Das Konzept «Schutz kritischer Infrastrukturen» hinterfragt

von Jan Metzger

1 Einleitung

Am 24. Januar 2003 wurde der ehemalige Gouverneur von Pennsylvania, Tom Ridge, durch Präsident Bush als erster Chef des neu gegründeten *Department of Homeland Security* (DHS) vereidigt. Am Ende der grössten Behörden-Umstrukturierung in den USA seit dem Zweiten Weltkrieg werden unter der Führung von Ridge 170 000 Angestellte in über 22 Institutionen versuchen, das Territorium der Vereinigten Staaten gegenüber der terroristischen Bedrohung sicherer zu machen. Ein respektabler Anteil des 35 Milliarden-Budgets für das Jahr 2003 wird wohl in den Bereich *Information Analysis and Infrastructure Protection* als einem der vier Haupt-Direktorate des DHS einfliessen. Eine der Hauptaufgaben des *Assistant Secretary for Infrastructure Protection*, Robert P. Liscouski, wird darin bestehen, eine umfassende Analyse kritischer Infrastrukturen vorzunehmen sowie eine nationale Schutz-Planung in Angriff zu nehmen.[1]

Was bedeutet *Critical Infrastructure Protection* (CIP)? Ist CIP ein taugliches Konzept, um nationale Interessen in bezug auf die klassischen sicherheitspolitischen Ziele wie «Unabhängigkeit» und «Sicherheit des Landes» zu verfolgen?[2]

Im folgenden wird ausgehend von der Definition des Begriffs CIP eine Beurteilung des Konzepts aufgrund der folgenden Kriterien vorgenommen:

a) Sprachgebrauch respektive Usanz (operative Perspektive)
b) Analytisch-terminologische Präzision (konzeptionelle Perspektive)

2 CIP aus operativer Sicht

Bereits vor der gegenwärtigen Terrorismus- und *Homeland Security*-Debatte war der Begriff «kritische Infrastruktur» Gegenstand der politischen Auseinandersetzung. In den 1980er Jahren fand in den Vereinigten Staaten eine intensive Diskussion über Infrastrukturen sowie deren Sicherheit statt. Bereits damals wurden allerdings eine allgemeine Definition und ein gemeinsames Verständnis

1 Vgl. *U.S. Department of Homeland Security*, http://www.dhs.gov.

2 Für den Fall der Schweiz siehe Artikel 2 der schweizerischen Bundesverfassung sowie Sicherheit durch Kooperation. Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz (SIPOL B 2000) vom 7. Juni 1999. http://www.vbs-ddps.ch/internet/vbs/en/home/publikationen/berichte.html. Weitere sicherheitspolitische Interessen wie «Solidarität» oder «Stabilität und Frieden jenseits der Grenzen» werden in diesem Zusammenhang bewusst ausgeklammert.

vermisst.[3] Der Schlussbericht der *President's Commission on Critical Infrastructure Protection* (PCCIP) vom Oktober 1997 definierte kritische Infrastrukturen so breit, dass er eine Reihe möglicher thematischer Stossrichtungen offen liess. In der Folge wurden in vielen Ländern CIP-Aktivitäten lanciert, welche leider oftmals ein praktisch ausschliessliches Schwergewicht auf den Bereich der Internet- oder *Cyber*-Kommunikation legten.[4] So wurde beispielsweise im Jahr 2000 in vermeintlicher Erfüllung der Forderung nach einem nationalen CIP-Plan unter dem Titel *Defending America's Cyberspace: National Plan for Information Systems Protection* ein Internet-Sicherheits-Strategieplan unter weitgehender Vernachlässigung des physischen Infrastrukturschutzes vorgelegt.[5]

Es ist wichtig, zwischen dem Schutz kritischer Infrastrukturen (CIP) im allgemeinen und dem Teilauftrag des Schutzes der kritischen Informations- und Telekommunikationsinfrastrukturen (*Critical Information Infrastructure Protection*, CIIP) zu unterscheiden. Diese Abgrenzung ist oft nicht so offensichtlich und auch nicht so leicht, weil CIIP eine entscheidende Rolle in einer CIP-Gesamtstrategie spielt. In offiziellen Berichten werden für den Sachverhalt des Schutzes der Informations- und Telekommunikationsinfrastrukturen oft beide Begriffe verwendet. Dennoch ist es entscheidend zu verstehen, dass CIP sämtliche kritische Sektoren einer nationalen Infrastruktur umfasst, währendem CIIP lediglich ein Teilauftrag im Rahmen einer umfassenden Schutzstrategie darstellt.[6]

Das *International CIIP Handbook* definiert CIIP als ein Teilbereich von CIP. CIIP fokussiere erstens auf den Schutz von Systemen und Werten inklusive Komponenten wie Telekommunikation, Computer/Software, Internet, Satelliten, Fiber-Optiken etc., und zweitens auf Computer-Netzwerke sowie alle hierdurch geschaffenen Dienstleistungen.[7]

Der Schutz der kritischen Informations- und Telekommunikationsinfrastrukturen (CIIP) ist aus dreierlei Gründen besonders bedeutsam: Erstens stellen sie als Wirtschaftssektor einen wichtigen Bestandteil der ökonomischen Wertschöpfung dar. Zweitens bilden sie ein wichtiges vernetzendes Glied zwischen den anderen Infrastrukturbereichen. Bereits in der normalen Lage stellen sie die Grundvoraussetzung für das Funktionieren aller anderen Infrastrukturen dar. Drittens sind sie

3 «*With no standard or agreed definition, the concept of infrastructure in policy terms has been fluid, as it appears to be today, including both public and private systems, services, and even amenities.*» *Critical Infrastructures: What makes an Infrastructure Critical? Report for Congress. Appendice. What is Infrastructure?*. Washington, DC: Congressional Research Service, 30. August 2002. http://www.fas.org/irp/crs/RL31556.pdf.

