PUBLIC-PRIVATE PARTNERSHIPS UND DIE GRENZEN EINER VERMEINTLICHEN WUNDERLÖSUNG: EIN ERWEITERTES GOVERNANCE-MODELL FÜR DEN SCHUTZ KRITISCHER INFRASTRUKTUREN

von Myriam Dunn Cavelty und Manuel Suter

EINLEITUNG

Der Schutz kritischer Infrastrukturen – besser bekannt als *Critical Infrastructure Protection* oder kurz CIP – nimmt in der heutigen Sicherheitsdebatte weltweit einen wichtigen Platz ein. Auch in der Schweiz beschäftigen sich verschiedene Bundesstellen mit CIP, allerdings aus stark unterschiedlichen Blickwinkeln. Um die Koordination zwischen den Aktivitäten zu verbessern, wurde das Bundesamt für Bevölkerungsschutz (BABS) Mitte 2005 vom Bundesrat beauftragt, zusammen mit allen beteiligten Departementen den Handlungsbedarf zu konkretisieren und entsprechende Massnahmen zu erarbeiten, die bis 2012 in eine nationale Strategie münden sollen.[1] Der vorliegende Artikel will in Form eines Denkanstosses einen Beitrag zu den laufenden Arbeiten leisten.

Die Privatisierung und Deregulierung vieler Bereiche des öffentlichen Sektors seit den 1980er Jahren und die Globalisierungsprozesse der 1990er Jahre haben dazu geführt, dass sich heute ein grosser Teil der kritischen Infrastrukturen in privater Hand befindet. Aus der Sicht des Staates, der CIP als ein Problem der nationalen Sicherheit sieht, sorgen die Kräfte des Marktes allein in den meisten Sektoren nicht für genügend Sicherheit.[2] Gleichzeitig

1 Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS), Bundesamt für Bevölkerungsschutz (BABS). *Erster Bericht an den Bundesrat zum Schutz Kritischer Infrastrukturen*. Bern, 20.6.2007. Einsehbar unter: http://www.bevoelkerungsschutz.admin.ch/internet/bs/de/home/aktuell.parsys.51233.downloadList.66685.DownloadFile.tmp/9039.pdf.

2 Siehe z.B.: Anderson, Ross. Why Information Security is Hard – An Economic Perspective. In: IEEE Computer Society (Hrsg.). *Proceedings of the 17th Annual Computer Security Applications Conference.* Washington, DC: IEEE Computer Society, 2001, S. 358–365. http://www.acsac.org/2001/papers/110.pdf.

sieht sich der Staat jedoch ausserstande, selbstständig für das öffentliche Gut Sicherheit zu sorgen. Ein zu massiver Eingriff in den Markt ist keine valable Option, denn dieselben Infrastrukturen, die der Staat aus der Perspektive nationaler Sicherheit schützen will, sind fast immer auch die Basis für die Wettbewerbsfähigkeit und die Prosperität einer Nation. Eine Politik zur Sicherung der kritischen Infrastrukturen muss also die aus Sicht der Sicherheitspolitik negativen Konsequenzen der Liberalisierung, Privatisierung und Globalisierung auffangen, ohne deren positive Effekte zu verhindern.

Als Allheilmittel gegen dieses Problem gelten *Public-Private Partnerships* (PPP), eine Form der Partnerschaft von Staat und Privatwirtschaft. Entsprechende Kooperationsprogramme sind denn auch Teil aller bestehenden Initiativen im CIP-Bereich.[3] Einige dieser Partnerschaften funktionieren erfolgreich, indem die Akteure gegenseitig Informationen austauschen. Andere Kooperationen gehen kaum über eine gemeinsame Willensbekundung der involvierten Parteien hinaus. Vermehrt wurden deshalb in den letzten Jahren kritische Stimmen laut, die die Ineffizienz bestehender Arrangements beklagten[4] oder gar das Konzept der Zusammenarbeit insgesamt in Frage stellten.[5] Dass teilweise eine Korrektur der hohen Erwartungen eingesetzt hat, ist nicht weiter verwunderlich: Die Idee von PPP entstand ursprünglich in einem völlig anderen Kontext, nämlich im Bereich der Verwaltungsreform und des *New Public Management* in den 1980er Jahren. Danach wurde das Konzept der PPP Ende der 1990er Jahre praktisch unreflektiert von vielen Staaten für ihre CIP-Politik übernommen. Bis heute ist es daher nur vage bis gar nicht definiert und vor allem theoretisch nicht fundiert. Dies führt zu

3 Suter, Manuel/Brunner, Elgin. *The International CIIP Handbook 2008. An Inventory of Protection Policies in 25 Countries and 6 International Organizations*. Zürich: Center for Security Studies, im Erscheinen.

