ABHANDLUNGEN

Völkerrechtliche Aspekte von Informationsoperationen

Torsten Stein und Thilo Marauhn***

I. Einleitung

Sogenannte Informationsoperationen stellen ein relativ neuartiges Phänomen dar. Im weitesten Sinne bedeuten sie den Einsatz von Information und Informationstechnologie zur Erreichung staatlicher Ziele[1]. Nach einer etwas engeren Definition sollen Informationsoperationen diejenigen Maßnahmen sein, die darauf abzielen, die eigene Informationsinfrastruktur vor Ausforschung, Störung bzw. Verfälschung oder Zerstörung zu schützen, daneben aber auch in "gegnerische" Informationssysteme in vergleichbarer Absicht einzudringen, um sich Vorteile zu verschaffen[2]. Aus völkerrechtlicher Perspektive ist zu fragen, wie ein Staat einer Bedrohung durch Informationsoperationen in zulässiger Weise begegnen und in welchem Rahmen er selbst derartige Maßnahmen durchführen darf. Dabei sind nur jene Informationsoperationen eines Staates relevant, die – defensiv oder offensiv – grenzüberschreitende Wirkungen haben (sollen) oder gegen völkerrechtlich geschützte Einrichtungen auf dem eigenen Territorium durchgeführt werden (z.B. diplomatische Vertretungen, Stationierungsstreitkräfte, Hauptquartiere internationaler Organisationen). Die darauf anwendbaren völkerrechtlichen Regeln gelten in gleichem Maße für einen einzelnen Staat wie für die Bündnisse, denen er angehört. Bei der Frage, wie ein Staat oder Bündnis auf "feindliche Informationsoperationen" reagieren darf, werden sich die folgenden Ausführungen nicht auf "defensive Informationsoperationen" beschränken. Es soll vielmehr auch untersucht werden, ob und in welchem Ausmaß die "klassischen"

---

* Dr. iur., o. Prof. und Direktor des Europa-Instituts der Universität des Saarlandes. Dem Beitrag liegt ein im Auftrag der Industrieanlagen-Beteiligungsgesellschaft mbH (IABG) für das Amt für Studien und Übungen der Bundeswehr erstattetes Gutachten zugrunde.

** Dr. iur. (Heidelberg), M.Phil. (Wales), Wissenschaftlicher Referent am Institut.

1 G.J. Stein, Information Warfare, Airpower Journal 9 (1995), 31 (32).

2 M.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), N. 3, 1 (3f.); vgl. auch Th. Theuerkauf, Informations-Operationen, in: Europäische Sicherheit 2 (2000), 14ff.

völkerrechtlichen Gegenmaßnahmen (physische Gewalt, gewaltlose Repressalien) eingesetzt werden dürfen.

Um herauszuarbeiten, ob und inwieweit das geltende Völkerrecht Regeln für das Phänomen der Informationsoperationen enthält, wird die Untersuchung in möglichst enger Anlehnung an vertraute völkerrechtliche Kategorien gegliedert: Aggression, Intervention, nachrichtendienstliche Aktivitäten und Kriegsführungsrecht. So lassen sich die Anwendungsprobleme und etwaigen Regelungslücken am klarsten beschreiben. Ohnehin muß sich jede Informationsoperation zunächst einmal am geltenden Völkerrecht messen lassen, unabhängig davon, ob das Völkerrecht für die Besonderheiten von Informationsoperationen ausreichende Differenzierungen aufweist. Insbesondere Staaten, die Informationsoperationen abwehren wollen, hätten gar keine andere Möglichkeit als sich an der bestehenden völkerrechtlichen Konfliktterminologie auszurichten. Ob das Völkerrecht angesichts neuer Bedrohungslagen ausreicht oder vertrags- bzw. gewohnheitsrechtlich weiterentwickelt werden muß, ist eine ganz andere Frage.

Technische Fragen sind nicht Gegenstand der folgenden Überlegungen. Zum einen beruht hier vieles noch auf wissenschaftlich nicht oder wenig gesicherten Annahmen, zum anderen sind Völkerrechtswissenschaftler für diese Fragen nicht ausreichend kompetent. Die Studie unterstellt, daß es angesichts der weltweiten Vernetzung der Informationsinfrastruktur technische Möglichkeiten gibt oder geben wird, um Informationsangriffe und -eingriffe der unterschiedlichsten Intensitätsstufen durchzuführen – oder sich dagegen zu wehren.

Eine (denkbare) Definition von Informationsoperationen unter speziell völkerrechtlichen Aspekten erübrigt sich insoweit, als es aus der Sicht des Völkerrechts nicht in erster Linie auf das eingesetzte Mittel ankommt, sondern darauf, ob die von einem Staat mit diesem Mittel verfolgten Ziele völkerrechtsgemäß oder völkerrechtswidrig sind. Angesichts der in internationalen Menschenrechtsinstrumenten garantierten Informationsfreiheit wäre z.B. die Verbreitung wahrheitsgemäßer Informationen auch auf dem Gebiet von Staaten, die diese Information lieber unterdrückt sähen, nicht zu beanstanden[3]. Für die völkerrechtliche Bewertung ist zunächst die Intention maßgeblich, gegebenfalls das Ausmaß des jenseits der Informationssysteme eingetretenen Schadens, nicht aber primär die Ausforschung oder Störung der "gegnerischen Informationsinfrastruktur" als solcher. Bei bewußter Zerstörung mag das anders sein.

Die Möglichkeiten und Anlässe, sich der Informationstechnologie und -infrastruktur für die Erreichung eigener Ziele zu bedienen, sind sehr vielfältig. Die "gewöhnliche" Computerkriminalität ist nicht Gegenstand dieser Untersuchung. Zudem sind unter völkerrechtlichen Aspekten nur jene Informationsoperationen relevant, die von staatlichen Organen ausgehen, von einem Staat angeregt, gefördert oder geduldet werden und deren Unterbindung völkerrechtliche Pflicht eines Staates wäre.

---

[3] Vgl. nur Art. 19 der Allgemeinen Erklärung der Menschenrechte vom 10.12.1948.

Im folgenden wird zunächst untersucht, ob Informationsoperationen (jedenfalls ab einer gewissen Intensität) als Aggression angesehen werden können, gegen die sich ein Staat durch Einwirken auf "gegnerische" Ressourcen nach geltendem Völkerrecht verteidigen darf, und welche Grenzen eine solche Verteidigung zu beachten hätte (defensive Informationsoperationen) (II.). Danach wird dargelegt, welche gewaltlosen Reaktionsmöglichkeiten ("counter-measures short of force") ein Staat gegen solche Informationsoperationen ergreifen könnte, die unterhalb der Schwelle der Aggression bleiben, nach geltendem Völkerrecht aber gegebenenfalls als verbotene Intervention klassifiziert werden könnten (III.). Ein letzter Abschnitt wird sich der Frage zuwenden, welche Informationsoperationen ein Staat (oder eine Allianz) im Frieden oder im bewaffneten Konflikt selbst durchführen darf (offensive Informationsoperationen) (IV.). Soweit diese Fragen in der völkerrechtlichen Literatur überhaupt behandelt worden sind, wird immer wieder die Auffassung vertreten, das Völkerrecht habe zwar in der Vergangenheit neue technische Entwicklungen auffangen können, die aktuelle Abhängigkeit von der Informationsinfrastruktur im zivilen wie im militärischen Bereich habe aber nicht nur mögliche Konflikte graduell verändert, sondern eine ganz neue Art "systemischer Verwundbarkeit" geschaffen, der das Völkerrecht mit leeren Händen gegenüberstehe[4]. Das muß nicht notwendig so sein.

II. Informationsoperationen als Aggression?

1. Aggression, Anwendung von Gewalt, bewaffneter Angriff

Im Zusammenhang mit der Anwendung unerlaubten Zwanges auf andere Staaten und der Verletzung ihrer territorialen Unversehrtheit und politischen Unabhängigkeit finden sich im Völkerrecht und insbesondere in der Satzung der Vereinten Nationen (SVN) verschiedene Begriffe, die nicht immer deckungsgleich erscheinen[5]: Art. 2 Ziff. 4 SVN untersagt jede Androhung oder Anwendung von Gewalt. Gemäß Art. 39 SVN stellt der Sicherheitsrat fest, ob eine Bedrohung oder ein Bruch des Friedens oder eine Angriffshandlung (Aggression) vorliegt. Nach Art. 51 SVN haben die Staaten das naturgegebene Recht zur Selbstverteidigung im Falle eines bewaffneten Angriffs. Die Satzung der Vereinten Nationen definiert keinen dieser Begriffe in rechtlich verbindlicher Weise. Für einige gibt es unverbindliche und nicht notwendig erschöpfende Definitionen in Resolutionen

[4] Vgl. nur S.P. Kanuck, Information Warfare: New Challenges for Public International Law, Harvard International Law Journal 37 (1996), 272 (285). Siehe auch R.W. Aldrich, Legal Implications of Information Warfare, INSS Occasional Paper, April 1996 (http:// www.usafa.af.mil/inss/ocp9.htm).

[5] Vgl. K. Kenny, Self-Defence, in: R. Wolfrum (Hrsg.), United Nations Law, Policies and Practice, Vol. 2 (1995), 1162, Rn. 4f.; A. Randelzhofer, Art. 2 Ziff. 4, Rn. 14, in: B. Simma (Hrsg.), Charta der Vereinten Nationen, Kommentar (1991). Für den vorliegenden Zusammenhang vgl. jüngst M.N. Schmitt, Angriffe im Computernetz und das *ius ad bellum*, NZWehrR 1999, 177 (180ff.).

("Deklarationen") der UN-Generalversammlung, die jedoch weitgehend als Ausdruck akzeptierten Völkergewohnheitsrechts gewertet werden können.

Nach jedenfalls überwiegender Ansicht meint Gewalt im Sinne von Art. 2 Ziff. 4 SVN "Waffengewalt" bzw. "militärische Gewalt"[6]. Das hilft im vorliegenden Kontext nicht viel weiter, weil der Begriff "Waffe" nicht definiert ist[7] und auch das Adjektiv "militärisch" dann keine Eingrenzung bewirken kann, wenn andere als die herkömmlichen militärischen Einsatzmittel als Waffe dienen und durch das Militär eingesetzt werden könnten. Andere wiederum definieren den Begriff der Gewalt in Art. 2 Ziff. 4 weiter und lassen jeden Zwang ausreichen[8], z.T. unter Hinweis[9] auf die "Friendly Relations"-Deklaration der Generalversammlung der UN[10], die sich u.a. mit dem Gewaltverbot und dem Interventionsverbot auseinandersetzt.

Eine weder abschließende (so ausdrücklich deren Art. 4) noch rechtlich verbindliche, sondern als Grundlage für die Anwendung von Art. 39 SVN gedachte Definition der Aggression enthält die Resolution der UN-Generalversammlung vom 14. Dezember 1974[11]. Ungeachtet ihres unverbindlichen Charakters gilt sie zumindest als Leitlinie für die Definition des bewaffneten Angriffs[12]. Die Resolution definiert die Aggression als Anwendung von Waffengewalt (Art. 1) und zählt dazu u.a. (Art. 3): Invasion oder Angriff durch Streitkräfte; Beschießung oder Bombardierung des Hoheitsgebietes eines anderen Staates oder die Anwendung von Waffen jeder Art durch einen Staat gegen das Hoheitsgebiet eines anderen Staates; Blockade der Häfen und Küsten; Duldung der Benutzung des Territoriums durch einen anderen Staat, um Angriffshandlungen gegen einen dritten Staat zu begehen. Fraglos geht auch diese Definition aus dem Jahre 1974 vom herkömmlichen militärischen Arsenal aus. Aber wenn "Invasion" nicht mehr auf eine physische beschränkt wäre, dennoch vergleichbare Schäden anrichtete; wenn "Waffen jeder Art" auch Computer einschlössen; wenn "Blockade" viel wirkungsvoller über das Netz als durch Kriegsschiffe vor den Häfen und Küsten verhängt werden könnte, und wenn man statt "Duldung der Benutzung des Hoheitsgebietes" lesen würde "Duldung der Benutzung der Informationsinfrastruktur", dann bliebe doch der Grundansatz der Aggressionsdefinition erhalten: Schutz der

---

[6] Randelzhofer (Anm. 5), Rn. 15 und 18.

[7] Näher dazu unten Text bei Anm. 24ff.

[8] So z.B. O. Schachter, International Law in Theory and Practice (1991), 110–113 ("As long as the act of force ... compels a State to take a decision it would not otherwise take, Article 2 (4) has been violated"). Siehe auch Kanuck (Anm. 4), 289.

[9] M. Shaw, International Law (4. Aufl. 1997), 782f.; a.A. Randelzhofer (Anm. 5), Rn. 18.

[10] Res. 2625 (XXV) vom 24.10.1970; in Abs. 9 der Präambel heißt es: "... Pflicht der Staaten, sich in ihren internationalen Beziehungen jedes militärischen, politischen, wirtschaftlichen oder anderen Zwanges ... zu enthalten". Siehe dazu T. Tanca, The Prohibition on the Use of Force in the U.N. Declaration on Friendly Relations of 1970, in: A. Cassese (Hrsg.), The Current Regulation of the Use of Force (1986), 397ff.

[11] Res. 3314 (XXIX). Vgl. dazu N. Nyiri, The United Nations' Search for a Definition of Aggression (1989).

[12] Kenny (Anm. 5), Rn. 9.

Souveränität, der territorialen Unversehrtheit und politischen Unabhängigkeit der Staaten.

Die Definition des "bewaffneten Angriffs" ist deshalb von besonderer Bedeutung, weil allein der bewaffnete Angriff das Selbstverteidigungsrecht im Sinne von Art. 51 SVN auslösen kann. Aber was ist ein "bewaffneter Angriff"? Auch hier fehlen verbindliche Definitionen im Vertragsrecht und in der Rechtsprechung. Der Internationale Gerichtshof (IGH) hat sich im *Nicaragua*-Urteil[13] zwar zu einzelnen Aspekten geäußert, aber viele Fragen offengelassen. In der Literatur findet sich verbreitet der Versuch, den "bewaffneten Angriff" enger zu fassen als die "Angriffshandlung (Aggression)" oder die "Gewalt"[14]. Dahinter steht fraglos das Motiv, einem ausufernden Mißbrauch des Selbstverteidigungsrechts vorzubeugen. Jedoch kann die behauptete strikte Trennung von "Aggression" und "bewaffnetem Angriff" weder überzeugen noch wird sie durchgehalten[15]. Letztlich sind "Aggression" und "bewaffneter Angriff" – wie das im französisch-sprachigen Schrifttum auch gesagt wird[16] – weitestgehend identisch; dies aber mit der Einschränkung, daß die wesentliche Beteiligung eines Staates an der Entsendung bewaffneter Banden[17], wozu nach dem *Nicaragua*-Urteil des IGH auch private Gruppen gehören können, erst ab einer gewissen Intensität einem "bewaffneten Angriff" gleichgesetzt werden kann[18]; der IGH ließ dafür Waffenlieferungen oder logistische Hilfe nicht genügen[19]. Zurückhaltend war die Staatengemeinschaft bislang auch darin, wiederholte Übergriffe geringerer Intensität ob ihrer Kumulation als bewaffneten Angriff zu bewerten; insbesondere das frühere Südafrika und Israel haben auf eine derartige "Nadelstichtaktik" mit massiven Vergeltungsschlägen geantwortet[20].

Aus dem zuvor Gesagten wird deutlich, daß allen Begriffen die Vorstellung zugrunde liegt, es bedürfe eines Waffeneinsatzes. Ebenso deutlich ist, daß man dabei an die herkömmlichen (militärischen) Waffen denkt – und an ihre Wirkungen. "Bewaffneter Angriff" setzt ein gewisses Maß an physischer Zerstörung vor-

---

[13] ICJ Reports 1986, 14.

[14] So A. Randelzhofer, Art. 51 Rn. 16 und 19, in: Simma (Anm. 5); Kenny (Anm. 5), Rn. 9; Schmitt (Anm. 5), 191.

[15] Kenny (Anm. 14) spricht davon, daß die Aggressionsdefinition "mit Vorsicht als Hilfe zur Eingrenzung des bewaffneten Angriffs herangezogen werden kann"; Randelzhofer (Anm. 14), Rn. 20, ist deutlicher, wenn er sagt, die Angriffsdefinition gebe "wertvolle Hinweise" und zähle einzelne Angriffshandlungen auf, die "sämtlich – allerdings mit gewissen Einschränkungen [die nicht genannt werden] – als 'bewaffnete Angriffe' i.S.d. Art. 51 zu qualifizieren" seien.

[16] Nachweise bei Randelzhofer (Anm. 14), Rn. 16 mit dortiger Anm. 51.

[17] Art. 3 *lit.*g der Aggressionsdefinition (Anm. 11).

[18] Randelzhofer (Anm. 14), Rn. 30f. Dies ist von Bedeutung für Informationsangriffe Privater.

[19] *Nicaragua*-Urteil (Anm. 13), 104 (§195). Siehe dazu u.a. R. Mullerson, Self-Defense in the Contemporary World, in: L. Fisler Damrosch/D.J. Schaffer (Hrsg.), Law and Force in the International Order (1991), 13ff.