4 Siehe Dunn, Myriam/Wigert, Isabelle. *The International Critical Information Infrastructure Protection (CIIP) Handbook*. Zürich: Forschungsstelle für Sicherheitspolitik, 2004.

5 Vgl. http://www.ciao.gov/publicaffairs/np1final.pdf. Für die neuere Version vom Februar 2003 siehe http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf.

6 Siehe Dunn/Wigert, *The International Critical Information Infrastructure Protection (CIIP) Handbook*, S. 19–21.

7 Ebd., S. 363.

in der Krise ein entscheidendes Führungsinstrument zur Risikobewältigung und Wiederinstandstellung.[8] Trotz der Bedeutung von CIIP ist dieses Konzept allerdings nicht mit dem Überbegriff CIP gleichzusetzen, sondern muss als wesentlicher Spezialauftrag verstanden werden: Die verschiedentlich feststellbare Reduzierung des Konzepts Schutz kritischer Infrastrukturen auf den Aspekt der Computer-Sicherheit und die oftmals damit einhergehende Fokussierung auf technologische Aspekte – in Begriffen wie «*Cyber*-Terrorismus», «*Cyber*-Kriminalität» und «*Cyber-Warfare*» – ist problematisch, ja gefährlich. Terroristen tendieren nicht dazu, ihre Optionen a priori einzuschränken, indem sie lediglich auf einer Ebene tätig werden. Warum sollten sie auch? Politisch motivierte Gewalttäter werden niemals ausschliesslich «*Cyber*»-Terroristen sein, sondern sich vielmehr diejenige Dimension aussuchen respektive dasjenige Instrument wählen, mit welchem sie ihre politischen Ziele besser erreichen können. Um erfolgreich der terroristischen Herausforderung begegnen zu können, müssen die westlichen Wissensgesellschaften versuchen, wie die Attentäter zu denken – und zwar nicht unlogisch, sondern der Logik der Terroristen entsprechend. Die Natur der Bedrohung und nicht die Art und Weise wie sie sich manifestiert (physisch, *cyber*-basiert, biologisch, psychologisch) gilt es als Anhaltspunkt der Analyse sowie als Leitstern der institutionellen Abwehr zu erkennen. Ein ausschliesslicher Fokus auf *Cyber*-Bedrohungen unter Vernachlässigung des konventionellen physischen Schutzes kritischer Infrastrukturen ist deshalb ebenso abzulehnen wie das völlige Ausblenden der Verwundbarkeit von Computer-Netzwerken im Rahmen einer nationalen und internationalen Schutzstrategie.

3 CIP aus konzeptioneller Sicht

Wenn schon kein allgemeiner Gebrauch des Begriffes feststellbar ist, wie steht es dann mit der analytisch-terminologischen Schärfe von CIP? Hierzu gilt es, die Begriffe «Infrastruktur», «kritisch» und «Schutz» näher zu beleuchten.

Der Begriff «Infrastruktur», gebildet aus den lateinischen Silben «infra» (unter) und «Struktur», beschreibt die zugrundeliegende Basis einer Organisation oder eines Systems, beispielsweise eines Landes. Informations- und Telekommunikationsmittel, Banken und Finanzwesen, die Versorgung mit Wasser, Strom, Öl und Gas, die Transport- und Logistikstrukturen sowie das Gesundheits- und Rettungswesen sind Infrastrukturen, welche das tägliche Überleben von uns allen sicherstellen.

Und hier liegt bereits ein Hauptproblem begründet. Geht man davon aus, dass Sicherheitspolitik als «Politik des Ausserordentlichen» oder als «Politik existentieller Bedrohungen» ausserhalb der Alltagspolitik liegt – oder zumindest eine spezielle

8 Wenger, Andreas/Metzger, Jan/Dunn, Myriam. Critical Information Infrastructure Protection: Eine sicherheitspolitische Herausforderung. In: Spillmann, Kurt R./Wenger, Andreas (Hrsg.). *Bulletin 2002 zur schweizerischen Sicherheitspolitik*. Zürich: Forschungsstelle für Sicherheitspolitik und Konfliktanalyse, 2002, S. 119–142.

