Internationale Sicherheitspolitik im Internet-Zeitalter

Alexander Siedschlag

Humboldt-Universität zu Berlin, Institut für Politikwissenschaft
und
Hochschule für Politik München

E-Mail alexander.siedschlag@rz.hu-berlin.de

Mehr als der Schutz „kritischer Infrastrukturen“: Internationale Sicherheitsrisiken im IT-Sektor

Gemeinhin sehen deutsche, aber auch amerikanische Experten für internationale Politik in der internationalen Wirkung des Internets vor allem eine neue Stufe auf dem Weg zur Verwirklichung einer globalen Zivilgesellschaft, zur Durchsetzung des Prinzips öffentlicher, vollkommen transparenter Diplomatie und zur weltweiten Ausbreitung der Demokratie (infolge der digitalen Durchdringung autoritärer Staaten mit westlichen Werten und Informationen).[1] Es ist eine schöne Utopie, zu glauben, das Internet erhöhe automatisch den friedenbringenden Impetus der Weltöffentlichkeit. Die fundamentalen Herausforderungen, die das Internet an die internationale Politik und dabei vor allem an die Sicherheitspolitik stellt, übersieht man damit allerdings – oder man hofft jedenfalls, sie würden sich im Zuge der erwarteten Herausbildung einer digitalen Weltgesellschaft und eines freien globalen Informationsaustauschs von alleine bewältigen.

Sofern demgegenüber etwas realistischer nach den Folgen – auch nach den negativen Folgen – der „*internet*ionalen Politik“[2] für die nationale und internationale Sicherheit gefragt wird, geschieht das meist nur in Hinblick auf den Schutz „kritischer Infrastrukturen“ vor im weiteren Sinn „terroristischen“ Angriffen.[3] Auch die staatlichen Strategien – zum Beispiel die deutsche, von Innenminister Schily initiierte Internet Task Force – beschränken sich in der Regel auf diesen Bereich. Technischer Infrastrukturschutz ist selbstverständlich ein grundlegender Aspekt, allein muss er aber zu kurz greifen. Vor allem gibt es nämlich ungelöste *politische Probleme* internationaler Sicherheitspolitik im Internet-Zeitalter. Zum Beispiel lässt sich kaum entscheiden, ob ein Angriff auf eine entscheidend wichtige Datenbank eine kriegerische oder eine kriminelle Handlung ist und welche Art von Reaktion er erfordert bzw. rechtlich erlaubt. Die Waffen des Informationszeitalters sind unsichtbar, man kommt leicht an sie heran, sie sind kostengünstig und wirksam. Die Zerstörung von Infrastruktur (in den Bereichen Energie, Transport, Telekommunikation und Finanzen) und die Beschädigung von Befehls- und Kommandosystemen könnte eine Form annehmen, die von der internationalen öffentlichen Meinung gebilligt wird – kein großes Blutvergießen, keine hohen Zahlen an Opfern. Amerikanische Experten sprechen bereits davon, dass der Cyberspace zu einem neuen internationalen Schlachtfeld geworden sei.[4]

Vorabdruck aus: Kursbuch Internet und Politik, Bd. 2/2002

Was ist politische IT-Sicherheit im internationalen Maßstab?[5] Wodurch ist sie gefährdet? Wie lässt sie sich verwirklichen? – Dieser Beitrag skizziert das Panorama der Herausforderungen, die „Cyberwarfare“, „Cyberterrorism“ und „Information Warfare“ an staatliches Handeln stellen. Daran schließen sich einige Bemerkungen zu den Potenzialen und Problemen der verfügbaren *staatlichen* Antworten auf diese Herausforderungen an. Zunächst sind jedoch einige begriffstechnische Anmerkungen nötig.

Cyberwarfare und *Cyberterrorism* sind von den Maßnahmen her eng miteinander verwandt, wobei Cyberwarfare staatliches Handeln bezeichnet und zum Beispiel auch eine Verteidigung gegen, eine Vergeltung für cyberterroristische Handlungen oder ein virtueller Erstschlag sein kann.[6] In der Literatur wird Cyberwarfare als ein in erster Linie mit dem Faktor „Information“ operierendes strategisches Konzept definiert, das konventionelle Streitkräfteeinsätze nicht ersetzt, sondern unterstützt.[7] Sowohl bei Cyberwarfare als auch bei Cyberterrorism sind Informationssysteme oder Digitaltechnik (Computer oder Computernetze) entweder Instrument oder Ziel des offensiven Unternehmens.