4 Auerswald, Philip E./Branscomb, Lewis M./La Porte, Todd M./Michel-Kerjan, Erwann O. Who Will Act – Integrating Public and Private Interests to Make a Safer World. In: Dieselben (Hrsg.). *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. New York: Cambridge University Press, 2006, S. 483–505; Andersson, Jan J./Malm, Andreas. Public-Private Partnerships and the Challenge of Critical Infrastructure Protection. In: Dunn, Myriam/Mauer, Victor (Hrsg.). *International CIIP Handbook 2006, Vol. II: Analyzing Issues, Challenges, and Prospects*. Zürich: Center for Security Studies, 2006, S. 139–168.

5 Gespräch und E-Mail-Austausch mit einem Experten des *Joint Research Centre* der EU in Ispra.

einer Reihe von Problemen bei der Umsetzung, worin der Hauptgrund für die konstatierten Ernüchterungserscheinungen liegt.

Die Kritiker der PPP laufen aber Gefahr, das Kind mit dem Bad auszuschütten: Die Zusammenarbeit zwischen Staat und Privatwirtschaft für den Schutz kritischer Infrastrukturen ist nämlich nicht nur sinnvoll, sondern schlichtweg unumgänglich. Deshalb geht dieser Artikel den folgenden Fragen nach: *Was ist der Nutzen des PPP-Konzepts und wo sind seine Grenzen für CIP? Welche anderen Konzepte kommen als Lösungsansätze (eher) in Frage?* Im ersten Kapitel zeigen wir, wo der PPP-Begriff herkommt und aus welchem grösseren, wirtschaftspolitischen Kontext er entstammt. Im zweiten Kapitel beleuchten wir die spezifische Ausprägung von PPP im CIP-Bereich und analysieren die Probleme des Konzepts. Dabei wird nicht die öffentlich-private Zusammenarbeit generell in Frage gestellt, sondern nur die Art und Weise, wie sie bisher organisiert wurde. Insbesondere wird darauf hingewiesen, dass die direkte Partnerschaft zwischen öffentlichen und privaten Akteuren nicht die einzig mögliche Form der Zusammenarbeit darstellt, sondern nur eines von vielen Instrumenten ist, die im Bereich CIP für die *Governance* eingesetzt werden können.[6] Für die Entwicklung eines neuen, breiteren Verständnisses der öffentlich-privaten Kooperation greifen wir darum im dritten Kapitel auf die *Governance*-Theorie zurück. Das aus dieser Theorie entwickelte Modell wird im abschliessenden vierten Kapitel auf die Schweiz angewendet. Wir argumentieren, dass CIP-Politik möglichst auf sich selbst regulierende und sich selbst organisierende Netzwerke setzen sollte. Die Rolle der Regierung beinhaltet dann nicht mehr die direkte Steuerung und die enge Kontrolle, sondern vielmehr die Koordination von Netzwerken und die Bestimmung von Instrumenten, mit denen diese Netzwerke für CIP-Aufgaben motiviert werden können.

6 Im hier verwendeten Zusammenhang wird *Governance* in Abgrenzung zu traditionellem *Government* verstanden und bezeichnet die Koordination von sozialen Beziehungen auf lokaler, nationaler oder internationaler Ebene in Absenz einer zentralen Autorität.

1 DER URSPRUNG EINER IDEE: DIE KRISE DER STAATLICHKEIT UND VERWALTUNGSREFORMEN

Experten lokalisieren den Ursprung von PPP in den 1940er Jahren an der Ostküste der USA, wo sie erstmals bei der Restrukturierung und ökonomischen Erneuerung der Pittsburgh-Region eine Rolle spielten.[7] Wirklich populär wurde das Konzept im Zuge der Entbürokratisierungswelle ab Ende der 1970er Jahre vor dem Hintergrund der Weltwirtschaftkrise. Die neoliberale Staatskritik diagnostizierte damals statt eines Marktversagens Staats- und Bürokratieversagen, wobei «Bürokratisierung» als Sammelbegriff für viele unterschiedliche Kritikpunkte am modernen Wohlfahrtsstaat verwendet wurde. Neo-konservative Regierungen gingen – basierend auf einer angebotsorientierten Wirtschaftspolitik – dazu über, günstige Investitionsbedingungen für Unternehmen zu schaffen, um so deren internationale Wettbewerbsfähigkeit zu fördern.[8] Die Bürokratie war angehalten, Aufgaben an private Akteure zu übergeben oder sie zumindest in Partnerschaft mit der Privatwirtschaft zu erfüllen, um so die Effizienz der öffentlichen Verwaltung zu erhöhen.[9] Auch die Kosten für die Problemlösung sollten auf die verschiedenen privaten und öffentlichen Akteure verteilt werden.