Form der Politik darstellt –, so stellt sich eine ganz praktische Abgrenzungsfrage: Wann ist der Schutz kritischer Infrastrukturen eine ganz normale Aufgabe eines individuellen, betrieblichen oder lokalen Akteurs und wann Gegenstand einer nationalen und allenfalls sogar internationalen Sicherheitspolitik?[9] Erschwert wird die Abgrenzungsproblematik zwischen Alltags- und Sicherheitspolitik zusätzlich dadurch, dass viele der genannten Infrastrukturen privatwirtschaftlich, ja sogar ausländisch kontrolliert sind und sich zum Teil nicht einmal auf dem Territorium des eigenen Landes befinden. Infrastrukturen werden deshalb heute wahlweise als Tatobjekte der Kriminalitätsbekämpfung, als privatwirtschaftliche Wettbewerbsvorteile, als technisch-betriebliche Systeme, als verteidigungsrelevante und strategische Güter oder als Objekte einer nationalen und internationalen Sicherheitspolitikformulierung gesehen. Diese Aufzählung ist nicht vollständig und soll um einen letzten, sehr oft vernachlässigten Aspekt ergänzt werden: Infrastrukturen sind vor allem auch Objekte der individuellen Kognition sowie der öffentlichen Reflexion und Wahrnehmung. Sowohl als Gegenstände eines historischen Bewusstseins, aber auch als Streitobjekte der gegenwärtigen politischen Debatten werden sie untrennbar assoziiert mit Begriffen wie «Risiko», «Bedrohung», «Vertrauen», «Krise» oder «Katastrophe».

Weitet man entsprechend die Perspektive, so stösst man unweigerlich auf die fundamentale Frage: Sind es wirklich die Infrastrukturen, welche wir vor allem schützen müssen? Nein, denn es sind eher die durch Infrastrukturen vermittelten Dienste (*services*), die physischen und elektronischen (Informations-)Flüsse, die Funktionen und vor allem die Werte (*core values*), welche die eigentlichen Objekte unserer Schutzinteressen darstellen. Infrastrukturen werden von Menschen konstruiert, unterhalten und betrieben. Aus diesem Grunde sind sie bezüglich organisatorischer und institutioneller Hierarchien relativ leicht aufzuzeichnen. Dienste, Flüsse und vor allem auch Werte sind viel komplexer in ihrer Vernetzung miteinander darzustellen und zu verstehen. Trotzdem würde es der realen Systemdynamik und unseren Schutzinteressen eher gerecht werden, einen von diesen Begriffen zu verwenden, als von an sich statischen «kritischen Infrastrukturen» zu sprechen.

4 Arten von Kritikalität

Das Adjektiv «kritisch» eignet sich wohl besser als das Substantiv «Infrastruktur» dazu, die Grenze zwischen operativem Normalbetrieb und strategischer Sicherheitspolitik begrifflich einzufangen. So unterscheidet beispielsweise das deutsche Bun-

9 Buzan, Barry/Wæver, Ole/de Wilde, Jaap. *Security: A New Framework for Analysis.* London: Lynne Rienner, 1998, S. 24.

desamt für Sicherheit in der Informationstechnik zwischen dem Schutz «kritischer Infrastrukturen» und dem Schutz «unternehmenskritischer Infrastrukturen».[10]

Gilt dies aber auch für die Abgrenzung zwischen Alltag und Krise? In diesem Zusammenhang sind zwei Trends erwähnenswert: Erstens gibt es in der öffentlichen Wahrnehmung immer weniger eigentlich «natürliche» Katastrophen, die einfach als Akt Gottes oder als Schicksalsschläge hingenommen werden (müssen). Unglücke entstehen durch Politik- respektive Politikerversagen und der Ruf nach politischer Verantwortung wird zunehmend zum eingefleischten Reflex. Zweitens wandelt sich dadurch das Kriterium, was «gute» Politik ist: Nicht mehr die administrative Fähigkeit der Alltagsbewältigung, sondern das Management vor, mit und nach einer Krise entscheidet über die berufliche Zukunft eines politischen Entscheidungsträgers – mit positivem oder negativem Vorzeichen.

Der englische Ausdruck «*critical*» wird in der gegenwärtigen Infrastrukturdebatte parallel und weitgehend unreflektiert in mindestens zwei verschiedenen Bedeutungen verwendet:

a) im Sinne einer *symbolischen* Kritikalität: Eine Infrastruktur ist aufgrund ihrer Bedeutung *an sich* kritisch. Dies bedeutet, dass im Falle ihres Ausfalls oder ihrer Beschädigung ein existentielles sicherheitspolitisches Ziel nicht mehr wahrgenommen werden könnte, z.B. territoriale Unversehrtheit. In diesem Fall ist im Grunde weniger die Infrastruktur als das Staatsziel kritisch. Theoretisch spielt die Frage, ob und wie stark die Infrastruktur vernetzt ist keine Rolle. Der US-Kongress oder das Weisse Haus in Washington stellen nicht aufgrund ihrer Vernetzung, sondern als Symbole nationaler Macht für Terroristen verschiedener Couleur ein attraktives Ziel dar. [11]

b) im Sinne einer *systemischen* Kritikalität: Eine Infrastruktur ist aufgrund ihrer *strukturellen Positionierung* im System als wichtiges Verbindungsglied zwischen anderen Infrastrukturbereichen kritisch, z.B. sind Strom- sowie Informations- und Telekommunikationsnetze aufgrund ihrer Vernetzungsgrösse und -stärke von besonderer Bedeutung. Die PCCIP beispielsweise legte ein besonderes Gewicht auf den Vernetzungsaspekt: In ihrem Schlussbericht 1997 definierte sie Infrastrukturen als ein Geflecht von interdependenten Netzen und Systemen.[12]

10 Bundesamt für Sicherheit in der Informationstechnik. http://www.bsi.bund.de/fachthem/kritis.

11 Für ein Beispiel einer symbolischen Sicht eines *Criticality Assessment* ohne Bezug zum Vernetzungsaspekt siehe House Committee on Government Reform. *Homeland Security, Key Elements of a Risk Management Approach. Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations*. Washington, DC: United States General Accounting Office, 2002, S. 6. http://www.house.gov/reform/ns/statements_witness/GAO-02-150T.pdf.