[20] Vgl. N.M. Feder, Reading the UN Charter Connotatively: Toward a New Definition of Armed Attack, N.Y.U.J. International Law and Politics 19 (1987), 393 (412). Südafrika antwortete letztendlich mit bilateralen Nichtangriffsverträgen (vgl. T. Stein, South Africa's Non-Aggression Agreements with the Frontline States, South African Yearbook of International Law 10 [1984], 1ff.).

aus, verbunden mit dem Eindringen in die Hoheitsgrenzen, innerhalb derer sich das angegriffene Ziel befindet[21]. Aber was gilt als Waffe? Einig ist man sich im durch die Satzung der Vereinten Nationen geprägten Völkerrecht, daß wirtschaftlicher Zwang oder Druck weder als Gewalt, noch als Aggression oder gar bewaffneter Angriff angesehen werden können[22]. Boykotte oder Embargos mögen als solche das Interventionsverbot verletzen, gelten aber nicht als verbotene Gewalt, selbst wenn im Zusammenhang mit den Ereignissen im Winter 1973/74 von der "Arab Oil Weapon"[23] gesprochen wurde. Das besagt aber noch nicht, daß nur ein mit Handfeuerwaffen, Bomben oder Granaten geführter Angriff ein "bewaffneter" wäre. Es mag eine Epoche im Völkerrecht gegeben haben, in der allein Handwaffen bekannt waren und als solche galten. Es war nie ein Problem, mit ihrer Erfindung und Einführung auch Distanzwaffen in den Begriff der Waffen einzubeziehen. Maßgeblich ist nicht das Mittel, sondern die Absicht, mit der es eingesetzt wird, und seine (zerstörende) Wirkung.

Man kann sich für die völkerrechtliche Bewertung nicht auf dasjenige beschränken, was etwa (und für ganz andere Zwecke) in einem nationalen Kriegswaffenkontrollgesetz aufgelistet ist[24]. Eine "Waffe" ist ein Mittel, um eine bestimmte Aufgabe zu erfüllen[25], eine gewollte Wirkung hervorzurufen[26]. Die Zerstörung von Sachen ist ebensowenig Voraussetzung; chemische und biologische Waffen, wie auch die seinerzeit diskutierte Neutronenwaffe, zerstören nicht, aber töten. Chemische und biologische Waffen sind nicht lediglich als Mittel verboten[27], ihr Einsatz wäre fraglos ein "bewaffneter" Angriff. "Bewaffnet" auch im Kontext von Art. 51 SVN kann heute nur bedeuten, ausgerüstet zu sein mit einem Mittel, das geeignet ist, einen militärischen Vorteil gegenüber dem Gegner zu erzielen und dabei zu zerstören oder zu töten[28].

---

[21] Vgl. L.T. Greenberg/S.E. Goodman/K.J. Soo Hoo, Information Warfare and International Law (1998), zitiert nach www.dodccrp./org/iwihindex.htm, dort bei Anm. 199.

[22] Randelzhofer (Anm. 5), Rn. 18. Siehe aber auch R. Zedalis, Some Thoughts on the UN Charter and the Use of Military Force Against Economic Coercion, Tulsa Law Journal 17 (1982), 487ff.

[23] Siehe J. Paust/A. Blaustein (Hrsg.), The Arab Oil Weapon (1977) sowie Shaw (Anm. 9), 783.

[24] Vgl. etwa die Kriegswaffenliste im Anhang zum Kriegswaffenkontrollgesetz (BGBl. 1990 I, 2506).

[25] Jacobson (Anm. 2), 14f.

[26] Das Oxford English Dictionary definiert "Weapon" als: "Anything used, or designed to be used, in destroying, defeating or injuring a person".

[27] Vgl. das Chemiewaffenübereinkommen vom 13.1.1993 (BGBl. 1994 II, 806) und das B-Waffenübereinkommen vom 10.4.1972 (BGBl. 1983 II, 132).

[28] So auch Jacobson (Anm. 2), 15: "Armed simply means equipped with the weapons of war".

2. Selbstverteidigung gegen Informationsoperationen?

a) Reaktionsmöglichkeiten gegenüber eindeutig identifizierbaren staatlichen Informationsoperationen

Nach herrschender Meinung schließt das Völkerrecht jede andere Selbstverteidigung als die gegen einen bewaffneten Angriff im Sinne von Art. 51 SVN aus[29]. Nur in Extremfällen soll Selbstverteidigung auch zulässig sein gegen physische Gewalt, die nicht im Einsatz der herkömmlichen militärischen Waffen besteht, deren Wirkung aber jener gleichgesetzt werden kann, die als bewaffneter Angriff das Selbstverteidigungsrecht auslöst[30].

Wenn es aber auf die "Wirkung" ankommt, dann ist nicht entscheidend, ob das eingesetzte Mittel unter den herkömmlichen Waffenbegriff fällt, solange es nur vergleichbare Schäden verursacht. Ebensowenig berechtigt nur die physische Zerstörung des Zieles zur Selbstverteidigung. Wenn der Gegner die Kraftwerke eines anderen Staates bombardiert, um landesweit die Stromversorgung lahmzulegen, wäre das ohne Frage ein bewaffneter Angriff. Auch die Zündung eines nuklearen Sprengkörpers in größerer Höhe über dem Boden, um durch einen elektromagnetischen "Schock" die Systeme auszuschalten, würde man als bewaffneten Angriff ansehen. Dann kann es aber keinen wesentlichen Unterschied machen, wenn dieses Ergebnis mittels eines Computervirus erreicht würde[31]. 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[32], die durch Einsatz von Informationstechnologie bewirkte komplette Ausschaltung der Energieversorgung oder des Finanztransfersystems aber nicht. Eine andere Frage ist, ob Folgeschäden hinzutreten müßten.

Im Grundsatz sind daher die Staaten berechtigt, auch gegen "Informationsangriffe" ihr Selbstverteidigungsrecht auszuüben, sofern nur die Wirkungen eines solchen Informationsangriffes jenen eines herkömmlichen "bewaffneten" Angriffes gleichkommen. Dies auch deshalb, weil das "naturgegebene Recht zur Selbstverteidigung" (Art. 51 SVN) nicht davon abhängt, ob das Völkerrecht ein bestimmtes neues Einwirkungsmittel schon als "Waffe" klassifiziert hat, sondern letztlich darauf abstellt, ob ein Staat und seine Einrichtungen, seine Souveränität, territoriale Unversehrtheit oder politische Unabhängigkeit[33] in massiver Weise beeinträchtigt werden. Dies ist aber nur der Grundsatz, die Schwierigkeiten stecken im Detail; sie können im vorgegebenen Rahmen nur angedeutet werden.

---

[29] Randelzhofer (Anm. 14), Rn. 10.

[30] Randelzhofer (Anm. 5), Rn. 20. Ebenso K. Hailbronner, Die Grenzen des völkerrechtlichen Gewaltverbots. Berichte der Deutschen Gesellschaft für Völkerrecht, Bd. 26 (1986), 49 (76).

[31] So auch Jacobson (Anm. 2), 3ff. und 18: "The Walls of Jericho can ... be taken down with a laptop computer".

[32] Randelzhofer (Anm. 14), Rn. 21, will allerdings "Bombardierungen" erst ab einer gewissen Intensität als "bewaffneten Angriff" werten. Die Praxis beispielsweise an der israelisch-libanesischen Grenze ist eine andere.

[33] Vgl. Art. 1 der Aggressionsdefinition (Anm. 11).

Nach wie vor gelten im Völkerrecht die sogenannten "Webster-Prinzipien", wonach Selbstverteidigungsmaßnahmen unabweisbar notwendig und verhältnismäßig sein müssen[34]. Notwendigkeit bedeutet im vorliegenden Zusammenhang, daß es zur Anwendung von "Gegengewalt" keine praktikable Alternative gibt, daß also z. B. Selbstschutzmaßnahmen ("Firewalls") einen erneuten Informationsangriff nicht abwehren können. Hier käme es auch auf die informationstechnologischen Möglichkeiten des Angegriffenen an; stehen ihm bestimmte "high-tech"-Mittel nicht zur Verfügung, präjudiziert das nicht sein Recht, mit Gegenmaßnahmen zu antworten[35].

Eine andere Frage ist, ob Informationsangriffe nur dann im Wege der Selbstverteidigung beantwortet werden dürfen, wenn nicht nur die Informationsinfrastruktur gestört oder zerstört wurde, sondern sich daraus Folgeschäden ergeben. Das wird man bejahen müssen, um die Parallele zu den Konsequenzen herkömmlicher bewaffneter Angriffe nicht zu verlieren. Maßgeblich wäre demnach, ob nach der durch Computer bewirkten Störung der Elektronik eines Kernkraftwerkes der Kern durchzuschmelzen droht, ob nach dem Ausfall der Stromversorgung im Winter Menschen zu erfrieren drohen, oder ob die Ausschaltung jeglicher Flugsicherung den Absturz von Passagierflugzeugen zur unvermeidlichen Folge hätte[36]. Das alles hätte auch eine quantitative Komponente; der Ausfall einzelner Beatmungsgeräte in Krankenhäusern würde einen massiven Gegenschlag kaum rechtfertigen.

Eine weitere Frage wäre, wie auf die computergestützte Ausschaltung der militärischen Führungs- und Verbindungssysteme geantwortet werden dürfte. Nach Art. 3 *lit.* d der Aggressionsdefinition der Generalversammlung der UN gilt "ein Angriff durch die Streitkräfte eines Staates gegen die Land-, See- oder Luftstreitkräfte oder die See- und Luftflotte eines anderen Staates" als Aggression. Ein solcher Angriff mit herkömmlichen Waffen hätte die Ausschaltung dieser Streitkräfte zum Ziel; ein Informationsangriff würde faktisch zum gleichen Resultat führen können, wenn er z. B. sämtliche Feuerleitsysteme außer Gefecht setzte. Mit anderen Worten: Wenn sich heute ein "Pearl Harbour" (das Ausschalten eines erheblichen Teiles der Flotte) auch durch einen computergestützten Informationsangriff erreichen ließe, dann müßte auch dies das Selbstverteidigungsrecht auslösen können. Möglicherweise wäre hier zu differenzieren: Soll das (evtl. nur vorübergehende) Lahmlegen der Waffenelektronik dem anderen nur seine "systemische Verwundbarkeit" verdeutlichen und ihn zu entsprechenden politischen Entscheidungen veranlassen, wäre das vielleicht nur Intervention, aber nicht Aggression[37].

---

[34] "A necessity of self-defense, instant, overwhelming, leaving no choice of mean, and no moment for consideration" (vgl. W. Meng, The Caroline, in: R. Bernhardt [Hrsg.], Encyclopedia of Public International Law, Vol. I [1992], 538). Siehe auch Kenny (Anm. 5), Rn. 18; Jacobson (Anm. 2), 11; Greenberg [*et al.*] (Anm. 21), bei dortigen Anm. 199–201.

[35] Hier gibt es eine gewisse Parallele zu der Diskussion über "smart weapons", die eine bessere Differenzierung zwischen militärischen Zielen und Kollateralschäden gewährleisten.

[36] Vgl. Jacobson (Anm. 2), 16.

[37] So auch *ibid.*, 17.

Gäbe es deutliche Hinweise darauf, daß der Informationsangriff der Vorbereitung eines Angriffs mit konventionellen Waffen diente, käme "präventive" Selbstverteidigung in Betracht[38].

Das wohl schwierigste Problem bezüglich der Verhältnismäßigkeit der Reaktion auf einen Informationsangriff ist die Frage, ob nur in der gleichen Weise, mit den gleichen (elektronischen) Mitteln geantwortet werden darf, oder auch mit herkömmlicher (kinetischer) Gewalt. Einigermaßen gesichert erscheint nur, daß ein massiver konventioneller Gegenschlag dann unverhältnismäßig wäre, wenn der Informationsangriff zwar die Informationsinfrastruktur lahmlegte, aber keine weiteren Schäden oder Zerstörungen zur Folge hätte[39]. Unter Umständen wäre dann erst der Gegenschlag eine Aggression[40]. Selbstverteidigungsmaßnahmen sollen im Verhältnis stehen zur Intensität und zum Umfang des Angriffs, um eine Eskalation des Konfliktes zu verhindern[41]. Schwierigkeiten würde dabei im vorliegenden Kontext das vom IGH im *Nicaragua*-Urteil[42] bekräftigte Prinzip bereiten, demzufolge Selbstverteidigung nicht Rache oder Strafe sein, sondern nur das Ziel verfolgen dürfe, einen Angriff zum Stehen zu bringen oder zurückzuschlagen. Auch das geht aber vom traditionellen Bild einer Invasionstruppe aus. Ein Informationsangriff wäre mit der Ausschaltung der gegnerischen Rechnersysteme beendet, es gäbe nichts mehr zu stoppen, zurückzuschlagen oder aus dem Territorium zu drängen. Dennoch muß auch hier eine Reaktion zulässig sein, und sei es nur, um von Wiederholungen abzuschrecken. Sie sollte nach Möglichkeit mit den gleichen Mitteln ("in kind")[43] erfolgen.

Fehlten dem Angegriffenen aber die technologischen Mittel, um auf einen Informationsangriff in gleicher Weise zu reagieren, oder gäbe es bei dem als solchen identifizierten Aggressor[44] keine Ziele für einen Informationsangriff, oder nur solche, deren Ausschaltung unverhältnismäßig wäre[45], dann dürfte – immer im Rahmen der Verhältnismäßigkeit – auch konventionell militärisch reagiert werden.

Unter verschiedenen Aspekten würden Informationsangriffe und ihre Abwehr auch das schon für herkömmliche bewaffnete Angriffe im geltenden Völkerrecht umstrittene Recht auf präventive Selbstverteidigung berühren[46]. Präventive bzw. antizipierte Selbstverteidigung bedeutet, daß ein Staat nicht als "sitting duck" abwarten muß, bis ein bewaffneter Angriff tatsächlich beginnt, wenn alle Anzeichen (objektiv) darauf hindeuten, daß er unmittelbar bevorsteht. In der Theorie ist ein solches Recht wohl anerkannt, in den Fällen, in denen es in Anspruch genom-

---

38 Näher dazu sogleich unten.
39 Greenberg [*et al.*] (Anm. 21), bei dortiger Anm. 202.
40 *Ibid.*, Executive Summary.
41 Kenny (Anm. 5), Rn. 23.
42 *Nicaragua*-Urteil (Anm. 13), 94 (§ 176).
43 Greenberg [*et al.*] (Anm. 21), bei dortiger Anm. 203.
44 Vgl. dazu unten II.2.b).
45 Vgl. Greenberg [*et al.*] (Anm. 21), bei dortiger Anm. 204.
46 Siehe dazu Randelzhofer (Anm. 14), Rn. 34f., Kenny (Anm. 5), Rn. 11.

men wurde, ist allerdings oft das unmittelbare Bevorstehen eines Angriffs in Abrede gestellt worden[47].

Bezüglich eines Informationsangriffes würde sich beispielsweise die Frage stellen, ob die großangelegte Störung oder Ausschaltung der militärischen Führungs- und Verbindungssysteme als hinreichendes Anzeichen dafür gewertet werden könnte, daß ein konventioneller Angriff unmittelbar bevorsteht, oder ob weitere Anhaltspunkte (z.B. Mobilmachung, Truppenkonzentration in Grenznähe) hinzukommen müßten. Da präventive Selbstverteidigung eine an strikt auszulegende Voraussetzungen gebundene Ausnahme ist, spricht mehr für die zweite Alternative.

Eine weitere Frage wäre, ob und wie gegen einen als unmittelbar bevorstehend vermuteten Informationsangriff als solchen präventive Verteidigung zulässig sein könnte. Wie dürfte ein Staat reagieren, der feststellt, daß wiederholt und systematisch, aber bisher noch ohne Störung oder Zerstörung, sondern eher als Test in seine sicherheitsrelevante Informationsinfrastruktur eingedrungen wurde? Darf er – sofern der Eindringling identifiziert werden konnte – dessen Informationsinfrastruktur so stören oder zerstören, daß ein größerer Informationsangriff nicht mehr möglich wäre? Darf er dazu auch konventionelle Gewalt einsetzen? Dürfte er Informationsinfrastruktur im Eigentum Dritter stören oder zerstören, die für die Test-Eingriffe benutzt wurde? Hier würde wohl mehr dafür sprechen, den betroffenen Staat auf passive Schutzmaßnahmen zu beschränken, weil nicht mit der notwendigen Sicherheit gesagt werden könnte, ob das testweise Eindringen der Vorbereitung eines Angriffs oder doch nur der Ausforschung (Spionage) diente.

b) Maßnahmen gegenüber "Unbeteiligten"?

Allgemein wird davon ausgegangen, daß es – wenn auch nicht unmöglich – so doch zumeist sehr schwierig sein würde, den Urheber eines Informationsangriffes zu identifizieren[48]. Oft sei nicht einmal mit hinreichender Sicherheit feststellbar, ob die Störung oder der Ausfall eines Computersystems Folge eines Eingriffs von außen oder eines Software-Fehlers sei[49]. Für das Völkerrecht stellt sich hier die Frage, welcher Grad an Sicherheit bei der Identifizierung eines Angreifers erreicht sein muß, damit der Angegriffene reagieren kann, und ob Reaktionen zulässig wären gegen einen "unbeteiligten" Dritten, dessen Ressourcen lediglich zur Durchleitung benutzt wurden.