Diese Entwicklungen waren mit einem grundlegenden Wandel des Funktions- und Rollenverständnisses von Staat und Verwaltung verbunden.[10] Die «klassische, ordnungspolitisch begründete Dichotomie von Staat und Markt» wurde in zwei Richtungen relativiert. Zum einen erhielten Markt und Wettbewerb in den öffentlichen Diensten mehr Bedeutung – zum anderen bildeten sich neue Organisations- und Kooperationsformen zwischen privaten und öffentlichen Aufgabenträgern.[11] In diesem Zusammenhang entstanden auch

7 Budäus, Dietrich/Grüning, Gernod. Public Private Partnership – Konzeption und Probleme eines Instruments zur Verwaltungsreform aus Sicht der Public Choice Theorie. In: Budäus, Dietrich/Eichhorn, Peter (Hrsg.). *Public Private Partnership – Neue Formen öffentlicher Aufgabenerfüllung*. Nomos Verlagsgesellschaft: Baden-Baden, 1997, S. 25–65, hier S. 26.

8 Willke, Gerhard. *Neoliberalismus*. Campus: Frankfurt, 2003.

9 Vgl. Savas, Emanuel S. *Privatizing the Public Sector – How to Shrink Government*. Chatham: Chatham House Publishers, 1982.

10 Budäus, Dietrich/Eichhorn, Peter. Vorwort. In: Budäus/Eichhorn, *Public Private Partnership*, S. 11–12, hier S. 11.

11 Ebd.

Public-Private Partnerships.[12] Sie waren ein Element der Modernisierung des öffentlichen Sektors, die auf eine Effizienzsteigerung der staatlichen Dienstleistungen abzielte und Zwang und Regulierung durch eine *freiwillige* Zusammenarbeit zwischen öffentlichen und privaten Partnern ablöste.[13]

PPP wurden zunächst vor allem im Städtebau verwirklicht, um «gemeinsam die Entwicklung und Erneuerung städtischer Problemzonen zu betreiben».[14] Dies hiess beispielsweise, dass eine Stadt mit vernachlässigtem Innenstadtbereich einen Vertrag mit einem privaten Immobilien-Entwickler abschloss, die Planungs- und Genehmigungsverfahren beschleunigte und der *Developer* anschliessend Bürogebäude oder Einkaufszentren errichtete und vermarktete.[15] Später wurden auch gemeinsame Technologie- oder Umweltschutzprojekte sowie Partnerschaften im Bereich der Bildung, des Gesundheitswesens oder des Strafvollzugs dazu gezählt.[16] Unterdessen sind PPP ein ausserordentlich heterogenes Konzept, das sich über die Jahre immer wieder verändert hat.[17] Kritische Stimmen bemängeln, dass das Konzept zu einem undifferenzierten Sammelbegriff «für alle möglichen neuen und bereits bekannten Formen der Zusammenarbeit zwischen öffentlicher Hand und Privaten» geworden sei.[18]

Bei aller definitorisch-konzeptionellen Schwammigkeit kann der Grundcharakter von PPP wie folgt beschrieben werden: Das Ziel von PPP ist es, Synergien bei der gemeinsamen, innovativen Nutzung von Ressourcen sowie bei der Anwendung von Managementwissen zu schaffen. Die Zusammenarbeit soll es den involvierten Parteien ermöglichen, ihre Ziele besser zu errei-

12 Hodge, Graeme/Greve, Carsten (Hrsg.). *The Challenge of Public-Private Partnerships – Learning from International Experience*. Cheltenham: Edward Elgar Publishing, 2005.

13 Mirow, Thomas. Public Private Partnership – eine notwendige Strategie zur Entlastung des Staates. Beispiele aus der Freien und Hansestadt Hamburg. In: Budäus/Eichhorn, *Public Private Partnership*, S. 13–24, hier S. 22.

14 Budäus/Grüning, *Public Private Partnership*, S. 42f.

15 Ebd., S. 39; Siehe auch: Moteff, John D./Copeland, Claudia/Fischer, John. *Critical Infrastructures: What Makes an Infrastructure Critical?* Congressional Research Report for Congress, RL31556, 29. Januar 2002. Washington, DC: Congressional Research Service, S. 14.

16 Vaillancourt Rosenau, Pauline (Hrsg.). *Public-Private Policy Partnerships*. Cambridge: The MIT Press, 2000.

17 Linder, Stephen H. Coming to Terms with the Public-Private Partnership – a Grammar of Multiple Meanings. In: Vaillancourt Rosenau, *Public-Private Policy Partnerships*, S. 19–36.