12 «*The framework of interdependent networks and systems comprising identifiable industries, institutions, (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole*». President's Commission on Critical Infrastructure Protection. *Protecting America´s Infrastructures*, 1997, S. 2–3. http://www.ciao.gov/resource/pccip/report_index.htm.

Das symbolische Kritikalitätskonzept erlaubt es, sowohl nicht-vernetzte als auch nicht-technische Objekte, Systeme und Prozesse in die Schutzplanung zu integrieren. Personenziele wie beispielsweise der Präsident eines Landes oder auch natürliche Sehenswürdigkeiten mit stark symbolischem Charakter – die Präsidentenportraits am Mount Rushmore für die USA oder der Bundesbrief in Schwyz für die Schweiz – sind nicht aufgrund ihrer Vernetzung «kritische» Ziele, sondern aufgrund ihrer Funktion sowie aufgrund ihrer Bedeutung für das nationale Interesse, beispielsweise für den Zusammenhalt als Willensnation.

Natürlich ist die oben entwickelte Typologie in dem Sinne idealtypisch, ja künstlich, als dass in der Realität Infrastrukturen niemals völlig isoliert voneinander vorkommen: Die Energiegewinnung hängt vom Transport ab. Transportmittel wiederum hängen von Energie ab. Und beide setzen funktionierende Informationsnetzwerke voraus. Informationsnetzwerke hängen von Energie ab, etc. Im Fall des *World Trade Centers* kumulierten sich am 11. September 2001 verschiedene Kritikalitäten: die Bedeutung im finanzwirtschaftlichen System als Knotenpunkt globaler Geldströme, die Funktion als Arbeitsort und Ausflugsziel sowie die Bedeutung an sich, eben als *World Trade Center*.

Das systemische Verständnis von Kritikalität mit seinem Verständnis von Infrastrukturen als «komplexe adaptive Systeme» bildet die Alltagsrealität in ihrer Komplexität wohl besser ab. Sie ist eher als die symbolische Kritikalität einer empirischen Analyse aufgrund statistischer Daten zugänglich. Aus Sicht des Sicherheitspolitik-Analysten hat die systemische Kritikalität den Nachteil, dass hier die Abgrenzung zwischen der Optimierung des Alltags-Krisenmanagements und der «Politik des Ausserordentlichen» schwieriger zu ziehen ist. Im Gegensatz dazu kann die symbolische Kritikalität definitionsgemäss und zum vornherein einem existentiell-sicherheitspolitischen Kontext zugeordnet werden.

Ein Hauptproblem besteht darin, dass der Begriff «kritische Infrastruktur» in den letzten Jahren von einer technisch-naturwissenschaftlichen und allenfalls systemtheoretischen Expertenebene auf eine politische Agenda überführt wurde, ohne dass eine gedankliche Anpassung an den soziopolitischen Kontext stattgefunden hat. Der Begriff «kritisch» ist nicht zufällig etymologisch mit dem Wort «Krise» verbunden. Krisen sind von ihrer Natur her soziale Ereignisse: Sie werden stets von jemandem erfahren, sei es von einem Individuum, einer Gruppe, einer Organisation, einer Gesellschaft oder einem Staat, und zeichnen sich gerade dadurch aus, dass in ihnen «kritische» Entscheidungen gefällt werden (müssen).[13]

Systemkritikalität, -resilienz und -robustheit lassen sich erstens im Rahmen der Optimierung des Normalfalls und zweitens auf einem technischen Infrastrukturniveau zu einem gewissen Grad sicherlich objektiv messen. Auf einem sicher-

13 Zur Definition der Krise siehe Stern, Eric. *Crisis Decisionmaking: A Cognitive-Institutional Approach*. Stockholm: Swedish National Defence College, 2001 (Publications of the Crisis Management Europe Research Program 6), S. 4–6.

heitspolitischen Niveau sind Risiken, Bedrohungen und Krisen allerdings weder zu quantifizieren noch objektiv miteinander vergleichbar. In dem Masse, als sich in jeder Krise Kritikalität definitionsgemäss manifestiert, macht es wenig Sinn, nicht-technische und nicht-vernetzte Schutzobjekte auszuschliessen.

Nicht die Vernetzung, sondern die Bedeutung an sich – vernetzt oder nicht, *man-made* oder nicht – stellt auf einer sicherheitspolitischen Ebene das entscheidende Kriterium bei der Erfassung einer Infrastruktur als «kritisch» dar. Sicherheitspolitisch relevante Krisen sind definitionsgemäss kritische und komplexe Ereignisse in bezug auf den zeitlichen und örtlichen Ablauf, die Interaktion der involvierten Institutionen auf vertikaler und horizontaler Ebene, die Identifizierung der sich stellenden Probleme sowie die offenbarten Informationsbedürfnisse und -überschüsse.[14]