Zunächst erscheint unstreitig, daß der vom Eingriff betroffene Staat nach dem im Völkerrecht anerkannten "Wirkungsprinzip" auf einen von fremdem Territorium ausgehenden Akt auch dann reagieren darf, wenn der Eingriff nicht die

---

[47] Vgl. Resolution 488 des UN-Sicherheitsrates vom 19.6.1981 zur Bombardierung des irakischen Atomreaktors Osiraq durch Israel.

[48] Siehe Greenberg [*et al.*] (Anm. 21), Kap. 3; Jacobson (Anm. 2), 8; Kanuck (Anm. 4), 287.

[49] Greenberg [*et al.*] (Anm. 21), Kap. 3.

Intensität einer Aggression erreicht, nicht einmal eine verbotene Intervention darstellt, oder einem anderen Staat zuzurechnen ist[50]. Selbstverteidigung mittels Anwendung von Gewalt ist aber fraglos nur zulässig gegen einen zweifelsfrei identifizierten Aggressor. Zwar soll ein Übergreifen auf fremdes Staatsgebiet zur Abwehr eines bewaffneten Angriffs selbst dann erlaubt sein, wenn der Angriff dem Staat, von dessen Gebiet er ausgeht, nicht zugerechnet werden kann, z.B. wenn feindliche Streitkräfte von neutralem Gebiet aus einen bewaffneten Angriff unternehmen, den der neutrale Staat zu unterbinden nicht fähig oder willens ist[51]. Hier wäre eine Parallele zum Informationsangriff aber allenfalls dann zu ziehen, wenn der "neutrale" Staat in kollusivem Zusammenwirken bewußt an der Verschleierung der Herkunft eines Informationsangriffes mitwirkt. In den meisten Fällen wird er nicht nur nicht verhindern können, daß ein Informationsangriff über seine Rechner oder Satelliten geleitet wird, sondern er wird es gar nicht wissen. Überdies geht nach der Durchleitung von seinem Gebiet oder seiner Informationsstruktur kein Angriff mehr aus, der bekämpft werden könnte[52]. Lediglich im Ausnahmefall eines entschuldigenden bzw. rechtfertigenden Notstandes ("necessity"[53]), d.h. bei extremer Gefährdung lebenswichtiger Interessen eines Staates, könnte der Eingriff in Rechtspositionen oder Ressourcen eines an sich unbeteiligten anderen Staates dem Vorwurf der Völkerrechtswidrigkeit entgehen[54]. Würden z.B. Informationsangriffe (durch wen und woher auch immer) auf die Steuerungselektronik von Kernkraftwerken die dringende Gefahr eines größeren Nuklearunfalles heraufbeschwören, und würden sie mit Masse und ohne dessen Zutun oder Wissen über die Rechner eines bestimmten Staates geführt, so könnte die Ausschaltung dieser Rechner durch den bedrohten Staat unter Umständen gerechtfertigt sein[55].

c) Reaktionsmöglichkeiten auf Angriffe "Privater"

Werden Angriffe auf die zivile oder militärische Informationsinfrastruktur eines Staates nicht durch fremde Staatsorgane geführt, sondern durch "Private" (z.B. Terroristen), die vom fremden Staatsgebiet aus operieren, so hängt das zulässige Maß einer Abwehr zunächst davon ab, ob diese Angriffe dem Staat zugerechnet werden können, von dessen Territorium sie ausgehen.

---

[50] Vgl. dazu auch Kanuck (Anm. 4), 287.

[51] Randelzhofer (Anm. 14), Rn. 28 mit weiteren Nachweisen.

[52] Skeptisch gegenüber Maßnahmen gegen "Neutrale" auch Greenberg [*et al.*] (Anm. 21), bei dortiger Anm. 203.

[53] Vgl. Art. 33 der ILC Draft Articles on State Responsibility, ILM 37 (1998), 442.

[54] Vgl. dazu M. Schröder, in: Graf Vitzthum (Hrsg.), Völkerrecht (1997), 539, Rn. 27 mit weiteren Nachweisen zu den insoweit noch sehr umstrittenen Regeln für die Staatenverantwortlichkeit.

[55] Es gehört allerdings zu den Charakteristika des Netzes, daß sich die Informationen oder Teile davon unterschiedliche Wege suchen und auf den verschiedensten Umwegen geschickt werden können, so daß die Zerstörung einzelner Knotenpunkte als weder geeignet noch verhältnismäßig erscheinen könnte.

Zunächst ist daran zu erinnern, daß das Entsenden (privater) bewaffneter Banden oder Gruppen durch oder im Namen eines Staates, die dann Gewaltakte gegen einen anderen Staat ausführen, als Aggression gilt, wenn diese Gewaltakte die Intensität der anderen beispielhaft in der UN-Aggressionsdefinition[56] genannten Aggressionsformen erreichen. Soweit auch Informationsangriffe als Aggression angesehen werden können, käme es hier dann auf die Schwere der dadurch bewirkten Schäden an. Ob die bloße Duldung von Informationsangriffen seitens Privater die Verantwortlichkeit des Territorialstaates auslösen könnte, erscheint fraglich[57]. Grundsätzlich ist ein Staat für Handlungen, die Private auf oder von seinem Hoheitsgebiet aus begehen, nicht verantwortlich[58], es sei denn, es träfe ihn eine besondere Schutzpflicht. Eine solche Schutzpflicht wird z.B. angenommen für diplomatisches Personal[59], für Ausländer gegen systematische Übergriffe oder allgemein bezüglich der Einhaltung von Verpflichtungen aus internationalen Menschenrechtsinstrumenten[60]. Für die Informationsinfrastruktur eines Staates haben die anderen Staaten ebensowenig eine Schutzpflicht wie für andere staatliche Einrichtungen. Dies würde sich erst ändern, wenn Cyberspace durch völkervertragliche Einigung – vergleichbar dem Weltraum und den Himmelskörpern[61] – zum geschützten internationalen Raum würde[62], nicht nur mit Handlungsverboten für die Vertragsstaaten, sondern auch entsprechenden Schutzpflichten.

Selbst wenn man annehmen wollte, daß alle Staaten verantwortlich sind für schädigende Handlungen Privater, die von ihrem Territorium ausgehen, sofern sie diese Handlungen bei Anwendung üblicher Sorgfalt ("due diligence") hätten verhindern können[63], wäre fraglich, ob man es einem Staat vorwerfen könnte, daß er Informationsangriffe nicht entdeckt und unterbunden hat, die von seinem Hoheitsgebiet ausgehen oder nur durchgeleitet werden.

3. Zwischenergebnis

Es sprechen keine stichhaltigen Gründe dagegen, auch Informationstechnologie als "Waffe" im völkerrechtlich relevanten Sinne anzusehen, wenn ihr so beabsichtigter Einsatz Schäden an zivilen oder militärischen Zielen hervorriefe, die jenen vergleichbar wären, die durch herkömmliche Waffen bewirkt würden. Eine dagegen geübte Selbstverteidigung dürfte sich – außer im Falle des extremen Notstan-

---

[56] Oben Anm. 11.

[57] Vgl. K. Doehring, Völkerrecht (1999), Rn. 832.

[58] Schröder (Anm. 54), 538 Rn. 25.

[59] Vgl. die Entscheidung des IGH im *Teheraner Geisel*-Fall, ICJ Reports 1980, 3 (28).

[60] Vgl. G. Sperduti, Responsibility of States for Activities of Private Law Persons, in: R. Bernhardt (Hrsg.), Encyclopedia of Public International Law, Inst. 10 (1987), 373.

[61] Vgl. den Weltraumvertrag vom 27.1.1967, BGBl. 1969 II, 1967.

[62] Vgl. dazu den Vorschlag von J.A. Graham, Der virtuelle Raum – sein völkerrechtlicher Status, JurPC (Internet-Zeitschrift für Rechtsinformatik), Web-Doc. 35/1999 (www.jura.uni-sb.de/jurpc/aufsatz/19990035.htm).

[63] Zur "Due Diligence" siehe H. Blomeyer-Bartenstein, Due Diligence, in: Bernhardt (Anm. 34), 1110.

des – nur gegen den zweifelsfrei ermittelten "Aggressor" richten und hätte die Gebote der Notwendigkeit und Verhältnismäßigkeit zu beachten. Ginge der Informationsangriff von Privaten aus, wäre Selbstverteidigung dagegen nur bei entsprechender Verantwortlichkeit des Territorialstaates zulässig, die nach dem jeweils geltenden Völkerrecht zu ermitteln wäre. Selbstverteidigung wäre nicht grundsätzlich auf den "Informationsangriff" beschränkt, der Einsatz konventioneller militärischer Gewalt wäre aber wohl nur verhältnismäßig, wenn der vorausgegangene Informationsangriff erhebliche physische Folgeschäden zeitigte oder mit an Sicherheit grenzender Wahrscheinlichkeit einem unmittelbar bevorstehenden konventionellen Angriff den Weg ebnen sollte.

Staaten, die gegen einen Informationsangriff mit Informations- oder konventionellen Operationen reagieren, sollten sich über zwei Dinge im klaren sein: Jede Informationsoperation, die sie als "quasi-bewaffneten Angriff" bewerten, wäre auch ihnen künftig als "Ersteinsatz" versagt. Und die Ausübung der Selbstverteidigung gegen einen Informationsangriff (jedenfalls mit konventioneller militärischer Gewalt) würde zunächst von einer Reihe von Staaten als Verletzung von Völkergewohnheitsrecht gerügt werden; sie wäre aber auch ein Schritt auf dem Wege zur Bildung neuen bzw. veränderten Völkergewohnheitsrechts[64].

Gerade was Informationsangriffe durch "Private" betrifft, wäre es angezeigt, durch völkerrechtlichen Vertrag Cyberspace entweder zum international geschützten Bereich zu erklären[65], oder aber die Informationsinfrastruktur – wie die zivile Luftfahrt – durch entsprechende Konventionen in die international-strafrechtliche Obhut der Staaten zu geben[66]; dann würde auch die Duldung von Informationsangriffen seitens Privater die Staatenverantwortlichkeit auslösen.

III. Informationsoperationen unterhalb der Schwelle des Einsatzes bewaffneter Gewalt

Bei Informationsoperationen unterhalb der Schwelle des Einsatzes bewaffneter Gewalt i.S.v. Art. 2 Ziff. 4 SVN ist zu erörtern, ob diese Maßnahmen gegen das Interventionsverbot verstoßen und welche Gegenmaßnahmen zulässig sind. Das völkerrechtliche Interventionsverbot untersagt alle Versuche, einen anderen Staat unterhalb der Schwelle bewaffneter Gewalt Zwang auszusetzen, um zu erreichen, daß er die Ausübung seiner souveränen Rechte einem fremden Willen unterordnet[67]. Die Subsumtion unter diesen weiten Obersatz bringt nur selten eindeutige Ergebnisse hervor. Es ist daher zu prüfen, ob es weitere Rechtssätze gibt, an denen

---

64 Vgl. dazu auch Greenberg [*et al.*] (Anm. 21), Conclusion: Resolution of Legal Ambiguities.

65 Vgl. Graham (Anm. 62), Abs. 38ff.

66 Vgl. das Übereinkommen vom 23.9.1971 zur Bekämpfung widerrechtlicher Handlungen gegen die Sicherheit der Zivilluftfahrt (BGBl. 1977 II, 1229). Siehe Greenberg [*et al.*] (Anm. 21), Conclusion: Protection of Critical Systems.

67 Vgl. allgemein U. Beyerlin, Intervention, Prohibition of, in: Wolfrum (Anm. 5), 805ff., und T. Oppermann, Intervention, in: R. Bernhardt (Hrsg.), Encyclopedia of Public International Law, Vol. II (1995), 1436ff.

Informationsoperationen in Friedenszeiten zu messen sind. Dabei ist zu unterscheiden zwischen Informationsoperationen, die gegen die informationstechnische Infrastruktur gerichtet sind und solchen, die eine inhaltliche Ausrichtung haben, wie etwa die Verunsicherung der Bevölkerung durch Desinformation.

Technisch ausgerichtete Informationsoperationen können sowohl die nationale als auch die grenzüberschreitende informationstechnische Infrastruktur beeinträchtigen. Letztere genießt in der Regel den Schutz besonderer völkerrechtlicher Vereinbarungen, darunter die Konvention zum Schutz von unterseeischen Kabeln[68], die Konstitution und Konvention der Internationalen Fernmeldeunion (ITU)[69] (einschließlich des von der ITU gesetzten Rechts) und die Verträge zur Gründung der verschiedenen Satellitenorganisationen (INTELSAT[70], INMARSAT[71] und EUTELSAT[72]). Zu beachten sind aber auch die weltraumrechtlichen Abkommen[73] und solche des grenzüberschreitenden Medienrechts[74]. In bezug auf den Schutz der nationalen Infrastruktur spielt dann das völkerrechtliche Interventionsverbot eine zentrale Rolle.

1. Der vertragliche Schutz grenzüberschreitender Informationsinfrastruktur

a) Festinstallierte Einrichtungen

Nach Art. 2 des Übereinkommens zum Schutz von unterseeischen Kabeln aus dem Jahre 1884 stellt jeder Vertragsstaat das vorsätzliche oder fahrlässige Beschädigen eines Kabels unter Strafe und sieht eine privatrechtliche Ersatzpflicht für Schäden an Kabeln wie auch für jene Nachteile vor, die aus der Vermeidung solcher Schäden entstehen[75]. Geschützt sind alle rechtmäßig, also mit einer etwa erforderlichen staatlichen oder sonstigen Genehmigung verlegten Kabel, die auf dem Hoheitsgebiet eines Vertragsstaats landen. Der Vertrag enthält detaillierte Bestimmungen über Maßnahmen bei Vertragsverletzungen. Nicht anwendbar sind die Bestimmungen des Übereinkommens während eines bewaffneten Konflikts (Art. 15)[76].

---

[68] RGBl. 1884, 151.

[69] Konstitution der Internationalen Fernmeldeunion, BGBl. 1996 II, 1316; Konvention der Internationalen Fernmeldeunion, BGBl. 1996 II, 1340. Die beiden Vereinbarungen lösen den Internationalen Fernmeldevertrag in den bis dahin geltenden Fassungen ab.

[70] BGBl. 1973 II, 250; BGBl. 1997 II, 538; BGBl. 1998 II, 1743.

[71] BGBl. 1979 II, 1081; BGBl. 1988 II, 511; BGBl. 1991 II, 451.

[72] BGBl. 1984 II, 683; BGBl. 1997 II, 696; BGBl. 1998 II, 1739.

[73] Zu nennen sind hier der Weltraumvertrag aus dem Jahre 1967 (Anm. 61) und der Mondvertrag aus dem Jahre 1979 (UN GA Res. 43/68, Annex).

[74] Darunter etwa das Übereinkommen des Europarats über grenzüberschreitendes Fernsehen aus dem Jahre 1989 (BGBl. 1994 II, 639).

[75] S. dazu R. Lagoni, Cables, Submarine, in: Bernhardt (Anm. 34), 516 (518f.).

[76] Vgl. dazu etwa die Praxis während des Ersten Weltkriegs, illustriert bei Jacobson (Anm. 2), dortige Anm. 63.

Die in Art. 2 des Übereinkommens von 1884 enthaltene Verpflichtung fand sowohl in die Genfer Konvention über das Regime der Hohen See von 1958[77] (Art. 27) als auch in das Seerechtsübereinkommen der Vereinten Nationen von 1982[78] (Art. 113) Eingang. Art. 113 des Seerechtsübereinkommens bezieht sich allerdings nicht nur auf Telegrafen- oder Fernsprechverbindungen, sondern darüber hinaus auch auf Rohrleitungen und Hochspannungskabel. Im Gegensatz zu Art. 10 des Übereinkommens von 1884 enthält keines der späteren Abkommen besondere Betretensrechte für Kriegsschiffe (vgl. Art. 110 des Seerechtsübereinkommens).

Festinstallierte grenzüberschreitende Einrichtungen (etwa Telegraphenkabel und andere Überlandleitungen) setzen regelmäßig eine zwischenstaatliche Einigung über deren Installation, die technischen Eigenschaften der entsprechenden Leitungen und die Nutzungsrechte voraus. Eine solche Einigung kann einzelfallbezogen oder – wie im Fall der Konstitution und Konvention der internationalen Fernmeldeunion[79] – allgemein erzielt werden. Vor dem Hintergrund des in Art. 33 der ITU-Konstitution enthaltenen Rechts der Öffentlichkeit auf Benutzung des internationalen Fernmeldedienstes verpflichten sich die Mitglieder der Fernmeldeunion in Art. 38 Abs. 1 der Konstitution dazu, "alle zweckdienlichen Maßnahmen (zu treffen), um die Übertragungswege und Einrichtungen, die zur Sicherstellung eines schnellen und ununterbrochenen Nachrichtenaustausches im internationalen Fernmeldeverkehr notwendig sind, in der technisch besten Weise zu erstellen". Die Einrichtungen müssen – "soweit wie möglich" – "in gutem Betriebszustand und auf dem Stand des wissenschaftlichen und technischen Fortschritts gehalten werden" (Art. 38 Abs. 2 der Konstitution). Insbesondere sorgen die Mitglieder innerhalb ihrer Zuständigkeit "für den Schutz dieser Übertragungswege und Einrichtungen" und für die "Instandhaltung der ihrer Kontrollbefugnis unterliegenden Teilstrecken von internationalen Fernmeldeverbindungen" (Art. 38 Abs. 3 und 4 der Konstitution). Fernmeldeverkehr im Sinne der Konstitution ist "jede Übermittlung, jede Aussendung oder jeder Empfang von Zeichen, Signalen, Schriftzeichen, Bildern, Lauten oder Nachrichten jeder Art über Draht, Funk, optische oder andere elektromagnetische Systeme" (Anlage zur Konvention). Damit sind auch moderne Formen der Telekommunikation erfaßt.