18 Budäus/Grüning, *Public Private Partnership*, S. 47.

chen oder diese überhaupt erst realisieren zu können.[19] Zentrale Bedingungen für eine solche Kooperation sind die Komplementarität der jeweiligen Ziele sowie das Vorhandensein von Interdependenzen zwischen den Akteuren und ihren Zielen.[20] Eine Zusammenarbeit im Rahmen von PPP wird dabei vertraglich formalisiert.[21] Weitere Bedingungen, auf die in der Literatur hingewiesen wird, sind das gegenseitige Vertrauen sowie Vorrichtungen, die möglichen Missbrauch begrenzen; das Vorhandensein von klaren, unumstrittenen, schriftlich fixierten Zielen und Strategien; eine klare Risikoverteilung; klare Teilung von Verantwortung und Autorität sowie markt- und erfolgsorientiertes Denken.[22] Angesichts dieser umfassenden Voraussetzungen für den Erfolg von PPP stellt sich die Frage, inwiefern sich die PPP-Idee überhaupt auf CIP übertragen lässt.

2 KRITISCHE INFRASTRUKTUREN UND PUBLIC-PRIVATE PARTNERSHIPS

Das Fundament für das CIP-Konzept, das in den letzten Jahren weltweit ständig an Bedeutung gewonnen hat, bildete die 1997 in den USA vorgelegte Studie der *President's Commission on Critical Infrastructure Protection* (PCCIP).[23] Der Erscheinungszeitpunkt dieser Studie ist nicht zufällig: Der Diskurs über den adäquaten Schutz von Infrastrukturen ist damals wie heute eng mit dem Diskurs über die Rolle des Staates in einer durch die Globalisierung veränderten Welt verknüpft. Zwei miteinander verwobene Debatten prägen die Gefahrenperzeption und die möglichen Lösungsansätze:

19 Linder, Stephen H./Vaillancourt Rosenau, Pauline. Mapping the Terrain of the Public-Private Policy Partnership. In: Vaillancourt Rosenau, *Public-Private Policy Partnerships*, S. 1–19, hier S. 5f.

20 Kouwenhoven, Vincent. Public-Private Partnership: A Model for the Management of Public-Private Cooperation. In: Kooiman, Jan (Hrsg.). *Modern Governance – New Government-Society Interactions*. London: SAGE, 1993, S. 119–130, hier S. 120. Zu verschiedenen Arten von PPP siehe Linder, *Coming to Terms with the Public-Private Partnership*.

21 Budäus/Grüning, *Public Private Partnership*, S. 54.

22 Kouwenhoven, *Public-Private Partnership*, S. 124.

23 President's Commission on Critical Infrastructure Protection. *Critical Foundations. Protecting America's Infrastructures*. Washington, DC, 13.10.1997, S. B-1. Nachfolgend zitiert als PCCIP-Report. Siehe auch Wenger, Andreas/Metzger, Jan/Dunn, Myriam. Critical Information Infrastructure Protection (CIIP) – Eine sicherheitspolitische Herausforderung. In: *Bulletin 2002 zur schweizerischen Sicherheitspolitik*. Zürich: Forschungsstelle für Sicherheitspolitik, 2002, S. 119–142.

Zum einen geht es um den strukturellen Wandel von der Industrie- hin zur Informationsgesellschaft und um die damit einhergehende Globalisierung der Märkte. Zum anderen findet auch eine Globalisierung der Risiken statt.[24] In diesem Umfeld sieht sich der Staat in zunehmendem Masse von nichtstaatlichen Akteuren bedroht, während er gleichzeitig auch auf nichtstaatliche Akteure angewiesen ist, wenn es um den Schutz kritischer Infrastrukturen geht. Im ersten Unterkapitel wird dieser breitere Kontext genauer beschrieben. Im zweiten Unterkapitel gehen wir dann der Frage nach, welche Art von PPP sich im Bereich von CIP als Lösungsansatz herauskristallisiert hat. Im dritten Kapitel zeigen wir die Grenzen dieser «Lösung» auf.