Selbst wenn sich ein Sachverhalt nicht quantitativ-exakt messen lässt, folgert daraus allerdings nicht zwangsläufig, dass dieser nicht von Belang ist und nicht mit Massnahmen der Risikoreduktion angegangen werden kann. Ein Beispiel soll dies verdeutlichen: Auf einer individuellen Ebene stellt das Risiko, von einem Auto überfahren zu werden, eines der grössten Extremereignisse überhaupt dar. Es bestehen umfangreiche Statistiken, welche Auskunft darüber geben, wie viele Fussgänger jedes Jahr in verschiedenen Ländern von Autos angefahren werden. Dem Normalbürger sind diese empirischen Daten nicht bekannt. Und trotzdem verhält er sich jeden Tag im Sinne einer Risikominimierungs-Strategie richtig, indem er den Fussgängerstreifen benützt. Dieses Beispiel illustriert, dass die Aussage «nur was man messen kann, lässt sich verbessern» falsch ist. Nicht primär das quantitative, sondern das qualitative Wissen um Risiken und Verwundbarkeiten stellt die notwendige Voraussetzung für den Schutz von Verkehrsteilnehmern wie von Infrastrukturen gegenüber terroristischen Bedrohungen dar.

Für die sicherheitspolitische Analyse besteht die Herausforderung weniger darin, Krisen exakt zu messen, als darin, herauszufinden, wie sie entstehen, ablaufen und enden. Einem inhaltlich breiten und methodisch interdisziplinären Verständnis folgend sind die Charakteristiken von Krisen, die tiefenstrukturellen Umstände, welche dazu führten, sowie deren Konsequenzen offenzulegen. Extremereignisse werden geschaffen und charakterisiert durch ihren Kontext. Drei Risikoanalyse-Experten hielten unlängst fest, sowohl das Verständnis als auch die Verminderung von Verwundbarkeiten würden nicht eine exakte Vorhersage von Extremereignissen bedingen.[15]

Im Gegensatz zur technischen Infrastrukturanalyse geht es für die sicherheitspolitische Forschung somit weniger darum, objektiv-reale Krisenschwellen

14 Ebd., S. 14–16.

15 Sarewitz, Daniel/Pielke, Roger/Keykhah, Mojdeh. Vulnerability and Risk: Some Thoughts from a Political and Policy Perspective. In: *Risk Analysis* 23 (2003), Nr. 4, S. 807. http://www.cspo.org/products/articles/Vulnerable.pdf.

zu identifizieren, sondern zu untersuchen, wer wann was in welchem Kontext wie und mit welchem Resultat zu einer Krise werden lässt. Dahinter steht die Auffassung, dass auf einer strategischen Planungsebene die Hauptsorge vor allem darin bestehen muss, kein Risiko zu vergessen, und weniger darin, bereits identifizierte Risiken präzise zu messen. Menschen, aber auch menschliche Kollektive wie Staaten, handeln nicht unmittelbar in Reaktion auf eine objektiv konstituierte Umgebung, sondern aufgrund ihres empfundenen Abbildes der Wirklichkeit. Es ist darum weder politisch noch analytisch hilfreich, «objektive Sicherheit» ausserhalb des politischen Kontexts identifizieren zu wollen.[16] Verstärkt wird die Problematik der Abgrenzung zwischen technisch-operativer und sozio-politischer CIP-Analyse im deutschsprachigen Raum noch dadurch, dass im Deutschen sowohl die Unterscheidung zwischen *safety* und *security* für den Begriff der «Sicherheit» als auch diejenige zwischen *critical* und *critic* für das Adjektiv «kritisch» zusammenfallen.

Die Frage der Kritikalität einer Infrastruktur ist untrennbar verbunden mit der Frage, wie die Beeinträchtigung einer Infrastruktur politisch wahrgenommen, behandelt und ausgeschlachtet wird. Wann wird das Bild einer Bedrohung ein sicherheitspolitisches Thema und wann nicht? Eriksson und Noreen nennen verschiedene Faktoren, welche zur individuellen Kognition und Gestaltung von Bedrohungsbildern hinzukommen. In ihrer Gesamtheit sind sie mitverantwortlich dafür, ob Bedrohungen auf der politischen Agenda erscheinen, verschwinden, verharren oder sogar priorisiert werden: Krisenerfahrungen einer Gemeinschaft, Identitätsaspekte, politischer und institutioneller Kontext sowie der Einfluss der öffentlichen Meinung.[17]

Interessant ist in diesem Zusammenhang, dass verschiedene Parteien unterschiedliche Bedrohungsbilder priorisieren. Typischerweise haben sogenannt «grüne» Parteien im allgemeinen ein eher weites und rechtskonservative Parteien ein traditionelles, auf die militärische Bedrohung ausgerichtetes Konzept von Sicherheit.

Dieser Aspekt ist auch im Kontext der gegenwärtigen *Fight against terrorism*-Debatte von entscheidender Bedeutung. Denn Terrorismus ist nicht nur, aber vor allem auch Kommunikation. Das eigentliche Ziel des Terroristen ist nicht primär die Ausübung von Gewalt am Terroropfer an sich, sondern die bewusste Beeinflussung eines breiteren Publikums.[18]

Hieraus folgt, dass CIP-Studien auf einer sicherheitspolitischen Ebene vor allem auch die Themen der politischen Kultur, des politischen Diskurses sowie der politischen (Partei-) Konstellation thematisieren sollten. CIP-Forschung ist so gesehen vor allem eine Untersuchung des politischen Kontextes, in welchem

16 Buzan/Wæver/de Wilde, *Security: A New Framework for Analysis*, S. 31.

17 Eriksson Johan/Noreen Erik. *Setting the Agenda of Threats: An Explanatory Model*. Uppsala: Uppsala University, Department of Peace and Conflict Research, 2002 (Uppsala Peace Research Paper 6), S. 12–15.