Die sicherheitspolitischen Herausforderungen, die mit Cyberterrorism und mit möglichem offensiven Cyberwarfare durch Pariastaaten zusammenhängen, sind äußerst vielfältig.[8] So nutzen beispielsweise lateinamerikanische Terrorgruppen wie die „Zapatista“ in Mexiko oder die „Fuerzas Armadas Revolucionarias de Colombia (FARC)“ das Internet, um Anfragen der Presse zu beantworten, aber auch, um Aktionen zu koordinieren. Der „Leuchtende Pfad“ in Peru verbreitet über seine Internetseite nicht nur aktuelle „revolutionäre Meldungen“, sondern vertreibt auch Produkte wie T-Shirts, Plakate und Videos. Islamistische militante Organisationen gehen einen Schritt weiter: Einerseits verbreiten sie über ihre die Internetseiten antiwestliche, anti-israelische Propaganda; anderseits nutzen sie das Internet zum Fundraising und sogar zur Rekrutierung von Personal.

Information Warfare (oder abgeschwächter *Information Operations*) ist ein allgemeinerer Begriff.[9] Er bezeichnet alle Aktionen, die unternommen werden, um Informationsüberlegenheit zu erzielen, indem sie Informationen des Feindes beeinflussen oder dazu beitragen, eigene Ziele zu erreichen. Diese Aktionen stützen sich auf Prozesse, Informationssysteme und rechnergestützte Netze, die den systematischen Angriff auf „critical infrastructure“ möglich machen. Letztlich ist Information Warfare ein Konzept der Informationsherrschaft auf dem Schlachtfeld.

Was sind die konkreten materiellen Bedrohungen, gegenüber denen internationale Sicherheitspolitik im Internet-Zeitalter abwehrbereit sein muss? Sie erschließen sich, wenn man zusammenstellt, welche Arten virtueller Waffen es zum Angriff auf Computernetzwerke und Telekommunikationssysteme gibt. Cyberwaffen können die unterschiedlichsten Funktionen erfüllen. Sie lassen sich verwenden, um Informationsüberlegenheit zu gewinnen, Informationsquellen und Informationssysteme zu beschädigen, traditionelle und neue Arten von Waffen zu verbessern, die zivile Infrastruktur und die Versorgungssysteme zu beeinträchtigen, die Staatstätigkeit zu stören, ökonomisches Chaos zu verursachen und Sabotage zu erleichtern, das nationale Finanzsystem zum Erliegen zu bringen und psychologische Kriegführung zu betreiben, um ganze Gesellschaften zu destabilisieren. Folgende gebräuchliche Grundformen von Cyberwaffen können unterschieden werden:[10]

- sich selbst reproduzierende *Computerviren*, die über Software transportiert werden und sich über Kommunikationskanäle und Datennetzwerke verbreiten. Sie dringen in elektronische Telefonstationen und Überwachungssysteme ein und stören deren Funktion.
- *logische Bomben*, die in die Software militärischer und ziviler Steuerungszentralen eingebaut werden und auf ein Signal hin oder zu einem voreingestellten Zeitpunkt explodieren, Daten vernichten oder verändern und die Arbeit der Soft- und Hardware stören. Eine Variante ist das *trojanische Pferd*, das geheimen unberechtigten Zugang zu den Informationsquellen des Feindes ermöglicht, um nachrichtendiestliche Daten zu erhalten.
- Die *Verstopfung* („jamming“) des Informationsaustauschs in Telekommunikationsnetzwerken, die Verfälschung dieser Information und die Benutzung staatlicher und militärischer Kommunikations- und Kontrollkanäle sowie der Massenmedien, um die benötigten Informationen abzuzapfen.
- Die Technologie, Computerviren zu im Netz zu übertragen und logischen Bomben in die staatlichen und unternehmerischen Informationsnetzwerke und -systeme einzubauen, um sie *fernsteuern* zu können. Zum Beispiel der Einbau eines Chips oder einer anderen Komponente in weltweit vertriebene Elektrogeräte.

