Working Paper
Print-Version 1.0

[Cyber-Außenpolitik]

KONZEPTIONELLE UMRISSE EINER DEUTSCHEN AUßENPOLITIK UND EINER GEMEINSAMEN AUßEN- UND SICHERHEITSPOLITIK DER EUROPÄISCHEN UNION FÜR DIE VERNETZTE GESELLSCHAFT DES 21. JAHRHUNDERTS AUF GLOBALER EBENE

von
Bruck M. Kimmerle
Halle 1999

MARTIN-LUTHER-UNIVERSITÄT
HALLE-WITTENBERG
INSTITUT FÜR POLITIKWISSENSCHAFT
INTERNATIONALE BEZIEHUNGEN
UND DEUTSCHE AUßENPOLITIK
EMIL-ABDERHALDEN-STR. 7
06108 HALLE
kimmerle@politik.uni-halle.de
www.politik.uni-halle.de / rode / projekte / kimmerle / cyber-aussenpolitik.htm
oder www.cyber-aussenpolitik.de

Inhaltsverzeichnis

1. Vom Sinn einer Cyber-Außenpolitik

Definition:
Cyber-Außenpolitik ist die interessengeleitete Ordnung und Beeinflussung des Verhältnisses eines Staates oder der EU zu seinem/ihrem Umfeld in der transnational-vernetzten Gesellschaft des Informationszeitalters, sowie die Beeinflussung der entsprechenden Politik anderer Staaten und Nicht-Staaten.

Das Working Paper befaßt sich mit Erfordernissen, Rahmenbedingungen und Optionen einer „Cyber-Außenpolitik“ zu Beginn des 21. Jahrhunderts. Es versucht den Sinngehalt eines solchen *Politikfelds* zu ergründen. „Globalisierung“, „Vernetzung“ und „digitale Revolution“ sind Eckpunkte der nachfolgenden Analysen und Betrachtungen. Das Papier ist der Versuch einer notwendigen Reflexion neuer Ideen und Konzepte. Selbstverständlich wird nicht alles und jeder zum Vasallen eines unbeherrschbaren digitalen Imperiums. Weder wäre diese unvertretbare Übersteigerung der digitalen Revolution für die Außenpolitik angemessen, noch für irgendein anderes Politik- oder sonstiges Feld menschlichen Handelns. Aber nach den tiefgreifenden Veränderun-

gen in der Kommunikations- und Informationstechnologie am Ende des 20. Jahrhunderts wird vermutlich wenig bleiben wie es einmal war. Dinge ändern sich, insbesondere in Phasen sprunghafter Innovation. Das gilt natürlich auch für die Inhalte und Mittel der Außenpolitik. Wenngleich sich an vielen althergebrachten Anforderungen an eine gute Außenpolitik wenig ändern dürfte, so treten doch neue Politikfelder hinzu, während sich die Regeln und Gewichte des Bewährten verschieben. Das vorliegende Working Paper ist gleichsam als Byproduct einer Dissertation zum Information Highway im globalen Wettbewerb in der akademischen Disziplin Internationale Beziehungen entstanden. Befruchtet wurden die in diesem Working Paper enthaltenen Gedanken durch einen Beitrag des Autors für die Tageszeitung DIE WELT, welcher sich mit den regulativen Ansätzen autoritärer Staaten in bezug auf das Internet auseinandersetzte[1]. Das Papier ist bemüht, die vorläufigen theoretischen Erkenntnisse des eigentlichen Dissertationsprojekts auf eine konkret politikrelevante Ebene herunterzubrechen. Dem Arbeitsstab „Globale Fragen" des Auswärtigen Amts der Bundesrepublik Deutschland und den GASP-Partnern in der EU soll ein neues globales Handlungsfeld für eine zu entwicklende Gemeinsame Außen- und Sicherheitspolitik (GASP)[2] der Europäischen Union (EU) aufgezeigt werden.
Darüber hinaus entfaltet das Plädoyer dieses Working Papers auch eine starke transatlantisch-kooperative Dimension. Dies gilt insbesondere, da wesentliche Punkte dieses Papiers im innen-, außen- und sicherheitspolitischen Policy-Design der USA bereits in wichtigen Ansätzen verwurzelt sind; eine adäquate europäische GASP ginge daher Hand in Hand mit dem atlantischen Partner. Partielle Konfliktbereiche dürften die Entwicklung einer deutschen und europäischen Cyber-Außenpolitik auf der Grundlage gemeinsamer transatlantischer Werte und Interessen eher dynamisch befruchten. Dauerhafte Partnerschaft erfordert annähernd vergleichbare bzw. sich gegenseitig ergänzende Potentiale. Das ist wie in einer guten Ehe. Dies gilt in der gegenwärtigen Umbruchphase von der industriellen Ordnung hin zur neuen Ordnung der digital-vernetzten Gesellschaft mehr denn je. Die Interessen sind beiderseitig des Atlantiks weitestgehend vergleichbar – die Europäer sollten eine aktivere Rolle in der globalen Formung der vernetzten Gesellschaft übernehmen: im wohlverstandenen eigenen Interesse.

Die OECD-Welt durchläuft seit den sechziger und siebziger Jahren des 20. Jahrhunderts einen dramatischen Wandlungsprozeß. Die Arenen des Umbruchs sind vornehmlich die Gesellschaften und die Volkswirtschaften der entwickelten Wettbewerbsordnungen. Der Soziologe Daniel Bell beschrieb diese Vorgänge bereits zu Beginn der

[1] Siehe: DIE WELT, vom 31.8.1999
[2] Der Vertrag von Maastricht vom 7.2.1992 erwähnt in Artikel J 1 f. die Einführung einer Gemeinsamen Außen- und Sicherheitspolitik der Mitgliedsstaaten (GASP) der EU; der Europäische Rat der Staats- und Regierungschefs der 15 EU-Staaten bestimmte 1999 in Köln den ehemaligen NATO-Generalsekretär Javier de Solana zum ersten Repräsentanten der GASP

siebziger Jahre in seinem Klassiker „Die nachindustrielle Gesellschaft“. Hiernach arbeite ein immer größerer Teil der zunehmend hochqualifizierten Erwerbstätigen der OECD-Welt in sogenannten Informationsindustrien. Nicht mehr die manuelle Bearbeitung natürlicher Rohstoffe stehe im Mittelpunkt der volkswirtschaftlichen Wertschöpfung, sondern Wissensarbeit und Know How. Das Ziel: Die Informationsgesellschaft – im Gegensatz zur Industriegesellschaft. Nun hat dieser theoretische Ansatz zweifelsohne seine Schwachstellen. Jedoch ist die Zielgerichtetheit dieser frühen Prognosen seit der explosiven Ausbreitung des Internet und mit diesem neuen Medium verbundener Digital-Industrien in der zweiten Hälfte der neunziger Jahre des 20. Jahrhunderts nicht mehr zu leugnen. Das Internet ist trotz aller Bedenkenträgerei politischer und wirtschaftlicher Entscheidungsträger zum Leitmedium der Globalisierung geworden. Der entscheidende Punkt ist: es wird seine Rolle als Netz der Netze vermutlich auch ohne die frühen und beharrlichen Zweifler spielen. Das neue Medium wird 1999 von geschätzten 179 Millionen transnationalen Usern definiert, welche hierzu allein ihre individuellen Interessen in den drei Hauptfeldern Entertainment, Information und Kommerz zum Maßstab nehmen. Fazination, Nutzenmaximierung und Gewinnstreben treiben die Millionen Networker voran, welche durchgängig über ein eher gehobenes Bildungsniveau, überdurchschnittliches Einkommen und Zugang zu den Elite-Positionen der Zukunft verfügen. Die Rolle von Staaten wird noch anzusprechen sein, denn sie spielen auch in Zukunft eine gewichtige Rolle; insbesondere als Vertreter territorialer Gemeinschaften (Nationen) und als Träger des außen- und innenpolitischen Gewaltmonopols.

Region	**Millionen User**
Summe (Welt), Stand Juni 1999	179
Afrika	1,14
Asien/Pazifik (inkl. Australien)	26,97
Europa (EU, plus)	42,69
Mittlerer Osten (inkl. Golf-Staaten)	0,88
Kanada und U.S.A.	102,03
Latein Amerika	5,29

Tabelle 1 – Geografische Verteilung der Internet-User, Stand Juni 1999 - Quelle: NUA Internet Surveys, Dublin 1999, www.nua.ie

Auf dem Sprung in das 21. Jahrhundert stellt sich also für die OECD-Gesellschaften die Frage, wie das neue Umfeld der transnationalen Vernetzung beschaffen sein wird. Entspricht es den eigenen Stärken ? Verstärkt es sogar die eigenen Schwächen ? Welche politischen Zielkategorien müßen angepaßt werden, welche werden gar durch die Vernetzung befördert ? Und was treibt diese in der Menschheitsgeschichte einmalige Entwicklung ? Ronald J. Deibert bezeichnet diese Wechselwirkung zwischen hypermedialer Umgebung und gesellschaftlichen Kräften als „Ecological Holism“[3] und sieht dieses Feedback in „Distributional Changes“[4] münden: „...distributional changes are those, that take place in the relative power of social forces as a result of a „fitness“ between the interests of these social forces and the communications environment.“[5] Fakt ist, historisch erstmalig werden zu Beginn des 21. Jahrhunderts viele Bewohner der Kontinente Amerika, Europa und Asien über ein einheitliches, das Individuum unmittelbar mit anderen Individuen und Organisationen verbindendes, die Beschränkungen von Raum, Zeit und finanziellem Vermögen in weiten Teilen aufhebendes Medium zur Kommunikation, Information und Organisation von Wirtschaften und Gesellschaften verfügen. „Within the next generation, almost everyone on earth will be linked on an electronic network."[6] Dieses Mega-Projekt hat wenig mit Illusionen oder Utopien zu tun. Eher geht es um einen zivilisatorischen Bruch. Einen historischen Bruch, der technologisch-kommunikativ bestimmt sein wird. Dabei liegt es auf der Hand, das es um eine globale Entwicklung geht, welche in der Neuverteilung von Macht aufgehen kann. „Changes in the world power structure that are consequences of the Information Revolution are far more pervasive and demonstrable than many might understand, cutting across all areas of foreign policy."[7] Diese Entwicklung rechtzeitig, proaktiv und gezielt dergestaltig zu beeinflußen, daß die eigenen Stärken und Fähigkeiten durch die neu auszuformende Rahmenordnung begünstigt werden – das ist Cyber-Außenpolitik. Allerdings ist diese neue Dimension der Außenpolitik – egal ob auf deutscher oder europäischer Ebene – keine nationalstaatliche Domäne mehr. Sie

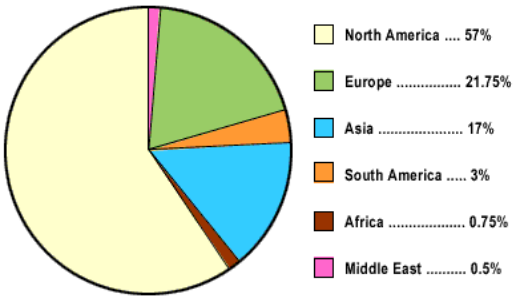

Abbildung 1 – Grafische Darstellung der geografischen Verteilung der Internet-User, Stand 1998 - Quelle: NUA Internet Surveys, Dublin 1999, www.nua.ie

[3] Ronald J. Deibert: Parchment, Printing, and Hypermedia, Communication in World Order Transformation, New York 1998, S. 37 f.
[4] ebd., S. 137 f.
[5] ebd., S. 137
[6] Wilson Dizard Jr.: Meganet, How the Global Communications Network Will Connect Everyone on Earth, Boulder 1997, S. IX
[7] David J. Rothkopf: Cyberpolitik: The Changing Nature of Power in the Information Age, in: Journal of International Affairs, Spring 1998, S. 330

vollzieht sich in einem Bündel aus transnationalen Akteuren, bestimmten Behörden, sozialen Gruppen und multilateralen Organisationen.

Aus der US-Position beschreibt David J. Rothkopf die neue Herausforderung: „The goals, capabilities and actions of individuals, legitimate NGOs, international organizations, terrorist groups, etc. will become central to U.S. policy and intelligence. Benign, non-state actors provide policymakers with alternative foreign policy tools. Their influence and ubiquity are dissolving the narrow focus of government-to-government diplomacy and creating a worldwide network that will be a key feature of the environment in which diplomats and generals operate.“[8]

Eine deutsche und europäische Cyber-Außenpolitik baut auf der adäquaten Vertretung der Interessen involvierter NGO und der digitalen Wirtschaft auf. Da es sich bei diesen Policy-Partnern qua definitionem um transnationale Akteure handelt, redefiniert sich das nationale Interesse der Bundesrepublik Deutschland und ihrer EU-Partner in Richtung dieser transnationalen Entfaltungsinteressen, soweit sie mittelbar oder unmittelbar in Deutschland und Europa verwurzelt sind und der EU-Bevölkerung Nutzen stiften bzw. neue Lebensperspektiven erschließen. Cyber-Außenpolitik löst sich vom Territorium. Die Ordnung von Münster wird ersetzt durch die Ordnung des Silicon Valley. In diesem Sinne können auf der einen Seite neue außenpolitische Partnerschaften mit großem globalem Potential erschloßen werden. Auf der anderen Seite gewinnen Deutschland und Europa stark an Attraktivität als Standort für die boomende und richtungsweisende digitale Wirtschaft, deren Entfaltungsinteresse hier vehement vertreten wird. Auf diesem Weg könnte zudem ein Beitrag zur Überwindung der strukturellen Probleme des alten Kontinents geleistet werden. Neue ökonomische und soziale Wachstumspotentiale werden erschloßen und freigesetzt. Die Wettbewerbsfähigkeit Deutschlands und Europas gewinnt unter den Bedingungen der Globalisierung.

Eine Cyber-Außenpolitik trägt der aktuellen weltweiten Diskussion um die aufkommende Weltordnung des Informationszeitalters Rechnung. „Knowledge, more than ever before, is power. The one country that can best lead the information revolution will be the more powerful than any other. For the foreseeable future, that country is the United States.“[9] Folgerichtig analysieren Nye und Owens aus dem Blickwinkel der U.S. Außenpolitik der 90er Jahre und unter Würdigung der Implikationen der digitalen Revolution, „America’s foreign and domestic policies are inextricably intertwined. A healthy democracy at home, made accessible around the world

[8] a.a.O. (Anm. 7), S. 330
[9] Joseph S. Nye, Jr. / William A. Owens: America’s Information Edge, in: Foreign Affairs, March/April 1996, S. 20

through modern communications, can foster the enlargement of the peaceful community of democracies, which is ultimately the best guarantee of a secure, free, and prosperous world.“[10] Wie so oft, führen die USA die Diskussion. Viele europäische Argumente sind jedoch identisch. Warum sollen die Europäer und die Deutschen beiseite stehen und schweigen ? Es ist Zeit für eine eigenständige Cyber-Außenpolitik und das Verlaßen der digitalen Provinz auf diesem Planeten. „Rules will be necessary to govern cyberspace, not only protecting lawful users from criminals but ensuring intellectual property rights. Rules require authority, whether in the form of public government or private or community governance. Classic issues of politics – who governs and on what terms – are as relevant to cyberspace as to the real world.“[11] Zwar bringen sich die Europäer gerade auch über die EU-Kommission in die Ausgestaltung dieser Herrschaftsregeln für das Informationszeitalter ein. Jedoch ist eine außenpolitische Doktrin zu vermissen, die entsprechende Schritte aus einem eher technischen Nischendasein befreit und in einen übergreifenden gesellschaftlichen Kontext einfügt. Viel zu häufig erfolgen im Fall der EU Willensbildungsprozesse zur Regulierung des Information Highway in kleinen Fach-Zirkeln – und geben dergestaltig Partikularinteressen freien Weg, die häufig eben nicht die Interessen der wirtschaftlichen Wachstumssektoren vertreten, sondern auf der Seite überkommener, auf Marktschließung und Verteidigung alter Positionen orientierender Interessen stehen. Die notwendigen Diskussionen um die EU-Datenschutzrichtlinie, das deutsche Multimediagesetz oder die Software-Patentierung in der EU sind beispielhaft anzuführen.