18 Hoffmann, Bruce. *Terrorismus – Der unerklärte Krieg: Neue Gefahren politischer Gewalt.* Frankfurt am Main: Fischer, 2001, S. 48.

Infrastrukturen identifiziert, analysiert und geschützt werden. Nicht der CIP-Analyst, sondern die politischen Akteure, vor allem auch die Bevölkerung, bestimmen dabei, ob eine Bedrohung als «kritisch» akzeptiert wird oder nicht.

Zum politischen Kontext gehört auch der politisch motivierte Gewalttäter oder Terrorist, welcher bewusst eine Infrastruktur angreift. In vielen Infrastrukturstudien erfolgt die Bestimmung der Kritikalität allerdings auch nach dem 11. September 2001 weitgehend systemintern, indem überlegt wird, welche Infrastrukturen wie und wo miteinander verbunden sind. Als problematischer Analyseansatz muss hier die Infrastrukturanalyse des deutschen Bundesamts für Sicherheit in der Informationstechnik genannt werden, in welchem erklärtermassen die Betrachtung von Verwundbarkeiten «unabhängig von der Art der Bedrohung» durchgeführt wurde.[19] Verwundbarkeiten manifestieren sich aber gerade eben erst in ihrem Kontext, das heisst mit Blick auf die entscheidungsrelevanten Bedrohungen!

Sofern Kritikalität nicht durch Struktur, sondern durch die Gewalt und Symbolik bestimmt wird, muss der Analyseansatz verbreitert werden. Wie Doron Zimmermann ausführt, handelt es sich beim Terrorismus um ein *people business*, welches intrinsisch nicht-quantifizierbar ist: Zuerst müsse man wissen, mit wem (Akteur, Motive und Ziele) und womit (Organisation und Fähigkeiten) man es zu tun habe, bevor man irgendwelche Schlussfolgerungen ziehen dürfe.[20]

Obwohl sich Kritikalität nicht objektiv messen lässt, lassen sich dennoch Indikatoren feststellen, ob ein Infrastrukturschaden kritisch ist oder nicht. So wird in der *Presidential Decision Directive Number 63* (PDD-63) vom Mai 1998 festgehalten: «Jede Beeinträchtigung oder Manipulation dieser kritischen Funktionen muss kurz, selten, bewältigbar, geographisch isoliert und minimal schädlich für die Wohlfahrt der Vereinigten Staaten sein.»[21]

Die Kritikalität einer Infrastruktur lässt sich jedoch in Ergänzung hierzu auch von einem anderen Faktor her analysieren: Wie gross ist der Vertrauensverlust, welchen der Staat erleidet, wenn eine Dienstleistung ausfällt? Dies ist insofern ein guter Gradmesser, als dass der Rückgriff des Volkes auf staatliche Verantwortlichkeit selbst bei privatwirtschaftlicher Eigentumsregelung ein sicherer Beleg dafür

19 Blattner-Zimmermann, Marit. *Schutz Kritischer Infrastrukturen in Deutschland*. Referat gehalten im Rahmen der Luzerner Tage für Informationssicherung (LUTIS), Folie 7. http://www.infosurance.ch/lutis/vortraege/bsi_kritische_infrastruktur.pdf. Siehe auch http://www.bsi.bund.de/fachthem/kritis/kritis.htm.

20 «*We should first know who (actors, motives and objectives) and what (organizations and capabilities) we are dealing with, before jumping to conclusions, comparing and referencing with a known, but possibly inapplicable, body of knowledge and committing resources to protect and counteract on that basis*.» Zimmermann, Doron. *The Transformation of Terrorism: The «New Terrorism,» Impact Scalability and the Dynamic of Reciprocal Threat Perception.* Zürich: Forschungsstelle für Sicherheitspolitik, 2003, S. 61.

21 «*Any disruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.*» *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive No. 63*, White Paper, 22. Mai 1998, S. 2. http://www.fas.org/irp/offdocs/paper598.htm.

ist, dass ein existentieller Punkt betroffen ist. Obwohl die Gepäckkontrollen des inländischen Flugverkehrs am 11. September 2001 im New Yorker Flughafen weitgehend von privaten Firmen abgewickelt wurden, fiel der öffentliche Vorwurf der Schlamperei auf die Bundesbehörden und damit auf den Staat zurück. Mit anderen Worten: Letzten Endes entscheidet nicht der Analyst, sondern die Risikoperzeption und -reaktion der Bevölkerung darüber, ob ein Ereignis eine Katastrophe darstellt, ob ein Anschlag eine existentielle Krise auslöst und ob eine Infrastruktur oder Dienstleistung «kritisch» ist oder nicht. So gesehen lässt sich die Kritikalität einer Infrastruktur nicht präventiv aufgrund empirischer Daten, sondern immer nur *ex post facto*, als Ergebnis eines normativen Prozesses bestimmen.

Auch der Begriff «Schutz» ist in seiner Absolutheit nicht geeignet, der Komplexität moderner Infrastrukturverwundbarkeiten gerecht zu werden. Denn: Ein hundertprozentiger Schutz ist nicht möglich. Aus diesem Grunde würde man in Entlehnung eines naturwissenschaftlich-technischen Vokabulars wohl besser von Robustheit oder Resilienz und umgangssprachlich von Überlebens- oder Regenerationsfähigkeit, von Verfügbarkeit, Stabilität oder Verlässlichkeit sprechen.