2.1 SCHUTZ KRITISCHER INFRASTRUKTUREN IM GRÖSSEREN SICHERHEITSPOLITISCHEN KONTEXT

Die Entstehung und Etablierung des CIP-Konzepts geht auf zwei zentrale Faktoren zurück. Erstens hat der Wandel der sicherheitspolitischen Lage nach dem Ende des Kalten Krieges die Schutzbedürftigkeit von Infrastrukturen erhöht. Während des Ost-West-Konflikts wurden sicherheitspolitische Probleme in erster Linie als militärische und akteurbezogene «Bedrohungen» verstanden. Die Identifizierung und Einschätzung dieser Bedrohungen erfolgte aufgrund des so genannten Bedrohungsdreiecks, bestehend aus dem gegnerischen Akteur, dessen feindlichen Absichten sowie dessen Mittel zur Schadensverursachung. War das daraus resultierende Bedrohungsbild während des Kalten Kriegs relativ klar, so sind die Formen und Verläufe sicherheitspolitischer Herausforderungen seither wesentlich diffuser geworden. Statt einer begrenzten Anzahl «Bedrohungen» ist eine Vielzahl von «Risiken» in den Blickpunkt der Sicherheitspolitik gerückt.[25] Risiken sind gekennzeichnet durch Ungewissheit und Komplexität. Als Folge dieses diffusen Lagebilds

24 Bailes, Alyson J. K. Introduction: A World of Risk. In: SIPRI (Hrsg.). *SIPRI Yearbook 2007: Armaments, Disarmament and International Security*. Oxford: Oxford University Press, 2007, S. 1–20.

25 Daase, Christopher/Feske, Susanne/Peters, Ingo (Hrsg.). *Internationale Risikopolitik: Der Umgang mit neuen Gefahren in den internationalen Beziehungen*. Baden-Baden: Nomos Verlagsgesellschaft, 2002; Habegger, Beat. Von der Sicherheits- zur Risikopolitik: eine konzeptionelle Analyse für die Schweiz. In: *Bulletin 2006 zur schweizerischen Sicherheitspolitik*. Zürich: Forschungsstelle für Sicherheitspolitik, 2006, S. 133–164.

wurde der sicherheitspolitische Fokus nach 1989/91 weniger auf die (schwer identifizierbaren) Akteure, sondern mehr auf die generellen Verwundbarkeiten der gesamten Gesellschaft gelegt.[26]

Die zweite Antriebskraft hinter dem CIP-Konzept war die Globalisierung und speziell die Informationsrevolution, die diesen Prozess wesentlich mitgestaltete und vorantrieb. Neue Informations- und Kommunikationstechnologien lösten in den 1990er Jahren eine dynamische und tiefgehende Transformation der Gesellschaft aus. Neben einer Vielzahl von positiven Folgen sticht vor allem eine negative Konsequenz dieser hervor: Die erhöhte Verwundbarkeit moderner industrialisierter Gesellschaften durch ihre Abhängigkeit von den zahlreichen nationalen und internationalen Informationsinfrastrukturen. Diese gelten nicht nur als inhärent unsicher, sondern auch als besonders anfällig für asymmetrische Massnahmen.[27]

Durch die Zunahme transnationaler Ströme von Kapital, Gütern, Dienstleistungen und Personen hat die staatliche Ordnungs- und Regulierungsfähigkeit abgenommen. Der Staat scheint einen substantiellen Teil seiner Autorität für das Kollektivgut Sicherheit an die Wirtschaft «verloren» zu haben. Dieser kommt deshalb sowohl bei der Definition als auch bei der Umsetzung einer Schutzpolitik eine bedeutende Rolle zu.[28] Unternehmen sind heute sogar eigentliche Ziele von Bedrohungen geworden, die von islamistischem Terrorismus oder von der organisierten Kriminalität ausgehen. Eine längere Unterbrechung von wichtigen Infrastrukturen haben nicht nur für den Staat, sondern auch für die Privatwirtschaft gravierende negative Folgen, wenn auch aus teilweise unterschiedlichen Gründen. Eine Kooperation scheint deshalb für beide Seiten von Nutzen.

26 Dunn Cavelty, Myriam/Kristensen, Kristian Søby (Hrsg.). *Securing the Homeland: Critical Infrastructure, Risk, and (In)Security*. London: Routledge, 2008.

27 Dunn Cavelty, Myriam/Mauer, Victor/Krishna-Hensel, Sai-Felicia (Hrsg.). *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace*. Aldershot: Ashgate, 2008.

28 Vgl. Bailes, Alyson J. K./Frommelt, Isabel (Hrsg.). *Business and Security: Public-Private Sector Relationships in a New Security Environment*. Oxford: Oxford University Press, 2004.

