift für Internationale Beziehungen 14: 1, 129-164.