So zeigt es sich, dass CIP im Grunde gar kein technisch-abstraktes, sondern ein existentiell-natureigenes Phänomen beschreibt. Jeder Baum vollzieht im Herbst einen Prozess, welchen man als Schutz kritischer Infrastrukturen bezeichnen könnte: Er reduziert seine Aktivitäten auf ein für das Überleben während einer Stressperiode, dem Winter, notwendiges Mindestmass. Diesen Gedanken kennen wir im übrigen nicht nur aus der Natur, sondern auch in einem militärischen Kontext: Die Verteidigungsstrategie der Schweiz im Zweiten Weltkrieg, der Rückzug in die Alpenfestung des Réduit, basierte auf derselben Überlegung.

5 Schlussfolgerungen und Empfehlungen

Zusammenfassend lässt sich festhalten, dass der Begriff «Schutz kritischer Infrastrukturen» weder aus operativer noch aus konzeptioneller Sicht befriedigt. Aufgrund seiner Verbreitung liesse es sich jedoch durchaus damit leben. Das Hauptproblem ist jedoch ein anderes: CIP ist ein Begriff, welcher seinen Ursprung in einem technisch-naturwissenschaftlichen Kontext geschlossener Systeme hat. Ab 1996 wurde der Begriff in einen sicherheitspolitischen Diskurs eingeführt, ohne dass die Analyse-Methoden diesem veränderten Kontext eines offenen Systems entsprechend angepasst wurden. Infrastrukturanalyse wird vor diesem Hintergrund und auch nach dem 11. September 2001 sehr oft als präzise Messung unter weitgehender Vernachlässigung des sozio-politischen Kontexts in bezug auf Machtverhältnisse, Akteure, Kulturen und Interessen verstanden. Oft wird beispielsweise die terroristische Bedrohung entweder ausgeklammert – weil sie sich nicht quantifizieren lässt – oder ohne Einbezug nachrichtendienstlicher Expertise und damit Plausibilität als eine gegebene *Blackbox* antizipiert. Auch ein britischer Regierungsbericht zog

unlängst denselben Schluss, dass einige der Anwendungen des Risikomanagement-Konzeptes zu mechanistisch und zuwenig an die Entscheidungsfindung auf oberster strategischer Ebene angepasst seien: Je höher die Risiken veranlagt seien, umso schwieriger sei deren Identifikation und Quantifizierung, umso zerstörerischer die Auswirkungen und oft umso instabiler der Zustand. Deshalb sei die Risikoidentifikation, das *horizon scanning,* breit auszulegen und die Risikoanalyse eher auf Urteilen denn auf messbaren Fakten zu gründen.[22] Katastrophen-Risiken, szenariotechnisch auch als *Wild Cards* bezeichnet, stellen mit ihrer geringen Wahrscheinlichkeit bei grossem Schadensausmass a) definitionsgemäss existentielle Risiken und b) nicht empirisch vorhersehbare Ereignisse dar. Aus diesem Grunde, und gerade auch in bezug auf die terroristische Bedrohung, stellt im Rahmen der strategischen Verteidigungs- und Schutzplanung der Leitspruch «Nur was man messen kann, lässt sich verbessern» eine Sackgasse dar.

In den letzten Jahren sind eine Reihe von Methoden entwickelt worden, um die Interdependenzen von kritischen Infrastrukturen ganzheitlich erfassen zu können. So gehen beispielsweise Rinaldi, Peerenboom und Kelly von einem konzeptionellen Rahmen mit sechs Dimensionen aus: a) der Infrastrukturcharakteristik (organisatorisch, operationell, zeitlich, räumlich), b) der Art der Interdependenz (physisch, *cyber*-basiert, logisch, geographisch), c) der Umwelt (politisch/sozial, technisch, rechtlich, ökonomisch), d) dem Verhalten der Rückkopplung, e) der Art des Ausfalls sowie f) dem Betriebszustand.[23]

Da Verwundbarkeiten grundsätzlich unendlich sind, sind Risikoanalysen definitionsgemäss niemals vollständig und niemals exakt. Selbst Yacov Haimes, Grandseigneur der *Society for Risk Analysis*, schreibt in seinem Lehrbuch über die Risikoanalyse, dass diese a) dort, wo sie präzis sei, nicht der Wirklichkeit entspreche und b) dort, wo sie real sei, nicht exakt sein könne. Dies gelte insbesondere für die Risiken von Extremereignissen, welche nicht in gleicher Weise wie Ereignisse mit grosser Wahrscheinlichkeit und tiefem Schadensausmass analysiert werden könnten.[24]

Gerade im Bereich der Terrorismusbekämpfung lässt sich eine fundamentale Asymmetrie feststellen zwischen der offensichtlichen Fähigkeit der Terroristen, den Eindruck zu erwecken, überall und zu jeder Zeit zuschlagen zu können, und der Unfähigkeit der Sicherheitskräfte, alle erdenklichen Ziele zu schützen.[25]

22 *Risk: Improving Government´s Capability to Handle Risk and Uncertainty*. *Strategy Unit Report*. London: Prime Minister's Strategy Unit, November 2002, S. 29. http://www.number-10.gov.uk/SU/RISK/REPORT/01.HTM.