2.2 PPP IN FORM VON INFORMATIONSAUSTAUSCH ALS LÖSUNG?

Die *Presidential Commission on Critical Infrastructure Protection* (PCCIP) wurde von Präsident Bill Clinton eingesetzt, um einen umfassenden Bericht über die Sicherheit aller Infrastruktursysteme der USA zu erstellen. Das Hauptaugenmerk war auf die noch weitgehend unbekannten Bedrohungen aus dem Cyberspace gerichtet: Die globale Informationsinfrastruktur schien anonyme Angriffe von überallher auf der Welt zu ermöglichen und machte gleichzeitig Hackertools einfach zugänglich. Die PCCIP sollte diese Risiken abschätzen, defensive Massnahmen entwickeln und zur Klärung des institutionellen und gesetzlichen Reformbedarfs beitragen. In der Kommission waren *alle* relevanten Ministerien vertreten, nicht mehr nur der sicherheitspolitische Apparat. Zusätzlich wurden auch die privaten Infrastrukturbetreiber mit einbezogen.[29]

Mit dieser Erweiterung der sicherheitspolitischen Akteure um andere Ministerien und zivile Unternehmen wurde das Spektrum der möglichen Strategien im CIP-Bereich über den traditionellen Kernbereich der Sicherheitspolitik ausgedehnt. Gleichzeitig vollzog sich ein Wandel im Objekt der Sicherheitspolitik – weg von der «Nation» als Kollektiv, hin zur Sicherung (technischer) Infrastrukturen.[30] Diese Vorgehensweise beruhte auf der Annahme, dass die Sicherheitspolitik im Falle von CIP nicht mehr eine exklusive Aufgabe des Staates sein konnte, sondern eine Teilung der Verantwortung notwendig machte. Bereits in der Zusammensetzung der Kommission kam die Verschmelzung des PPP-Gedankens mit demjenigen der kritischen Infrastrukturen zum Ausdruck.[31]

Der PCCIP-Bericht betonte nachdrücklich, dass CIP ein Problem war, dass nur durch gemeinsame Anstrengungen von Staat und Privatwirtschaft

29 Lopez, Brian. Critical Infrastructure Protection in the United States since 1993. In: Auerswald, Philip E./Branscomb, Lewis M./La Porte, Todd M./Michel-Kerjan, Erwann O. (Hrsg.). *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. New York: Cambridge University Press, 2006, S. 37–50.

30 Bendrath, Ralf. Elektronisches Pearl Harbor oder Computerkriminalität? Die Reformulierung der Sicherheitspolitik in Zeiten globaler Datennetze. In: *S+F. Vierteljahresschrift für Sicherheit und Frieden* 18 (2000), Nr. 2. http://userpage.fu-berlin.de/~bendrath/SuF_2000.rtf.

31 Die Clinton-Regierung setzte generell stark auf PPP in allen Bereichen, was zum Beispiel in der *National Performance Review* (später *National Partnership for Reinventing Government*) zum Ausdruck kam.

gemeistert werden konnte. Er hielt fest, dass die interdependenten Infrastrukturen ein Umfeld gemeinsamer Risiken generierten, die ein gemeinsames Risikomanagement erforderten. Dabei appellierte der Bericht nicht nur an die Verantwortung der Privatwirtschaft, die als Besitzerin und Betreiberin der meisten Infrastrukturen ihren Teil zur Sicherheit beitragen sollte,[32] sondern auch an deren Eigeninteresse, da sie direkt von Cyber-Attacken bedroht war.[33] Als unmittelbarste Notwendigkeit für den Schutz kritischer Infrastrukturen bezeichnete die Kommission den Informationsaustausch *(Information-Sharing)* zwischen allen relevanten Akteuren im CIP-Bereich.[34] Durch den Austausch von Informationen sollten gegenseitige *Win-Win*-Situationen geschaffen werden.[35] Wie könnte ein solcher Informationsaustausch aussehen? Beispielsweise könnte die Regierung proprietäre geheimdienstliche Informationen über die Bedrohungslage zur Verfügung stellen, während der private Sektor dem Staat im Gegenzug Information über die Schwachstellen und das Funktionieren der Infrastruktur liefert. Solche Informationen sind für die Regierung unerlässlich, um eine gesamtheitliche Gefahrenabschätzung vornehmen und eine Frühwarnung gewährleisten zu können. Der Austausch von Informationen über Attacken und mögliche Gegenmassnahmen unter den verschiedenen Unternehmen führt dazu, dass diese kostengünstig Know-how gewinnen und ihre Schutzmassnahmen gezielter einsetzen können[36] – was wiederum die Sicherheit des Gesamtsystems erhöht. Darüber hinaus können Regierungen Firmen direkten Zugang zu den Strafvollzugs-

32 Im Wortlaut: «*Because the infrastructures are mainly privately owned and operated, we concluded that critical infrastructure assurance is a shared responsibility of the public and private sectors.*» PCCIP-Report, S. i.

33 Ebd.

34 Ebd., S. 21; S. 27.

35 Im Wortlaut: «G*overnment can help by collecting and disseminating information about all the tools that can do harm. Owners and operators can help by informing government when new tools or techniques are detected.*» Ebd., S. 20.