Die so umschriebene staatliche Verantwortung könnte in der Folge der zunehmenden Privatisierung der Dienstleistung Telekommunikation ausgehöhlt werden. Dem ist aber nicht so. Art. 6 Abs. 1 der Konstitution stellt zunächst sicher, daß sämtliche von den Vertragsparteien eingerichteten Fernmeldestellen und von ihnen betriebenen Funkstellen mit grenzüberschreitender Ausrichtung die Verpflichtungen aus den Grundsatzdokumenten der ITU zu beachten haben. Lediglich Funk-

---

[77] BGBl. 1972 II, 1089; abgelöst vom Seerechtsübereinkommen.

[78] BGBl. 1994 II, 1799.

[79] Zur Internationalen Fernmeldeunion vgl. G. Nolte, International Telecommunication Union, in: Bernhardt (Anm. 67), 1379ff.; zu neueren Entwicklungen vgl. auch F. Lyall, The Role of the International Telecommunication Union, in: G. Lafferranderie (Hrsg.), Outlook on Space Law over the Next 30 Years (1997), 253ff.

anlagen für die nationale Verteidigung unterliegen nach Art. 48 der Konstitution besonderen Regeln[80]. Festzuhalten ist, daß sich diese Bestimmung allerdings nur auf den Fernmeldeverkehr mit Hilfe von Funkwellen bezieht[81] und daß diese Anlagen, soweit sie am öffentlichen Nachrichtenaustausch oder an anderen vom Sekundärrecht der Organisation geregelten Diensten teilnehmen, "im allgemeinen nach den für diese Dienste geltenden Bestimmungen betrieben werden" müssen (Art. 48 Abs. 3 der Konstitution). Hinsichtlich privater Betreiber sind die Mitglieder nach Art. 6 Abs. 2 der Konstitution verpflichtet, die Beachtung sowohl der ITU-Grundsatzdokumente als auch der Vollzugsordnungen sicherzustellen.

b) Nicht leitungsgebundene Telekommunikationseinrichtungen

Im Unterschied zur leitungsgebundenen Telekommunikation setzt die nicht leitungsgebundene Telekommunikation jedenfalls im Grundsatz keine Vereinbarung zwischen sendenden und empfangenden Staaten voraus. Allerdings sind beispielsweise Fragen der Frequenzzuteilung und der Zuteilung von Positionen des geostationären Orbits vertraglich geregelt[82]. Informationsoperationen in Friedenszeiten können die damit verbundenen Rechtspositionen verletzen und daher – vorbehaltlich besonderer Rechtfertigungen – als völkerrechtswidrig zu qualifizieren sein.

Abgesehen von den oben dargelegten allgemeinen Bestimmungen über den Fernmeldedienst sind die ITU-Vertragsparteien verpflichtet, ihre Funkstellen so zu betreiben, daß sie keine schädlichen Störungen der Funkverbindungen oder -dienste bei den übrigen Mitgliedern verursachen (Art. 45). Dies ist auch mit Blick auf private Dienstleister sicherzustellen. Selbst militärische Funkanlagen sind nicht völlig ausgenommen (Art. 48 Abs. 2 der Konstitution)[83]. Falsche und irreführende Zeichen sind zu verhindern (Art. 47), und das Fernmeldegeheimnis ist – vorbehaltlich der in Art. 34 enthaltenen besonderen sicherheitsbedingten Eingriffsbefugnisse – zu wahren (Art. 37). Die Verpflichtung, die Telekommunikation anderer Staaten nicht zu beeinträchtigen, wird im Seerechtsübereinkommen für bestimmte Situationen weiter präzisiert. So sind Handlungen, "die auf die Störung eines Nachrichtenübermittlungssystems oder anderer Einrichtungen oder Anlagen des Küstenstaates gerichtet" sind, mit dem Recht der friedlichen Durchfahrt nicht zu vereinbaren (Art. 19 Abs. 2 k des Seerechtsübereinkommens). Darüber hinaus

[80] Art. 48 Abs. 1 beläßt den Mitgliedern "ihre volle Freiheit in bezug auf militärische Funkanlagen". Nach Abs. 2 müssen "beim Betreiben dieser Anlagen soweit wie möglich die Bestimmungen, welche die Hilfeleistung in Notfällen und die Maßnahmen zur Verhütung schädlicher Störungen betreffen, sowie die Bestimmungen der Vollzugsordnungen über die Sendearten und Frequenzen, die je nach Art des betreffenden Funkdienstes zu benutzen sind, beachtet werden". Zu Abs. 3 vgl. sogleich.

[81] Dazu unten III.1.b).

[82] Vgl. dazu E. Dahinden, Die rechtlichen Aspekte des Satellitenrundfunks (1990), 185ff.

[83] Zur Vorgängerregelung vgl. R.D. Scott, Legal Aspects of Information Warfare: Military Disruption of Telecommunications, Naval Law Review XLV (1998), 57 (62f.). Vgl. auch Aldrich (Anm. 4), bei dortigen Anm. 72ff.

haben sich die Staaten verpflichtet, nicht genehmigte, von der ausschließlichen Wirtschaftszone eines Staates oder der Hohen See ausgehende Rundfunksendungen zu bekämpfen (Art. 58 Abs. 2 und 109 des Seerechtsübereinkommens)[84].

Im übrigen sind die weltraumrechtlichen Vereinbarungen zu beachten. So gewährleistet der Weltraumvertrag aus dem Jahre 1967 zwar bestimmte Freiheiten (Art. I), enthält aber auch nutzungsbezogene Beschränkungen. Art. IV Abs. 1 untersagt militärische Aktivitäten insoweit, als es sich um das Verbringen und Stationieren von mit Kernwaffen oder anderen Massenvernichtungswaffen bestückten Weltraumobjekten in eine Erdumlaufbahn oder auf einem Himmelskörper handelt. Darüber hinaus formuliert Art. IV Abs. 2 ein Gebot der Nutzung von Himmelskörpern zu ausschließlich friedlichen Zwecken. Dieses Gebot spart den sonstigen Weltraum, einschließlich der Erdumlaufbahnen, aus. Entscheidend für die Beurteilung der Zulässigkeit von Informationsoperationen im Weltraum ist, was unter "friedlichen Zwecken" zu verstehen ist. Während von den sozialistischen Staaten früher die These vertreten wurde, dies schließe eine wie auch immer geartete militärische Nutzung des Weltraums aus, dürfte heute insoweit Einigkeit bestehen, daß der Begriff "friedlich" aufgrund der durch Art. III des Weltraumvertrages gesicherten Anwendung des Art. 51 SVN im Sinne von "nicht-aggressiv" zu verstehen ist[85]. Auch Informationsoperationen für militärische Zwecke verstoßen daher nicht *per se* gegen den Weltraumvertrag. Unproblematisch ist dies, soweit Rüstungskontrollverträge zumindest implizit die nationale Satellitenverifikation anerkennen[86]. Was die militärische Aufklärung aus dem Weltraum im übrigen betrifft, so hilft die nicht verbindliche Resolution der Generalversammlung der Vereinten Nationen zu den Fernerkundungsprinzipien aus dem Jahre 1986[87] nicht wesentlich weiter. Unabhängig davon, ob man hinsichtlich der militärischen Satellitenaufklärung auf positives Gewohnheitsrecht abstellt oder nicht, wird man jedenfalls konstatieren können, daß sie grundsätzlich erlaubt ist, auch wenn es "keine den zulässigen Rahmen absteckende oder inhaltlich ausfüllende vertragliche Regelung gibt"[88].

Insgesamt haben sich damit insbesondere, aber nicht nur die Vertragsstaaten der ITU-Konstitution zu einem umfassenden Schutz der internationalen informationstechnischen Infrastruktur verpflichtet. Informationsoperationen in Friedens-

---

[84] Vgl. hierzu auch das Europäische Übereinkommen vom 22.1.1965 zur Verhütung von Rundfunksendungen, die von Sendestellen außerhalb der staatlichen Hoheitsgebiete gesendet werden (BGBl. 1969 II, 1939).

[85] H. Fischer, in: K. Ipsen (Hrsg.), Völkerrecht (3. Aufl. 1990), 780f. Rn. 34; vgl. auch K.-H. Böckstiegel, Die Nutzung des Weltraums – Allgemeine Grundsätze, in: *id.* (Hrsg.), Handbuch des Weltraumrechts (1991), 265 (270), und W. von Kries, Die militärische Nutzung des Weltraums, in: Böckstiegel (*ibid.*), 307ff. Siehe auch Aldrich (Anm. 4), bei dortigen Anm. 58f.

[86] Vgl. nur Art. XII des ABM-Vertrages (Deutsche Übersetzung bei G. Fahl, Internationales Recht der Rüstungsbeschränkung [Loseblatt-Sammlung], Ziff. 8.2.1.), Art. XV des KSE-Vertrags (BGBl. 1991 II, 1154), Art. IV Abs. 5 und 6 des Vertrags über ein umfassendes Verbot von Nuklearversuchen von 1996 (BGBl. 1998 II, 1211). Allgemein vgl. auch J.H. Wallner, Konventionelle Rüstungskontrolle und Fernerkundung in Europa (1995).

[87] Res. 41/65 vom 3.12.1986.

[88] von Kries (Anm. 85), 343.

zeiten, die auf eine Beeinträchtigung oder gar Zerstörung von Teilen dieser Infrastruktur hinauslaufen, dürften daher vorbehaltlich anderer Rechtfertigungsgründe als völkerrechtswidrig zu qualifizieren sein[89]. Es werden allerdings Zweifel an der Durchsetzbarkeit und tatsächlichen Durchsetzung dieser Bestimmungen geäußert[90]. Diese Sorge ist letztlich nicht begründet. Zwar trifft es zu, daß die Organe der ITU weniger Aufsichtsfunktionen als vielmehr Koordinationsaufgaben wahrnehmen und außerdem über keinerlei zentrale Rechtsdurchsetzungsmechanismen verfügen. Die Staaten respektieren die übernommenen Verpflichtungen aber im Zweifelsfall schon deshalb, weil sie sicherstellen wollen, daß ihre eigene Telekommunikation in gleicher Weise geschützt wird.

Neben der ITU-Konstitution und -Konvention verdienen auch die Vereinbarungen zur Gründung und zum Betrieb der Satellitenorganisationen INTELSAT, INMARSAT und EUTELSAT Beachtung. Bei diesen Vereinbarungen stellt sich die Frage, ob und gegebenenfalls in welchem Umfang die von diesen Organisationen zur Verfügung gestellten Weltraumsegmente für die Durchführung von Informationsoperationen genutzt werden können.

INTELSAT[91] wurde 1971 gegründet und ist die weltweit bedeutendste Institution für die Nachrichtenübermittlung durch Satelliten. Ihr Hauptzweck liegt in der Bereitstellung sogenannter Weltraumsegmente. Dazu gehören nicht nur Fernmeldesatelliten, sondern auch die für ihren Betrieb erforderlichen Einrichtungen und Ausrüstungsgegenstände. Die Bereitstellung der im Eigentum von INTELSAT befindlichen Weltraumsegmente erfolgt auf kommerzieller Basis unter Beachtung des Grundsatzes der Nichtdiskriminierung (Art. III a). INTELSAT stellt sicher, daß die Nutzung der Weltraumtechnik für den Informationsaustausch nicht auf die Weltraummächte beschränkt ist. Mit INMARSAT[92] wurde 1976 eine weitere Satellitenorganisation gegründet, deren Ziel die Verbesserung der Nachrichtenverbindungen für die Schiffahrt ist. Seit 1985 betreibt INMARSAT auch Fernmeldesatelliten für den Flugverkehr. EUTELSAT schließlich wurde 1982 als regionale Organisation gegründet[93].

Die rechtlichen Grundlagen aller drei Organisationen sind miteinander vergleichbar. Es handelt sich jeweils um einen Gründungsvertrag mit Anhängen und ein Betriebsübereinkommen, das die näheren Einzelheiten der Bereitstellung der Weltraumsegmente regelt.

Art. III des INTELSAT-Übereinkommens legt als Hauptzweck der Organisation die Bereitstellung "internationaler öffentlicher Fernmeldedienste" fest. Das INTELSAT-Weltraumsegment kann zwar auch für "internationale oder nationale

---

[89] Rechtlich stellen diese Bestimmungen eine Schranke für die Durchführung von Informationsoperationen in Friedenszeiten dar; im Fall eines bewaffneten Konflikts sind sie nicht anwendbar. Vgl. Greenberg [*et al.*] (Anm. 21), bei dortiger Anm. 44 mit weiteren Nachweisen.

[90] *Ibid.*, bei dortigen Anm. 44ff.

[91] Näher dazu J. Fawcett, Intelsat, in: Bernhardt (Anm. 67), 1000ff. mit Addendum 1992 (G. Schuster).

[92] Vgl. J. Fawcett, Inmarsat, in: Bernhardt, *ibid.*, 991ff. mit Addendum 1992 (G. Schuster).

[93] S. dazu R. Wolfrum, Eutelsat, in: Bernhardt, *ibid.*, 300ff.

Sonderfernmeldedienste" benutzt werden, allerdings ausdrücklich nicht für "militärische Zwecke" (Art. III d). Unabhängig vom INTELSAT-Weltraumsegment kann INTELSAT Satelliten oder damit zusammenhängende Einrichtungen auch für Sonderfernmeldedienste bereitstellen, wiederum allerdings ausdrücklich nicht für "militärische Zwecke". Damit bleibt festzuhalten, daß INTELSAT-Einrichtungen nicht für militärische Zwecke zur Verfügung gestellt werden können. Wie Art. XIV g ausdrücklich klarstellt, findet das Übereinkommen allerdings keine Anwendung auf von INTELSAT unabhängige Weltraumsegmenteinrichtungen, die ausschließlich für Zwecke der nationalen Sicherheit bestimmt sind.

Im Vergleich zu INTELSAT enthält das INMARSAT-Übereinkommen eine zwar allgemeinere, aber auch weichere Nutzungsbeschränkung. Art. 3 Abs. 3 bestimmt: "Die Organisation wird nur für friedliche Zwecke tätig". Wie das INTELSAT-Übereinkommen so steht auch das INMARSAT-Übereinkommen der Nutzung von INMARSAT unabhängiger Weltraumsegmenteinrichtungen nicht entgegen, die ausschließlich für Zwecke der nationalen Sicherheit bestimmt sind (Art. 8 Abs. 5). Die Beschränkung auf friedliche Zwecke im INMARSAT-Übereinkommen schließt bestimmte militärische Nutzungen nicht aus. Dies ist schon in der Vergangenheit von INMARSAT selbst so gehandhabt worden. So waren Kriegsschiffe in Friedenszeiten nicht von der Nutzung von INMARSAT-Einrichtungen ausgeschlossen. Während eines bewaffneten Konflikts konnten INMARSAT-Einrichtungen darüber hinaus etwa für Notrufe oder bestimmte humanitäre Zwecke genutzt werden[94]. Darüber hinaus wird man die Nutzung von INMARSAT-Einrichtungen durch von den Vereinten Nationen autorisierte Streitkräfte auch dann für zulässig erachten können, wenn diese in Kampfhandlungen verwickelt werden sollten. Dies ergibt sich nicht allein aus der in Art. 27 des INMARSAT-Übereinkommens enthaltenen Kooperationsverpflichtung gegenüber den Vereinten Nationen oder der in Art. 12 Abs. 1 b enthaltenen Verpflichtung auf die Ziele und Grundsätze der SVN, sondern vor allem daraus, daß von den Vereinten Nationen autorisierte friedenserhaltende oder friedensschaffende Maßnahmen friedlichen Zwecken im Sinne von Art. 3 Abs. 3 des INMARSAT-Übereinkommens dienen[95]. Darüber hinausgehend wird heute die Auffassung vertreten, daß die Nutzung von INMARSAT-Einrichtungen für Maßnahmen der Selbstverteidigung im Rahmen von Art. 51 SVN zulässig ist – und zwar sowohl im internationalen als auch im internen bewaffneten Konflikt[96]. Die hierfür vorgetragenen Argumente können bei einer restriktiven Interpretation des Rechts auf Selbstverteidigung durchaus überzeugen. Insbesondere greift hier der Verweis auf die Ziele der Vereinten Nationen, wie er in der Satzung enthalten ist.

Die im EUTELSAT-Übereinkommen enthaltenen Bestimmungen entsprechen hinsichtlich der Nutzungsbeschränkung weitgehend denen des INTELSAT-Über-

---

94 Vgl. dazu die Nachweise bei W.D. von Norden, Inmarsat Use by Armed Forces: A Question of Treaty Interpretation, Journal of Space Law 23 (1995), 1 (2f.). Vgl. auch Aldrich (Anm. 4), bei dortigen Anm. 60f.