Auf der anderen Seite muten diese Beispiele wie eine Nabelschau an, trägt man der Tatsache Rechnung, daß die Struktur des Cyberspace sich in den kommenden Jahren verändern wird. In der Phase bis Ende der neunziger Jahre des 20. Jahrhunderts war der Ausbau des Information Highway und die Setzung der Verkehrsregeln eine transatlantische Veranstaltung unter Führung der USA.
Im ersten Jahrzehnt des 21. Jahrhunderts werden nicht-westliche Akteure mit ihren eigenen, teilweise autoritären Ordnungsvorstellungen die digitale Bühne betreten. Schätzungen nehmen an, das allein die Volksrepublik China bis 2003 mit 33 Millionen Usern im Netz Flagge zeigen wird[12]. Gerade China weist einige signifikante Initiativen zur Umgestaltung, Kontrolle und Regulierung des Webs auf, welche z.B. in einem China Wide Web (CWW) zum Ausdruck kommen[13]. Indien ist zwar heute die größte Demokratie der Welt und ein relevanter Software-Produzent; die weitere innenpolitische Entwick-

[10] Ebd., S. 36
[11] Robert O. Keohane / Joseph S. Nye, Jr.: Power and Interdependence in the Information Age, in: Foreign Affairs, September/October 1998, S. 82 f.
[12] a.a.O. (Anm. 1)
[13] Ebd.

lung bleibt indessen abzuwarten. Auch die islamische Welt – hier insbesondere die Golf-Region, aber auch der Iran – dürften bis dato ungenutzte Potentiale aufweisen und im frühen 21. Jahrhundert in die Waagschale werfen. Saudi Arabien hat 1999 eines der restriktivsten Kontroll-Regime des Internet implementiert[14]. Es ist eine Frage der Zeit, bis diese wachsenden Netz-Akteure ihre Werte und regulativen Ziele vehement in den Cyberspace tragen. Der Koran impliziert andere Inhalte und Dynamiken des Cyberspace als die amerikanische Unabhängigkeitserklärung. Exakt in der vor der Tür stehenden Phase wahrhaft globaler/planetarer Expansion des Netzes muß eine deutsche und europäische Cyber-Außenpolitik im engen Verbund mit den US-Partnern auf eine maximale Kompatibilität mit westlichen Ordnungsvorstellungen hinwirken und einen Dialog für die Freiheit des Netzes im 21. Jahrhundert entfachen.
Auch Datennetze sind nicht ohne Geopolitik. Nach wessen und welchen Vorstellungen teilt sich der virtuelle Raum auf ? Wer kontrolliert welche Netz-Knoten nach welchen Regeln ?

2. Der Aufstieg der „vernetzten Gesellschaft“ und der digitalen Wirtschaft

Früher vernetzten sich große, multinationale Unternehmen, Organisationen und Verwaltungen. Die Kosten der Datenverarbeitung ließen das Know How und den Erwerb der proprietären Systeme des elektronischen Datenaustauschs für Individuen und kleine Organisationen unerschwinglich sein.
Heute ist aus der Herrschaftstechnologie der Dinosaurier des Industriezeitalters ein Gemeinplatz geworden. Zwar sind nach wie vor große Teile der OECD-Gesellschaften nicht unmittelbar in das globale Datennetz integriert. Jedoch weitet sich das Feld der Vernetzten beständig aus. Mit der Popularisierung des Internet ist eine grundsätzlich überall verfügbare Infrastruktur in die Welt getreten. Das World Wide Web hat die Technologie auch für Normalsterbliche ohne Ingenieurdiplom beherrschbar gemacht. Deregulierung der Telekommunikationsmärkte und technische Revolutionen in der Datenübertragung haben binnen eines halben Jahrzehnts den Engpaß verfügbarer Bandbreite faktisch eliminiert. Innerhalb von nicht einmal fünf Jahren haben sich vollkommen neue Unternehmen um diese Bedingungen herum gruppiert. Etablierte Firmen haben ihre internen Prozesse angepaßt. Neue Konsum- und Freizeitmuster sind

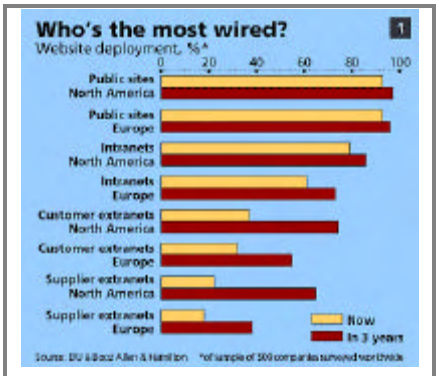

Abbildung 2 - Wer ist in den USA und in der EU am meisten vernetzt und in welchen Bereichen ist man "wired" ? Quelle: The ECONOMIST, 1999

[14] a.a.O. (Anm. 1)

entstanden. Auch das Argument einer materiell begründeten Aufsplitterung der Gesellschaft in „Information Haves“ und „Information Have-Nots“ kann so nicht gehalten werden, da die Preise für Zugang und Equipment dynamisch fallen. So besagt das in der Digital-Branche propagierte „Moore’sche Gesetz“, daß sich die Leistung eines Mikroprozessors alle 18 Monate verdoppelt[15], wobei im gleichen Zeitraum der Preis um die Hälfte fällt. Kurz und bündig: Die Kosten des Eintritts in die vernetzte Welt fallen permanent, die dafür erhältliche System-Leistung explodiert, die Benutzung wird immer einfacher und immer mehr Menschen profitieren von diesen Punkten. Das gilt zumindest für die entwickelten spät-modernen Industriegesellschaften der OECD-Welt.

Häufig entfaltet das aus vielfältigen medialen Anwendungen zu einem integrierten Kommunikationsmedium konvergierte Internet bereits im unmittelbaren Lebensumfeld der Menschen seine Wirkung. Lokale, regionale, nationale oder transnationale Interaktionsgruppen wirken zusammen. Egal ob dies Bürgernetzwerke, Stadtinformationssysteme oder auf räumlich weitverstreuten gemeinsamen Interessen und Motivationen aufbauende User-Gemeinschaften sind, sie verfügen über ein in dieser Form ungekanntes Maß an Mobilisierungs-, Interaktions- und Kampagnenfähigkeit. „In the Netherlands alone, sixty towns have embaced computer-mediated communication (CMC) and have civic networks of some kind.“[16] Mittlerweile gibt es kaum mehr eine deutsche oder europäische Großstadt, in der sich nicht ein ernstzunehmender Teil der personellen und politisch relevanten Interaktion im Netz abspielt. Verschiedene europäische Telekommunikationskonzerne (z.B. Deutsche Telekom, Telefonica) mußten die neue Netz-Macht 1998 und 1999 spüren, als nationale User-Communities die vermeintlich überteuerten Internet-Aktivitäten der Giganten boykottierten. Eine Cyber-Außenpolitik macht sich diese Lage zur Vermittlung ihrer eigenen Ziele zu Nutze. Sie hat aber auch auf ihren Zielen zuwiderlaufende Trends und kurzfristige Aktionen adäquat zu reagieren. Das geht heute in vielen Fällen nur im Cyberspace selbst – unter Nutzung seiner Möglichkeiten.

Ein unumkehrbarer Prozeß hat sich entfaltet, den Magnaten, wie Microsoft-Gründer Bill Gates, in einen „Web-Lifestyle“ münden sehen. Häufig ist hier der Wunsch der Vater des Gedanken – aber die Veränderungen sind evident. Und sie ziehen sich durch alle Gesellschaften der westlichen Welt. Dort macht die Transformation nicht Halt, sondern setzt zu einer globalen „Dritten Welle“[17] nach dem primären Übergang von der Nomaden- zur Agrargesellschaft und dem sekundären Sprung von dort zur Industriegesellschaft an. Schenkt man den Tofflers und Newt Gingrich, dem ehemaligen republikani-

[15] Vgl.: OECD: OECD Workshops on the Economics of the Information Society: A Synthesis of Policy Implications, Paris 1999, S. 10

[16] Cathy Bryan / Roza Tsagarousianou / Damian Tambini: Electronic Democracy and the Civic Networking Movement, in: dieselben (Hrsg.): Cyberdemocracy, Technology, Cities and Civic Networks, London 1998, S. 1

[17] Alvin Toffler: The Third Wave, London 1981

schen Mehrheitsführer im US-Kongreß, Glauben, dann läuft dieser dritte Sprung auf eine neue zivilisatorische Stufe hinaus[18].
Eine Welt, in der sich ein deutscher oder europäischer Durchschnittsbürger nur per Telefonleitung in das globale Medium einloggen muß, um ohne weitere Beschränkungen seinen Informations- und Kommunikationsbedürfnissen über kontinentale Grenzen hinweg frei nachzugehen, ist ohne jeden Zweifel grundverschieden von bisherigen Epochen. Die Mittler der Vergangenheit werden in der überkommenen Form überflüssig oder sie richten sich neu aus. Das gilt auch für Staaten und ihre Außenpolitik.
Woran hat die Neuausrichtung zu erfolgen ? Die Antwort: An dem, was mit hoher Wahrscheinlichkeit morgen die Standards setzt, weil dies heute schon erkennbar ist. Dabei handelt es sich a) um die strukturellen Grundlagen und Wirkungsweisen der transnationalen, vernetzten Gesellschaft und b) ihren ökonomischen Trägern in der neuen Digital-Wirtschaft. Auf diesen beiden Flanken der spätmodernen Industriegesellschaften des Westens vollziehen sich tiefgreifende Änderungen. Ebenso müßen sich außenpolitische Konzeptionen um das Neue ergänzen. Das Publikum hat sich geändert. Nicht mehr das Konzert der Mächte, sondern der Marktplatz der Ideen beherrscht das Parkett. Also muß auch der Spielplan angepaßt werden.

[18] Alvin Toffler / Heidi Toffler: Creating a New Civilisation, The Politics of the Third Wave, Atlanta 1995; Vorwort von Newt Gingrich

2.1 Die Analyse von Manuel Castells und ihre außenpolitischen Herausforderungen: „The Rise of the Network Society“

Als „Max Weber des Informationszeitalters“ müßte der in Berkeley Soziologie lehrende Castells wohl bezeichnet werden, entspräche man dem von ihm selbst an sein dreiteiliges Werk „The Information Age: Economy, Society, and Culture“ gerichteten Anspruch. Markus Perkmann billigt dem Mitglied der High Level Expert Group der EU-Kommission zur Informationsgesellschaft in der PVS immerhin zu: „...auf jeden Fall bietet Castells‘ visionäre und zugleich empirisch unterlegte Arbeit – ausgestattet mit dem Flair des großen Wurfs – eine fazinierende Analyse gegenwärtiger gesellschaftlicher Entwicklungen.“[19] Wenngleich die Verwendung des Begriffs „Network“ in diesem Zusammenhang sehr allumfassend erfolgt, so umschließt er doch die in diesem Papier relevanten Dimensionen auf eine erschöpfende Art. Aus diesem Grund sei Castells‘ Analyse auch nachstehend hervorgehoben; in der Natur dieses Working Paper liegend, kann das natürlich nur oberflächlich geleistet werden.

Catells erkennt einen globalen, „informationellen“ Kapitalismus als Quelle und definierendes Umfeld des Informationszeitalters. Informationstechnologie, veränderte organisatorische und institutionelle Strukturen und kulturelle Dynamiken konvergieren zu einer neuartigen sozialen Konfiguration in den vom informationellen Kapitalismus am meisten durchdrungenen Gesellschaften[20]. Hieraus resultiert seine „Network Society“ als neue, transnationale und mit neuen Konflikten kollidierender Pluralismen durchzogene epochale Großorganisationsform globalen bis planetaren Ausmaßes.
Die Folgen – oder: die Phänomene - sind vielfältig. Zum einen erkennt Castells eine „newest international division of labor“, welche die Welt-Gemeinschaft in vier verschiedene Gruppen aufteilt[21]:

- Die Produzenten von „High Value“, welche auf informationeller Arbeit aufbauen.
- Die Produzenten von „High Volume“, welche in industriegesellschaftlicher Tradition auf niedrigpreisiger Arbeitskraft aufbauen.
- Produzenten von Rohstoffen und Rohmaterialien. Sie leben von natürlichen Ressourcen.
- Schlußlichter sind die „redundanten“ Produzenten, welche auf entwertete Arbeit reduziert sind.

[19] Markus Perkmann: Die Welt der Netzwerke, in: PVS, 39. Jahrgang, 1998, S. 875
[20] a.a.O. (Anm. 19), S. 874
[21] Nachfolgend entnommen aus: Manuel Castells: The Information Age: Economy, Society and Culture, Volume I, The Rise of the Network Society, 3. Auflage, Oxford 1997, S. 147

Nun ist das alarmierende Merkmal der Castell'schen neuesten Arbeitsteilung, daß dieser Vier-Wege-Split nicht territorial oder regional zusammenhängend erfolgt. Da zumindest die ersten drei Kategorien von Produzenten in der „Network Society" in vielfältige Netze von Interdependenzen integriert sind, von denen das globale Daten- und Kommunikationsnetz das umfassendste ist, benötigen sie keinen räumlichen Zusammenhalt mehr. Sie können innerhalb einer nationalen oder regionalen Gesellschaft gleichzeitig und nebeneinander existieren – oder sie können miteinander über Kontinente hinweg in kooperativer bzw. konfliktiver Beziehung stehen. Es entsteht sozusagen eine totale Interdependenz. Zwischen diesem Gewebe können jedoch „schwarze Löcher" aufreißen. In ihnen verschwände die vierte Kategorie der „Redundanten".

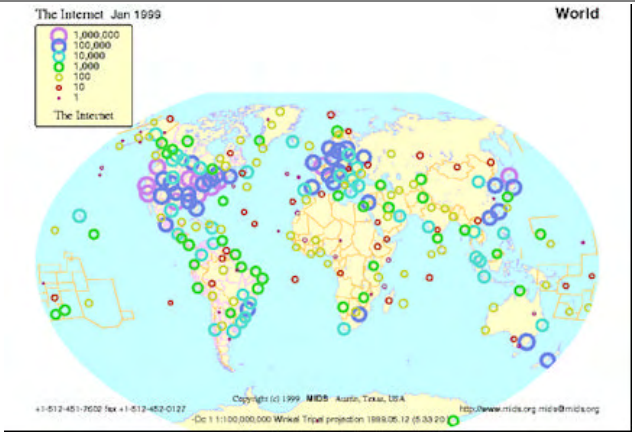

Abbildung 3 - Verteilung und Dichte der Host-Rechner des Internet im Januar 1999, weltweit. Quelle: http://www.mids.org

„By ‚black holes' I mean areas of social exclusion that can be marginalized and the system doesn't suffer at all. They're not valuable as producers, consumers – in fact, if they would disappear, the logic of the overall system would improve. If you are outside the network, in other words, you don't even exist."[22] Castells weiter: „...some rural regions of China, India, and Latin America, entire countries around the world, and large segments of the population everywhere are becoming irrelevant (*from the perspective of the dominant economic interests*) in the new pattern of international division of labor, and thus they are being socially excluded."[23] Das Netz der umherrasenden Elektronen kennt Inseln der Finsternis. Sie werden abgeschaltet.

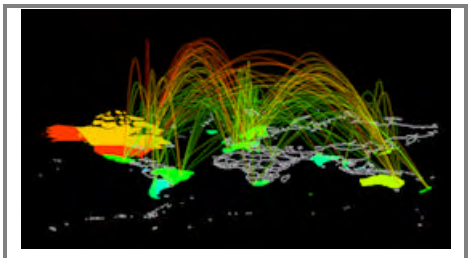

Abbildung 4 - Karte des globalen Datenflußes im Internet, 1996. Quelle: Bell Labs, entnommen aus: Martin Dodge / Rob Kitchin: Mapping the Network Society, 1999

Die Herausforderungen für eine Cyber-Außenpolitik liegen auf der Hand. Eine solche Politik kann sich in ihren Aktionsgeflechten nicht mehr an Grenzen (gleich welcher Art) orientieren. Vielmehr ist ihr Spielfeld die raumtranszendierende Struktur der Netzwerke. Sollte die Analyse von Castells auch nur ansatzweise zutreffen, so fordern die hieraus resultierenden globalen Bruchstellen und Konfliktpotentiale globale Politik heraus. Cyber-Außenpolitik hat auf diese für den territorial definierten und regional/global vernetzten Nationalstaat neue Konfliktlage rechtzeitig zu reagieren. Sie vertritt die Interessen, Ziele und

[22] Interview mit Manuel Castells, in: WIRED, November 1998, S. 188
[23] a.a.O. (Anm. 21), S. 113

Werte der „High Value“ produzierenden Gesellschaften im Dialog mit den Gesellschaften der anderen drei Kategorien.
Wie sieht eine solche Welt der vernetzten Knoten und abgeschalteten Sektoren aus ? Abstrakt formuliert kann gesagt werden, daß die „Network Society“ eine spezifische Topografie aufweist, innerhalb derer zu denken ist. Dies ist durchaus vergleichbar mit der Topografie einer Landkarte; solche Formen der Abstraktion gehören seit altersher zu den fundamentalen Werkzeugen der Außenpolitik. Die Landkarte der transnational-global vernetzten Gesellschaft entsteht gemäß der obenstehenden Aussage von Castells durch das Faktum der Integration eines Knotens (eines Landes, einer Stadt, einer sozialen Gruppe) in das Netzwerk. Jeder Knoten gehört dazu. Die Entfernung zwischen zwei Knoten ist per definitionem gleich Null. Jeder Nicht-Knoten ist nicht Bestandteil der vernetzten Gesellschaft. Er ist nicht-existent. Seine Entfernung zu einem Knoten der vernetzten Gesellschaft ist unendlich. Entfernung kann in diesem Sinne auch ganz praktisch mit der Häufigkeit von Interaktionen gleichgesetzt werden[24].