36 Anderson, Ross/Moore, Tyler. The Economics of Information Security. In: *Science* 314 (2006), Nr. 5799, S. 610–623; Gordon, Lawrence A./Loeb, Martin P./Lucyshyn, William. Sharing Information on Computer Systems Security: An Economic Analysis. In: *Journal of Accounting and Public Policy* 22 (2003), Nr. 6, S. 461–485; Gal-Or, Esther/Ghose, Anindya. The Economic Incentives for Sharing Security Information. In: *Information Systems Research* 16 (2004), Nr. 2, S. 186–208.

behörden ermöglichen, die bei internationalen Cyber-Kriminalitätsvorfällen behilflich sein können.[37]

Nach der Vorlage des PCCIP-Berichtes folgte Präsident Clinton im Mai 1998 mit den *Presidential Decision Directives* PDD-62 und -63[38] weitgehend den dort formulierten Empfehlungen. Unter anderem sollten in den einzelnen Sektoren *Information Sharing and Analysis Centers* (ISAC) gegründet werden, deren genaue Form und Arbeitsweise von den privaten Betreibern selbst bestimmt werden sollten.[39] 1999 wurde im Finanzsektor das erste ISAC gegründet, bald folgten weitere ISAC in anderen wichtigen Sektoren.[40] Diese ISAC dienen dem Austausch von Informationen über Sicherheit, Störungen und *Best Practices* unter den ISAC-Mitgliedern (Unternehmen der gleichen Branche) und auch mit anderen ISAC. Obwohl die meisten ISAC subventioniert sind oder sogar vollständig von der Regierung finanziert werden, steht es den Unternehmern völlig frei, wie sie ihre ISAC organisieren. Es gibt daher grössere Unterschiede in den Strukturen sektorspezifischer ISAC.[41]

Neben den USA unterhalten auch viele andere Regierungen ähnliche Programme, die den Informationsaustausch zwischen den Betreibern kritischer Infrastrukturen fördern sollen. Viele bezeichnen den Informationsaustausch sogar als oberste Priorität.[42] Solche Informationsaustauschgremien haben sich weltweit als Hauptform von PPP im Bereich CIP etabliert. Jenseits des alten

37 Suter Manuel. *A Generic National Framework for Critical Information Infrastructure Protection. Meeting Background Paper for the 2nd Facilitation Meeting for WSIS Action Line C5*. Genf: International Telecommunication Unit (ITU), 2007.

38 Clinton, William J. *Protection Against Unconventional Threats to the Homeland and Americans Overseas: Presidential Decision Directive 62*. Washington, DC, 22. Mai 1998; Clinton, William J. *Protecting America's Critical Infrastructures: Presidential Decision Directive 63*. Washington, DC, 22. Mai 1998.

39 Vgl. National Security Council. *White Paper. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*. Washington, DC, Mai 1998. http://www.fas.org/irp/offdocs/paper598.htm.

40 United States General Accounting Office. *Critical Infrastructure Protection: Establishing Effective Information Sharing with Infrastructure Sectors*. Washington, DC: General Accounting Office, 2004.

41 Prieto, Daniel B. Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects. In: Auerswald/Branscomb/La Porte/Michel-Kerjan, *Seeds of Disaster*, S. 404–428.

42 Vgl. Suter/Brunner, *CIIP Handbook 2008*. Auch die Schweiz setzt mit der Melde- und Analysestelle Informationssicherung MELANI auf ein Kooperationsmodell mit Partnern, die im Bereich Computer- und Internetsicherheit sowie dem Schutz der schweizerischen kritischen Infrastrukturen tätig sind.

staatlichen Gewaltmonopols entstand so eine Art Selbsthilfe-System, in dem der Staat die privaten Sicherheitsaktivitäten teilweise nur noch moderiert, seine repressive Rolle durch die Strafverfolgung und ähnliche Instrumente aber immer noch wahrnimmt.

2.3 DIE GRENZEN EINER WUNDERLÖSUNG

Die Idee des Informationsaustauschs zwischen Staat und Wirtschaft wird im CIP-Bereich inzwischen weltweit in die Praxis umgesetzt. Dabei sind in den letzten Jahren Schwierigkeiten aufgetaucht, die teilweise auf praktische, teilweise auf konzeptionelle Probleme zurückzuführen sind.[43] Die Kernprobleme bestehen darin, dass erstens der PPP-Begriff das Phänomen der bestehenden Partnerschaften nur sehr rudimentär zu beschreiben vermag bzw. dass die Mehrheit der sogenannten PPP zum Schutz kritischer Infrastrukturen gar keine PPP im eigentlichen Sinne sind. Zweitens sind die Interessen der Privatwirtschaft und des Staates bei CIP häufig nicht konvergent und PPP scheinen als Lösung daher ungeeignet. Drittens schliesslich sind die bestehenden Zusammenarbeitsformen zu limitiert ausgestaltet. Sie tragen den Interdependenzen zwischen den Infrastrukturen viel zu wenig Rechnung und beziehen einige wichtige Akteure nicht mit ein.