95 So zutreffend von Norden, *ibid.*, 4ff.

96 *Ibid.*, 8ff.

einkommens und schließen die Nutzung für militärische Zwecke aus (Art. III e und f). Ebenso wird wiederum klargestellt, daß die Bestimmungen keine Anwendung auf den Erwerb von anderen Weltraumeinrichtungen finden, die "ausschließlich für Zwecke der nationalen Sicherheit bestimmt sind" (Art. XVI c(ii)).

Festzuhalten ist damit zunächst, daß militärische Informationsoperationen nicht unter Nutzung von INTELSAT- oder EUTELSAT-Einrichtungen durchgeführt werden dürfen. Etwas anderes gilt für die Nutzung von INMARSAT-Einrichtungen. Diese dürfen insoweit für Informationsoperationen genutzt werden, als letztere von Art. 3 Abs. 3 des INMARSAT-Übereinkommens gedeckt sind, also friedlichen Zwecken dienen. Dementsprechend sind in der Vergangenheit INMARSAT-Ressourcen etwa von VN-autorisierten Streitkräften in Somalia, Bosnien und Kroatien genutzt worden[97].

Die hier erörterten Übereinkommen bieten allerdings keinen rechtlichen Schutz vor Informationsoperationen durch Nicht-Vertragsparteien – und selbst die Vertragsstaaten dürften nur aufgrund der zwischen ihnen bestehenden allgemeinen Treuepflichten daran gehindert sein, Einrichtungen von INTELSAT, INMARSAT oder EUTELSAT durch Informationsoperationen zu schädigen. Dies läßt sich auch Art. 26 WVK entnehmen, wonach ein in Kraft getretener Vertrag von den Vertragsparteien nach Treu und Glauben zu erfüllen ist.

c) Sonstige völkerrechtliche Vereinbarungen

Selbstverständlich müssen Informationsoperationen unterhalb der Schwelle des Einsatzes bewaffneter Gewalt auch weitere einschlägige völkerrechtliche Vereinbarungen respektieren, etwa medienrechtliche Abkommen wie das Übereinkommen des Europarats über grenzüberschreitendes Fernsehen aus dem Jahre 1989[98]. Bedingt durch die Vielzahl ineinandergreifender unterschiedlicher vertraglicher Regime gestalten sich die völkerrechtlichen Rahmenbedingungen für Informationsoperationen in Friedenszeiten ausgesprochen komplex. Eindeutige Aussagen zur Zulässigkeit bestimmter Maßnahmen lassen sich nur unter Berücksichtigung des gesamten Regelwerks treffen. Dies sollte jedenfalls bei rechtlich zweifelhaften Maßnahmen zur Vorsicht gemahnen[99].

2. Der gewohnheitsrechtliche Schutz der nationalen Informationsinfrastruktur

Unterhalb der Schwelle bewaffneter Gewalt schützt das Völkerrecht die territoriale Integrität und die staatliche Handlungsfreiheit durch das Schädigungsverbot

---

[97] Nachweise im einzelnen bei R.A. Morgan, Military Use of Commercial Communications Satellites: A New Look at the Outer Space Treaty & "Peaceful Purposes", Georgetown University Law Center, December 1993 (nachgewiesen bei von Norden, *ibid.*, dortige Anm. 3).

[98] Oben Anm. 74.

[99] Scott (Anm. 83), 58: "The legal conditions applicable to the use of such a weapon, particularly during peace operations, are extremely complex".

und das Interventionsverbot. Hinter beiden steht die staatliche Souveränität, wie sie vor allem in Art. 2 Ziff. 1 SVN im Grundsatz der souveränen Gleichheit der Staaten ihren Niederschlag gefunden hat.

a) Das Schädigungsverbot

Das im völkerrechtlichen Nachbarrecht entwickelte Schädigungsverbot (*sic utere tuo ut alienum non laedas*) gehört als allgemeiner Rechtsgrundsatz zum universellen Völkerrecht[100]. Auch wenn es vor allem im Umweltvölkerrecht Anwendung gefunden hat, so ist es nicht auf dieses beschränkt. Es schützt den Staat vor schädlichen Fremdeinwirkungen und untersagt entsprechende Beeinträchtigungen der territorialen Integrität. In Anbetracht der zentralen Bedeutung der Informationsinfrastruktur und der damit zusammenhängenden Verwundbarkeit der Staaten[101] ist eine Verletzung der Informationsinfrastruktur unabhängig davon, ob sie mit elektronischen Mitteln oder anderweitig durchgeführt wird, einer solchen der territorialen Integrität gleichzusetzen. Allerdings können nicht nur offensive Informationsoperationen das Schädigungsverbot verletzen. Auch rein defensive Informationsoperationen, die nur auf dem Territorium des eigenen Staates durchgeführt werden, können durchaus (unbeabsichtigte) Auswirkungen auf dem Territorium eines benachbarten Staates haben und würden dann gegen das Schädigungsverbot verstoßen.

Ein Staat darf nämlich zwar im Prinzip sein Territorium und seine eigene Informationsinfrastruktur nach Belieben nutzen. Er hat aber nicht das Recht, dies in einem Maße tun, das einen anderen Staat in der Nutzung seiner Informationsinfrastruktur erheblich beeinträchtigt. Bislang nimmt das Nachbarrecht unerhebliche Beeinträchtigungen vom Schädigungsverbot aus[102], wobei allerdings kein Konsens über die Höhe der Schwelle der Erheblichkeit besteht. Insbesondere hat es sich immer wieder als schwierig erwiesen, die Kriterien für den Erheblichkeitsmaßstab festzulegen.

Die Anwendung des nachbarrechtlichen Schädigungsverbots auf Informationsoperationen wirft neben der Frage nach der staatlichen Pflicht, bestimmte private Aktivitäten zu unterbinden, das Problem auf, ob das Schädigungsverbot nicht im Bereich besonders risikobehafteter Tätigkeiten mittlerweile weiterentwickelt worden ist, insbesondere ob eine Pflicht zur Risikovorsorge, zur Information und zur Zusammenarbeit bei Störfällen und zur schonenden Nutzung gemeinsamer Ressourcen besteht. Die zuletzt genannten Fragen werden gegenwärtig vor allem im Umweltvölkerrecht diskutiert. Sie scheinen aber auch in Fragen der modernen Kommunikationstechnik von Bedeutung zu sein. Soweit das Internet etwa nicht

---

100 W. Graf Vitzthum, in: ders. (Anm. 54), 459 Rn. 95.

101 M.E. Bowman, Is International Law Ready for the Information Age?, Fordham International Law Journal 19 (1996), 1935 (1937ff.).

102 Vgl. für das Umweltvölkerrecht U. Beyerlin, Grenzüberschreitender Umweltschutz und allgemeines Völkerrecht, in: FS Karl Doehring (1989), 38ff.

der Verfügungsgewalt eines Staates zugerechnet werden kann[103] – und daran dürften abgesehen von bestimmten Elementen der Infrastruktur grundsätzlich keine Zweifel bestehen –, könnte man von einer gemeinsamen Ressource sprechen, hinsichtlich derer die Pflicht zur schonenden Nutzung besteht. Über Störfälle, die grenzüberschreitende Konsequenzen haben können, müßten Nachbarstaaten gegebenenfalls nicht nur informiert, sondern auch konsultiert werden. Man wird zum gegenwärtigen Zeitpunkt allerdings noch keine eindeutigen, über das Schädigungsverbot hinausgehenden Aussagen treffen können.

b) Das Interventionsverbot

Das Interventionsverbot liegt gleichsam zwischen dem Schädigungsverbot und dem Gewaltverbot. Es untersagt die gegen einen Staat gerichtete Drohung mit anderen empfindlichen Übeln als bewaffneter Gewalt und ist insoweit deutlich vom Gewaltverbot zu unterscheiden. Vom Schädigungsverbot unterscheidet es sich insoweit, als das Interventionsverbot mehr oder weniger gezielte Einwirkungen auf einen anderen Staat unterbinden will, nicht dagegen Auswirkungen, die sich aus der an sich zulässigen Nutzung eigener Ressourcen ergeben.

Das zwischenstaatliche Interventionsverbot ist in der Charta der Vereinten Nationen nicht ausdrücklich geregelt. Insbesondere enthält Art. 2 Ziff. 7 SVN kein solches Verbot, da sich diese Bestimmung nur an die Organisation richtet. Demgegenüber können Art. 1 Ziff. 2 und Art. 2 Ziff. 1 SVN zur Begründung eines zwischenstaatlichen Interventionsverbots herangezogen werden. Das Interventionsverbot hat durch eine Reihe von Resolutionen der Generalversammlung der Vereinten Nationen eine weitere Ausgestaltung erfahren, die im Kernbereich jedenfalls als Gewohnheitsrecht angesehen werden kann[104]. Dabei geht es um einen normativen Ausgleich zwischen der staatlichen Souveränität und der wachsenden zwischenstaatlichen Interdependenz, die im Zusammenhang mit den neueren Entwicklungen in der Kommunikationstechnologie besonders deutlich wird.

Einen wichtigen Schritt zur Präzisierung des zwischenstaatlichen Interventionsverbots bildete die 1965 von der Generalversammlung der Vereinten Nationen angenommene Deklaration über die Unzulässigkeit der Intervention in die inneren Angelegenheiten der Staaten[105]. Der wesentliche Inhalt dieser Resolution fand Eingang in die sogenannte "Friendly Relations"-Deklaration[106]. Dort heißt es, daß "(b)ewaffnete Intervention und jede andere Form der Einmischung oder versuchten Bedrohung der Persönlichkeit des Staates oder seiner politischen, wirtschaftlichen und kulturellen Elemente ... Verletzungen des Völkerrechts dar(stellen). Kein Staat darf wirtschaftliche, politische oder andere Mittel gebrauchen oder den Gebrauch solcher Mittel unterstützen, um einen anderen Staat zu zwingen,

---

[103] Bowman (Anm. 101), 1937ff.
[104] Zu den Einzelheiten vgl. Fischer (Anm. 85), 897ff. Rn. 52ff.
[105] Res. 2131(XX).
[106] Vgl. oben Anm. 10.

die Ausübung seiner souveränen Rechte ihm zu unterwerfen oder sich von ihm irgendwelche anderen Vorteile zu sichern". Die Erklärung ist zwar nicht als solche verbindlich, dokumentiert jedoch die für die Existenz eines entsprechenden Gewohnheitsrechtssatzes erforderliche *opinio iuris*[107]. Dies hat der IGH im *Nicaragua*-Fall bestätigt[108]. Demgegenüber kann und muß an dieser Stelle die 1981 von den blockfreien Staaten durchgesetzte Annahme einer neuen Deklaration über die Unzulässigkeit der Intervention und Einmischung in die inneren Angelegenheiten der Staaten[109] außer Betracht bleiben. Diese Resolution fand nicht die Zustimmung der westlichen Staaten, weil in ihr u. a. der Kampf gegen Intervention durch "falsche oder verzerrte Nachrichten" und das Verbot der Ausbeutung und verzerrten Darstellung von Menschenrechtsproblemen zur Druckausübung auf andere Staaten enthalten waren.

Schutzobjekt des Interventionsverbots ist entsprechend der Formulierung der "Friendly Relations"-Deklaration die Gesamtheit der "political, economic, social and cultural systems" eines Staates, allerdings nur insoweit, als diese Angelegenheiten nicht durch Verträge oder Gewohnheitsrecht aus dem "domaine réservé" ausgeschieden sind[110].

Informationsoperationen, die sich gegen die Informationsinfrastruktur eines Staates richten, nicht die Schwelle verbotener Gewalt überschreiten und auch nicht vom Schädigungsverbot erfaßt werden, können im Regelfall als verbotene Intervention qualifiziert werden, denn die Infrastruktur fällt in den nationaler Jurisdiktion vorbehaltenen und damit vom Interventionsverbot geschützten Bereich. Dies gilt auch, soweit die Informationsoperationen andere Ziele haben, sich aber der Informationsinfrastruktur bedienen, letztere also nur stören, nicht aber zerstören. Etwas anderes würde nur dann gelten, wenn die Informationsoperationen in Übereinstimmung mit vertraglich oder gewohnheitsrechtlich fixierten Regeln durchgeführt werden. Näher spezifizierte Regeln dieses Inhalts sind allerdings gegenwärtig nicht ersichtlich[111].

Nicht näher einzugehen ist an dieser Stelle auf physische Eingriffe, die schon die territoriale Integrität eines Staates verletzen. Deren Völkerrechtswidrigkeit ist unzweifelhaft.

Komplizierter stellt sich die Lage dar, wenn Informationsoperationen eine inhaltliche Ausrichtung haben. Früher hat man hier vor allem an Radio- und Fernsehsendungen gedacht, aber auch an das Abwerfen von Flugblättern und ähnliche Maßnahmen. Im Zeitalter des Internets können diese Maßnahmen noch ganz andere Formen annehmen. So wäre etwa die bloße Bereitstellung entsprechender

---

[107] Für eine differenzierte Analyse des rechtlichen Charakters der Deklaration vgl. H. Neuhold, Internationale Konflikte – verbotene und erlaubte Mittel ihrer Austragung (1977), 51f. mit weiteren Nachweisen; vgl. auch G. Arangio-Ruiz, Friendly Relations Resolution, in: Berrnhardt (Anm. 67), 485 (487).

[108] *Nicaragua*-Urteil (Anm. 13), 106 (§202).

[109] Res. 36/103.

[110] B. Simma, Das Problem des grenzüberschreitenden Informationsflusses und des "domaine réservé", Berichte der Deutschen Gesellschaft für Völkerrecht, Bd. 19 (1979), 39 (66).

[111] Vgl. auch Kanuck (Anm. 4), 290f.

Informationen auf einer Homepage oder die Mitteilung über Newsgroups und Mailing-Listen denkbar, alles Maßnahmen, die auf das eigene Territorium beschränkt wären, allerdings aufgrund der Struktur des Internets weltweit abgerufen werden könnten. In Anbetracht des damit verbundenen Auseinanderfallens von "online phenomenon" und "physical location"[112] scheint es ausgeschlossen, die völkerrechtliche Beurteilung dieser Maßnahme allein von der Wahl des Handlungs- oder Wirkungsortes abhängig zu machen. Unter Berücksichtigung des "Wirkungsprinzips" dürfte die völkerrechtliche Beurteilung einer solchen Maßnahme, wenn sie denn auch auf den betroffenen Staat zielt, allein von der Zielsetzung der Maßnahme abhängen.

Dabei ist nicht nur zwischen der verbotenen Intervention und zulässiger politischer Einflußnahme zu unterscheiden. Vielmehr kommt es entscheidend auch auf die menschenrechtlichen Gewährleistungen in Sachen Informationsfreiheit an. Diese dürften jedenfalls den staatlicher Jurisdiktion vorbehaltenen Bereich radikal reduziert haben[113]. Die einschlägigen Abkommen garantieren dem einzelnen Bürger das Recht, Informationen zu suchen, zu empfangen und weiterzuverbreiten. Zwar sehen sie auch Einschränkungen vor. Dabei muß es sich aber um gesetzlich vorgesehene Regelungen handeln, die dem Schutz der nationalen Sicherheit, der öffentlichen Ordnung und der Achtung der Rechte anderer dienen. Es dürfte heute unumstritten sein, daß Informationsoperationen, die lediglich auf eine umfassende Information des einzelnen Bürgers – auch im Ausland – zielen, jedenfalls nicht als völkerrechtswidrige Intervention angesehen werden können. Eine andere Frage ist es, inwieweit ein Staat aufgrund der Einschränkungsmöglichkeiten der menschenrechtlichen Vereinbarungen seinen eigenen Bürgern den Informationszugang erschwert. Für Fernmeldeverbindungen gilt darüber hinaus die entsprechende Eingriffsbefugnis aus Art. 34 der ITU-Konstitution. Dort heißt es, daß die Mitglieder "jede ... private Fernmeldeverbindung ... unterbrechen (können), die als für die Sicherheit des Staates gefährlich oder als seinen Gesetzen, der öffentlichen Ordnung oder den guten Sitten zuwiderlaufend erscheinen kann".

Zielen Informationsoperationen dagegen auf die politische Beeinflussung des Adressaten, dann rückt die Abgrenzung von Interzession und Intervention in den Mittelpunkt. Dabei geht es um die Frage, wann "persuasion" in "coercion" umschlägt[114]. Hiervon hängt die völkerrechtliche Beurteilung entsprechender Informationsoperationen ab.

Gerade im Zusammenhang von Informationsoperationen dürfte die ohnehin schwierig zu bestimmende Grenze zwischen Interzession und Intervention weitere Probleme aufwerfen, denn nicht alle Formen der Einflußnahme auf fremde Staaten sind völkerrechtswidrig. Dies sind sie nur dann, wenn die angewandten

---

[112] D.R. Johnson/D. Post, Law and Borders – The Rise of Law in Cyberspace, Stanford Law Review 48 (1996), 1358 (1370); Bowman (Anm. 101), 1944.

[113] Vgl. insoweit schon J.A. Frowein, Das Problem des grenzüberschreitenden Informationsflusses und des "domaine réservé", Berichte der Deutschen Gesellschaft für Völkerrecht, Bd. 19 (1979), 1 (18ff.) und die eingehende Untersuchung von Dahinden (Anm. 82), 136ff.