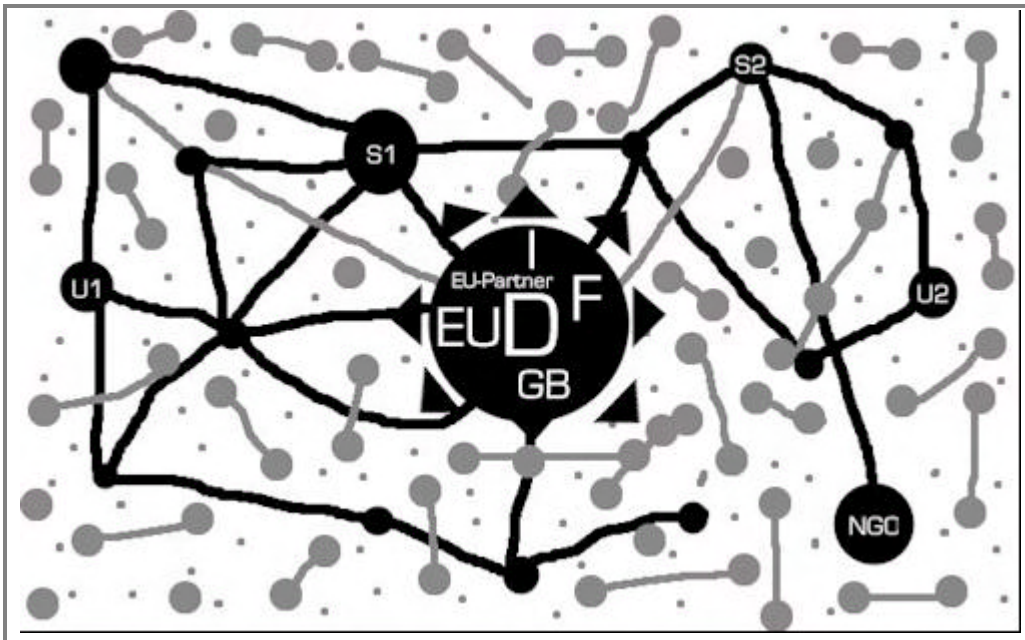

Abbildung 5 - Vereinfachte Modell-Skizze einer Cyber-Außenpolitik der EU-Partner in der global-transnational vernetzten Gesellschaft[25]. Legende: S=Staat, U=Unternehmen, NGO=Non-Governmental Organization

Die gute Nachricht ist, daß sich die Lage auch ändern kann. Netzwerke sind im allgemeinen – und für das Internet gilt das im besonderen – expansive Strukturen, welche eher auf Einbeziehung als auf Ausgrenzung gerichtet sind. Dennoch wird die Exklusion häufig durch kulturelle oder politische Faktoren eine unweigerliche Folge des von Mehrheiten oder Macht-Oligarchien gewählten Andersseins im westlichen Sinne sein. Autoritäre oder traditionale Gesellschaften sind latent von den Castells’schen schwarzen Löchern bedroht.

[24] Analog: a.a.O. (Anm. 21), S. 470
[25] Eigenes Modell und eigene Grafik (Halle, 1999)

Vice versa kann die OECD-Welt von eben diesen „Drop Outs“ durch transnationale Aktionen und soziale Verflechtungen bedroht werden. Hierzu folgen Betrachtungen unter 3.3, dem Abschnitt zur digitalen GASP. Aus diesem Grund muß rechtzeitig agiert werden, wenn nicht überrascht reagiert werden soll. Cyber-Außenpolitik wirkt durch aktives Tun auf die bestmögliche Kompatibilität der Klasse-4-Kandidaten mit der Logik der „Network Society“ hin.

Abbildung 5 skizziert die Struktur einer Cyber-Außenpolitik unter Würdigung der vorstehend umrissenen theoretischen Bedingungen. Die Skizze ist in bezug auf eine EU-Perspektive vereinfacht. Bestimmte, in Hinblick auf räumlich-geografische Distanz nicht spezifizierte Akteure oder Akteursgruppen stehen in einem engeren Verhältnis zum Epi-Zentrum der europäischen Cyber-Außenpolitik. Sie sind schwarz gekennzeichnet. Es kann sich um transnationale Key-Player der Digital-Wirtschaft handeln, welche Standards setzen und den Information Highway ausbauen. Aber auch andere staatliche Akteure (z.B. bestimmte US-Behörden oder einzelne Institutionen anderer Staaten) und Nichtregierungsorganisationen werden in das Web der europäischen Cyber-Außenpolitik eingebunden. Das ist nicht allzu neu. Tatsächlich finden solche politikfeldorientierten Kooperationen bereits statt; denken wir z.B. an Kriminalitätsbekämpfung im Cyberspace. Jedoch ermangelt es einer übergreifenden außenpolitischen Konzeption, welche von den einzelnen (nationalen) Knoten einer Cyber-Außenpolitik der EU-Partner kohärent realisiert wird. Andere (graue) Akteure sind nicht in das Policy-Web integriert. Sagen wir, weder technisch, noch politisch. Sie können integriert werden – oder sie können im Fall eskalierender Konflikte dekonnektiert werden. Natürlich sind dies nur erste theoretische und grob vereinfachte Ansätze zur Skizzierung des Rahmenkonzepts einer Cyber-Außenpolitik. Weitere Aspekte, Strategien und Szenarien werden nachfolgend beschrieben.

2.2 Um wessen Interessen geht es ? Hier kommt die „New Economy“ !

Im Agrar- und Feudalzeitalter wurden politische Konflikte und Kriege um den Schlüsselfaktor Boden und Territorium geführt. Das Industriezeitalter ließ im 19. Jahrhundert den Fokus auf den Zugang zu produktionsrelevanten Rohstoffen schwenken. Noch im 20. Jahrhundert wurden Konflikte und Kriege um den Faktor Rohstoffe ausgetragen. Das muß nicht heißen, das im Informationszeitalter notwendigerweise Kriege um den Zugang zu Informationen und Netzwerken geführt werden. Wahrscheinlich ist aber, daß um diese neuen Schlüssel-Ressourcen Info-Konflikte, gleich welcher Form, entbrennen. Westliche Außenpolitik wird für diese neue Konflikt-Kategorie Antworten und Strategien finden müßen. Dies gilt insbesondere, da die ersten Konflikte dieser Art in der westlichen Welt selbst entbrennen könnten.

Im Feudalzeitalter waren die konflikttragenden Akteure adlige Grundbesitzer. Im Industriezeitalter hatten die Krupps, Rockefellers und sonstige Industrie-Magnaten ihren Anteil an den kollidierenden Interessen. Das Informationszeitalter bringt die Köpfe hinter und in den Unternehmen der Digital-Wirtschaft (der sogenannten „New Economy“) auf das Spielfeld. Ihre Interessen gewinnen an Einfluß. Cyber-Außenpolitik nimmt sich dieser für eine neue Epoche wegweisenden Interessen an.

Als „New Economy“ (der in den USA gebräuchlichste Begriff), „Digitale Wirtschaft“, „Internet Economy“ oder „Electronic Economy“ soll die Gesamtheit aller mittelbar oder unmittelbar mit dem Internet als globales Netz der Netze kommerziell in Verbindung stehenden Unternehmungen verstanden werden. Ihr wesentliches Merkmal ist, das im Zentrum der Geschäftsmodelle der Unternehmungen die Entwicklung, Produktion und Distribution von Waren und Leistungen rund um das Internet steht. Die Leistungserbringung erfolgt entweder ausschließlich oder zumindest in wesentlichem Umfang über das Datennetz; in jedem Fall sind die Waren und Leistungen der „New Economy“ aber in wesentlichem Umfang auf solche Aktivitäten ausgerichtet. Die wohl bekannteste Erscheinungsform der Mitte der neunziger Jahres des 20. Jahrhunderts neu entstandenen Branche ist der Electronic Commerce (E-Commerce). Schätzungen über die Höhe des E-Commerce, welcher nur einen Teil der Digital-Wirtschaft darstellt, variieren. Sie werden gemeinhin eher nach oben korrigiert. „At present, electronic commerce over the Internet is relatively small (some $26 billion) but is growing very rapidly and may approach a trillion dollars by 2003-05.“[26] Franco Monti, Manager bei Andersen Consulting, lieferte in der NEUE ZÜRCHER ZEITUNG (NZZ) die nachfolgende Definition des Sujets:

> „Electronic Economy und Electronic Commerce stehen in einem ähnlichen Verhältnis zueinander wie Wirtschaft und Handel. Die Wirtschaft definiert sich als Gesamtheit aller Einrichtungen, Massnahmen, Pläne und Entscheidungen zur Befriedigung des menschlichen Bedarfs nach knappen Gütern. Als Handel wird der Austausch von wirtschaftlichen Gütern und Dienstleistungen zwischen Wirtschaftssubjekten gegen Geld bezeichnet. Electronic Economy entspricht der modernen Wirtschaft; in ihr wird der Handel aber mehrheitlich über Electronic Commerce abgewickelt. Die Electronic Economy kann nicht mehr alleine durch altbewährte volkswirtschaftliche Gesetze erklärt werden. Ihr zentrales Element ist die Beschleunigung. Märkte in der Electronic Economy werden in kürzester Zeit besetzt und über die Grenzen hinweg dominiert.“[27]

Monti sieht einen „unaufhaltsamen Wandel zur Electronic Economy“, welche auf einem zentralen Interesse aufbaut: „Ein Anbieter in der

[26] OECD: The Economic and Social Impact of Electronic Commerce, Executive Summary, Paris 1999, S. 12
[27] NZZ vom 30.4.1999; online: http://www.nzz.ch

Electronic Economy kann die vom Kunden geforderte Qualität der Dienstleistung nur unter einer Voraussetzung erreichen: Er muss die Geschäftsprozesse über die Ländergrenzen hinweg innerhalb des Unternehmens und entlang der Wertschöpfungskette integrieren und automatisieren.“[28] Ergo ergibt sich das Meta-Interesse der Unternehmen der „New Economy“ auf ungehinderte Interaktionsfreiheit der Anbieter und Nachfrager über alle politischen Grenzen hinweg.
Desweiteren sind alle Beeinträchtigungen abzulehnen, welche die Automatisierung von kommerziellen Abläufen behindern (egal ob dies eine nationale Buchpreisbindung ist oder ob es sich um sozialstaatliche Standards handelt).
Aus der Sicht der Digital-Wirtschaft können diese existentiellen Interessen am besten über die weitestmögliche Deregulierung von a) Märkten und b) Gesellschaften erreicht werden. Es wäre vermutlich zu kurz gegriffen, diese Branche als Avantgarde des Neo-Liberalismus oder als turbo-liberales Bollwerk gegen den Sozialstaat zu verstehen. Der Liberalismus ordnet dem Staat und seinen Institutionen immerhin eine Schutzfunktion zu. Wenn diese Schutzfunktion aber im Sinne industriegesellschaftlicher Kerne (Stahl, Kohle, Low-Tech, Bau, gemeinhin alle auf „Atomen“ aufbauende Branchen[29]) ausgeübt wird, dann liegt sie quer zu den Ordnungsvorstellungen der „New Economy“. Liberale sehen den Staat als notwendige gesellschaftliche Kategorie; sonst wären sie Anarchisten. Liberale tendieren zur Bewahrung von Institutionen, die New Economy tendiert jedoch zur Auflösung überkommener Institutionen. Liberale sind Verfechter einer Wettbewerbsordnung. Die New Economy spielt in wesentlichen Bereichen nach den Regeln des monopolistischen Wettbewerbs und kann durchaus monopolistische oder olygopolistische Strategien bevorzugen, welche auf partielle Marktschließung und Proprietarisierung des Internets gerichtet sind.
Das Interesse der Digital-Wirtschaft ist massiv darauf gerichtet, daß der Staat nach innen zur Digitalisierung erforderliche Hilfsleistungen erbringt, im übrigen aber dem Markt die Global-Ordnung überläßt; auch wenn diese keine Wettbewerbsordnung sein muß. Der Staat ist ein territorialer und regionaler Akteur, der in seinem Um- und Tätigkeitsfeld eine moderierende sowie unterstützende Rolle spielt. Überlagert wird er vom freien Datenfluß im Cyberspace. Die staatliche Kernfunktion ist, für die Aktivitäten der Digital-Wirtschaft in eben diesem Cyberspace die adäquaten Entfaltungsmöglichkeiten sicherzustellen. Dabei sind ggf. etablierte Institutionen und Regulierungen aufzulösen oder zu redefinieren. Weitere fundamentalen Interessen der New Economy – als Avantgarde der Globalisierung - sind beispielsweise:

[28] Ebd.
[29] Angelehnt an: Nicholas Negroponte: Total digital, Die Welt zwischen 0 und 1 oder die Zukunft der Kommunikation, 4. Auflage, München 1995; der Gründer des MIT Media Lab stellt in diesem Buch die Welt der Atome der Welt der Bits metaphorisch gegenüber

- Ein möglichst hohes Bildungs- und Wohlstandsniveau der Bevölkerung
- Ein optimales Maß an transatlantischer Integration als Rückrat des zukünftig planetaren Information Highway
- Deregulierte Telekommunikationsmärkte als Katalysatoren des Wandels zur vernetzten Gesellschaft
- Weitestmöglicher individueller Zugang zum Netz und bestmöglicher öffentlicher Einsatz für die globale Ausbreitung des Internet, ergo für eine globale Informationsinfrastruktur; Beförderung von Interkonnektivität und Interoperabilität
- Difussion des Netzes in alle sozialen Bereiche; starke Anwendung des Mediums in öffentlichen Verwaltungen und entsprechendes Reengineering der öffentlichen Hand
- Befähigung zur Geschwindigkeit, Beschleunigung des gesellschaftlichen, mikro- und makroökonomischen Wandels sowie der drastischen Reduzierung von Produktions- und Lebenszyklen von Wissensprodukten
- Freier Marktzugang zu allen von der Digitalisierung mittelbar oder unmittelbar erfaßten nationalen Teil-Märkten; Eliminierung entsprechender Hürden und rechtlicher Abgrenzungen
- In diesem Sinne: Beseitigung regulativer Sonderregeln für unterschiedliche Informationsinfrastrukturen (Telefon, Kabel, Funk, Strom, Satelliten)
- Ermöglichung eines freien, grenzüberschreitenden Kapitalflußes
- Rechtliche Zurückhaltung bei der Regulierung des Cyberspace
- Steuerliche Abstinenz bezüglich des E-Commerce
- Aktiver Einsatz der „cyberfreundlichen“ Staaten für die Verbreitung dieser Prinzipien in der Welt

Die Frage liegt nahe, warum soll man sich für solche Interessen einsetzen ? Eine Antwort liefert die Zeit. Denn bei der Tiefenwirkung des Wandels – in vielen Unternehmen, in vielen Wohnzimmern – bricht sich die neue Branche so oder so ihre Bahn. Die Frage ist, wer von diesem Trend profitiert und wer die größtmögliche Zusammenballung relevanter Digital-Akteure um sich scharren kann. Denn: Sie sind die Machtbasis der Zukunft. Es geht um die Wahrung und Neuverteilung von regionalem Wohlstand. Warum – um die Gegenfrage aufzumachen – sollte eine Region, welche gute Karten in der Hand hält, ihren temporären Vorteil nicht ausspielen, anstatt ihre Chancen zu verwarten ? In Deutschland und in der EU sind bezüglich vorstehender Eckpunkte im laufe der neunziger Jahre viele Hausaufgaben gemacht worden. Andere deregulative Maßnahmen sind auf dem Weg. Jetzt geht es darum, aus der gegebenen Lage das Beste zu machen und globale Aktionsräume zum eigenen Vorteil zu öffnen. In diesem Punkt stellt sich eine Interessenharmonie zwischen der Internet-Economy und führenden EU-Staaten ein. Darauf könnte aufgebaut werden.

E-Commerce ist nur eine Tranche der „New Economy“. In Anlehnung an eine Systematik des Center of Research in Electronic Commerce der University of Texas, welche in Auftrag von Cisco Systems entwickelt worden ist, soll nachstehend ansatzweise umrissen werden, welche Teil-Branchen die kommerzielle Entwicklung der „Network Society“ treiben[30]:

Schicht 1: Internet-Infrastruktur
Internet Backbone Provider (z.B. MCI Worldcom)
Internet Service Provider (z.B. AOL)
Auf Vernetzung spezialisierte Hardware- und Software-Hersteller (z.B. Cisco)
PC- und Server-Hersteller (z.B. Dell, Compaq)
Sicherheitsexperten
Hersteller von Glasfaser-Produkten
Hersteller von Produkten zur Datenbeschleunigung
Schicht 2: Internet-Anwendungen
Internet-Berater
Anwendungen für den internetbasierten Handel (z.B. Netscape, Microsoft, Sun, IBM)
Software zur Web-Entwicklung (z.B. Adobe)
Software für Suchmaschinen
Online-Training
Web-basierte Datenbanken für das Internet und für Intranets
Schicht 3: Internet-Zwischenhändler
Organisatoren von Märkten in vertikalen Industrien
Online-Reiseagenturen
Online-Broker (z.B. E*Trade, Schwab.com in den USA, Consors in Deutschland)
Content-Börsen
Portale und Content-Provider (z.B. Yahoo!, Geocities)
Werbe-Broker im Internet (z.B. Doubleclick)
Online-Werbung
Schicht 4: Internet-Handel
Elektronischer Einzelhandel (z.B. Amazon.com bzw. Amazon.de, Buch.de, Libri.de, Boxman.de in Deutschland)
Hersteller, die ihre Waren online verkaufen (z.B. Dell)
Abo-basierte Anbieter
Airlines, die Tickets online verkaufen
Online-Entertainment
Tabelle 2 - Die vier Schichten der "Internet Economy", analog www.internetindicators.com

Diese Systematik der New Economy, Internet Economy oder digitalen Wirtschaft (wie einem beliebt) erscheint sinnvoll. Die OECD schält in einem umfassenden Report zu den Funktionsprinzipien der neuen Wirtschaft zwei Hauptfelder heraus, welche sich in überraschendem Umfang mit der Systematik in Tabelle 2 decken:

[30] Vgl.: University of Texas / Cisco Systems: The Internet Economy Indicators, 1999; online: http://www.internetindicators.com

> „Growth areas point in two main directions. First is the economic activity around building the information infrastructure. This includes manufacture of hardware, in the form of computers, routers and fibre optic cable, largely by big companies, as well as the operation of networks themselves. The second direction is in applications, content and services, the reasons why people interact electronically. This latter area is dependent on the former as an enabling foundation for their existance, in the same way that motels are dependent on highways.“[31]

Nach Bereinigung von statistischen Überlappungen erzielte die Branche 1998 allein in den USA einen Gesamtumsatz von 301,4 Milliarden US-Dollar und war für 1,2 Millionen Arbeitsplätze verantwortlich. Nicht nur, das einzelne Unternehmen eine höhere Marktkapitalisierung ausweisen, als die traditionellen Giganten der US-Wirtschaft (Auto, Chemie, etc.). Zusammen genommen wuchs die Internet Economy im Zeitraum 1995 bis 1998 allein in den USA um 174,5 Prozent (weltweite Wachstumsrate im Vergleichszeitraum: 3,8 Prozent). Für Europa liegen vergleichbare Daten noch nicht vor. Allgemein dürfte es ohnehin Abgrenzungsprobleme geben, da die bekannte Problematik des Intrakonzernhandels in dieser Branche ins Extreme gesteigert wird. Nimmt man die transatlantische Ebene als Bezugspunkt, ist davon auszugehen, das die aggregierten und bereinigten Zahlen nochmal ein gutes Stück über den obenstehenden Werten liegen.