23 Rinaldi, Steven M./Peerenboom, James P./Kelly, Terrence K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. In: *IEEE Control Systems Magazine*, Dezember 2001, S. 11–24.

24 Haimes, Yacov Y. *Risk Modeling, Assessment, and Management.* New York: Wiley-Interscience, 1998, S. 45.

25 Hoffmann, *Terrorismus,* S. 76.

Dieser Umstand bedeutet allerdings nicht, dass eine Priorisierung unserer Infrastrukturen in bezug auf die terroristische Bedrohung nicht möglich ist. Dies bedingt allerdings einen Gesamt-Risiko-Dialog als deliberativen Prozess auf vertikaler (Bund/Kantone) und horizontaler Ebene (zwischen Bundesinstitutionen) sowie über die Landesgrenzen hinaus.

Der effektive Schutz kritischer Infrastrukturen setzt eine holistische Problemerkennung auf physischer, *cyber*-basierter und psychologischer Ebene als Grundlage der Formulierung einer umfassenden Schutz- und Überlebensstrategie voraus. Hierzu braucht es Partnerschaften. Gegenwärtig oft gefordert werden in diesem Zusammenhang starke *public-private partnerships* (PPP). Weniger oft thematisiert wird sowohl in der Praxis als auch in der Literatur die notwendige Partnerschaft zwischen den wissenschaftlichen Disziplinen, derjenigen zwischen Sozialwissenschaften und Naturwissenschaften. Im Bewusstsein, dass es eine absolute Sicherheit niemals geben wird, müssen wir beginnen, von vermeintlichen fremden Wissensgebieten sowie aus der Vergangenheit zu lernen. Wenn uns der Blick in die Geschichte Möglichkeiten öffnen und nicht verschliessen soll, dann gilt es sich vor Augen zu halten, dass viele Folgen von Ereignissen heute nur deshalb plausibel erscheinen, weil sie sich tatsächlich ereignet haben. Kahn und Wiener hielten schon Jahrzehnte vor dem 11. September 2001 fest: «Zukünftige Ereignisse müssen nicht immer der engbegrenzten Liste entnommen werden, die wir als möglich kennengelernt haben; wir müssen auf weitere Überraschungen gefasst sein.»[26] So gesehen gilt es gerade im Kontext des aktuellen Kampfs gegen den Terrorismus nicht nur aus der Vergangenheit, sondern mindestens ebenso aus der Zukunft zu lernen – Stichwort «Szenario-Technik». Hier ist institutionelle und individuelle Kreativität gefragt. Diese hat gegenüber dem Wissen nicht zuletzt denjenigen Vorteil, dass sie grundsätzlich unbeschränkt ist. Im einzelnen sollte vermieden werden, weiterhin Infrastrukturanalysen ohne Verständnis des Motivs, des Potentials sowie der Vorgehensweise politisch motivierter Akteure durchzuführen mit der Begründung, dass sich diese eben nicht exakt beschreiben liessen.

In neueren *Policy*-Berichten des US-Kongresses findet man denn auch den Schluss, dass Bedrohungs-, Verwundbarkeits- und Kritikalitätsanalysen nicht getrennt vorgenommen werden sollten, sondern sich vielmehr im Sinne eines umfassenden Risikomanagement-Ansatzes ergänzen müssten.[27] Dies bedingt eine Anpassung des Analyseansatzes, welcher Aspekte weniger aufgrund ihrer Messbarkeit, sondern vielmehr aufgrund ihrer Entscheidungsrelevanz beurteilt – seien sie quantitativer

26 Kahn, Hermann/Wiener, Anthony J. *Ihr werdet es erleben. Voraussagen der Wissenschaft bis zum Jahre 2000*. Wien, München, Zürich: Oldenburg, 1967, S. 254.

27 House Committee on Government Reform. *Homeland Security, Key Elements of a Risk Management Approach. Testimony before the Subcommittee on National Security, Veterans Affairs, and International Relations*. Washington, DC: United States General Accounting Office, 2002, S. 1: «*A good risk management approach includes three primary elements: a threat assessment, a vulnerability assessment, and a criticality assessment*». http://www.house.gov/reform/ns/statements_witness/GAO-02-150T.pdf.

oder qualitativer Natur. Es gibt zwar eine Vielzahl von detaillierten Einzelanalysen, aber nur wenige Gesamtbetrachtungen. So meint auch Gebhard Geiger von der Stiftung für Wissenschaft und Politik, die sicherheitswissenschaftliche und schliesslich auch sicherheitspolitische Forschungs- und Entwicklungsaufgabe bestehe nicht so sehr darin, eine neue Disziplin der angewandten Forschung zu konzipieren, sondern darin, vorhandene Ansätze, Modelle und Methoden auf die Probleme des gesellschaftlichen Infrastrukturschutzes angemessen zu übertragen.[28]

So gesehen gilt es, disziplinäre Scheuklappen zu vermeiden und sich den Ausspruch von Albert Einstein zu vergegenwärtigen: Nicht alles was zählt, ist zählbar; und nicht alles was zählbar ist, zählt!

28 Geiger, Gebhard. *Information und Infrastruktursicherheit: Grundzüge eines sicherheits- und technologiepolitischen Forschungs- und Entwicklungsprogramms.* Ebenhausen: Stiftung Wissenschaft und Politik, Mai 2000, S. 33.