Politische Probleme der „Verteidigungsfähigkeit“ im Internet-Sektor

Aus den durch Cyberwaffen gegebenen Möglichkeiten resultieren unmittelbar wichtige Probleme sozusagen „virtueller“ Sicherheitspolitik. An erster Stelle steht dabei die Frage nach der Richtgröße: Was ist *politische* IT-Sicherheit? Daraus folgt sich die Frage, was überhaupt ein Cyberangriff (im Gegensatz zu Cyberterrorismus oder zu Computerkriminalität) ist und wann und inwieweit er völkerrechtlich gesehen einen aggressiven Akt darstellt, einer Kriegserklärung gleichkommt und individuelle bzw. kollektive Selbstverteidigung gemäß Artikel 51 der Satzung der Vereinten Nationen erlaubt.[11] Dieses Definitionsproblem ist ein unmittelbar politisches Problem; denn es betrifft die Legitimierbarkeit möglicher Vergeltungsmaßnahmen: Wie darf ein Staat – oder ein Bündnis – einer Bedrohung durch Informationsoperationen in zulässiger Weise begegnen, und in welchem Rahmen darf er selbst derartige Operationen durchführen, zum Beispiel als antizipierte Selbstverteidigung oder als Vergeltungsmaßnahme?

In der völkerrechtlichen Debatte steht an erster Stelle die Frage, unter welchen Voraussetzungen eine Informationsoperation als „bewaffneter Angriff“ im Sinn von Artikel 51 der Satzung der Vereinten Nationen gewertet werden kann. In der Diskussion relativ unbestritten ist, dass die bloße Unterbrechung von Kommunikationswegen keinen Einsatz von Gewalt und daher auch keinen bewaffneten Angriff darstellt, ebenso wie minimal-invasive Informationsoperationen (zum Beispiel Port-Scanning).[12] Demgegenüber sind all solche Informationsoperationen als Einsatz von Gewalt und entsprechend im gegebenen Fall als bewaffneter Angriff zu werten, die tödliche Wirkungen einkalkulieren, militärischen Waffen vergleichbare Zerstörung bewirken und invasiv sind, das heißt, sich gegen die Souveränität und/oder die Unverletzlichkeit der Grenzen eines Staates richten.[13]

Einige Autoren nehmen als Kriterium die faktische Wirkung der Cyberattacke: Sie sei dann als bewaffneter Angriff zu werten, wenn der angerichtete Schaden einem herkömmlichen Angriff vergleichbar ist. Da man zum Beispiel die Zündung eines nuklearen Sprengkör-

pers in größerer Höhe über dem Boden, um durch einen elekromagnetischen Impuls „critical infrastructure“ lahm zu legen, fraglos als bewaffneten Angriff ansehen würde, könne es keinen wesentlichen Unterschied bedeuten, wenn dieser Effekt etwa mithilfe eines Computervirus erzielt würde.[14]

„Es wäre fast absurd, den Abwurf einer Bombe, die begrenzte Zerstörungen anrichtet oder ihr Ziel sogar verfehlt, ob des eingesetzten Mittels als zur Selbstverteidigung berechtigenden Angriff anzusehen, die durch Einsatz von Informationstechnologie bewirkte komplette Ausschaltung der Energieversorgung oder des Finanztransfersystems aber nicht. [...] Im Grundsatz sind daher die Staaten berechtigt, auch gegen ‚Informationsangriffe‘ ihr Selbstverteidigungsrecht auszuüben, sofern nur die Wirkungen einen solchen Informationsangriffes jenen eines herkömmlichen ‚bewaffneten‘ Angriffes gleichkommen.“[15]

Dennoch lässt sich derzeit kaum – und schon gar nicht völkerrechtlich verbindlich – feststellen, ob ein Angriff auf eine entscheidend wichtige Datenbank eine kriegerische oder eine kriminelle Handlung ist und welche Art von Reaktion er erfordert. Das gilt vor allem für Cyberangriffe, die von „Privaten“ (zum Beispiel Hackern oder nicht mit dem Staat, aus dem heraus sie operieren, verbundenen Terrorgruppen) ausgehen; denn „grundsätzlich ist ein Staat für Handlungen, die Private auf oder von seinem Hoheitsgebiet aus begehen, nicht verantwortlich.“[16] Die Staaten haben für die Informationsinfrastruktur eines anderen Staates keine Schutzpflicht.

Dieser Zustand würde erst durch eine internationale Vertragsregelung geändert, in der der Cyberspace – vergleichbar dem Weltraum und den Himmelskörpern – zum geschützten internationalen Raum erklärt würde.[17] Darüber hinaus darf sich eine gegen Cyberangriffe gerichtete Selbstverteidigung im Regelfall nur gegen den zweifelsfrei ermittelten „Aggressor“ richten und muss die Gebote der unmittelbaren Notwendigkeit und der Verhältnismäßigkeit beachten. Bei Cyberattacken, die von „Privaten“ ausgehen, ist Selbstverteidigung nach dem derzeitigen Stand des Völkerrechts nur bei zweifelsfrei nachgewiesener Verantwortlichkeit eines Territorialstaats zulässig.[18] Genau dieser Nachweis ist aber schwierig, wenn nicht unmöglich.