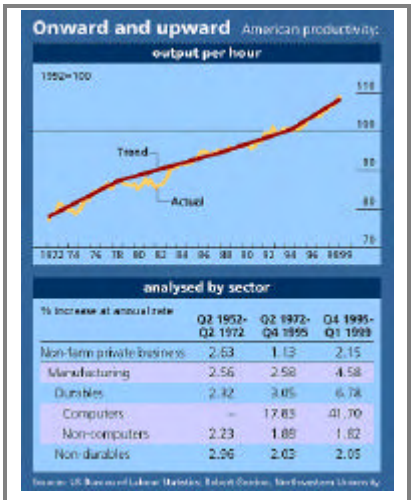

Abbildung 6 - Die IT-orientierte Entwicklung der Produktivität in verschiedenen Sektoren der US-Wirtschaft bis 1999. Quelle: www.economist.com

Außerdem ist der Kreis jener, die zur Internet Economy gehören in der Logik der Digitalisierung immer weiterer Bereiche im Prinzip nicht endgültig abgegrenzt. Die Musikindustrie klagt über die Herausforderung durch den neuen MP3-Kompressionsstandard für per Download aus dem Netz verfügbare Musik. Microsoft führt sein eigenes Musik-Kompressionsverfahren ein und geht auf die Musik-Industrie zu. Amerikanische Film-Produzenten überlegen, ob man zukünftige Kino-Filme nicht auf alternativen Wegen (teilweise an den Kinos vorbei) zu den Kunden bringen kann. Insgesamt ist ein Großteil der etablierten Entertainment-Industrie dabei, zur Internet Economy zumindest partiell hinzuzustoßen. Das Netz sickert in Produkte der Haushaltsgeräte-, Automobil- und Finanzindustrie ein. Auch hier liegen Potentiale, welche sich in der Bilanz der New Economy niederschlagen werden. Die neunziger Jahre des 20. Jahrhunderts haben einen Giganten geboren, der sich verwundert die Augen reibt: und weiter wächst. Politik im frühen 21. Jahrhundert wird ohne ein Ohr für die Wünsche des digitalen Riesen nicht auskommen kön-

[31] OECD: OECD Workshops on the Economics of the Information Society: A Synthesis of Policy Implications, Paris 1999, S. 12

nen. Das gilt konsequenterweise auch für die Außenpolitik. Sie wird in diesem Politikfeld ihren Weg finden müssen. Der richtige Weg kann die Mission zur globalen Ausweitung der Funktionsprinzipien der digitalen Wirtschaft sein, welche „daheim“ boomt.

„How real is the new economy ?“, fragte der ECONOMIST im Juli 1999[32]. Ein kritischer Bericht nahm das verwunderliche Phänomen der neunziger Jahre näher unter die Lupe. Der Tenor: auch wenn man den digitalen Mythen nicht allzu weit trauen sollte, so vollzieht sich doch sehr Erstaunliches in der realen Wirtschaftswelt. Allerdings nicht überall. Robert Gordon, Professor an der Northwestern University, untersuchte das Produktivitätswachstum in der US-Wirtschaft und „...has found that more than 100% of the acceleration in productivity since 1995 happened not across the economy as a whole, nor even across IT at large, but in computer manufacturing, barely 1% of the economy.“[33] Nur ein sehr geringer Sektor der US-Wirtschaft vermochte voll und ganz die neuen Potentiale auszuschöpfen. In Europa wäre entsprechende Forschung angebracht. Es steht fest, daß ein sehr kleiner Teil der Volkswirtschaften beiderseits des Atlantik verblüffende bis sensationelle Produktivitäts- und Wachstumssprünge macht. Dieser Sektor könnte die besten Chancen – von einigen Börsen-Korrekturen einmal abgesehen – haben, sein Wachstum in das 21. Jahrhundert hinein fortzusetzen. Es ist eine neue Kraft geboren. Quantitativ ist sie eher klein. Qualitativ ist sie sehr groß. Auf diesem Hintergrund sollte sie als strategischer Partner für die Außenpolitik Deutschlands und seiner Partner auf beiden Seiten des Atlantik adressiert werden.

3. Zeit zum Handeln – Ansatzpunkte für eine Cyber-Außenpolitik und eine adäquate GASP für das Informationszeitalter

Neben den eher standort- und außenwirtschaftspolitisch orientierten Ausführungen der vorstehenden Abschnitte sollen nun die strukturellen und zielbezogenen Voraussetzungen einer deutschen und europäischen Cyber-Außenpolitik angedacht werden. Auch die Bereiche Krieg und Frieden, Sicherheit und Macht werden auf globalem Niveau tangiert.

Unterschiedliche Vorstellungen bezüglich der globalen Ausgestaltung der vernetzten Gesellschaft bedingen die Notwendigkeit zum Dialog. Die Abhängigkeit der westlichen High-Tech-Volkswirtschaften beiderseits des Atlantiks von optimalen Entfaltungsbedingungen der digitalen Wirtschaft und der vernetzten Gesellschaft verlangt proaktives Handeln der führenden EU-Staaten und der USA.

[32] The ECONOMIST, 24.7.1999
[33] Ebd.

Nachfolgend wird beispielhaft auf unterschiedliche Ziele bezüglich der Architektur der vernetzten Gesellschaft eingegangen. Das transnationale und die Konfliktaustragung im und um den Cyberspace begünstigende Element der aufziehenden globalen Ordnung in den Netzen fordert eine kohärente Konzeption mitgliedsstaatlicher und europäischer Politik. Die Kollission verläuft zwischen Offenheit und Abschottung/Kontrolle des Netzes. Sie betrifft mithin die Alternativen Wohlstand für kommende Generationen in der OECD-Welt versus Netz-Nutzung auf niedrigem Niveau. Es ist zu erwarten, daß divergierende Vorstellungen bezüglich der Entscheidung dieses Zusammenpralls der Netz-Visionen im Zusammenspiel mit Konflikten in der realen Welt in der Nutzung des Internet (auch) zur Konfliktaustragung münden.

Die Bezugsgröße einer Cyber-Außenpolitik ist die vernetzte Gesellschaft, nicht primär ein anderer Staat. Aber natürlich muß ein Dialog im vorstehenden Sinne auch mit staatlichen Stellen anderer Nationen geführt werden; insbesondere, wenn Regulierungs- und Abschottungsstrategien ihre Wurzeln in autoritären Regierungen und dem Versuch ihres Machterhalts haben. Erfolge werden letztlich nur durch die Moderation eines gesellschaftlichen Dialogs erreichbar sein. „Die Welt des ausgehenden 20. Jahrhunderts ist keine Staatenwelt mehr.“[34] Czempiel verweist mit dem Begriff der Gesellschaftswelt auf einen Eckpunkt für eine erfolgreiche Cyber-Außenpolitik:

> „Überall ... ist die Partizipation und der Wunsch dazu vorhanden, überall steigen beide. Subjekte in der internationalen Politik sind nicht mehr, wie in der Staatenwelt, nur die Regierungen, sondern auch schon die Gesellschaften. Das ist die differentia specifica, die die moderne von der vormodernen Welt unterscheidet. Bedeutung und Einwirkung der Gesellschaften sind in den Weltregionen höchst unterschiedlich verteilt. Nirgendwo aber sind sie, wie früher, irrelevant.
>
> Diese Entwicklung läßt sich mit der politischen Metapher der „Gesellschaftswelt“ wiedergeben. Der Begriff soll ausdrücken, daß die Welt noch keine Weltgesellschaft, aber auch keine Staatenwelt mehr ist, daß sie nach wie vor eine staatlich geordnete Welt darstellt, in der aber das politische Gewicht der Gesellschaften wächst.“[35]

Diese Begrifflichkeit hilft beim Entwurf einer Cyber-Außenpolitik weiter. Vernetzt sind vornehmlich gesellschaftliche Akteure, welche durch die Konnektierung in der Tat auf dem langen Weg zu einer „Weltgesellschaft“ sind. Eine solche im globalen Netz der Netze tendenziell angelegte Weltgesellschaft ist jedoch in Kulturkreise, Regionalismen und sprachliche Sub-Netze zerklüftet. Außenpolitische Aktionen und Reaktionen müßen auf diese Tatsachen Rücksicht nehmen. Das kann am besten durch die Einbindung gesellschaftlicher

[34] Ernst-Otto Czempiel: Weltpolitik im Umbruch, Das internationale System nach dem Ende des Ost-West-Konflikts, München 1993, S. 106
[35] Ebd., S. 106 f.

Akteure aus diesen Sub-Netzen erreicht werden. Cyber-Außenpolitik bedeutet das Schmieden transnationaler Allianzen zur Beförderung der Offenheit des Cyberspace. Staaten motivieren, lenken, moderieren und unterstützen die Elemente solcher Handlungszusammenhänge. Sie garantieren die Sicherheit der Infrastruktur und der Artikulationsfähigkeit ihrer gesellschaftlichen Partner.

In diesem Zusammenhang ist ein weiterer Schlüssel-Terminus einer Cyber-Außenpolitik zu nennen. Da Zwang im gesellschaftlichen Dialog grundsätzlich ausscheidet, muß die Kohärenz der gewählten Akteure in den Ziel-Gesellschaften außenpolitischer Aktion mit den Interessen der vernetzten Gesellschaften des Westens auf freiwilliger Basis herbeigeführt werden. Hierbei geht es um die Organisation und Ausübung von „Soft Power" durch die Europäer. „Soft Power ... is the ability to get desired outcomes because others want what you want. It is the ability to achieve goals through attraction rather than coercion."[36] Gemäß Keohane und Nye geht es bei der erfolgreichen Ausübung von „Soft Power" um die Anziehungskraft der eigenen Ideen und Kultur. Zudem sei es wichtig, die Agenda des Dialogs durch Standards und Institutionen zu setzen, welche die Präferenzen des Counterparts beeinflussen.[37] Da es sehr wahrscheinlich ist, daß das Bild der schönen neuen Multimedia-Welt mit einem hohen Maß an Attraktivität für Teile der Eliten in nichtwestlichen Gesellschaften verbunden ist, sind Optionen zur Gewinnung dieser Kräfte für die Vision einer offenen, vernetzten Gesellschaft denkbar. Solche Lobbies oder Interessengruppen wären zu unterstützen. Hierfür bieten sich insbesondere koordinierte Aktionen von an Markterschließung interessierten Digital-Unternehmen an. Die Europäer sollten aufgrund der Vielfalt ihrer Kultur und ihrer nicht puristisch amerikanischen Ausrichtung in den Augen solcher Gesellschaften eine faire Chance zur erfolgreichen Anwendung von „Soft Power" in diesem Sinne haben. *Vernetzung* der transnationalen Gesellschaftswelt, europäische *Soft Power* und das *Internet* könnten zu einem machtvollen Instrument der Öffnung und Demokratisierung der Welt werden.

3.1 Dialog für offene Netze und gegen Abschottung

Für autoritäre Regierungen liegt es nahe, Ansätze der Pluralisierung und des grenzüberschreitenden Kontakts ihrer Bürger mit möglicherweise Andersdenkenden oder gar mit oppositionellen Bewegungen zu erschweren – oder ganz zu unterbinden. Da das Internet und jede Form der computervermittelten Kommunikation über Datennetze eine Art puristischer Alptraum für Diktatoren & Co. sind, verwundert es wenig, wenn die neue Leittechnologie Europas und Nordamerikas den Zorn so mancher Regierung auf diesem Glo-

[36] a.a.O. (Anm. 11), S. 86
[37] Analog: Ebd.

bus auf sich gezogen hat. Der Irak ist ein Beispiel par exellance. Aus Angst vor unerwünschten und unkontrollierten Informationsflüssen wird das Internet gleich ganz aus den Landesgrenzen verbannt. Lediglich die UN-Vertretung des seit dem 2. Golfkrieg wirtschaftlich und technologisch ausgebluteten Landes besitzt eine Homepage. Freilich ist in diesem Fall die autoritäre „Tugend“ aus der Not geboren: Die UN-Sanktionen verhinderten während der neunziger Jahre weitestgehend ein Upgrade der ohnehin nur rudimentären Computer-Basis und des zerbombten Telekommunikationsnetzes.
Aber auch in anderen Fällen ist das Internet keine erwünschte Technologie. Ein im August 1999 veröffentlichter Report der Organisation „Reporters Sans Frontières“ definierte 45 Staaten als das Internet „ernsthaft behindernd“ und 20 dieser Staaten als „...richtige Feinde dieses neuen Kommunikationsmittels.“[38] Wenngleich die wissenschaftliche Güte dieser Quelle durch subjektive und nicht immer nachvollziehbare Angaben gemindert wird, so deckt sich das Bild im Detail doch mit Analysen Dritter. Die gängigen Methoden zur Eindämmung des meistens in politischer Hinsicht als „schädlich“ empfundenen Netz-Einflußes sind a) Zwang zum Internet-Zugang über einen häufig monopolistischen Internet Service Provider (ISP) unter staatlicher Kontrolle, b) Zwang zur Registrierung als Internet-Nutzer bei staatlichen Behörden (z.B. bei der Polizei in der VR China), c) software- oder/und auf der nationalen Netzarchitektur basierte Filterung unerwünschter Inhalte bzw. Sperrung solcher Adressen. Als weitere, durchaus effiziente und häufig dem (politisch gewollten) mangelnden Telekommunikationswettbewerb geschuldete regulative Maßnahme, kann ein hohes Preisniveau für den lokalen Internet-Zugang angesehen werden.