[114] Simma (Anm. 110), 68.

Mittel und Methoden die Grenze vom erlaubten politischen Druck zum unerlaubten Zwang überschreiten. Allerdings sind weder in der Staatenpraxis noch in der Lehre bislang Kriterien entwickelt worden, die eine überzeugende Unterscheidung ermöglichen. Zweifelsohne darf die Schwelle des Interventionsverbotes nicht zu niedrig ansetzen, wenn dieses Verbot überhaupt ernst genommen werden soll. Vorgeschlagen wurde, daß die Schwelle erst überschritten ist, wenn "an action ... has such a massive impact on the victim state so as to coerce it in vital matters of its internal order or its foreign policy into behaviours which it would not have chosen in free self-determination as an independent and sovereign state"[115]. Aber auch hier bleibt weiter Ungewißheit, ob das Interventionsverbot tatsächlich nur im Falle der Beeinträchtigung vitaler staatlicher Interessen greifen kann und wie diese Interessen dann zu bestimmen sind.

3. Handlungen "Privater"

Grundsätzlich muß der Staat nur für Völkerrechtsverletzungen einstehen, die durch seine Organe entstehen[116]. Rechtsverletzungen, die Privatpersonen begehen, liegen regelmäßig außerhalb der Staatenverantwortlichkeit. Die Staaten haben nur für diese einzustehen, wenn ihnen diesbezüglich eigenes Fehlverhalten vorgehalten werden kann. Häufig wird es dabei um ein Unterlassen gehen, etwa in der Gestalt, daß der Staat nicht die den Umständen nach gebotene Sorgfalt aufgewendet hat, um private Übergriffe auf Rechte fremder Staaten zu verhindern, oder er unterläßt es, die privaten Rechtsbrecher zu verfolgen und zu bestrafen[117]. Eine staatliche Verantwortlichkeit kommt aber auch in Betracht, wenn der Staat private Unrechtstatbestände positiv unterstützt oder gefördert hat[118].

In einer Reihe von schon erörterten vertraglichen Vereinbarungen sind staatliche Handlungspflichten zur Verhinderung bestimmter privater Aktivitäten enthalten. Schon das Übereinkommen zum Schutz von unterseeischen Kabeln aus dem Jahre 1884 verpflichtet die Vertragsparteien, das vorsätzliche oder fahrlässige Beschädigen eines Kabels unter Strafe zu stellen. Entsprechendes gilt auch nach dem Seerechtsübereinkommen. Art. 6 Abs. 2 der ITU-Konstitution verpflichtet die Vertragsstaaten, die Beachtung sowohl der ITU-Grundsatzdokumente als auch der Vollzugsordnungen seitens privater Betreiber sicherzustellen[119]. Kommt eine Vertragspartei diesen Verpflichtungen nicht nach, so wird sie völkerrechtlich verantwortlich. Auch das gewohnheitsrechtliche Schädigungsverbot beinhaltet eine Pflicht des Staates, die territoriale Integrität des Nachbarstaates schädigende Maßnahmen Privater zu unterbinden oder auf ein unterhalb der Erheblichkeit liegendes Maß zu reduzieren. Schließlich wird in der "Friendly Relations"-Deklaration die staatliche Pflicht formuliert, das eigene Territorium nicht zur Operationsbasis

---

115 Beyerlin (Anm. 67), 809.
116 Schröder (Anm. 54), 538 Rn. 25.
117 K. Ipsen, in: ders. (Anm. 85), 517ff. Rn. 30ff.
118 Vgl. dazu die Entscheidung des IGH im *Teheraner Geisel*-Fall (Anm. 59), 31f.
119 Vgl. dazu oben III.1.a) und III.1.b).

Privater gegen fremde Staaten werden zu lassen. Es heißt dort, daß kein Staat den Gebrauch wirtschaftlicher, politischer oder anderer Mittel unterstützen darf, um einen anderen Staat zu einem bestimmten Verhalten zu zwingen. "Auch soll kein Staat subversive, terroristische oder bewaffnete Handlungen organisieren, unterstützen, schüren, finanzieren, anstiften oder dulden, die auf den gewaltsamen Sturz des Regimes eines anderen Staates abzielen, oder sich in Bürgerkriege eines anderen Staates einmischen".

Mit Blick auf von Privaten durchgeführte Informationsoperationen wird man auf der Grundlage dieser Rechtsnormen regelmäßig zu einer staatlichen Verantwortlichkeit kommen, wenn der Staat nicht die erforderliche Sorgfalt bei der Überwachung Privater hat walten lassen[120]. Dies gilt nicht nur für terroristische Gewalttaten, die mittels moderner Kommunikationstechnik ausgeübt werden[121]. Das Interventionsverbot wäre auch verletzt, wenn Private in völkerrechtswidriger Weise Aufständische mittels moderner Kommunikationstechnologie unterstützen. Schließlich wird man davon ausgehen müssen, daß eine entsprechende Aufsichts- und Verhinderungspflicht auch in bezug auf die normale Computerkriminalität besteht, die allerdings nicht Gegenstand dieser Studie ist. Schwachpunkt der hierauf gestützten staatlichen Verantwortlichkeit ist – abgesehen von den wenigen vertraglichen Verhinderungspflichten – die mangelnde Präzision der gewohnheitsrechtlichen Grundlagen. Es wäre vor diesem Hintergrund begrüßenswert, wenn sich die Staaten auf völkerrechtliche Vereinbarungen zur Bekämpfung von Kriminalität im Bereich der Telekommunikation, insbesondere auch zur Bekämpfung terroristischer Gewalttaten verständigen könnten.

4. Gegenmaßnahmen

Ohne Zweifel kann ein Staat seine Informationsinfrastruktur auf seinem Territorium auf jede technisch mögliche Art gegen Eingriffe schützen. Fraglich ist, wie der von Informationsoperationen unterhalb der Schwelle des Einsatzes bewaffneter Gewalt betroffene Staat mit Wirkung über sein Territorium hinaus auf derartige Maßnahmen reagieren kann.

a) Repressalien

Die Repressalie ist ein an sich völkerrechtswidriger Akt, der als Antwort auf einen erlittenen Unrechtsakt gerechtfertigt ist. Mit der Repressalie wird das Ziel verfolgt, die Rückkehr des Verletzerstaates zum Recht zu erreichen[122].

Da die Repressalie an vorangegangenes rechtswidriges Tun anknüpft, muß der von Informationsoperationen betroffene Staat zunächst diese Maßnahmen recht-

---

[120] Zum Sorgfaltsmaßstab vgl. oben II.2.c), insbesondere Anm. 63.

[121] Zum Problem terroristischer Informationsoperationen vgl. auch G. Rattray, The Emerging Global Information Infrastructure and National Security, The Fletcher Forum of World Affairs 21 (1997), 81 (84, dortige Anm. 17); Kanuck (Anm. 4), 284, dortige Anm. 57.

[122] Vgl. dazu Fischer (Anm. 85), 894 Rn. 45.

lich bewerten. Schwierigkeiten können sich zum einen daraus ergeben, daß nicht eindeutig feststellbar ist, ob ein technischer Defekt oder ein Eingriff von außen vorliegt[123]. Zum anderen ist der Urheber solcher Maßnahmen im allgemeinen sehr schwierig zu identifizieren. Da der die Repressalie ergreifende Staat regelmäßig die Beweislast für das tatsächliche Vorliegen einer Rechtsverletzung trägt[124], wird im folgenden noch zu klären sein, wie hoch die Anforderungen an die Identifizierung des Störers sind und ob gegebenenfalls auch Maßnahmen gegenüber "Unbeteiligten" zulässig sind. Darüber hinaus stellt sich die Frage, ob der reaktive Charakter der Repressalie ihre Anwendung in Situationen ausschließt, in denen Informationsoperationen unmittelbar bevorstehen. Dies ist nicht der Fall, sofern etwa die Drohung mit Informationsoperationen selbst einen Verstoß gegen das Interventionsverbot darstellt. Es handelt sich dann nämlich um keine präventiv-antizipatorische Maßnahme, sondern um eine Reaktion auf einen vorverlagerten Unrechtstatbestand[125].

Nicht jede Maßnahme ist als Repressalie zulässig. Nach heute herrschender Meinung schließt das Völkerrecht gewaltsame Repressalien aus. Damit ist nicht jede Form von Gewalt gemeint, sondern bewaffnete Gewalt im Sinne von Art. 2 Ziff. 4 SVN. Insoweit ist auf die obigen Ausführungen zu verweisen[126]. Darüber hinaus ist aber auch nicht jede Form der gewaltfreien Repressalie zulässig, sondern nur solche Maßnahmen, die dem Proportionalitätsgrundsatz genügen. Ob dieser allerdings so strikt zu handhaben ist, wie er im *Naulilaa*-Schiedsspruch von 1928 formuliert wurde[127], wird heute bezweifelt[128], denn der Schiedsspruch betraf die damals grundsätzlich zulässige gewaltsame Repressalie. Zueinander ins Verhältnis zu setzen sind die völkerrechtswidrig ausgeübten Informationsoperationen und die vom betroffenen Staat ergriffene Repressalie samt den von beiden jeweils ausgelösten Folgen. Soweit es sich nicht um die Verletzung von im Äquivalenzverhältnis stehenden Verpflichtungen handelt, müssen die Schwere der Primärrechtsverletzung und das Ziel der Gegenmaßnahme einbezogen werden. Zweifelsohne handelt es sich dabei um einen sehr allgemeinen Maßstab[129], der vorsichtig zu handhaben ist. Der Gegenmaßnahmen ergreifende Staat genießt allerdings insoweit einen gewissen Spielraum, als das Völkerrecht nicht das Erfordernis positiver Verhältnismäßigkeit enthält, sondern nur den Ausschluß der Unverhältnismäßig-

123 Vgl. dazu schon oben II.2.b).

124 E. Klein, Gegenmaßnahmen, Berichte der Deutschen Gesellschaft für Völkerrecht, Bd. 37 (1998), 39 (46f.).

125 Zutreffend Klein, *ibid.*, 47.

126 Vgl. oben II.1.

127 RIAA 2 (1949), 1011 (1025 und 1027).

128 Vgl. nur Klein (Anm. 124), 61.

129 Kritisch etwa R. Higgins, Problems and Process. International Law and How We Use It (1995), 236.

keit[130]. Unzutreffend ist daher die Auffassung, daß Repressalien nur bei evidenten Rechtsbrüchen zulässig sein sollen[131].

Eine weitere Einschränkung der Repressalie folgt aus ihrem Beugezwang-Charakter. Sie soll den Verletzerstaat veranlassen, den Völkerrechtsverstoß zu beenden und – sofern dies damit gleichzusetzen ist – seine völkerrechtlichen Pflichten zu erfüllen. Dies setzt voraus, daß der Verletzerstaat weiß, welche Ansprüche gegen ihn verfolgt werden. Der Anspruch muß daher zuvor geltend gemacht werden. Der von Informationsoperationen betroffene Staat muß also den tatsächlichen oder vermeintlichen Schädiger auffordern, die schädigenden Handlungen einzustellen. Außerdem müssen die Gegenmaßnahmen selbst eingestellt werden, wenn der Verletzerstaat zum Recht zurückgekehrt ist. Schließlich darf die Repressalie auch keine nicht wieder rückgängig zu machenden Tatsachen schaffen. Sie soll nämlich nur zur Rückkehr zum "Normal-Recht" veranlassen[132].

Zweifelsohne wird es für die Staaten in Anbetracht der engen Voraussetzungen immer schwieriger, Repressalien zu verhängen. Dies gilt insbesondere für Repressalien, deren Ausgangspunkt eine Verletzung der Informationsinfrastruktur oder vergleichbare Maßnahmen darstellen. Hier geht es nämlich darum, nicht nur zielgerichtet, sondern auch zeitnah zu reagieren. Es ist zweifelhaft, ob beides mit der Repressalie erreicht werden kann.

b) Retorsion, Reziprozitätsregel und sonstige Maßnahmen der Selbsthilfe

Der von Informationsoperationen betroffene Staat ist in seinen Reaktionen nicht auf die Möglichkeit der Repressalie beschränkt. Das Völkerrecht kennt noch eine Reihe weiterer Gegenmaßnahmen, die hier nicht alle im einzelnen erörtert werden können.

Eine besonders naheliegende, weil regelmäßig rechtlich unproblematische Gegenmaßnahme ist die sogenannte Retorsion. Dabei handelt es sich um eine dem Völkerrecht nicht widersprechende, aber unfreundliche Handlung[133]. Solche Maßnahmen, etwa die Nichtverlängerung eines Vertrages, die Aussetzung von Vertragsverhandlungen, die Einstellung rechtlich nicht veranlaßter finanzieller oder anderer Hiflsleistungen oder gar die Ausweisung von Diplomaten, sind nicht wirkungslos. Im Gegenteil: Im Zeitalter wirtschaftlicher Interdependenzen und wechselseitiger informationstechnischer Abhängigkeit können Retorsionsmaßnahmen durchaus ein taugliches Mittel gegen Informationsoperationen unterhalb der Schwelle des Einsatzes bewaffneter Gewalt sein.

Zweifelhaft ist demgegenüber die behauptete Existenz einer allgemeinen Reziprozitätsregel. Danach soll der verletzte Staat die Erfüllung seiner Verpflichtungen

---

[130] Vgl. dazu nur den *Naulilaa*-Schiedsspruch (Anm. 127), 1028; Schiedsspruch betreffend das amerikanisch-französische Luftverkehrsabkommen, ILR 54, 331 (Ziff. 83); vgl. auch Art. 49 des ILC-Entwurfs zur Staatenverantwortlichkeit.

[131] So aber A. Bleckmann, Gedanken zur Repressalie, in: FS Schlochauer (1981), 193 (213).

[132] Klein (Anm. 124), 59.

[133] Schröder (Anm. 54), 573f. Rn. 102f.

suspendieren können, wenn diese Verpflichtungen der (zuerst) gebrochenen Verpflichtung entsprechen oder unmittelbar mit ihr verbunden sind. Sinnvoll ist die Behauptung einer solchen Regel nur, wenn sie sich in den Voraussetzungen von der Repressalie unterscheidet. So wird denn vor allem auf bestimmte einschränkende Voraussetzungen der Repressalie verzichtet, insbesondere solle die Reziprozitätsregel sofortige gleichartige Gegenmaßnahmen erlauben. Dies überzeugt letztlich nicht. Vielmehr dürfte das Konzept einer voraussetzungslosen Reziprozität "ein gefährlicher Rückschritt gegenüber dem geltenden Recht"[134] sein. Soweit aber keine von der Repressalie abweichenden Voraussetzungen formuliert werden, handelt es sich bei der Reziprozität weniger um eine Regel als vielmehr um ein Prinzip, um einen Rechtsgedanken, der letztlich auch der Repressalie und der Retorsion zugrunde liegt[135].

Weitere Möglichkeiten der Selbsthilfe lassen sich schwerlich klassifizieren. Der Begriff der Selbsthilfe ist ohnehin äußerst unbestimmt[136].

Soweit ein völkerrechtlicher Vertrag spezielle Regelungen über Gegenmaßnahmen enthält, wird man davon ausgehen müssen, daß der von Informationsoperationen betroffene Staat zunächst diese Maßnahmen ergreifen muß, auch wenn es sich nicht um ein sogenanntes "self-contained regime" handelt. Darüber hinaus kann man mit guten Argumenten verlangen, daß der betroffene Staat vor dem Ergreifen einseitiger Gegenmaßnahmen Verhandlungen mit dem Verletzerstaat durchzuführen sucht oder gegebenenfalls Dritte einschaltet. Diese Regel gilt allerdings nur eingeschränkt. Denn in keinem Fall kann es dem von Informationsoperationen betroffenen Staat verwehrt sein, unbedingt erforderliche wirksame Maßnahmen zu ergreifen. Andernfalls würde der Rechtsbruch des Verletzerstaates auch noch prämiert[137].

c) Anforderungen an die Identifizierung des Störers

Es ist schon dargelegt worden, daß die Identifizierung des Störers ausgesprochen schwierig sein kann[138]. Ebenso wie im Fall der als bewaffneter Angriff zu qualifizierenden Maßnahmen stellt sich hier die Frage, welches Maß an Sicherheit bei der Identifizierung eines Störers erreicht sein muß, um Gegenmaßnahmen zu ergreifen – und vor allem, welche Gegenmaßnahmen dann im Einzelfall zulässig sind. Die an die Identifizierung zu stellenden Anforderungen dürften sich zum

---

[134] B. Simma, Grundfragen der Staatenverantwortlichkeit in der Arbeit der International Law Commission, AVR 24 (1986), 357 (395).

[135] P. Malanczuk, Zur Repressalie im Entwurf der International Law Commission zur Staatenverantwortlichkeit, ZaöRV 45 (1985), 293 (315).

[136] Vgl. B.-O. Bryde, Self-Help, in: R. Bernhardt (Hrsg.), Encyclopedia of Public International Law, Inst. 4 (1982), 215ff. Zu Maßnahmen der staatlichen Selbsterhaltung allgemein vgl. Doehring (Anm. 57), 318ff. Rn. 757ff.

[137] So Klein (Anm. 124), 60; auch unter Berufung auf C. Tomuschat, Are Counter-Measures Subject to Prior Dispute Settlement Procedures?, EJIL 5 (1994), 77 (84ff.).