E-Intifada, Take-home Battle und digitaler Volkskampf – die sicherheitspolitische Kehrseite digitaler Demokratie

Verschärft wird die Problematik dadurch, dass Information Warfare auch zivile Ziele kennt, und selbst ohne physische Gewalt kann dem Angegriffenen ein fremder Wille aufgezwungen werden. Elektronisches Eindringen in Versorgungssysteme, Banken, Handelsplätze kann ganze Gesellschaften erpressen oder in Panik versetzen. Diese Bedrohungsszenarien haben unmittelbare Folgen für staatliches Handeln, weil sie weit reichende Fragen aufwerfen: Was sind die auf die Gesellschaften gerichteten Funktionen internationaler Sicherheitspolitik, und inwieweit kann die Legitimität des Staates durch Cyberbedrohungen infrage gestellt werden? Das Problem wird, wie die Erfahrung in den USA zeigt, durch die starke Stellung der privaten Infrastrukturbetreiber verschärft. Sie spielen nicht nur eine wichtige Rolle in der Umsetzung von Cyber-Sicherheitspolitik, sondern könnten dem Staat auch das Monopol der Definition von „Sicherheit“ streitig machen.[19]

Fakt ist jedenfalls: Informationswaffen und das Internet allgemein unterhöhlen das traditionelle Verständnis von Staatsgrenzen und machen sie technologisch durchsichtig. Das

könnte zu einer Destabilisierung der internationalen Beziehungen, zu globalen und regionalen Machtungleichgewichten führen, aber auch zur Stagnation des Systems internationaler Vereinbarungen über strategische Stabilität, ja sogar zu einem Rüstungswettlauf im Cyberspace.

Wenn man die Frage nach den auf die Gesellschaft gerichteten Funktionen staatlich ausgeübter internationaler Sicherheitspolitik im IT-Zeitalter konsequent zu beantworten sucht, kommt man zu einer seltsamen Lösung. Legt man nämlich traditionelle Staatsaufgaben wie allgemeine Sicherheitsvorsorge, Abschreckung möglicher Gegner und Protektion der Bürger und Unternehmen zugrunde, dann liegt die einzige effektive Antwort im Ausrufen eines allgemeinen Bedrohungszustandes und der organisierten Fähigkeit zur virtuellen Gegenoffensive im Volkskampf-Maßstab. Dem Muster nach entspräche das ungefähr dem, was die Volksrepublik China seit einiger Zeit betreibt:[20]

Seit die Versuche der chinesischen Regierung, eine Art Firewall nationale zu errichten, gescheitert sind, fährt Peking elektronische Angriffe gegen „feindliche“ ausländische und inländische Websites, verhaftet Aktivisten, die regierungskritische Inhalte im Internet veröffentlichen oder ihre Thesen per E-Mail verbreiten und bildet hunderte von Internet-Polizisten aus, um Webseiten zu durchforsten. Weit greifende Anordnungen verbieten die Online-Übertragung von Staatsgeheimnissen und von Inhalten, die die Staatsgewalt untergraben oder die „Ehre“ Chinas verletzen.[21] Dabei beruft man sich auf den altchinesischen Strategen Sun Zi: „Der Unbesiegbare ist der, der über sich *und* über den Anderen Bescheid weiß.“ Also müssen auf allen Wegen Informationen über mutmaßliche Feinde gesammelt und ausgewertet werden. Zu diesem Zweck hat die Staatsführung ab 1999 „digitale Miliztruppen“ geschaffen und das Konzept einer Take-home Battle eingeführt.[22] Das bedeutet, die „Kämpfer“ können mit ihrem Laptop den Krieg gleichsam mit nach Hause nehmen und ihre Offensiven vom Wohnzimmer aus unternehmen. Es gibt bereits zwei dokumentierte Beispiele für solche Take-home Battles: Vergeltung gegen Übergriffe gegen Chinesen in Indochina und das Hacken „westlicher“ Websites, vor allem der NATO-Homepage, als Vergeltung für die Bombardierung der chinesischen Botschaft in Belgrad im Mai 1999.[23]