Die Liste der „20 Feinde des Internets“ von Reporters Sans Frontières umfaßt u.a. Staaten, wie: Aserbaidschan, Kasachstan, Kirgisistan, Tadschikistan, Turkmenistan, Usbekistan, Weißrussland, Burma/Myanmar, die VR China, Kuba, Iran, Irak, Libyen, Nord Korea, Saudi Arabien, Sierra Leone, Sudan, Syrien, Tunesien und Vietnam. Zieht man in Betracht, daß sowohl die Bundesrepublik Deutschland, als auch ihre EU-Partner, zu einigen dieser Staaten teilweise gute Beziehungen unterhalten, so wird das Handlungsfeld für eine Cyber-Außenpolitik deutlich.
Auf der anderen Seite ist diese Liste der „Schurken“ mit Bedacht zu betrachten. Denn gerade die Fälle VR China, Iran und in engen Grenzen auch Saudi Arabien (dessen erst 1998/99 in Betrieb genommene, äußerst restriktive Internet-Infrastruktur auch mit beratender Unterstützung der dem BMZ nahestehenden Gesellschaft für Technische Zusammenarbeit realisiert worden ist) zeigen, daß es für

[38] Vgl. online: Reporters Sans Frontièrs: The Twenty Enemies of the Internet, http://www.rsf.fr/uk/alaune/ennemisweb.html (Stand:12.8.1999), Paris 1999 und WIRED NEWS: The Net: Enemy of the State?, http://www.wired.com/news, 12.8.1999

autoritäre Regierungen nicht ratsam ist, die Vernetzung total abzulehnen und abzuwürgen. Gemeinhin steht in diesen Fällen der Wille zur wirtschaftlichen Modernisierung der Angst vor unkontrollierbaren politischen Einflüssen gegenüber. Häufig werden Konzessionen zu Gunsten der Wirtschaft und interessierter Gruppen in den Eliten gemacht. Das Beispiel der VR China ist für diesen Spagat signifikant. Man sieht die betriebs- und volkswirtschaftlichen Chancen der Vernetzung innerhalb des Landes sowie mit der überseeischen Diaspora. Also wird versucht, die Vernetzung kontrolliert, z.B. durch eine hochentwickelte Abgrenzung der zugänglichen Inhalte nach Außen, durchzuführen. Der Preis dieser „sowohl-als-auch" Haltung ist eine gedrosselte Netz-Dynamik, die sich auch negativ auf wirtschaftliches Wachstum auswirken kann. Eine Klassifizierung Chinas als „Feind des Internet" erscheint auf diesem Hintergrund nicht angemessen. Diese Auffassung dürfte auch durch das Faktum bestärkt werden, daß das durchweg kapitalistisch und weltmarktorientierte Singapur eine durchaus ähnliche Strategie fährt: Strenge Kontrolle der zugänglichen Internet-Inhalte durch Proxy-Server bei gleichzeitigem, vehementen Ausbau der Netz-Infrastruktur.
Der Handlungsbedarf für eine Cyber-Außenpolitik sollte evident sein. Denn sollte es dem riesigen chinesichen Markt gelingen, eine monumentale Filter- und Regulierungsinfrastruktur in die Welt zu setzen, so könnte dies auch langfristig zu einer Bedrohung der Freiheit des Netzes in Europa führen. Damit stünden indirekt hunderttausende von Arbeitsplätzen in Gefahr – von der freiheitlichen Gesellschaftsordnung einmal ganz abgesehen. Eine der größten Gefahren des Informationszeitalters ist der Verlust von Dynamik. Es darf nicht verschwiegen werden, daß bei der Entwicklung entsprechender Technologien auch führende US-Unternehmen in der VR China engagiert sind. In ähnlichem Umfang ist auch die Klassifizierung Saudi Arabiens zu relativieren. Zwar mag es stimmen, daß das Königreich tatsächlich die restriktivste Filter-Infrastruktur auf diesem Planeten aufgebaut hat. Jedoch muß auch festgestellt werden, daß selbst innerhalb der königlichen Familie starke Geschäftsinteressen hinsichtlich des Netz-Ausbaus bestehen. Hier könnte im Sinne dieses Papiers außenpolitisch angesetzt werden, um die regulative Verfestigung entgegen der Interessen der vernetzten Wirtschaft in Deutschland, Europa und in den USA durch eine schrittweise Auflockerung zu ersetzen. Selbst im Iran existieren mittlerweile grundlegende Internet-Infrastrukturen, welche zudem „liberaler" (wenn der Begriff hier verwendet werden kann) als in Saudi Arabien sind. Gleiches gilt für die kleinen Golf-Staaten, wie Bahrain, die Vereinigten Arabischen Emirate, Kuwait, Qatar, den Jemen[39] und auch für Jordanien. Es kommt Bewegung auf, die in diesen teilweise doch recht kaufkräftigen Märkten für deutsche und europäische Interessen genutzt werden kann. Notwendig ist ein gesellschaftlicher Dialog, auf der Grundlage eines kohärenten außenpolitischen Konzepts. Es geht um einen milliardenschweren Markt, der sich entfaltet, wenn sich das Internet er-

[39] a.a.O. (Anm. 1)

folgreich über den gesamten Planeten ausbreitet. Und es geht um Menschenrechte[40], um ein Fundament deutscher und europäischer Außenpolitik.

3.2 Deutsche Cyber-Außenpolitik

Das Ende des Ost-West-Konflikts, die Erlangung der deutschen Einheit und die drastische Vertiefung der europäischen Einigung (nicht zuletzt durch die Wirtschafts- und Währungsunion) stellen Wendepunkte größter Tragweite in der Geschichte deutscher Außenpolitik dar. Jahrzehntelang war deutsche Außenpolitik bemüht, die Scherben des 2. Weltkriegs abzutragen. Dies gilt gleichermaßen für die Außenpolitik der Bundesrepublik Deutschland und der damaligen DDR. Allerdings war die Außenpolitik der Bundesrepublik Deutschland trotz der Korsage durch die Sachzwänge des Kalten Kriegs mit einem im Vergleich zur DDR weitaus größeren Maß an Bewegungsfreiheit versehen. Diese Freiheit richtete sich seit den fünfziger Jahren des 20. Jahrhunderts verstärkt auf die Erlangung eines gleichberechtigten Platzes in einem geeinten Europa. Dieses von Konrad Adenauer angestoßene Konzept wurde ein voller Erfolg – und stieß Deutschland letztlich auf die Siegerseite des Kalten Krieges. Fest in der Allianz westlicher Demokratien verwurzelt, sieht sich das geeinte Deutschland mit seinen EU-Partnern den Herausforderungen der neuen Weltordnung des beginnenden 21. Jahrhunderts gegenüber gestellt; eine neue Weltordnung, welche nur schemenhaft zu erkennen ist. Eines dieser Schemen, das sollte auf den vorstehenden Seiten klar geworden sein, ist das angebrochene Informationszeitalter und die global vernetzte Gesellschaft, welche die Tendenz zu einem planetaren System in sich birgt. Damit wird der Cyberspace indirekt zu einer Kategorie deutscher Außenpolitik. Vielleicht nicht heute – aber mit Sicherheit morgen. Das Netz gehört zur von deutscher Außenpolitik mitzugestaltenden neuen Weltordnung, wie die Ozeane im 16. Jahhundert zum Aufbruch Europas in die Welt gehörten.

Deutschland, als eine europäische Führungsmacht und als einer der engsten Verbündeten der USA, hat die Verantwortung, diese Transformation global mitzugestalten. Es liegt auf der Hand, daß dies nach Jahrzehnten der Orientierung deutscher Außenpolitik auf Europa-Politik und atlantische Bündnispolitik nicht leicht fällt. Es liegt auch auf der Hand, daß die verantwortungsvolle Rolle, welche Deutschland nach dem Ende des Kalten Kriegs gegenüber seinen ehemaligen Gegnern und heutigen Partnern in Mittel- und Osteuropa sowie der ehemaligen Sowjetunion übernommen hat, wertvolle außenpoliti-

[40] Art. 19 der allgemeinen Erklärung der Menschrechte der Vereinten Nationen gewährleistet die grenzüberschreitende Informationsfreiheit. 14 der vorstehend als „Feinde des Internet“ bezeichneten Staaten haben im übrigen selbige Erklärung bereits unterzeichnet.

sche Energie und Ressourcen bindet. Deutschland hat keine hinreichende Erfahrung im globalen Denken und Handeln. Offensichtlich waren frühere Versuche auch nicht allzu glücklich. Heute ist es aber an der Zeit, diese Herausforderung – auch im Cyberspace – zusammen mit den westlichen Partnern beiderseits des Atlantik anzunehmen. Dabei sollte deutsche Außenpolitik allen gesellschaftlichen Akteuren auf diesem Planeten die Hand reichen, welche mit den grundlegenden Werten und Zielen eben dieser Außenpolitik konform gehen: Einhaltung der Menschenrechte, Einsatz für eine marktfreundliche Wirtschaftsordnung, Öffnung der Märkte, Freihandel, Partizipation der Bevölkerung und friedliche Konfliktbewältigung. Diese Ziele können durch eine Cyber-Außenpolitik zumindest mit einem hohen Popularitätsgewinn versehen werden, da sie auf der einen Seite von jedem Wohnzimmer und Büro befördert werden können und zum anderen den Adressaten die faire Vision der Einbeziehung in die global vernetzte Welt bieten. Cyber-Außenpolitik kann den Frieden in der Welt nicht im Alleingang bringen. Sie kann aber einen konstruktiven Beitrag leisten. Und dies wäre nicht einmal der schlechteste. Eine solche Teil-Politik deutscher Außenpolitik wäre in der Lage, u.U. auch große gesellschaftliche Ressourcen in Deutschland für die Vertretung der Interessen der neuen Leitbranche zu gewinnen.

Es stellt sich die Frage, wie ein solches Projekt institutionell und organisatorisch auszugestalten wäre ? Theorie hin, Theorie her: Letztlich wird die arbeitsfähige Struktur einer deutschen Cyber-Außenpolitik – so sie darstellbar ist - durch jene festgelegt werden müßen, die damit arbeiten. Dies betrifft zwangsläufig auch die Ordnung der etablierten Institutionen zueinander und das Feld der potentiellen Ko-Akteure und non-gouvernementalen Partner. In Ermangelung einer koordinierten, kohärenten und institutionell gebündelten Politik-Doktrin und –Strategie für die Ausformung der Informationsgesellschaft auf nationaler und globaler Ebene könnte die außenpolitische Besetzung des offenen Politikfelds deutsche und europäische Interessen vermutlich besser vertreten, als dies bis dato der Fall ist. Nachstehend soll in Anlehung an das an David Easton orientierte vereinfachte Input-Output-Modell des Entscheidungssystems deutscher Außenpolitik von Reinhard Rode ein variiertes Modell für die hier behandelte Thematik zur Diskussion gestellt werden[41].

[41] Angelehnt an: Reinhard Rode: Deutsche Außenpolitik, Amsterdam 1996, S. 3

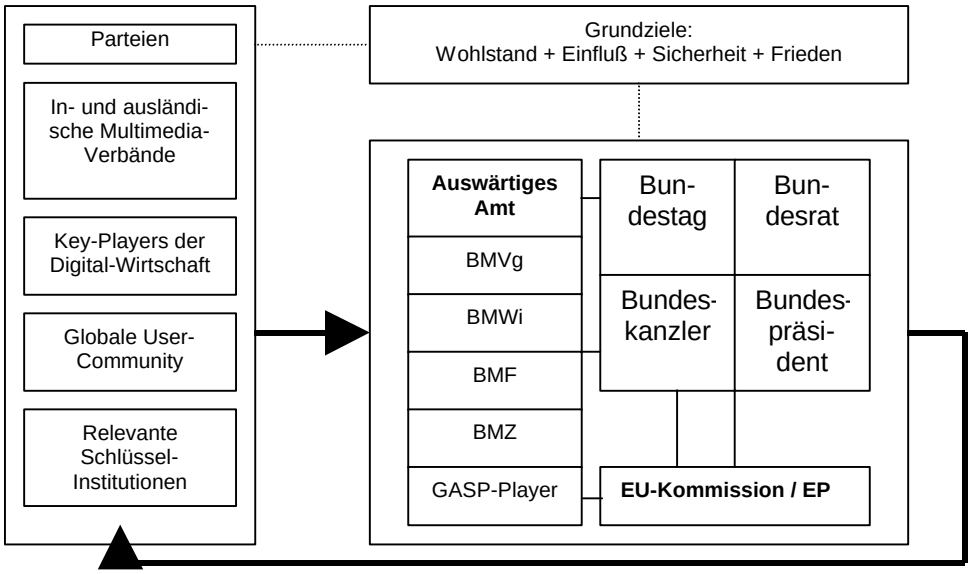

Abbildung 7 - Vereinfachtes Modell eines möglichen Entscheidungssystems deutscher Cyber-Außenpolitik. Quelle: Eigener Entwurf

Das obenstehende Modell ist behaftet mit dem Makel der Unvollständigkeit und des Neuen. Der Situation geschuldet, kann jedoch in dieser theoretischen und abstrakten Phase der Identifizierung von Handlungsoptionen einer deutschen Cyber-Außenpolitik nicht mehr geleistet werden. Klar werden sollte bei Betrachtung der Modell-Skizze, daß das neue Handlungsfeld eine Grenzen transzendierende Synergie aus etablierten nationalen Institutionen, hinzustoßenden EU-Strukuren (GASP), bestehenden Institutionen der Union, anderer EU-Partner und bis auf die individuelle Ebene hinabreichenden nichtgouvernementalen Akteuren ist. Es handelt sich um eine komplexe Struktur, welche sich der konkreten Aufgabenstellung flexibel anpassen muß. Wie bereits herausgestellt, handelt es sich um eine vereinfachte Input-Output-Struktur. Da das Ziel und die grundlegende Aufgabe deutscher Cyber-Außenpolitik die Initiierung und Moderation eines transnationalen gesellschaftlichen Dialogs über die Zukunft des globalen Cyberspace im Interesse Deutschlands und seiner staatlichen und nicht-staatlichen Partner sein soll, kann der Input von Forderungen in das politische, deutsche Entscheidungssystem erwartet werden.

Das Modell benennt als grundlegende Akteure und Akteurskonstellationen zur Artikulation solcher Forderungen (das kann auch Protest sein, wie z.B. im Fall des Compuserve-Urteils) mehrere mögliche Quellen. Sie sind von territorialen Zuordnungen grundsätzlich losgelöst. Zum einen – und für das nationale Politiksystem sicherlich sehr wichtig – sind die politischen Parteien zu nennen. Da Arbeitskreise und Gliederungen von SPD (dort gibt es z.B. einen virtuellen Ortsverband), GRÜNEN, CDU und FDP bereits entsprechende Positionen zur Cyber-Politik entwickelt und artikuliert haben, liegt die Einbeziehung in das Modell der Abbildung 7 nahe. In-

und ausländische Multimedia-Verbände sind eine Quelle von Expertise und von regulativen Vorstellungen in bezug auf technische Standards, Wettbewerbsfragen und Dimensionen des E-Commerce. Sie dienen auf der Input-Seite auch als Filter für kommerzielle und politische Partikularinteressen einzelner Unternehmen der Digital-Wirtschaft. So empfiehlt es sich, im Fall der Entwicklung von Politik-Strategien zur – sagen wir – Öffnung der Netzwerk-Architektur in der VR China, den Input der dort engagierten Firmen, wie z.B. Sun, Microsoft, Netscape, und örtlicher Anbieter aufzunehmen. Ein Dialog mit diesen Unternehmen kann dazu führen, daß eine allgemeine Interessenabstimmung erfolgt, welche sich dann in außenpolitisch relevanten Entscheidungen und Erfolgen niederschlägt. Eine wichtige Informationsquelle bezüglich entstehender oder latenter Info-Konflikte im globalen Netz stellt die unglaublich heterogene und faktisch unorganisierte globale User-Community dar. Der Input dieser Akteursgruppe ist von nationalen Grenzen vollkommen losgelöst und dürfte häufig auch nicht einmal geographisch lokalisierbar sein. Zu erwarten sind Protest- oder Unterstützungsaktionen. Zu denken ist an Boykott-Maßnahmen, die der Bundesrepublik Deutschland nahestehende wirtschaftliche, politische und gesellschaftliche Akteure treffen können. Aber es können bei geschickten außenpolitischen Manövern der Bundesregierung auch effiziente und aktive Unterstützungsmaßnahmen zu Gunsten deutscher Positionen erwartet werden. So z.B. im Menschenrechtsdialog oder im Fall der zwischenstaatlichen Konfliktaustragung bzw. bei Interaktionen mit nichtstaatlichen Akteuren.
Als offene Kategorie sind die „relevanten Schlüsselinstitutionen“ aufzufassen. Das können einzelne Behörden, Organisationen oder Autoritäten in Ziel-Staaten bzw. nicht-staatlichen Ziel-Gemeinschaften deutscher Außenpolitik sein. In diese Gruppe gehören auch internationale (WTO, WIPO, etc.) oder transnationale (z.B. User-Gruppen, ICANN) Organisationen. Auch hier kann prinzipiell Zustimmung oder Ablehnung fließen.

Das eigentliche Entscheidungssystem der deutschen Cyber-Außenpolitik wird im inneren Bereich von Abbildung 7 als deutsch/europäische Querschnittsstruktur umrissen. Damit wird dem hohen Maß der europäischen Integration deutscher Politikentwürfe und der werdenden GASP Rechnung getragen. Im Kern sind freilich die relevanten Ministerien der Bundesregierung zu sehen. Grundsätzlich variiert diese ministeriale Struktur wenig von der klassischen außenpolitischen Praxis. Allerdings sieht das Modell in Abbildung 7 bereits „GASP-Player“ vor und beschreibt damit vorsichtig etwas, das so faktisch noch nicht existiert. Die involvierten Ministerien und die außenpolitische Fachbürokratie stehen desweiteren in enger Abstimmung und Beziehung zu den Verfassungsorganen Bundesregierung (als umfassendes Kollegialorgan), Bundeskanzler (Richtlinienkompetenz), Bundespräsident und Bundesrat. Nicht aufgeführt, aber dennoch unter bestimmten Bedingungen relevant, ist das Bundesverfassungsgericht. Da das Bundesverfassungsgericht

durch seine Rechtssprechung aber nur mittelbare Wirkung auf die deutsche Außenpolitik entfaltet, wurde in der Modell-Skizze unter Abbildung 7 auf eine Listung verzichtet. Wichtig sind jedoch im Rahmen von die EU-Verträge tangierenden Politik-Initiativen die EU-Kommission und, seit dem Vertrag von Amsterdam in gestiegenem Umfang, das Europäische Parlament (EP). Sie stehen im möglichen Entscheidungssystem einer deutschen Cyber-Außenpolitik in enger Beziehung zu den Fachministerien (Ministerrat), den zukünftigen GASP-Institutionen und zu den Verfassungsorganen, insbesondere zu Bundeskanzler, Bundesrat und den Fraktionen des Bundestags. Sowohl dieser innere Kreis des außenpolitischen Entscheidungssystems, als auch relevante Akteure auf der Input-Seite (hier insbesondere die politischen Parteien in Deutschland) streben in der Modellannahme nach Verwirklichung bzw. Optimierung der cyber-außenpolitischen Grundziele Wohlstand (Erschließung und Kapitalisierung elektronischer Märkte), Einfluß (Mitformung der Grundstrukturen des offenen Cyberspace), Sicherheit (Abwesenheit von Bedrohungen der nationalen und globalen Informationsinfrastruktur) und Frieden (Dialog anstatt gewaltsame Konfliktaustragung als Reaktion auf die globale Netz-Expansion). Von diesen Grundlagen motivierte und in diesem System getroffene politische Entscheidungen wirken dann wieder als außenpolitischer System-Output auf die Akteure der Input-Seite zurück. In diesem „Feedback-Loop“ deutscher Cyber-Außenpolitik vollzöge sich die globale Einflußnahme der Bundesrepublik Deutschland im Verbund mit ihren Partnern.