[138] Vgl. oben II.2.b).

einen nach der Schwere der Störung richten, zum anderen aber auch nach der Qualität der in Aussicht genommenen Gegenmaßnahmen.

Im Fall einer Retorsion oder eines anderen völkerrechtlich unbedenklichen Aktes als Gegenmaßnahme dürfte die Identifizierung des Störers rechtlich unerheblich, politisch allerdings sehr wohl von Bedeutung sein.

Greift der Opferstaat zur Repressalie, so sind die Anforderungen an die Identifizierung des Störers entsprechend hoch. Denn mit der Repressalie ist stets ein einseitiger Eingriff in Rechtspositionen des Ziel-Staates verbunden. Im Verhältnis zwischen den beiden Staaten muß es deshalb darum gehen, wer das Risiko einer falschen Identifizierung trägt. Dies ist – wie oben schon deutlich gemacht wurde – letztlich eine Frage der objektiven Beweislast, die regelmäßig dem die Repressalie ergreifenden Staat auferlegt ist. Er muß das tatsächliche Vorliegen einer Rechtsverletzung beweisen, wozu auch die Identität des Rechtsverletzers gehört. Kann er dies nicht – und ergreift er gleichwohl Gegenmaßnahmen, so wird er die Folgen seiner Fehleinschätzung auch dann tragen müssen, wenn letztere auf einem unvermeidbaren Irrtum beruhte[139]. Lediglich im Fall eines entschuldigenden bzw. rechtfertigenden Notstandes im Sinne von Art. 33 des ILC-Entwurfs zur Staatenverantwortlichkeit[140] könnte ein solcher Irrtum dazu führen, daß der Eingriff in Rechtspositionen oder Ressourcen eines an sich unbeteiligten anderen Staates dem Vorwurf der Völkerrechtswidrigkeit entgeht.

Des weiteren ist festzustellen, daß sich eine zulässige Repressalie nicht gegen das Medium selbst richten muß, von dem die Maßnahme ausgeht. Sie muß sich gegen den Staat richten, dem die entsprechende Maßnahme zuzurechnen ist. Welches Rechtsgut dieses Staates dann aber konkret Gegenstand der Repressalie wird, ist dem verletzten Staat überlassen[141]. Er kann, muß aber nicht auf das Medium selbst zugreifen. Voraussetzung ist lediglich, daß er dabei die übrigen Rechtmäßigkeitsvoraussetzungen der Repressalie beachtet.

Eine Eskalation von Maßnahmen ist zulässig, sofern der Staat die Rechtsverletzungen nicht einstellt oder unterbindet. Hierbei sind allerdings der Grundsatz der Verhältnismäßigkeit und vor allem das Gewaltverbot zu beachten. So ist ein Staat etwa nicht darauf beschränkt, auf eine völkerrechtswidrige Rundfunksendung ebenfalls mit einer entsprechenden Sendung zu reagieren. Er kann vielmehr versuchen, den Empfang entsprechender Sendungen auf seinem Territorium durch technisches Stören ("Jamming") zu verhindern[142].

Des weiteren gilt, daß Drittstaaten im Fall zulässiger Repressalien lediglich faktische negative Auswirkungen einer solchen Gegenmaßnahme hinnehmen müssen[143]. Dieser Fall ist von dem zu unterscheiden, daß Rechte des Drittstaates

---

[139] Klein (Anm. 124), 47, in Anlehnung an den Kommentar der ILC zu Art. 47 Ziff. 1 ihres Entwurfs zur Staatenverantwortlichkeit.

[140] Vgl. dazu oben II.2.b), Anm. 53.

[141] Klein (Anm. 124), 54.

[142] Zur völkerrechtlichen Beurteilung des "Jamming" vgl. Simma (Anm. 110), 70f., und Dahinden (Anm. 82), 210ff.

[143] Doehring (Anm. 57), 445f. Rn. 1034.

gegenüber dem die Repressalie ergeifenden Staat verletzt werden. Gezielte Maßnahmen gegen einen völlig Unbeteiligten dürfen im Regelfall nicht ergriffen werden. Lediglich für den Fall der tatsächlichen Unmöglichkeit oder des Staatsnotstands führt ein Eingriff in Rechtspositionen oder Ressourcen eines an sich unbeteiligten anderen Staates nicht zur völkerrechtlichen Verantwortlichkeit[144].

5. Zwischenergebnis

Informationsoperationen unterhalb der Schwelle des Einsatzes bewaffneter Gewalt sind nicht nur am Schädigungs- und am Interventionsverbot zu messen. Die Beurteilung ihrer Rechtmäßigkeit hängt vielmehr von einem dichten Geflecht vertraglicher Regelungen ab. Man wird etwa die einschlägigen Regelwerke des Telekommunikations- und des Medienrechts zu berücksichtigen haben. Nur soweit keine vertraglichen Regelungen greifen, ist man auf das Schädigungs- und das Interventionsverbot verwiesen. Während das Schädigungsverbot vor allem auf den Schutz der territorialen Integrität und damit auch der Informationsinfrastruktur zielt, schützt das Interventionsverbot in erster Linie die Handlungs- und Entscheidungsfreiheit der Staaten.

Dabei erweist es sich insbesondere auch mit Blick auf die zulässigen Gegenmaßnahmen als problematisch, daß beide Rechtssätze des Völkergewohnheitsrechts ausgesprochen allgemein gefaßt sind und trotz aller Bemühungen kaum Konkretisierungen erfahren haben. Will man diese Rechtssätze im Zusammenhang mit Informationsoperationen konkreten Anwendungen zuführen, so bedarf es entweder einer – nicht leicht zu erreichenden – Konkretisierung der gewohnheitsrechtlichen Bestimmungen oder aber konkreter vertraglicher Festlegungen. Vorbild können insofern neben Vereinbarungen zur Terrorismusbekämpfung auch solche Verträge sein, die die Schaffung eines Regimes für einen bestimmten Raum vorsehen, der im Staatengemeinschaftsinteresse geschützt werden soll. Damit soll nicht der Eindruck erweckt werden, es handele sich etwa beim Internet um einen hoheitsfreien Raum. Allerdings bedarf es in Anbetracht der eingeschränkten staatlichen Kontroll- und Zugriffsmöglichkeiten wohl doch eines Regimes, das den Charakteristika hoheitsfreier Räume Rechnung trägt.

Es muß aber nicht gleich ein umfassendes vertragliches Regime geschaffen werden. Für eine Reihe von Fällen würde schon eine Angleichung bestehender Vereinbarungen oder deren punktuelle Ergänzung bzw. Präzisierung genügen. Zu denken ist hier etwa an die "friedlichen Zwecken" vorbehaltene Nutzung des Weltraums und die entsprechenden Bestimmungen der INTELSAT-, INMARSAT- und EUTELSAT-Verträge.

Was schließlich die zulässigen Gegenmaßnahmen betrifft, so sind die Spielräume begrenzt. Insbesondere die engen Voraussetzungen der Repressalie scheinen den von Informationsoperationen auch unterhalb der Schwelle des Einsatzes bewaffneter Gewalt betroffenen Staaten nur unzureichende Möglichkeiten der

144 Vgl. dazu schon oben II.2.b).

Gegenwehr an die Hand zu geben. Um eine Eskalation über das zulässige Maß hinaus zu vermeiden, wäre zu überlegen, in vertraglichen Vereinbarungen besondere Gegenmaßnahmen zu eröffnen. Vorbildcharakter kann insoweit Art. 34 der ITU-Konstitution haben. Ergänzend bedürfte es allerdings weiterer Regelungen in Anbetracht der Internet-spezifischen Gefahrenlagen, die den Schwierigkeiten der Identifizierung des Störers Rechnung tragen. Ob derartige Regelungen zu einer Veränderung der Verteilung der objektiven Beweislast führen sollten, kann die vorliegende Untersuchung nicht abschließend beantworten.

IV. Offensive Informationsoperationen

In den vorstehenden Abschnitten II. und III. ist untersucht worden, welche – letztlich immer defensiven – Reaktionsmöglichkeiten einem Staat nach geltendem Völkerrecht zur Verfügung stehen, der das Ziel eines Informationsangriffs oder -eingriffs geworden ist. Im folgenden soll noch kurz beleuchtet werden, welche eigenen "offensiven" Informationsoperationen ein Staat nach Völkerrecht legal durchführen darf, ohne zuvor Opfer eines derartigen Angriffs oder Eingriffs geworden zu sein; "private" Informationsoperationen bleiben dabei außer Betracht. Als offensive Informationsoperationen gelten zunächst alle Maßnahmen, die ergriffen werden, um die einem potentiellen Gegner zur Verfügung stehende Information, Informationstechnologie und Verbindungs- bzw. Führungssysteme im Frieden, in der Krise und im Konflikt zu beeinflussen[145]. Darüber hinaus müssen aber auch jene Informationsoperationen in den Blick genommen werden, die nicht gegen die Informationstechnologie eines (potentiellen) Gegners als solche, sondern gegen andere gegnerische Einrichtungen und Ressourcen gerichtet werden.

1. Nachrichtendienstliche Informationsoperationen ("Spionage")

Offensive Informationsoperationen können darin bestehen, die Informations- und Kommunikationssysteme eines (potentiellen) Gegners auszuforschen bzw. die Verletzlichkeit der gegnerischen Systeme zu testen[146], ohne diese Systeme dabei zu stören oder zu zerstören. Darauf würden die völkerrechtlichen Regeln für Spionage und (militärische) Aufklärung Anwendung finden.

Abgesehen von dem Grundsatz, daß die Staaten berechtigt sind, entdeckte und auf ihrem Territorium gefaßte Spione nach ihrem Strafrecht abzuurteilen, haben sich im Völkerrecht keine ausdrücklichen Regeln für die Spionage[147] bzw. militärische Aufklärung[148] im Frieden entwickelt. Spionage und Aufklärung als solche sind völkerrechtlich nicht verboten, unabhängig davon, ob sie durch Agen-

[145] Vgl. Ziff. 18 der InfoOps Related Definitions in Enclosure 2 to NATO Draft MC 422.

[146] Draft MC 422, Ziff. 11 a.

[147] Vgl. E. Rauch, Espionage, in: Bernhardt (Anm. 67), 114ff.

[148] Vgl. R. Hollweg, Military Reconnaissance, in: R. Bernhardt, Encyclopedia of Public International Law, Vol. III (1997), 400ff.

ten auf dem fremden Territorium, aus dem Luft- oder Weltraum oder elektronisch vom benachbarten Territorium oder von der Hohen See aus erfolgen[149]. Lediglich das unerlaubte Einfliegen in den Luftraum zu Spionagezwecken wird allgemein als Verletzung der Territorialhoheit angesehen[150], die Aufklärung durch Satelliten ("remote sensing")[151] aus dem Weltraum dagegen nicht. Es spricht daher alles dafür, daß das "Anzapfen" fremder Daten- und Informationssysteme mittels Computern (und übertragen durch Satelliten) völkerrechtlich nicht verboten ist, auch wenn der Zugriff auf die Information dann auf fremdem Territorium erfolgt[152].

Auch im Kriege sind Spionage und militärische Aufklärung jedenfalls solange nicht völkerrechtswidrig, wie sie nicht unter Verwendung neutraler oder schützender Zeichen erfolgen[153]. Informationseingriffe wären demgemäß nur dann verboten, wenn sie sich der Kennung z.B. des Roten Kreuzes oder der Vereinten Nationen bedienten[154].

2. Propaganda, Kriegslist, Perfidie-Verbot

Auch auf Propaganda, die mittels moderner Informationstechnologie verbreitet würde, wären die Regeln des geltenden Völkerrechts anwendbar, die sich – in eher begrenztem Umfang – auf den Inhalt der Propaganda beziehen, aber nicht auf das jeweilige Verbreitungsmedium. Völkerrechtlich relevant ist Propaganda, wenn sie von einem Staat ausgeht und in einem anderen empfangen werden soll. Kennzeichnend für Propaganda ist die Absicht der Desinformation durch bewußte Selektivität bzw. Manipulation bei der Verbreitung von Information mit dem Ziel, in systematischer Weise das Verhalten der Adressaten der Propaganda zu beeinflussen[155]. Die richtige und vollständige Information ist dagegen durch den völkerrechtlichen Grundsatz der Informations- und Kommunikationsfreiheit geschützt und erlaubt.

Völkerrechtlich zumindest mißbilligt, zum Teil aber auch illegal[156], ist Propaganda, die zum Krieg oder Friedensbruch aufruft, die Bevölkerung zu Ungehorsam oder subversiven Handlungen aufstachelt, ethnische, rassische oder religiöse Diskriminierung bewirken will, oder fremde Staaten und ihre Organe beleidigt[157]. Sofern solches nicht schon gegen das Gewaltverbot verstößt, wird es zum Teil als

[149] Hollweg, *ibid.*, 401f.

[150] Vgl. aber auch den Open Skies-Vertrag von 1992 (BGBl. 1993 II, 2046), der solches ausdrücklich erlaubt.

[151] Siehe dazu Kanuck (Anm. 4), 279f.; Greenberg [*et al.*] (Anm. 21), nach dortiger Anm. 163.

[152] Auch der "klassische" Spion, der sich Zugang zu Verschlußsachen im anderen Land verschaffte und sie photographierte, machte sich strafbar, verletzte aber nicht Völkerrecht.

[153] Rauch (Anm. 147), 115; vgl. insbesondere Art. 39 Abs. 3 des I. Genfer Zusatzprotokolls 1977.

[154] Zum Perfidie-Verbot vgl. unten IV.2.

[155] Vgl. K. Ioannou, Propaganda, in: Bernhardt (Anm. 148), 1135ff.

[156] Ob nur mißbilligt oder illegal hängt davon ab, ob das "Verbot" in einem rechtlich bindenden Text oder einer unverbindlichen Resolution enthalten ist.

[157] Siehe die Einzelheiten bei Ioannou (Anm. 155).

verbotene "ideologische Intervention" angesehen. Über diese inhaltlichen Schranken hinaus sind völkerrechtliche Verbote, die sich speziell auf das Medium "Informationstechnologie" beziehen, derzeit nicht erkennbar. Allenfalls wäre daran zu denken, daß die Möglichkeit, offizielle oder offiziöse Informationen, die der Zielstaat auf seinen Rechnern bereit hält, durch Informationsoperationen zu verändern bzw. zu verfälschen, die Grenze zur verbotenen Intervention früher überschreitet als die herkömmliche Propaganda, deren ausländischer Urheber leichter zu erkennen war.

Im Kriege dient Propaganda dazu, den Verteidigungswillen der gegnerischen Bevölkerung zu schwächen, die Streitkräfte zu demoralisieren oder Verwirrung innerhalb des militärischen und logistischen Systems zu stiften[158]. Sie ist grundsätzlich erlaubt, solange sie nicht die Grenze zwischen zulässiger Kriegslist[159] und verbotener Perfidie[160] überschreitet. Zur erlaubten Kriegslist bzw. psychologischen Kampfführung gehören die Verbreitung falscher Nachrichten ebenso wie der Gebrauch gegnerischer Signale und Zeichen. Die Grenze zur Perfidie (Heimtücke) wäre dann überschritten, wenn die Gegenpartei zur irrtümlichen Annahme einer völkerrechtlichen Schutzlage verleitet würde (z.B. humanitäre Vereinbarung zur Einstellung der Kämpfe in der Absicht, den darauf vertrauenden Gegner überraschend anzugreifen)[161]. Besonderheiten der Informationsoperationen kämen auch hier nur ins Spiel, wenn eine Streitpartei z.B. auf den Gedanken käme, Meldungen über Kampfeinstellungen über die Rechner des Roten Kreuzes oder der Vereinten Nationen zu verbreiten und ihnen damit den Anschein besonderer Glaubwürdigkeit zu geben. Ausschlaggebend für das Verbotensein einer solchen Handlung bliebe aber der Inhalt und nicht die Tatsache, daß sich das unerlaubte Vorgehen mit Hilfe moderner Informationstechnologie vielleicht leichter als früher realisieren ließe.

3. Einsatz von Informationstechnologie als "Waffe"

Wenn man entsprechend dem unter II. Gesagten davon ausgeht, daß Informationstechnologie ob der damit erzielten Wirkung als "Waffe" angesehen werden kann, dann würde ihr Einsatz denselben Regeln des humanitären Völkerrechts unterliegen wie der bewaffnete Konflikt mit herkömmlicher Bewaffnung. Einsatzbegrenzungen würden sich daraus jedenfalls dann ergeben, wenn "the use of information and information systems as weapons in a conflict where information and information systems are the target"[162] sich nicht auf die Störung oder Aus-

---

[158] Vgl. K. Madders, War, Use of Propaganda in, in: Bernhardt (Anm. 136), 334ff., sowie S. Oeter, Kampfmittel und Kampfmethoden, in: D. Fleck (Hrsg.), Handbuch des humanitären Völkerrechts in bewaffneten Konflikten (1994), 89 (164ff.; §§471–474).

[159] Siehe K. Ipsen, War, Ruses, in: Bernhardt (Anm. 136), 330f.; Oeter, *ibid.*

[160] Siehe Oeter, *ibid.*, 161ff. (§472).