Die Strategie des digitalen Volkskampfes wirft auch die Frage auf, was konventionelle militärische Überlegenheit unter den maßgeblich von IT beeinflussten Bedingungen der RMA (Revolution in Military Affairs) noch bedeutet. Ein frappantes Beispiel sind die USA, die trotz – oder gerade wegen – ihres technologischen Vorsprungs eine hohe eigene Verwundbarkeit an den Tag legen: Als das Pentagon zum Beispiel einen virtuellen Angriff auf seine eigenen Computer simulierte, um die Überlebensfähigkeit des Systems zu testen, stellte man fest, dass 24 700 der 38 000 Computer getroffen wurden. Das entspricht einer Trefferquote von 65 Prozent. Nur 998 (4 Prozent) stellten den Angriff fest und nur 267 (1 Prozent) der getroffenen 24 700 Computer meldeten den Angriff.[24] Dieses Experiment der virtuellen Verteidigungsfähigkeit wurde durchgeführt, nachdem es bereits breit angelegte virtuelle Überraschungsangriffe gegeben hatte. Der bekannteste wurde von den US-Ermittlern mit dem Codenamen „Moonlight Maze“ belegt und fand im März 1998 statt. Ziele waren hunderte Computernetzwerke der NASA, des Pentagons und anderer Regierungsbehörden, aber auch private Universitäten und Forschungslabore. Die Eindringlinge stahlen damals Technikdaten, Vertragsmaterial, Informationen über Verschlüsselungssysteme und Daten über die nationale Verteidigungsplanung.

Hier zeigt sich die *doppelte Asymmetrie* in der elektronischen Kriegführung: Relativ schwache Gegner durchkreuzen oder umgehen technologische Überlegenheit, und darüber hinaus setzt die eigene Hochtechnologie der Verteidigungsfähigkeit Grenzen, die die Gegner ausnutzen oder von vornherein in ihre Angriffsstrategie einbauen können.[25] Denn Cyberwaffen sind am effektivsten gegen die informationstechnologisch am stärksten fortgeschrittenen Staaten einsetzbar – die Staaten also, die heute in der Herstellung dieser Waffen führend sind.

Der Einsatz von Cyberwaffen gegen weniger entwickelte Staaten, in denen nur ganz große zivile Einrichtungen und Verteidigungsanlagen so ausgerüstet sind, dass sie von einem Internet-Angriff getroffen werden können, könnte zwar zu einem militärischen Sieg ohne Blutvergießen führen. Allerdings wäre die örtliche Bevölkerung in den Zielländern weniger vom Krieg betroffen und der Feind würde es deshalb kaum schaffen, einen psychologischen Sieg zu erringen. Für einen Siedler in weit abgelegenen Gegenden des Irak oder Afghanistans, der keinen Computer besitzt und dem manchmal sogar die Stromversorgung ausgeht, bedeutet der Zusammenbruch des Telekommunikations- oder Energiesystems eben keine nachvollziehbare Kriegsniederlage.

Demgegenüber hätte die Zerstörung eines Computers des US-Frühwarnsystems oder der erfolgreiche Angriff gegen Supercomputer in den Vereinigten Staaten oder Westeuropa dramatische Konsequenzen. Diese Wirkung psychologischer Abschreckung, die dem Abschreckungseffekt von Nuklearwaffen vergleichbar ist, arbeitet gegen die hoch entwickelten Länder. Das Problem wird dadurch verschärft, dass jeder Staat, der auf einen Cyberangriff mit Informations- oder konventionellen Operationen reagiert, dadurch den Cyberangriff als quasi-bewaffneten Angriff klassifiziert und ihn somit als eigene Handlungsoption der virtuellen Selbstverteidigung oder der Vergeltung ausschließt; denn sonst würde er ja selbst das Völkerrecht verletzen.[26]

Schätzungen der US-Regierung zufolge haben über 30 Staaten aggressive Information-Warfare-Software entwickelt, darunter Russland, China, Iran und Irak, aber auch Israel und Frankreich.[27] Newcomern wie Indien und Brasilien wird ebenfalls großes Engagement auf diesem Feld unterstellt. Derzeit sind die meisten Cyberattacken jedoch noch auf Webinhalte gerichtet, sie sind so genannte „defacements“, das heißt, eine Webseite wird entstellt durch eine andere ersetzt. So wurde zum Beispiel im Rahmen der „E-Intifada“ oder „Cyber-Jihad“ die Website des israelischen Parlamentes gegen eine Website mit pro-palästinensischen Inhalten ausgetauscht.[28] Zwischen Oktober 2000 und Januar 2001 brachten virtuelle Angriffe sowohl von palästinensischer als auch von israelischer Seite mehr als 250 Websites zum „Einsturz“, und die Aggressionen nahmen einen internationalen Maßstab an; denn auch Computernetzwerke ausländischer Firmen und für Sympathisanten des Gegners gehaltene Gruppen gerieten ins Visier.[29]

Ein Aktionsprogramm für die demokratische Staatengemeinschaft

Zunächst muss man betonen, dass das Internet und die Informations- und Kommunikationstechnologie allgemein zweischneidige Waffen sind: Einerseits können sie Demokratisierung und freien Informationsaustausch erleichtern, andererseits können sie den Propagandaapparat autoritärer Regime ausweiten und ethnische, religiöse oder rassische Intoleranz unterstützen.