Soviel zu einem möglichen theoretisch-strukturellen Rahmen. Was kann aber in concreto geleistet werden, um die aufgezeigten Ziele zu erreichen ? Nun, bereits mehrfach wurde das politikleitende Anliegen des gesellschaftlichen Dialogs und des Interesses der planetaren Expansion der digitalen Wirtschaft angesprochen. Auf dieser Ebene liegen konkrete Handlungsoptionen nahe. Zum einen besteht die Option der gezielten Unterstützung von exilierten Oppositionsbewegungen durch ein informationelles Upgrade ihrer kommunikativen und organisatorischen Fähigkeiten. Im Fall eines außenpolitischen Konflikts zwischen der Bundesrepublik Deutschland und dem Iran böte es sich an, die iranische Opposition in Deutschland und Europa bei dem Versuch der Vernetzung finanziell, technisch und logistisch zu unterstützen. Davon abgesehen, daß eine solche Unterstützung jederzeit eingestellt werden könnte, so es zu einer befriedigenden Konfliktbeilegung käme, hätte sie doch den Charme der Stärkung des externen, kommunikativen Drucks auf ein autoritäres Regime. Da der somit eintretenden Stärkung der kommunikativen Potentiale einer Oppositionsbewegung nur durch ein Gleichziehen einer autoritären Regierung, d.h. durch eine partiell-kommunikative Öffnung, begegnet werden könnte, bliebe unter dem Strich ein außenpolitischer Erfolg. Das Problem netzfeindlich eingestellter autoritärer Regierungen ist gemeinhin, daß die Nutzung der entsprechenden Potentiale durch die Opposition eine kommunikative Stärkung des politischen Gegners nach sich zieht. Das relative Gewicht zwischen beiden

Gruppierungen verschiebt sich somit auf globaler Ebene zu Gunsten der Opposition. Dieser Effekt kann durch deutsche oder europäische Cyber-Außenpolitik leicht genutzt werden, so dies politisch opportun erscheint.
Ein weiteres Mittel zur Expansion des Cyberspace – und damit zur Ausweitung des digitalen Marktes sowie individueller Kommunikations- und Informationsfreiheit – ist die Unterstützung alternativer, internetbasierter Informationsinfrastrukturen in Staaten, welche solche Netze gezielt behindern. Der Einwand, dies sei eine Einmischung in innere Angelegenheiten, kann kaum akzeptiert werden. Zum einen ist Informations- und Kommunikationsfreiheit qua definitionem keine innere Angelegenheit eines Staates, zum anderen fallen in diesem Punkt territoriale Abgrenzungen ohnehin schwer. Denken wir beispielsweise an die Vernetzung von Universitäten. Das Interesse deutscher Cyber-Außenpolitik müßte in diesem Fall auf eine frühzeitige Öffnung der Netz-Struktur und –Architektur in einem Ziel-Staat gerichtet sein, um eine spätere Schließung präventiv zu erschweren.

Bei all diesen Blicken in die Zukunft (noch spielen autoritäre Cyber-Großmächte keine konkrete Rolle) sollte nicht vergessen werden, das auf dem Gebiet der aktuellen transatlantischen Handels- und Technologie-Politik ebenfalls elementare außenwirtschaftliche und außenpolitische Interessen der Bundesrepublik Deutschland tangiert werden. Die innerwestliche Konfliktaustragung im und um den Cyberspace muß sich selbstverständlich anders gestalten, als im Umgang mit autoritären Staaten. In bezug auf internetorientierte Politikfelder haben transatlantische Dispute auch eine außenpolitische Dimension, die nicht verkannt oder verschlafen werden sollte. Das primär zwischen EU und USA ausgetragene Ringen um die zukünftige Regulierung des Internet, seines Adressen- und Domain-Systems, sei beispielhaft erwähnt. Die Mitsprache Deutschlands und Europas in der neuen regulativen Instanz ist durchaus von elementarem Interesse aus der Sicht einer entwickelten Informationsgesellschaft und der ihr nahe stehenden digitalen Wirtschaft. Deutschland kommt nicht umhin, für seine Positionen auf der gesellschaftlichen Ebene in den USA zu werben und entsprechende Diplomatie zu betreiben.

3.3 Eine GASP für die digitale Revolution

Wenngleich das Streben nach Dialog und Öffnung im Zentrum einer deutschen und europäischen Cyber-Außenpolitik stehen sollte, ist doch wahrscheinlich, daß der Gedanke an eine transnational vernetzte Gesellschaft globalen oder planetaren Ausmaßes nicht jedermann auf dem blauen Planeten verzückt. „The reaction to interconnection, dislocation and, by extension, globalization may be nationalism and a battle to maintain separate identities.“[42] Desweiteren begünstigt das Informationszeitalter eine Vielzahl von nicht-gouvernementalen Akteuren, welche feindselige und agressive Intentionen über die global integrierten Netzwerke verfolgen können. Die sozusagen im Sonderangebot, von der Kleiderstange erhältlichen Technologien des Informationszeitalters stehen auch Terroristen, der Mafia oder kleinen „Schurkenstaaten“ offen. Für diese Akteure kann es verlockend sein, die militärische und politische Überlegenheit der vernetzten Gesellschaften durch den „David-Effekt“ zu kontern. „The Information Age does not only offer ‚information dominance‘ as an option. It also introduces what could be called the David Effect...“[43]
Deutschland scheint momentan kaum in die Kategorie Goliat eingeordnet werden zu können, was die Fähigkeit zur Meisterung der sicherheitspolitischen Implikationen der digitalen Revolution betrifft. Sowohl die Bundeswehr als auch die gesamte Gesellschaft sind unvorbereitet. Michael J. Inacker wies 1997 in einem Aufsatz auf den Rückstand Deutschlands hin[44]. Etwas besser sieht es bei den EU-Partnern Großbritannien und Frankreich in puncto Vorbereitung auf Abwehr und Austeilung von Info-Attacken aus. Summa summarum sollten sich die global hochgradig verflochtenen und engagierten Europäer dringend Gedanken machen. Wischt man die lebendige Diskussion (vor allem in den USA) dieses neuen Bedrohungszenarios nicht als leeren „Hype“ vom Tisch, dann ist es für die Europäer im Rahmen einer eigenständigen Cyber-Außenpolitik an der Zeit, zur militärisch-technischen Revolution aufzuschließen. Zwar fehlen bis dato die empirischen Beweise für ein solche Bedrohungslage in massivem Umfang. Jedoch führte DER SPIEGEL Online im August 1999 eine ganze Reihe von kleinen Info-Attacken oder entsprechender Absichten zur Cyber-Kriegsführung in asiatischen Konflikten an[45]. Diese Aufstellung ist lesenswert.

[42] a.a.O. (Anm. 7), S. 341
[43] Ebd., S. 348
[44] Michael J. Inacker: Kriegführung im Computerzeitalter, der technologische Vorsprung der USA, in: Internationale Politik, September 1997, S. 43 ff.
[45] SPIEGEL ONLINE: Cyberwar, Der Krieg aus dem Netz, Stand 30.8.1999, http://www.spiegel.de/netzwelt/politik/0,1518,38605,00.html

Außenpolitisch ist besonders das neue Phänomen des „Information Umbrella“[46] von hervorstechender Bedeutung. Die Konflikte in Bosnien und im Kosovo haben den Europäern drastisch vor Augen geführt, was dieser von Nye und Owens geprägte Terminus für ihre außenpolitische und militärische Handlungsfreiheit bedeutet. Der Informationsschirm wird von den USA gehalten – und wer ohne ihn auf die Straße geht, der wird naß. Die einzigartigen Fähigkeiten der USA zur Sammlung, Prozessierung, Manipulation und Verteilung von konfliktentscheidenden Informationen „...point to what might be called an information umbrella. Like extended nuclear deterrence, they could form the foundation for a mutually beneficial relationship. The United States would provide situational awareness, particularly regarding military matters of interest to other nations. Other nations, because they could share this information about an event or crisis, would be more inclined to work with the United States.“[47] Die Rolle Deutschlands und seiner EU-Partner bei der diplomatischen und ggf. militärischen Lösung von ethnischen oder/und zwischenstaatlichen Konflikten in Mittel- und Osteuropa oder in anderen potentiellen Krisenregionen könnte sich also schnell auf eine Auxiliarfunktion reduzieren. Außenpolitische Optionen und Potentiale würden verspielt, wenn den außenpolitischen Herausforderungen der digitalen Revolution nicht Rechnung getragen wird. Die Leistung der 1992 in Artikel J 1 des Vertrags über die Europäische Union festgelegten GASP ist in diesem Punkt bis dato gleich null. Sieht man davon ab, daß es in anderen GASP-Bereichen nicht soviel besser aussieht, so drängt sich die digitale Dimension der GASP als Arbeitsfeld auf. Artikel J 4 des Vertrags über die Europäische Union bestimmt in Absatz 1: „Die gemeinsame Außen- und Sicherheitspolitik umfaßt sämtliche Fragen, welche die Sicherheit der Europäischen Union betreffen...“[48]

Gilt für die spät-modernen Gesellschaften Europas zu Beginn des 21. Jahrunderts nicht mehr die Clausewitz-Doktrin vom „Krieg als Fortsetzung der Politik mit anderen Mitteln“, so ist diplomatisch abgesicherte, multi-nationale, politisch flankierte und begrenzte Kriegführung nach 1990 doch wieder auf den alten Kontinent und in den Werkzeugkasten der Außenpolitik zurückgekehrt. Zusammen mit der militärisch-technischen und der digitalen Revolution in den zunehmend vernetzten Gesellschaften Europas ruft diese Lage nach einer adäquaten außenpolitischen Konzeption auf EU-Ebene, welche digitalen Attacken gegen einzelne EU-Staaten vorbeugt. Das wäre eine Cyber-Außenpolitik im Sinne der GASP. Neue Bedrohungsszenarien müssen rechtzeitig in Strategien umgewandelt werden, bevor ein russischer Drogen-Mogul, dessen Geschäftsinteressen durch eine deutsche Staatsanwaltschaft bedroht werden, den Flugverkehr nach Mallorca sabotiert oder gar die Sicherheitsvorrichtungen eines deut-

[46] Siehe: Joseph S. Nye, Jr. / William A. Owens: America’s Information Edge, in: Foreign Affairs, March/April 1996, S. 25 ff.
[47] Ebd., S. 27
[48] Vertrag über die Europäische Union, vom 7.2.1992

schen Atomkraftwerks durch bezahlte Hacker als Geisel nehmen läßt. Das konstruierte Beispiel scheint abstrus – aber es ist leider nicht irreal; und schon gar nicht virtuell. Ein kleiner „Schurkenstaat“ hat heute kaum Möglichkeiten, der Informationsdominanz der USA und ihrer europäischen Verbündeten auf konventionell-militärischem Weg zu begegnen, sobald er in einen heißen Konflikt eintritt. Der Irak-Krieg ist das beste Beispiel. Was also liegt näher, als a) durch Waffen der Massenvernichtung oder b) ggf. mietbare Info-Attacken einen gezielten, öffentlichkeitswirksamen Terror-Schlag gegen die USA oder Europa zu führen ?
Der vorgenannte Informationsschirm erlangt bei der außenpolitischen Bewältigung solcher Konflikte eine Schlüssel-Rolle. „Wenn der Faktor Information entscheidend für den Erfolg militärischer Operationen ist, dann wird im Rahmen von internationalen Bündnissen und Koalitionen nicht mehr nur die Überlegenheit im Bereich der Kräfte und der politische Wille zur militärischen Intervention, sondern auch die Überlegenheit bei der Informationsbeschaffung und –verarbeitung über die Führungsfähigkeit entscheiden.“[49] Führung heißt insoweit, Beherrschung der Schlüssel-Komponenten des Informationsmanagements.

> „As its capacity to provide this kind of information increases, America will increasingly be viewed as the natural coalition leader, not just because it happens to be the strongest but because it can provide the most important input for good decisions and effective action for other coalition members."[50]

Auf diesem Hintergrund stellt sich für deutsche und europäische Außenpolitik in der komplexer gewordenen Welt des neuen Millenniums die Aufgabe zur Erlangung eigenständiger Politik-Ressourcen. Nicht, um die transatlantische Partnerschaft zu schwächen, sondern um sie zu stärken. Nicht jede Herausforderung wird von den USA und ihren EU-Partnern gleichermaßen drängend empfunden. Situationen sind vorstellbar, in denen es der US-Seite Aufmerksamkeit und Kosten spart, wenn die Europäer von Anbeginn an zu eigenständigem Handeln fähig sind. Für potentielle Konflikte mit nicht-staatlichen Akteuren gilt dies besonders. Im Fall des Bosnien-Konflikts hätte eine solche Befähigung der Europäer zum adäquaten Handeln unter Nutzung eigener Info-Kapazitäten zu drastischen Einsparungen auf US-Seite und vermutlich auch zu einer schnelleren Konfliktlösung geführt. Die Zeit ist reif für eine gemeinsame Cyber-Außenpolitik unter dem Dach der GASP.

Zu Protagonisten der Diskussion um „Information Warfare“, „Cyberwar“ und „Netwar“ sind die Amerikaner John Arquilla[51] und David

[49] Andreas Wenger / Stephan Libiszewski / Patrik Schedler: Information als Machtfaktor in den internationalen Beziehungen, in: Bulletin zur schweizerischen Sicherheitspolitik, 1999; online: http://www.fsk.ethz.ch/publ/bulletin/bulle_99/b99/info.htm
[50] a.a.O. (Anm. 9), S. 27
[51] US Naval Postgraduate School, USA

Ronfeldt[52] geworden[53]. Zwar entspringt diese Diskussion bis zu einem gewissen Grad der Suche des militärisch-industriellen Komplexes in den USA nach neuen Aufgabenfeldern nach dem Ende des Kalten Krieges. Jedoch ist sie für das vorliegende Papier aufgrund objektiver Wahrscheinlichkeiten wichtig. „The Way any society engages in conflict reflects the way it does a lot of other things – especially the way its economy is organized."[54]
Die beiden Autoren regen eine Strategie der „Guarded Openness" an. Eine solche Ausrichtung der in letzter Instanz außenpolitischen Fähigkeiten eines Staates oder der EU zielt auf die präventive Eindämmung von Gefahren der Vernetzung im Spannungsfeld zwischen breitgefächertem Informationsaustausch und Wachsamkeit gegen feindseelige Attacken von Außenstehenden. Der sicherlich als solche zu sehenden Illusion einer friedlicheren Welt durch Vernetzung, bar jeglichen Konflikts, da alle gewinnen, halten Arquilla und Ronfeldt die Bedrohung durch neue Gefahren entgegen. „Prevailing hopes for the peace-enhancing tendencies of interconnectivity must be tempered by a realization that the information revolution augurs a new epoch of conflict, in which new modes of armed combat and social upheaval will emerge."[55]

Eine europäische GASP mit einer konsistenten Cyber-Außenpolitik wird jedoch nicht nur durch den Zwang zur Kohärenz gegenüber feindseeligem Verhalten von „Schurkenstaaten" und agressiven nicht-staatlichen Akteuren erzwungen. Die bewachte Offenheit der Netze, welche das Rückrat der EU-Wirtschaft im 21. Jahrhundert bilden, ist wichtig. Aber mindestens ebenso wichtig ist das außenpolitische Engagement der EU und ihrer Mitglieder in bezug auf unscheinbare Politikfelder transatlantischer Dimension. Info-Konflikte von strategischer Dimension finden sich auch in der atlantischen Familie. Heute werden die außenpolitischen Handlungsfreiräume von morgen definiert. Der Kernbereich des Cyberspace formt sich in der Interaktion der USA mit den EU-Staaten aus; freilich nicht immer in vollem Einklang mit den kulturellen- und wirtschaftlichen Potentialen der EU. Die Europäer werden durch mangelnde Kohärenz ihrer Politiken bei der Grundsteinlegung der vernetzten Gesellschaft zum Junior-Partner der USA degradiert; dies wäre eigener Ignoranz geschuldet. Negative Implikationen können leicht über Jahrzehnte andauern und zu einer Verfestigung außenpolitischer Impotenz im Informationszeitalter führen.