[161] Oeter, *ibid.*, und Aldrich (Anm. 4), nach dortiger Anm. 34.

[162] Vgl. die bei Aldrich (Anm. 4) wiedergegebene Definition der National Defense University für "infowar" (nach dortiger Anm. 15) und Scott (Anm. 83), 57ff.

schaltung der Informationssysteme beschränkt, sondern dies physische Folgeschäden zeitigte[163]. Daß im Konflikt gegnerische militärische Kontroll- und Führungssysteme ebenso konventionell wie mittels Informationstechnologie angegriffen und zerstört werden dürfen, erscheint selbstverständlich. Ebenso selbstverständlich ist, daß ein ziviles Ziel weder konventionell noch mit Informationstechnologie angegriffen werden darf, wenn sich daraus für die Zivilbevölkerung nicht nur Unannehmlichkeiten, sondern Gefahren für Leib und Leben ergeben. Das gleiche gilt für Kollateralschäden, die nicht durch militärische Notwendigkeiten gerechtfertigt erscheinen[164]. Die Art. 54 bis 56 des I. Genfer Zusatzprotokolls gelten auch für Informationsoperationen, wenn sie die in diesen Artikeln beschriebenen Konsequenzen haben können. Auf der anderen Seite erscheinen Informationsoperationen erlaubt, die nicht ob ihrer Folgen von diesen Artikeln erfaßt werden, sondern – wenn auch vielleicht wirksamer – lediglich den Effekt von Embargen oder Handelsblockaden hätten[165].

Weniger problematisch erscheint, daß es sich bei den Informationssystemen oder wesentlichen Teilen davon um solche handelt, die sowohl für zivile als auch militärische Zwecke genutzt werden. Gemäß Art. 52 Abs. 2 des I. Genfer Zusatzprotokolls gelten als militärische Ziele solche Objekte, die aufgrund ihrer Zweckbestimmung und Verwendung wirksam zu militärischen Handlungen beitragen und deren gänzliche oder teilweise Zerstörung einen eindeutigen militärischen Vorteil darstellt. Soweit technisch möglich und sinnvoll dürften daher im Konflikt auch Informationssysteme zerstört werden, die auch zivilen Zwecken dienen.

V. Zusammenfassung

Auch Informationstechnologie ist als "Waffe" im völkerrechtlich relevanten Sinne anzusehen, wenn ihr beabsichtigter Einsatz Schäden an zivilen oder militärischen Zielen hervorriefe, die jenen vergleichbar wären, die durch herkömmliche Waffen bewirkt würden. Eine dagegen geübte Selbstverteidigung dürfte sich – außer im Falle des extremen Notstandes – nur gegen den zweifelsfrei ermittelten "Aggressor" richten und hätte die Gebote der Notwendigkeit und Verhältnismäßigkeit zu beachten. Ginge der Informationsangriff von Privaten aus, wäre Selbstverteidigung dagegen nur bei entsprechender Verantwortlichkeit des Territorialstaates zulässig, die nach dem jeweils geltenden Völkerrecht zu ermitteln wäre. Informationsoperationen unterhalb der Schwelle des Einsatzes bewaffneter Gewalt sind nicht nur am Schädigungs- und am Interventionsverbot zu messen. Die Beurteilung ihrer Rechtmäßigkeit hängt darüber hinaus von einem dichten Geflecht vertraglicher Regelungen des Telekommunikations- und Medienrechts ab. Als Maßnahmen gegen Informationsoperationen unterhalb der Schwelle des Einsatzes bewaffneter Gewalt kommen die Repressalie, die Retorsion und weitere

[163] Siehe auch Greenberg [*et al.*] (Anm. 21), nach dortiger Anm. 140.

[164] Vgl. Aldrich (Anm. 4), III.B.1, sowie generell C. Greenwood, Geschichtliche Entwicklungen und Rechtsgrundlagen, in: Fleck (Anm. 158), 1 (26ff.; §§130ff.).

[165] So auch Greenberg [*et al.*] (Anm. 21), nach dortiger Anm. 130.

zulässige Selbsthilfemöglichkeiten (insbesondere auch vertraglich vorgesehene) in Betracht. Gerade was Informationsangriffe durch "Private" betrifft, wäre es angezeigt, durch völkerrechtlichen Vertrag Cyberspace entweder zum international geschützten Bereich zu erklären, oder aber die Informationsinfrastruktur – wie die zivile Luftfahrt – durch entsprechende Konventionen in die international-strafrechtliche Obhut der Staaten zu geben. Dann würde auch die Duldung von Informationsangriffen seitens Privater die Staatenverantwortlichkeit auslösen. Ergänzend bedürfte es weiterer Regelungen in Anbetracht der Internet-spezifischen Gefahrenlagen, die den Schwierigkeiten der Identifizierung des Störers Rechnung tragen. Das "Anzapfen" fremder Daten- und Informationssysteme mittels Computern (und übertragen durch Satelliten) dürfte völkerrechtlich nicht verboten sein, auch wenn der Zugriff auf die Information auf fremdem Territorium erfolgt. Auf Propaganda, die mittels moderner Informationstechnologie verbreitet würde, sind die Regeln des geltenden Völkerrechts anwendbar, die sich auf den Inhalt der Propaganda beziehen, aber nicht auf das jeweilige Verbreitungsmedium. Der Einsatz von Informationstechnologie als "Waffe" unterliegt denselben Regeln des humanitären Völkerrechts wie der bewaffnete Konflikt mit herkömmlicher Bewaffnung. Einsatzbegrenzungen ergeben sich insbesondere dann, wenn sich Informationsoperationen nicht auf die Störung der Ausschaltung der Informationssysteme beschränken, sondern physische Folgeschäden zeitigen.

Summary[166]

Information Operations and International Law

The concept of a Global Information Infrastructure based on an interconnected global telecommunication highway is highly attractive for various reasons: From an economic perspective, telecommunications belong to the fastest growing markets on both the European and the global level; from a general political perspective, the participation of individuals in international telecommunications contributes to building a global civil society. However, the information age also has a dramatic impact on security affairs. Today's dependence upon information technology and information networks has created new kinds of systemic vulnerabilities that may be exploited by a variety of actors for various purposes. The effects of hackers and information systems failures on air traffic control, the banking system or a national department of defence illustrate these vulnerabilities. We can also think of low-intensity conflicts on the scale of electronic terrorism compromising industrial secrets. Finally, the success of new technologies during recent military operations demonstrates that information operations can become a means of warfare.

Information operations have been defined as "actions taken to preserve the integrity of one's own information infrastructure from exploitation, corruption or destruction while at the same time exploiting, corrupting or destroying an adversary's information systems

[166] Summary by the authors.

thereby achieving a (political or) military advantage" (M.R. Jacobson). The legality of such information operations must be discussed not only in light of applicable treaty law, but above all in light of the prohibition of intervention and the prohibition of the use of force. Also, it is necessary to consider how a state may react *vis-à-vis* information operations, ranging from counter-measures short of force to self-defence.

While there is no international treaty governing the national or international information infrastructure as such, certain devices are protected by treaty provisions. Submarine cables have been protected by international law since 1884 when the Convention for the Protection of Submarine Cables was agreed upon. Today Article 113 of the UN Convention on the Law of the Sea provides that "every State shall adopt the laws and regulations necessary to provide that the breaking or injury by a ship flying its flag or by a person subject to its jurisdiction of a submarine cable beneath the high seas done wilfully or through culpable negligence, in such a manner as to be liable to interrupt or obstruct telegraphic or telephonic communications, and similarly the breaking or injury of a submarine pipeline or high-voltage power cable, shall be a punishable offence". In light of Article 33 of the Constitution of the International Telecommunication Union (ITU) whereby members of the Organization "recognize the right of the public to correspond by means of the international service of public correspondence", member states, under Article 38, paragraph 1, of the Constitution, "shall take such steps as may be necessary to ensure the establishment, under the best technical conditions, of the channels and installations necessary to carry on the rapid and uninterrupted exchange of international telecommunications". Further, "Members shall safeguard these channels and installations within their jurisdiction" and "shall take such steps as may be necessary to ensure maintenance of those sections of international telecommunication circuits within (their) control". It is noteworthy, that even military radio installations taking part in the service of public correspondence "must, in general, comply with the regulatory provisions for the conduct of such services". Under Article 6 of the ITU-Constitution members must ensure the observance by private persons of the relevant provisions.

With regard to the use of the radio-frequency spectrum and of the geostationary-satellite orbit there are further provisions. Article 45 of the already mentioned ITU-Constitution stipulates that all stations "must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Members"; false or deceptive signals have to be prevented according to Article 47 of the Constitution. The Convention on the Law of the Sea (Article 19, paragraph 2, *lit.* k) considers "any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State" commited by a foreign ship in the coastal state's territorial waters as passage "prejudicial to the peace, good order or security of the coastal State", thus no longer as innocent passage. The Outer Space Treaty of 1967 prescribes that the "moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes" (Article 4, paragraph 2). In light of the Treaty's reference to the UN Charter this today usually is understood as "non-aggressive" within the meaning of Article 51 of the Charter, which incorporates the right of self-defence. Article 3, paragraph 3, of the INMARSAT-agreement provides that the satellite organisation shall serve peaceful purposes. Reference to peaceful purposes does not exclude all military services. It may be argued that UN forces may use INMARSAT resources even if involved in actual fighting on the ground, not only because Article 27 of the Agreement ensures cooperation between

INMARSAT and the UN or because Article 12, paragraph 1b, refers to the aims and principles of the UN Charter, but primarily because UN actions under Chapters VI and VII of the Charter (peacekeeping and peace-enforcement) serve peaceful purposes.

Since specific treaty law does not cover all possible acts of information operations it is necessary to consider more general rules of international law, the first one being the prohibition of intervention. The UN Charter does not include an explicit provision on the prohibition of state-to-state intervention. The prohibition of UN intervention "in matters which are essentially within the domestic jurisdiction" of a member state according to Article 2, paragraph 7, of the Charter is not applicable because it only deals with the relationship between the UN and its member states. Rather it is possible to refer to Article 2, paragraph 1, of the UN Charter which incorporates the principle of sovereign equality of all member states. If all states are by law considered to be equal none may interfere or even intervene in domestic affairs of the other. Since this principle – which also is a rule of customary international law – seems to lack precision, the UN General Assembly in 1965 adopted the "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty", defining what is actually prohibited. The essential parts of this Declaration were included in the Friendly-Relations-Declaration adopted by the General Assembly in 1970 without a vote. This Declaration was and is designed as a catalogue of rules for inter-state-relations on the basis of the UN Charter. It specifies that no state has the right "to intervene, directly or indirectly, for any reason whatever, in the international or external affairs of any other State. ... armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, are in violation of international law". Although the Declaration as such is not binding, it may serve as proof of what is called *opinio iuris*, one of the elements required to prove the existence of a rule of customary international law. This was confirmed by the International Court of Justice in the *Nicaragua* Case.

Information operations addressed against the information infrastructure of a state may be qualified as unlawful intervention, since information technology and information networks form part of a state's "political, economic, social and cultural systems" protected by the prohibition of intervention. This also applies to information operations which only use or interfere with national information infrastructure without destroying parts of it. The same applies to the use of information put on a website or spread through newsgroups and mailing-lists if this amounts to more than admissible political pressure, in other words: if it amounts to coercion in stead of persuasion.

Briefly turning to acts of private individuals, hackers or information terrorists in particular, as a rule states cannot be held responsible for any of these breaches unless a state has failed to comply with its own obligations. Apart from particular treaty provisions already referred to above, *inter alia*, the obligation included in Article 113 of the LOS Convention to make injury to a submarine cable by a private person a punishable offence, we may again look into the Friendly Relations Declaration and the principle of non-intervention. The Declaration stipulates that "no State shall organise, assist, foment, finance, incite or tolerate, subversive, terrorist or armed activities directed towards the violent overthrow of the régime of another State, or interfere in civil strife in another State". With the exception of terrorist activities, information operations performed by private individuals or groups of individuals will – even on the basis of these rules of international law – however only lead

to the responsibility of the concerned state if the state has not acted with due diligence in respect of private persons.

Information operations can, however, lead to more than to a low-intensity conflict. It is debatable whether – under certain circumstances – information operations may amount to a prohibited use of force and thus may give rise to acts of self-defence. Again we have to consider provisions of the UN Charter. Article 2, paragraph 4, of the UN Charter prohibits "the threat or use of force (by a state) against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations". This prohibition also forms part of customary international law, it may even be argued that this is a peremptory rule of international law – in other words: it is *ius cogens*. The term "force" within Article 2, paragraph 4, is usually understood as armed or military force. However, this does not help much, since there is neither a general definition of "armed force" nor does the term "military" cover only traditional forms of military operations. Another term used in the UN Charter is the one of "aggression" in Article 39. According to this provision, the UN Security Council shall determine the existence of an act of aggression. The UN General Assembly, in 1974, adopted a resolution defining aggression. Aggression among others includes "the invasion or attack by the armed forces of a State of the territory of another State ...; bombardment by the armed forces of a State against the territory of another State or the use of any weapons by a State against the territory of another State; the blockade of the ports or coasts of a State by the armed forces of another State; or the action of a State in allowing its territory, which it has placed at the disposal of another State, to be used by that other State for perpetrating an act of aggression against a third State". While this definition is neither conclusive nor as such binding it nevertheless offers interpretative hints with regard to Article 39 of the UN Charter. This may be relevant for information operations although the definition obviously is based on traditional military weaponry. If "invasion" is not limited to physical invasion, if "any weapons" includes computers, if a "blockade" of the information infrastructure is much more effective than a blockade of the ports or coasts of a state, or if not the territory but the information infrastructure is placed at the disposal of another state to be used for acts of aggression against a third state, then the underlying idea of the definition would still be valid: the protection of sovereignty, of a state's territorial integrity and political independence.

Most important in this context is the term "armed attack" as used in Article 51 of the UN Charter, incorporating the right of individual or collective self-defence if an armed attack occurs. Neither treaty law nor the jurisprudence of international courts or tribunals have defined this term. There seems to be a consensus that an armed attack must be of a certain intensity. While the International Court of Justice in the *Nicaragua* Case considered participation of a state in the sending of armed bands, even private armed bands, into the territory of another state as amounting to an armed attack if of a certain intensity, on the other hand, the Court was of the opinion that logistical support or the sending of arms can not be considered an armed attack.

What may be taken from all this? All terms imply the use of armed force, with armed force understood as the use of traditional weaponry – and its effects. This usually implies a certain degree of physical destruction. While the use of economic force may not be considered as a weapon, on the other hand, there is no rule to limit the term of armed force to traditional weaponry. There was a time when only short-distant weapons were known. It

was never a problem to later consider guns and even longer-distant weapons such as artillery as weapons, their use as armed force. What is decisive is not the means, but the intention of its use and the destructive effects. An armed attack within the meaning of Article 51 today means to be equipped with means designed to achieve a military advantage and to destroy or kill, in other words: "Armed simply means equipped with the weapons of war" (Jacobson).

Turning to counter-measures taken against information operations: If an information operation amounts to an armed attack, which may be the case if information operations cause the break-down of all energy supply systems, the destruction of a nuclear power station, the break-down of military air traffic control, or the national department of defence, it is possible to exercise the right of self-defence, however, within its limits. This means to apply the principles of necessity and proportionality, the so-called *Webster-* or *Caroline-*Principles: "A necessity of self-defense, instant, overwhelming, leaving no choice of means, and no moment for consideration". Thus, a lot will depend on the information technology available in the attacked state. Can the attacked state protect itself e.g. by the installation of firewalls or similar systems? Has the attacked state high-tech means at its disposal which can be used without themselves amounting to high-scale military force? How far can a state resort to preventive self-defence? Is the break-down of the department of defence or military air traffic control sufficient to start military counter-measures or is it necessary that the other state has set its troops in motion?

Even more difficult is the situation if an attack on a state's information infrastructure occurs and it remains unclear where this attack comes from. Not only are computer-based attacks hard to distinguish from innocent malfunctions, but in the case attacks carried out across a network the culprits may never be physically close to the target, and they may even leave no tangible evidence. While apart from a situation of necessity self-defence is only admissible if the aggressor can be clearly identified, counter-measures short of force may be taken in such a case. This is definitely possible in the case of a retorsion which is only an unfriendly act (this may, however, entail high political costs). It is much more difficult if adopting a reprisal which itself is a violation of an obligation and is only justified because addressed against an earlier violation by the target state of the reprisal. Usually the attacked state must prove the existence of such earlier violation of an international obligation. This again means that a state may only adopt a reprisal against a state not involved or only seemingly involved in case of a state of necessity.

In conclusion, the legality of information operations has to be judged in light of international telecommunications law as well as in light of the prohibition of intervention and the prohibition of the use of force. It is, however, difficult to draw the lines not only between persuasion and intervention, but primarily between prohibited intervention and an armed attack. A state being the victim of illegal information operations does not have to wait as a sitting duck until having suffered severe damages. However, it should be careful in choosing counter-measures. In order to avoid all these difficulties of interpretation and for the sake of a higher degree of legal certainty it is desirable that states reach an agreement on the legal rules applicable to the protection of the national and the international information infrastructure. One option would be to declare cyberspace an internationally protected "area" or – and this applies in particular to the activities of private persons – to establish rules of international criminal law, as in the case of conventions dealing with civil aviation.