Eine weitere Gefahr, die in diesem Zusammenhang auftaucht, ist die Möglichkeit des Missbrauchs von Informationen, um Fehlwahrnehmungen und Konflikte zu schüren. Auch in der internationalen Sicherheitspolitik schlägt sich die *allgemeine Ambivalenz des Internets als politischem Mittel* nieder.

Zugleich gilt jedenfalls vorerst: *Kein digitaler Angriff oder Krieg ohne realen Zündstoff.* Die Gefahr von internationalen Cyberattacken entsteht nicht aus dem Nichts, sondern ihr müssen reale internationale Spannungen vorausgehen. Ebenso wie beim Cyberterrorismus schaffen die technischen Möglichkeiten des Internets keine neue Form und keine neue Rationalität von Akteuren und Strategien, sondern sie sind neue Mittel.

Internationalen Sicherheitsbedrohungen und die Gefährdung der internationalen Gemeinschaft durch Cyberangriffe und Cyberterrorismus problemangemessen und auf demselben Kanal zu begegnen, kann zu einem *Amplifikationsproblem* führen: Durch die Abwehrmaßnahmen werden die Optionen des Gegners ungewollt erweitert. Billiger und einfacher Zugang zu Informationstechnologie schafft eben nicht nur die Basis für verbesserte transnationale Beziehungen, demokratische Meinungsbildung und Informationsvielfalt und kann so zum Beispiel totalitären Ideologien und Volksverhetzung entgegenwirken, sondern schafft auch erweiterte Bedrohungsmöglichkeiten – Stichwort Take-home Battle. Ein Weg, dieses Problem zu bewältigen, wäre die Aufgabe des klassischen Paradigmas der nationalen und der Bündnisverteidigung zugunsten einer gemeinsamen Cyber-Sicherheitspolitik sowie die drastische Erhöhung der Qualität und der politischen Beachtung des präventiven internationalen Informationsaustauschs.[30] Dass vor allem die großen Staaten zu diesen Schritten bereit sind, ist derzeit nicht zu erkennen.

Sieht man die Problematik internationaler Sicherheit unter IT-Bedingungen im Zusammenhang mit der globalen digitalen Spaltung der Welt und der Politik zu ihrer Überwindung, dann ergibt sich ein *sicherheitspolitisches Dilemma demokratischer Netzpolitik* im Weltmaßstab: Es ist klar, dass in vielen sich entwickelnden Ländern finanzielle und politische Unterstützung durch den Staat nötig ist, damit die Informations- und Kommunikationstechnologien sich entwickeln können. Nichtdemokratische Regime könnten diese Situation ausnutzen und von internationaler Hilfe ebenso wie von der Dividende ihrer eigenen Investitionen in die Internet-Entwicklung profitieren. Selbst wenn autoritäre Führer Internet und IT zu Propaganda oder zu Cyberwar-Aktivitäten nutzen, können sie aber Nebenwirkungen nicht verhindern, zum Beispiel das Auftauchen alternativer Informationsquellen und den Aufbruch ihres Wahrheitsmonopols. Deshalb kann es sinnvoll sein, autoritäre Regierungspropaganda kurz- und mittelfristig zu tolerieren und die internationale Unterstützung nicht sofort einzustellen.[31]

Anregungen für einen weiter gefassten Lösungsansatz liefert die Debatte über eine auf die IT-Möglichkeiten gestützte Weltfriedenskultur, und zwar in Form des kontraintuitiven Prinzips: *Sicherheitsstiftende Desintegration durch fragmentierte virtuelle Identiäten.* Die UNESCO (die Kulturorganisation der Vereinen Nationen) zum Beispiel tritt für einen neuen interkulturellen Ansatz zur Sicherung des Weltfriedens und der internationalen Sicherheit ein: Weltweit verknüpfte, gemeinsame Kulturwerte verfechtende Sicherheitsgemeinschaften sollen zu einer neuartigen Friedensordnung führen, die auf weltumspannender, „planetarischer Solidarität“ aufbaut.[32] Ähnlich hat der Soziologe Richard Münch argumentiert, die Weltgesellschaft des 21. Jahrhunderts werde sich aus dem Schritt von der primordialen (territorial-

herkunftsbestimmten) über die mediale (kommunikationsbestimmte) zur „virtuellen“ Identität entwickeln, die abstrahiert, alltagsenthoben, nicht ohne weiteres in konkreten Handlungssituationen einlösbar und deswegen auch weniger konfliktschürend sei.[33]