---

[52] RAND, USA
[53] Eine Aufgliederung und kurze Erläuterung der Begriffe ist auch online verfügbar: Bruck M. Kimmerle: Informationssanktionen, Halle 1998, http://www.politik.uni-halle.de/rode/infosanktionen.htm
[54] Vorwort von Alvin Toffler / Heidi Toffler, in: John Arquilla / David Ronfeldt: In Athena's Camp, Preparing for Conflict in the Information Age, Santa Monica 1997, S. 13 (Vorwort)
[55] John Arquilla / David Ronfeldt: Preparing for Information-Age Conflict, Part 1, Conceptual and Organizational Dimensions, in: Information, Communication and Society, Volume 1, Spring 1998, S. 1

Beispiel Nummer 1 für einen Hauskrach in der Familie: Die EU-Datenschutzrichtlinie vom 24.10.1995[56]. In diesem Fall sind die Europäer die Bösen – zumindest aus US-Perspektive. Hinter der Aufregung um die *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr* verbirgt sich ein handfester Konflikt um leitende Prinzipien der globalen Informationsgesellschaft. In den Kreisen der US-Digitalwirtschaft wurde dieser europäische Vorstoß mit Unbehagen und verhaltener Panik aufgenommen. „Europe to U.S.: No Privacy, No Trade" – so titelte Simon Davis im kalifornischen Magazin WIRED[57]. Die Richtlinie intendiert primär die Harmonisierung des Datenschutzes zwischen den EU-Staaten zwecks Herstellung eines ungehinderten Datenflußes im gemeinsamen Markt und Kommunikationsraum. Sie sollte eigentlich bis zum 23.11.1998 in nationales Recht umgesetzt sein. Bis zum Zeitpunkt der Abfassung dieses Papiers sind wesentliche EU-Staaten aufgrund diplomatischen Drucks der USA in Umsetzungsverzug. Im August 1999 drohte die EU-Kommission mit einer Klage vor dem Europäischen Gerichtshof. Deutschland gehört zu den Nachzüglern, befindet sich dabei aber in guter Gesellschaft. So hat z.B. Großbritannien die Richtlinie mit Stand August 1999 nur teilweise umgesetzt. Worum geht es ?
„Under this régime, known as the European Data Protection Directive, any country that trades personal information with the UK, France, Germany, Spain, Italy, or any of the other 10 EU states will be required to embrace Europe's strict standards for privacy protection."[58]
Der Vorstoß im Konflikt freiwilliger US-Datenschutzstandards gegen ein hohes regulatives Schutzniveau in der EU blieb nicht ohne Erfolg für die Europäer. Es entfaltete sich schnell eine Sogwirkung, welche viele Drittstaaten zur Anpassung ihrer Datenschutz-Régime an die europäischen Vorgaben veranlaßte. Ein prominentes Beispiel ist Kanada. In Schweden, einer der ersten EU-Staaten, der die Richtlinie in nationales Recht überführte, wies die Datenschutzbeauftragte Anitha Bondestam American Airlines an, alle gesundheitlichen und medizinischen Daten über schwedische Passagiere zu löschen, so keine explizite Zustimmung der Fluggäste vorliegt[59]. Die Grundlage für solche Schritte ist Kapitel IV der Richtlinie. Es regelt, daß Übermittlungen „personenbezogener Daten, die Gegenstand einer Verarbeitung sind oder nach der Übermittlung verarbeitet werden sollen, in ein Drittland..." nur zulässig sind, „wenn dieses Drittland ein angemessenes Schutzniveau gewährleistet" (Art. 25 Abs. 1). In diesem Punkt prallen grundlegende Vorstellungen über die strategische Regulierung des Cyberspace aufeinander. Die außen- und außenwirt-

[56] Orginal-Text online: http://www2.echo.lu/legal/de/datenschutz/datensch.html
[57] Simon Davis: Europe to U.S.: No Privacy, No Trade, in: WIRED, May 1998, S. 135
[58] Ebd.
[59] Vgl.: Ebd., S. 187

schaftspolitische Brisanz ist klar erkennbar. Es handelt sich um ein originäres Feld von Cyber-Außenpolitik. Allerdings muß es auch als solches erkannt und behandelt werden, zumal die EU-Datenschutzrichtlinie eine gute Verhandlungsmasse in anderen konfliktiven Bereichen böte. Die Alternativen für die Europäer dürften sein, die Richtlinie a) in der bestehenden Form fallen zu lassen und dafür ein Entgegenkommen der US-Administration in anderen Bereichen zu erhalten oder b) eine Lobby für das EU-Régime bei potentiellen Unterstützern in den USA einzuwerben (z.B. Bürgerrechtsorganisationen).

Beispiel Nummer 2 für einen cyber-außenpolitisch relevanten Info-Konflikt: ECHELON und das US-Exportkontrollrégime für starke Kryptografie-Software. Ein Report des Fachjournalisten Duncan Campbell für das Scientific and Technological Options Assessment (STOA) Komitee des Europäischen Parlaments[60] legte im April 1999 lange bekannte – aber verschwiegene – Fakten auf den Tisch der europäischen Öffentlichkeit. „Seit den siebziger Jahren sollen Geheimdienste der USA, Großbritanniens, Kanadas, Australiens und Neuseelands unter dem Code-Namen ‚Echelon' ein globales Spionagenetzwerk betreiben, welches sich jetzt auch verstärkt gegen die Wirtschaft der EU richten soll."[61] Geführt wird ECHELON durch den für Signalaufklärung zuständigen US-Geheimdienst National Security Agency (NSA).

> „Worum es im transatlantischen ‚Infokrieg' geht, wird aus der NSA-Website deutlich. Dort führt Geheimdienstchef Michael V. Hayden aus: ‚Eine Informationsrevolution überschwemmt die Welt. Sie erzwingt Wandel, der genauso radikal ist, wie jener, der durch die Entwicklung der Atombombe hervorgerufen wurde. Genauso wie die Kontrolle über industrielle Technologie in den letzten zwei Jahrhunderten der Schlüssel zu militärischer und wirtschaftlicher Macht war, wird die Kontrolle über Informationstechnologie der Schlüssel zur Macht im 21. Jahrhundert sein.' NSA-Chef Hayden ruft nach einer neuen nationalen Kraftanstrengung, die ‚einem einzigen Ziel gewidmet sein soll: Informationsüberlegenheit für Amerika."[62]

Die gouvernementale Strukturen transzendierende Reichweite solcher Aktivitäten wird deutlich, wenn man das Augenmerk auf die mittelbare Einbindung der marktführenden Softwarehersteller in Europa richtet. Außenpolitische Aktionen der EU-Staaten können sich also nicht nur in zwischenstaatlichen Kontakten erschöpfen.

> „Der STOA-Report gerät in diesem Punkt zum Schwarzbuch für führende Software-Hersteller, wie die IBM-Tochter Lotus, Microsoft und Netscape.

[60] European Parliament, Directorate General for Research (STOA): Development of Surveillance Technology and Risk of Abuse of Economic Information, PE 168.184/Part3/4, Luxembourg, April 1999; online: Interception Capabilities 2000, http://www.gn.apc.org/duncan/stoa_cover.htm
[61] Die WELT, vom 8.6.1999
[62] Ebd.

> Er wirft den US-Softwarefirmen vor, der NSA Code-Bestandteile in den Europa-Versionen ihrer Programme zugänglich gemacht zu haben. Campbell: „Lotus baute eine NSA-Hintertür als ‚Hilfsinformation' in sein Notes System ein." Mit dieser Modifizierung der Export-Software für Europa können, so der STOA-Report, verschlüsselte Nachrichten leicht geknackt werden. Die US-Versionen von Lotus Notes hingegen sind von der „NSA-Amtshilfe" frei. Lotus Notes soll beispielsweise bis zum Jahr 2003 an bis zu 80 000 Arbeitsplätzen der Bundeswehr eingesetzt werden, weltweit nutzen 34 Millionen Anwender die Software. Die schwedische Regierung sah sich bereits 1997 mit einer Überraschung konfrontiert. Unter anderem nutzten 349 Parlamentsabgeordnete, 15 000 Beschäftigte der Finanzverwaltung, wie auch Mitarbeiter großer Unternehmen und des Verteidigungsministeriums Lotus Notes. Laut ‚Svenska Dagbladet' staunte der Datenschutz-Chef des schwedischen Verteidigungsministeriums, Jan Karlsson, nicht schlecht: „Ich wußte nicht, daß unsere Lotus Schlüssel hinterlegt wurden."
> Stefan Krüger, Senior Product Marketing Manager der Lotus Development GmbH in Deutschland, bestätigt Campbells Report im Kern. „Das US-Exportministerium verbietet den Export von Schlüsseln größer als 40 Bit. Lotus hat, um einen größeren Schlüssel für die internationalen Versionen verwenden zu können, folgende Vereinbarung mit den amerikanischen Behörden getroffen. Alle internationalen Versionen (außer Frankreich) haben ebenso wie die USA einen 64 Bit Schlüssel, mit der Einschränkung, daß das amerikanische NSA den Key für die oberen 24 Bit besitzt."[63]

In diesem Zusammenhang tritt auch die wichtige Frage der Krypto-Politik auf die außenpolitische Tagesordnung. Kryptografie (softwaregestützte Verschlüsselung von vertraulichen Daten durch Codes) ist eine der Grundlagen für den E-Commerce und viele Internet-Anwendungen in Unternehmen und Forschungseinrichtungen. Nur eine möglichst starke Verschlüsselung wettbewerbs- und sicherheitsrelevanter Daten in Wirtschaft und Verwaltung gewährleistet die Vermeidung des schädlichen Mißbrauchs durch unbefugte Dritte. Die vorstehenden Ausführungen zu „Information Warfare", „Cyberwar" und „Netwar" sollten entsprechende Bedrohungsszenarien und Gefährdungen der deutschen und europäischen Volkswirtschaft(en) aufgezeigt haben. Nun ist das US-Exportrégime für Krypto-Software sehr stringent, da dieses Know How – exakt aus den vorstehenden Gründen - als „Munition" bzw. „Kriegswaffe" klassifiziert worden ist. Mithin dürfen nur Verschlüsselungsverfahren in einer Stärke bis zu 40 Bit (64 Bit bei einer Lösung, wie bei Lotus Notes) für Normal-User und 128 Bit für Banken außerhalb der USA verwendet werden. Codes mit einer Stärke von 128 Bit können heute mit marktgängigen Computern schnell und zuverlässig geknackt werden. Da die meisten führenden Softwarehersteller eine starke Basis in den USA haben, besteht auf diesem Weg Kontrolle über ihren Krypto-Vertrieb. Diese Verfahrensweise ist nicht unumstritten. Somit bestehen auch hier Ansätze für außenpolitische Aktionen der Europäer im Rahmen der GASP. So hat das Electronic Privacy Information Center 1999 einen

[63] Ebd.

umfassenden Report über die weltweite Verfahrensweise in puncto Krypto-Regulierung vorgelegt und kam zu dem Schluß: „Most countries in the world today have no controls on the use of cryptography...Export controls remain the most powerful obstacle to the development and free flow of encryption.“[64] Das US-Kontrollrégime wankt zumindest in der EU stark. Frankreich hat im Januar 1999 eine totale Kehrtwende vom Verbot starker Kryptografie und dem Zwang zur Hinterlegung des Private-Key („Key Escrow“) hin zur totalen Freigabe von Verschlüsselung vollzogen. Auch die Bundesregierung hat am 2. Juni 1999 mit ihrem Beschluß „Eckpunkte der deutschen Kryptopolitik“[65] die Entwicklung und Anwendung starker Verschlüsselungssoftware freigegeben. Dort heißt es: „Die Bundesregierung hält aus Gründen der Sicherheit von Staat, Wirtschaft und Gesellschaft die Fähigkeit deutscher Hersteller zur Entwicklung und Herstellung von sicheren und leistungsfähigen Verschlüsselungsprodukten für unverzichtbar.“[66] Gemeinsam mit den europäischen Partnern habe die Bundesregierung im Rahmen einer Revision der EG-Dual-Use-Verordnung die innergemeinschaftliche Exportkontrolle für kryptografische Massengüter abgeschafft, heißt es in dem Eckpunkte-Papier vom 2.6.1999 weiterhin. Wenngleich dies nicht so deutlich ausgesprochen wird, so dürfte in diesen emanzipativen Schritten der EU-Staaten doch eine Reaktion auf Phänomene der vernetzten Gesellschaft wie ECHELON zu sehen sein. Eine den Herausforderungen eben dieser vernetzten Gesellschaft Rechnung tragende GASP wird diese Positionen vertreten müssen. Mithin handelt es sich bei diesem wichtigen Thema durchaus um eine außenpolitisch relevante Angelegenheit.

Beispiel Nummer 3 für potentielle Felder einer der digitalen Revolution Tribut zollenden GASP: Einflußnahme nichtlegitimierter Gruppen auf die Formulierung der Rahmenbedingungen für das Anzapfen des innereuropäischen Daten- und Kommunikationsverkehrs (ENFOPOL-Papiere). Im Mai 1999 setzten die Innen- und Justizminister der EU die Entschließung bezüglich der sogenannten ENFOPOL-Papiere von der Tagesordnung des Rates. Sie verordneten sich ein halbes Jahr Bedenkzeit. Was war passiert ? „Ein Skandal“ war dem Rückzieher vorausgegangen, schrieb das Handelsblatt[67]. Trotz Widerstands aus Industrie und Justizausschuß des Europäischen Parlaments[68] sollte die Entschließung zur Überwachung des Telekommunikations- und Internetkommunikationsver-

[64] Electronic Privacy Information Center (EPIC): Cryptography and Liberty 1999, An international Survey of Encryption Policy, Washington D.C. 1999; online: http://www2.epic.org/reports/crypto1999.html

[65] Bundesministerium des Innern / Bundesministerium für Wirtschaft und Technologie: Eckpunkte der deutschen Kryptopolitik, Bonn 2.6.1999; online: http://www.bmwi.de/presse/1999/0602prm1.html

[66] Ebd.

[67] Handelsblatt, vom 25.5.1999, „EU streitet über Lauschangriff“

[68] Der Justizausschuß des EP forderte am 7.5.1999 ohne Erfolg eine Verschiebung der ENFOPOL-Entschließung des Rats

kehrs ohne großes Aufsehen durchgepeitscht werden. Vordergründig schien es um eine den neuen Ansprüchen an die Kriminalitätsbekämpfung im Cyberspace angepaßte Rahmenregelung für die europäischen Sicherheits- und Polizeibehörden zu gehen. Den gesetzlich ermächtigten Behörden sollte gestattet werden, durch von den Telekommunikationsanbietern und Internet Providern auf eigene Kosten zu installierende Abhörschnittstellen (in der ursprünglichen Fassung: in jeder Telefonanlage) die Kommunikation relativ verdachtsunabhängig anzapfen und auswerten zu können. Tatsächlich hatten sich die Justiz- und und Innenminister der EU – teilweise ohne eigenes Wissen – vor den Karren einer Organisation spannen lassen, welche unter der Bezeichnung „International Law Enforcement Telecommunications Seminar“ (ILETS) die Entwürfe für die ENFOPOL-Entschließung in eigener Regie ausgearbeitet hatte. ILETS wurde 1993 von der US-Polizeibehörde FBI gegründet. Mit dabei: Vertreter der Geheimdienste und Strafverfolgungsbehörden von Kanada, Australien, Großbritannien, Deutschland, Frankreich, Spanien sowie skandinavischer Länder[69]. Bei einem Treffen in Bonn, 1994, sollen sich die ILETS-Mitglieder ohne jegliche Einbindung der Legislativen der EU-Staaten auf eine Überwachungsliste geeinigt haben, berichten übereinstimmend verschiedene Quellen. Die unverfänglich titulierten „internationalen Benutzeranforderungen“ (IUR) wurden sodann ohne Information der EU-Minister[70] über die Genese der IUR als ENFOPOL-Dokumente dem Rat zugeleitet. ENFOPOL ist eine Standard-Klassifizierung der EU-Kommission für Strafverfolgungs- und Polizeiangelegenheiten. Die ILETS-Gruppe soll zudem seit 1994 mit erheblichem Einfluß auf die International Telecommunications Union (ITU) und die International Standards Organization (ISO) eingewirkt haben, um ihre IUR-Konzeption der Telekommunikationsüberwachung im digitalen Zeitalter in die Systemspezifikationen dieser Organisationen einfließen zu lassen.

Der Vorwurf an ILETS und die von dieser Gruppe maßgeblich gesteuerte ENFOPOL-Initiative lautet: Weder einem Parlament eines EU-Staates, noch dem Europäischen Parlament oder dem US-Kongreß wurden die entsprechenden Pläne jemals vorgetragen. ILETS operierte geheim. Eine transnationale Gruppe, bestehend u.a. aus Vertretern nicht-europäischer Sicherheitsorganisationen und Geheimdienstkreise, schickte sich an, zu Lasten der europäischen Telekommunikationswirtschaft eine grundrechtseinschränkende Gesetzesinitiative ohne jegliche parlamentarische und öffentliche Kontrolle zu lancieren. Mag man dem Sinn einer flächendeckenden Telekommunikationsüberwachung in der EU auch zwiespältig gegenüber stehen (gerade aus der GASP-Perspektive gibt es gute Argumente für eine solche flächendeckende Option) – die eingetretene Verfahrensweise liegt wohl kaum im nationalen Interesse eines EU-Staates. Eine GASP für das Informationszeitalter wird nicht umhin kommen, sich solcher informeller Strukturen anzunehmen. Sie sind nicht nur

[69] a.a.O. (Anm. 67)
[70] Ebd.