An besser greifbaren *staatlichen Handlungserfordernissen* wird in einer Studie der amerikanischen RAND Corporation unter anderem Folgendes identifiziert:[34]

– Errichtung nationaler und internationaler Clearingstellen für Zwischenfälle im Cyberspace.
– Entwicklung von glaubwürdigen Frühwarn-Indikatoren.
– Förderung der Entwicklung internationaler Normen und Kooperationsanstrengungen.
– Deklaration einer – idealerweise international abgestimmten – Vergeltungspolitik gegen Informationsangriffe und Cyberterrorismus.
– Etablierung einer Minimum Essential Information Infrastructure (MEII): Zusammenstellung und Schutz des Minimalmixes von teils nationalen, teils internationalen und teils privaten, teils öffentlichen Informationssystemen, die das fortgesetzte Funktionieren der Staatstätigkeit und der öffentlichen Ordnung im Fall von Cyberattacken und Information-Warfare-Angriffen sicher stellen.

Anmerkungen

1 Z.B. Wilson Dizard: Digital diplomacy. US foreign policy in the information age. Westport, CT u.a.: Praeger 2001; Christoph Engel: Das Internet und der Nationalstaat, in: Berichte der Deutschen Gesellschaft für Völkerrecht 39 (2000), S. 353-425; Karl Kaiser: Wie verändert das Internet die Weltpolitik?, in: Jahrbuch internationale Politik 1997-1998. München: Oldenbourg 2000, S. 346-355.

2 Alexander Siedschlag: *Internet*ionale Politik. Außenpolitik und internationale Beziehungen im Netz, in: Klemens Joos/Alexander Bilgeri/Dorothea Lamatsch (Hg.): Mit Mouse und Tastatur – Wie das Internet die Politik verändert. München: Olzog 2001, S. 87-96.

3 Exemplarisch dafür sind Reinhard Hutter: Risiken im Informationszeitalter, in: Bundesakademie für Sicherheitspolitik (Hg.): Sicherheitspolitik in neuen Dimensionen. Kompendium zum erweiterten Sicherheitsbegriff. Hamburg u.a.: Mittler 2001, S. 483-500; Mark Maskow: Killer im Netz. Terrorismus und das Internet, in: Alexander Siedschlag/Alexander Bilgeri/Dorothea Lamatsch (Hg.): Kursbuch Internet und Politik, Bd. 1/2002. Opladen: Leske + Budrich 2002, S. 119-129. Weiter gefasst dagegen: Vierteljahresschrift für Sicherheit und Frieden 18 (2000), Nr. 2 (Themenheft „Cyberwar“), darin z.B. zur Problematik der Vermischung von Cyberterrorism und Cyberwar: Ralf Bendrath: Elektronisches Pearl Harbor oder Computerkriminalität? Die Reformulierung der Sicherheitspolitik in Zeiten globaler Datennetze, S. 135-144.

4 Z.B. James Adams: Virtual defense, in: Foreign Affairs 80 (2001), Nr. 3, S. 98-112, dort S. 98.

5 Weiterführende Literatur: John Arquilla/David Ronfeldt (Hg.): In Athena’s camp. Preparing for conflict in the information age. Santa Monica, CA: RAND 1997; Ralf Bendrath u.a.: Texte zur Sicherheitspolitik in der Informationsgesellschaft 1997-1999. Berlin: Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik, Arbeitspapier Nr. 1, November 1999, abrufbar unter http://userpage.fu-berlin.de/~bendrath/fogis/fogis-ap1.rtf; Dorothy E. Denning: Information warfare and security. Reading, MA: Addison Wesley

1999; Zalmay M. Khalilzad/John P. White (Hg.): The changing role of information in warfare. Santa Monica, CA: RAND 1999; Armin Medosch/Janko Röttgers (Hg.): Netzpiraten. Die Kultur des elektronischen Verbrechens. Hannover: Heise 2001. Weiterführende Internetseiten: http://www.fogis.de (Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik); http://www.infowar.com.

6 Siehe Ralf Bendrath: Informationskriegsabteilungen der US-Streitkräfte: Eine Zusammenstellung der mit offensiven Cyberattacken befassten Einheiten der US-Streitkräfte. Berlin: Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik, Arbeitspapier Nr. 3, Juni 2001, abrufbar unter http://www.fogis.de/fogis-ap3.pdf.

7 Siehe John Arquilla/David Ronfeldt/Michele Zanini: Networks, netwar and information-age terrorism, in: Zalmay M. Khalilzhad/John P. White (Hg.): The changing role of information in warfare. Santa Monica, CA: RAND 1999, S. 75-111.

8 Als weiterführender Überblick: Brent L. Smith/Kelly R. Damphousse: Two decades of terror. Characteristics, trends, and prospects of the future of American terrorism, in: Harvey W. Kushner (Hg.): The future of terrorism: Violence in the new millennium. Thousand Oaks, CA: Sage 1998, S. 82-112.

9 Ausführlich: Khalilzad/White, Changing role of information in warfare (Anm. 5).

10 Grundlegend: Lance J. Hoffman (Hg.): Rogue programs: Viruses, worms, and Trojan horses. New York: Van Nostrand Reinhold 1990.

11 Ausführlich: Gregory Grove/Seymour E. Goodman/Stephen J. Lukasik: Cyber-attacks and international law, in: Survival 42 (2000), Nr. 3, S. 89-103; Torsten Stein/Thilo Marauhn: Völkerrechtliche Aspekte von Informationsoperationen, in: Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 60/1 (2000), S. 1-40.

12 Grove/Goodman/Lukasik, Cyber-attacks (Anm. 11), S. 93.

13 Ebd.

14 Mark R. Jacobson: War in the information age: International law, self-defense, and the problem of “non-armed” attacks, in: Journal of Strategic Studies 21 (1998), Nr. 3, S. 1-23, abrufbar unter http://www.infowar.com/resource/warinfo.doc.

15 Stein/Marauhn, Völkerrechtliche Aspekte von Informationsoperationen (Anm. 11), S. 7.

16 Ebd., S. 12.

17 Ebd.

18 Ebd., S. 35.

19 Bendrath, Elektronisches Pearl Harbor oder Computerkriminalität? (Anm. 3), S. 143.

20 Insgesamt siehe Junhua Zhang: Phantom oder Realität? Zur chinesischen Konzeption und Praxis der *Information Warfare*, in: WeltTrends, Nr. 35 (2002). Thema: Krieg im 21. Jahrhundert, S. 103-119.

21 Nina Hachigian: China’s cyber-strategy, in: Foreign Affairs 80 (2001), Nr. 2, S. 118-133, dort, S. 124.

22 Tim Thomas: China’s technology stratagems, in: Jane’s Intelligence Review 12/2000, abrufbar unter http://www.infowar.com/MIL_C4I/00/mil_c4i_120100d_j.shtml.

23 Ebd.

24 Scott Charney: The internet, law enforcement and security. Internet Policy Institute, 2000, abrufbar unter http://www.internetpolicy.org/briefing/charney.html.

25 Siehe dazu Dmitry Polikanov: Ungleichheit und Verwundbarkeit im Netz – Die digitale Spaltung der Welt aufhalten, in: Alexander Siedschlag u.a. (Hg.): Kursbuch Internet und Politik. Bd. 1/2002. Opladen: Leske + Budrich 2002, S. 99-117.

26 Stein/Marauhn, Völkerrechtliche Aspekte von Informationsoperationen (Anm. 11), S. 13.

27 Adams, Virtual defense (Anm. 4), S. 102.

28 Izhar Lev: E-Intifada: Political disputes cast shadows in cyberspace, in: Jane's Intelligence Review, 3. November 2000, abrufbar unter http://www.janes.com/security/international_security/news/jir/jir001103_1_n.shtml.
29 Adams, Virtual defense (Anm. 4), S. 98.
30 Siehe Adams, Virtual defense (Anm. 4), S. 99 u. 112; James Wirtz: Organizing for crisis intelligence: Lessons from the Cuban missile crisis, in: Intelligence and National Security 13 (1998), Nr. 3, S. 120-149.
31 Polikanov, Ungleichheit und Verwundbarkeit im Netz (Anm. 25).
32 UNESCO (Hg.): Non-military aspects of international security. Paris: Presses Universitaires de France 1995.
33 Richard Münch: Globale Dynamik, lokale Lebenswelten. Der schwierige Weg in die Weltgesellschaft. Frankfurt/M.: Suhrkamp 1998, S. 314-322.
34 Martin Libicki/Jeremy Shapiro: Conclusion: The changing role of information in warfare, in: Zalmay M. Khalilzad/John P. White (Hg.): The changing role of information in warfare. Santa Monica, CA: RAND 1999, S. 437-452.