„Seminare“ von Sicherheitsexperten. Hier werden politische Strukturen für das Informationszeitalter geschmiedet, welche von dauerhaftem Bestand sind. Im Interesse der EU-Staaten sollte es liegen, daß solche Vorgänge demokratisch legitimiert oder marktgesteuert erfolgen. Das ist die beste Garantie gegen den Mißbrauch der nunmehr möglich gewordenen grenzüberschreitenden Kommunikationsüberwachung in den integrierten, digitalen Netzen.
Auf der anderen Seite zeigt der ENFOPOL-Fall sehr deutlich, daß Staaten unter den Bedingungen massenhafter, global-transnational vernetzter Datenkommunikation kooperieren müssen, wenn Sie ihre in der staatlichen Kernfunktion liegenden Sicherheitsfunktionen ausfüllen wollen. Der Balance-Akt wird in Zukunft geschickter zu meistern sein, als dies im ENFOPOL-Fall geschehen ist. Das Politikfeld für eine zukünftige GASP sollte klar geworden sein, da sie ohne jeden Zweifel auf die Verhinderung der mißbräuchlichen Datenanzapfung durch Dritte und auf die Ermöglichung des Zugriffs auf agressive Elemente angewiesen ist. Dieses Spannungsverhältnis angemessen auszufüllen ist auch eine außenpolitische Aufgabe der Europäer – keine rein innenpolitische Spielwiese für Geheimniskrämer. Die Tatsache, daß zu Zeiten der durch Bosnien und Kosovo offenkundig gewordenen Notwendigkeit einer funktionsfähigen GASP kein Außenminister in den dubiosen ENFOPOL-Prozeß eingebunden wurde, zeigt den Handlungsbedarf auf. Wegschauen verhindert nicht den Zwang zum frühzeitigen Handeln. Die Gewährleistung der europäischen Sicherheit gegen externe Bedrohungen via Anzapfung, Manipulation und Auswertung der vernetzten Datenkommunikation ist eine originäre GASP-Aufgabe. Wenn solche grundrechtseinschränkenden Initiativen legitimiert sein sollen, dann nur durch die Abwehr einer massiven Bedrohung für Staaten und Gesellschaften in Europa. Kleinkriminelle bedrohen die Sicherheit der EU nicht. Anders sähe das im Fall von Kapazitäten zur Information Warfare in den Händen von „Schurkenstaaten“ aus.

Die vorstehenden Beispiele für aktuelle außen- und sicherheitspolitisch relevante Vorgänge bei den Weichenstellungen für die vernetzte Gesellschaft im 21. Jahrhundert sind äußerst heterogen und von unterschiedlichem Erkenntniswert. Sie lassen aber einen gemeinsamen Schluß zu: Wenn die EU-Staaten weiterhin zögern, die Ausformung und Sicherung des Cyberspace als ein wichtiges Politikfeld einer kohärenten GASP zu definieren, wird ihre Außen- und Sicherheitspolitik in der vernetzten Gesellschaft von anderen staatlichen, nicht-staatlichen und sub-staatlichen Akteuren dominiert werden. Die Festung Europa verlöre ihren Schutzwall und ihre Bewohner müßten sich unter fremden Informationsschirmen drängen.

4. Cyberspace und Außenpolitik – ein Fazit

Zu Beginn des 21. Jahrhunderts liegt es im nationalen Interesse der am weitesten fortgeschrittenen High-Tech-Gesellschaften, den Cyberspace planetar zu expandieren. Deutschland gehört trotz aller Probleme und Rückstände in diese Gruppe. Gleiches gilt für EU-Partner, wie Großbritannien, die Niederlande, Frankreich, Nord-Italien und die skandinavischen Staaten. Die USA haben diese Notwendigkeit bereits seit Mitte der neunziger Jahre des 20. Jahrhunderts erkannt und tragen kraftvolle Initiativen, wie jene für die Global Information Infrastructure (GII), forciert nach vorne. Das virtuelle Zeitalter benötig in entsprechendem Umfang auch eine virtuelle Diplomatie[71]. Das ist eine der hauptsächlichen Schlußfolgerungen dieses Working Papers. Virtuell bedeutet nicht, daß etwas nicht real ist. Vielmehr kann in einer Zeit der vorherrschenden Vermittlung von entscheidungsrelevanten Informationen auf digitalem Wege eine Sache *in*existent sein, weil sie nicht virtuell, nicht digital ist. Richard Solomon führte in seiner Eröffnungsrede zur Konferenz über virtuelle Diplomatie im Jahr 1997 aus: „...one deals with reality even through virtual processes. And what we mean by virtuality, of course, is interactions that are mediated through electronic means rather than through face-to-face communication.“[72]

Die Expansion des Information Highway und der gesellschaftlichen Vernetzung ruft aber auch die Notwendigkeit auf den Plan, das Verhältnis dieser führenden Gesellschaften und Staaten zu anderen Akteuren zu ordnen. Es besteht eine Wettbewerbssituation zwischen den führenden High-Tech-Gesellschaften, ein möglichst großes Maß der Wachstumspotentiale auf sich zu konzentrieren. Soweit Staaten eine aktive Rolle in diesem High-Tech-Wettlauf spielen, werden sie nationale Interessen vertreten müssen. In diesem Punkt ist die Staatenwelt nicht tot. Auch wenn die Grenzen zwischen Außen- und Innenpolitik heutzutage bis zur Unkenntlichkeit ineinander verschwimmen können, so ist dies kein Grund die Vertretung kollektiver Interessen in globalem Umfang zu vernachlässigen oder wegzuanalysieren. Kollektive Interessen werden auch im 21. Jahrhundert territorial beeinflußte Interessen sein, da Menschen territoriale Wesen sind. Wir leben nicht im Cyberspace. Wir errichten, beeinflußen und nutzen die Welt der Bits und Bytes.
Was dies betrifft, so ist Außenpolitik im traditionellen Sinne aktueller denn je, auch wenn ihre Basis – der Nationalstaat – durch die Globalisierung und Digitalisierung relativiert wird. Freilich handelt es sich in wichtigen Bereichen nunmehr eher um eine global ordnende, digitale

[71] Das United States Institute of Peace, Washington, D.C., führte vom 1.4. bis 2.4.1997 eine internationale Wissenschaftskonferenz zur „Virtual Diplomacy“ durch; die Beiträge und Papers zu dieser Konferenz sind online zu finden: http://www.usip.org/oc/vd/vdpresents.html

[72] Ebd.: Richard Solomon: Virtual Diplomacy Conference, Opening Remarks, Washington/DC 1997

Außenwirtschaftspolitik. Diese Politik hat einen primär transnationalen Charakter. Im vorliegenden Working Paper erhielt dieser neue Teilbereich staatlich-transnationaler Außenpolitik das Label Cyber-Außenpolitik. Die visionäre Aufgabe für das außenpolitische Establishment in Deutschland und Europa wäre hiernach, das eigene Business und den Cyberspace zu einem neuen Modus Vivendi zu vereinen. Das ist zu tun, bevor es jemand anderes macht. Denn erinnern wir uns an die Passagen über die Interessen der New Economy: Die Währung des Informationszeialters ist Geschwindigkeit. Auf der anderen Seite ändert dieses Faktum nichts an der außerordentlichen Verantwortung der Außenpolitik. Sie benötigt auch im 21. Jahrhundert solide Information und Bedachtsamkeit bei der Entscheidungsfindung. „And no matter how much computer people instinctively lust after speed, in the diplomatic world it's not necessarily a good thing...Yes, it's slow, but it's designed to be slow: in the diplomatic world you do not want the two-second response to half-read messages so common in the email world. You want people to ask: what does this word mean in Nigeria ?"[73] Die Auflösung des Widerspruchs Geschwindigkeit versus Bedachtsamkeit ist, worum es bei der Entwicklung einer Konzeption der Cyber-Außenpolitik geht.

Eine Cyber-Außenpolitik gibt es noch nicht. Sie existiert derzeit als anerkanntes, eigenständiges Politikfeld weder in Deutschland, noch bei einem der EU-Partner. Zum Zeitpunkt der Abfassung dieses Papiers ist sie ein gedankliches Konstrukt, dessen Reichweite und Grenzen vorstehend in einem ersten Versuch ausgelotet werden sollten. Ob es eine eigenständige Cyber-Außenpolitik geben wird, wird sich zeigen. Das vorliegende Working Paper ist mit dem Bemühen angetreten, ergründen zu wollen, welche Handlungsoptionen und Herausforderungen der überkommenen deutschen Außenpolitik durch die vernetzte Gesellschaft eröffnet werden. Es wurde versucht, den denkbaren Platz des Netzes in der GASP zu lokalisieren.

Die Grundannahme dieses Papiers ist, daß Staaten auch im Zeitalter von Globalisierung und Vernetzung eine wichtige Rolle spielen können, um kollektive Werte und Ziele wie Demokratie, Wohlstand und individuelle Freiheit zu schützen. Wenn das Netz mehr und mehr in die Gesellschaft und Wirtschaft vordringt, dann muß sich auch eine die Interessen dieser Gesellschaft und Wirtschaft vertretende Außenpolitik des Netzes annehmen. Das Ende des Staates wird also nicht kommen. Staaten werden auch im Cyberspace Vertreter von Interessen sein. Sie werden gestaltend agieren und defensiv reagieren. In welchem Maße ihnen dies gelingt, entscheidet über ihre Macht und über ihre Handlungsfreiräume in der vernetzten Gesellschaft der Zukunft.

Außenpolitik wird aber auch im Informationszeitalter einen territorialen und nationalen Ursprung haben, da sie staatsgebunden ist. Dar-

[73] Zitiert aus: Wendy Grossman: Digital Diplomacy a two-edged Sword, in: Electronic Telegraph / The Daily Telegraph, 22.4.1997; online: http://www.telegraph.co.uk

aus folgert, daß sie sich gesellschaftlich legitimieren muß. Transformiert sich die deutsche Gesellschaft in Richtung auf die in 2.1 beschriebene „Network Society“, dann muß sich auch deutsche und europäische Außenpolitik in Teilbereichen adäquat anpassen. Krieg und Frieden sind Kernkategorien der Außenpolitik seit der Antike. Auch in der vernetzten Gesellschaft fordert diese Dimension ein hohes Maß an strategischer Verantwortung der Handelnden, wie im Abschnitt zur GASP in Anlehnung an die Diskussionen zur Information Warfare gezeigt wurde. Krieg und Frieden entscheiden sich im Informationszeitalter auch im Cyberspace.

Es sei nochmal an die eingangs gelieferte Arbeitsdefinition des künstlich anmutenden Begriffs der Cyber-Außenpolitik erinnert: „Cyber-Außenpolitik ist die interessengeleitete Ordnung und Beeinflussung des Verhältnisses eines Staates oder der EU zu seinem/ihrem Umfeld in der transnational-vernetzten Gesellschaft des Informationszeitalters, sowie die Beeinflussung der entsprechenden Politik anderer Staaten und Nicht-Staaten.“[74]
Die Definition und die in diesem Papier behandelten Beispiele weisen auf die grenzüberschreitende Querschnittsstruktur einer möglichen Cyber-Außenpolitik hin. Die Methoden erschöpfen sich nicht in einer Homepage. Vielmehr steht im Zentrum einer Cyber-Außenpolitik ein transnationaler Dialog zur Netzentwicklung. Ein Dialog, der sich für die Offenheit und Expansion des Netzes einsetzt. Denn eine „Technologie der Freiheit“ kann nur blühen und gedeihen, wenn sie sich in einem freiheitlichen Umfeld entfalten kann. Freiheit existiert aber nur solange, wie sie durch pro-aktives Handeln der Verantwortungsträger geschützt und bewahrt wird. Für ein globales Medium ist das Handlungsfeld ein globales. An der Nachhaltigkeit und am Erfolg dieses Unterfangens im Informationszeitalter hängt in letzter Instanz die Sicherheit der Europäer. Darum ist Außenpolitik gefordert und darum sollte sie sich mit dem Wort „Cyber“ verbinden.

Ernst-Otto Czempiel schreibt, „...daß Sicherheit nicht durch Verteidigung, sondern letztlich nur durch Demokratisierung der Umwelt erreicht werden kann. Damit entfällt der klassische topos des ‚Primats der Außenpolitik‘. Der politische Primat rückt auf die Existenzentfaltung des einzelnen.“[75] Sollte sich deutsche und europäische Außenpolitik im Informationszeitalter und in der vernetzten Gesellschaft der Mission annehmen, diese individuelle Existenzentfaltung global zu sichern, dann wäre sie fit für das 21. Jahrhundert. Und sie wäre global in allerbester Gesellschaft.

[74] Siehe Seite 1 dieses Working Papers
[75] a.a.O. (Anm. 34), S. 125 f.

5. Literatur

A

Arquilla, John / Ronfeldt, David: In Athena's Camp, Preparing for Conflict in the Information Age, Santa Monica 1997

B

Bell, Daniel: Die nachindustrielle Gesellschaft, Frankfurt/Main 1985

Bulletin zur schweizerischen Sicherheitspolitik, 1999; online: www.fsk.ethz.ch/publ/bulletin/bulle_99/b99/info.htm

Bundesministerium des Innern / Bundesministerium für Wirtschaft und Technologie: Eckpunkte der deutschen Kryptopolitik, Bonn 2.6.1999; online: http://www.bmwi.de/presse/1999/0602prm1.html

C

Castells, Manuel: The Information Age: Economy, Society and Culture, Volume I, The Rise of the Network Society, 3. Auflage, Oxford 1997

Czempiel, Ernst-Otto: Weltpolitik im Umbruch, Das internationale System nach dem Ende des Ost-West-Konflikts, München 1993

D

Deibert, Ronald J.: Parchment, Printing, and Hypermedia, Communication in World Order Transformation, New York 1998

Dizard Jr., Wilson: Meganet, How the Global Communications Network Will Connect Everyone on Earth, Boulder 1997

Dodge, Martin / Kitchin, Rob: Mapping the Network Society, Paper zum 95. Annual Meeting der Association of American Geographers, Honolulu, März 1999

E

The ECONOMIST, March 8, 1997

The ECONOMIST, July 24, 1999

Electronic Privacy Information Center (EPIC): Cryptography and Liberty 1999, An international Survey of Encryption Policy, Washington D.C. 1999; online: http://www2.epic.org/reports/crypto1999.html

Europäisches Parlament / Ministerrat: Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, online: http://www2.echo.lu/legal/de/datenschutz/datensch.html

European Parliament, Directorate General for Research (STOA): Development of Surveillance Technology and Risk of Abuse of Economic Information, PE 168.184/Part3/4, Luxembourg, April 1999; online: Interception Capabilities 2000, http://www.gn.apc.org/duncan/stoa_cover.htm

F

Foreign Affairs, March/April 1996

Foreign Affairs, September/October 1998

Foreign Policy, Summer 1997

G

Grossman, Wendy: Digital Diplomacy a two-edged Sword, in: Electronic Telegraph / The Daily Telegraph, 22.4.1997; online: http://www.telegraph.co.uk

H

Handelsblatt, vom 25.5.1999

I

Information, Communication and Society, Volume 1, Spring 1998

Internationale Politik, September 1997

J

Journal of International Affairs, Spring 1998, Jahrgang 51, No. 2

K

Kimmerle Bruck M.: Informationssanktionen, Halle 1998, Online-Paper: www.politik.uni-halle.de/rode/infosanktionen.htm

N

Negroponte, Nicholas: Total digital, Die Welt zwischen 0 und 1 oder die Zukunft der Kommunikation, 4. Auflage, München 1995

NZZ vom 30.4.1999

O

OECD: OECD Workshops on the Economics of the Information Society: A Synthesis of Policy Implications, Paris 1999

OECD: The Economic and Social Impact of Electronic Commerce, Executive Summary, Paris 1999

P

PVS, 39, 1998

R

Reporters Sans Frontières: The Twenty Enemies of the Internet, www.rsf.fr/uk/alaune/ennemisweb.html, Paris 1999

Rode, Reinhard: Deutsche Außenpolitik, Amsterdam 1996

S

Solomon, Richard: Virtual Diplomacy Conference, Opening Remarks, Washington/DC 1997; online: http://www.usip.org/oc/vd/vdpresents/rhsvdact.html

SPIEGEL ONLINE: Cyberwar, Der Krieg aus dem Netz, Stand 30.8.1999, http://www.spiegel.de/netzwelt/politik/0,1518,38605,00.html

T

TELEPOLIS, online: http://www.heise.de/tp

Toffler, Alvin: The Third Wave, London 1981

Toffler, Alvin / Toffler, Heidi: Creating a New Civilisation, The Politics of the Third Wave, Atlanta 1995

Tsagarousianou, Roza / Tambini, Damian / Bryan, Cathy (Hrsg.): Cyberdemocracy: Technology, Cities and Civic Networks, London 1998

U

United States Institute of Peace: Virtual Diplomacy Conference, 1.-2. April 1997, Presentations, Papers and Reactions, Washington/D.C., 1997; online: http://www.usip.org/oc/vd/vdpresents.html

V

Vertrag über die Europäische Union, vom 7.2.1992

W

Die WELT, 8.6.1999

Die WELT, 31.8.1999

WIRED, May 1998

WIRED, November 1998

WIRED NEWS: www.wired.com/news

6. Abbildungen und Tabellen

Abbildungen

Tabellen

7. Index