Wie oben beschrieben, brauchen PPP für ihr Funktionieren Zielkomplementarität, gegenseitiges Vertrauen, klare Ziele und Strategien, eine klare Risikoverteilung, die klare Aufteilung von Verantwortung und Autorität sowie markt- und erfolgsorientiertes Denken.[44] PPP sind darum projektbezogen und zielen auf eine Kostensenkung und eine Effizienzsteigerung ab. Zusammenarbeitsformen im CIP-Bereich hingegen sind programmbezogen (d.h. sie haben keine zeitliche Befristung) und haben nicht eine Effizienzsteigerung zum Ziel, sondern die Erhöhung der Sicherheit. Im Gegensatz zu projektbezogenen PPP ist es zudem oft schwierig, messbare Ziele zu formulieren, da

43 Algeier, Scott C. *Information Sharing, Success and Challenges: The U.S. Experience.* Konferenzpapier am Critical Infrastructure Protection (CIP) Workshop, Frankfurt a.M., 29.–30. September 2003; United States General Accounting Office. *Information Sharing – DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protection and Share Critical Infrastructure Information*. Washington, DC: General Accounting Office, April 2006.

44 Kouwenhoven, *Public-Private Partnership*, S. 124.

zunächst oft der Aufbau von gegenseitigem Vertrauen im Vordergrund steht, was den angestrebten Informationsaustausch überhaupt erst ermöglicht. Dieser Prozess ist zeitintensiv und kaum mit dem Gedanken der Effizienzsteigerung kompatibel, der traditionellen PPP zugrunde liegt. Darüber hinaus besteht eine schwer überbrückbare Dissonanz zwischen der Sicherheitslogik und der PPP-Logik: Das Generieren von Sicherheit für die Bevölkerung stellt eine Kernaufgabe des Staates dar, was die Delegation von Verantwortung in diesem Bereich zu einer ausserordentlich heiklen Angelegenheit macht.[45]

Es hat sich auch deutlich gezeigt, dass die Interessen der Privatwirtschaft und des Staates bei CIP nur teilweise konvergent sind und sich Synergieeffekte deshalb nicht immer automatisch einstellen. Private Unternehmen befürchten vor allem, dass sensible, mit dem Staat ausgetauschte Informationen über Sicherheitsprobleme vom Staat nicht mit der nötigen Sorgfalt behandelt werden und der eigene Ruf so Schaden nehmen könnte.[46] Darüber hinaus wickeln die meisten Firmen den Grossteil ihrer Geschäfte im Ausland ab und sehen die Notwendigkeit der nationalen Zusammenarbeit nur teilweise ein. Internationale Ansätze kämen solchen transnational agierenden Unternehmen weit besser entgegen. Schliesslich betrachtet die Privatwirtschaft die Problematik primär aus einer betriebswirtschaftlichen Perspektive und versteht sie in erster Linie als ein *Business-Continuity*-Thema und nicht als ein sicherheitspolitisches Thema. Dies führt zu Differenzen in der Beurteilung der Dringlichkeit der gemeinsam zu lösenden Aufgaben. Aber auch für Regierungen ist die Freigabe von Informationen über potentielle Gefährdungen mit Risiken behaftet. Die Freigabe klassifizierter Informationen kann die

45 Siehe z.B. auch: Percy, Sarah. Mercenaries: Strong Norm, Weak Law. In: *International Organization* 61 (2007), Nr. 2, S. 367–397.

46 Studien belegen, dass eine negative Korrelation zwischen der Veröffentlichung von Sicherheitslücken und dem Marktwert der betreffenden Unternehmen besteht. Siehe: Campbell, Katherine/Gordon, Lawrence A./Loeb, Martin P./Zhou, Lei. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. In: *Journal of Computer Security* 11 (2003), Nr. 3, S. 431–448; auch: Cavusoglu, Huseyin/Mishra, Birendra/Raghunathan, Srinivasan. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. In: *International Journal of Electronic Commerce* 9 (2004), Nr. 1, S. 69–104.

Aktivitäten der Geheimdienste und anderer Institutionen gefährden.[47] Zusätzlich müssen auch die Bestimmungen im Bereich des Datenschutzes und zum Schutz der Privatsphäre berücksichtigt werden.[48]

Das noch schwerwiegendere Problem ist jedoch, dass die Mehrheit der bestehenden PPP zu limitiert sind. Die meisten PPP im Bereich CIP sind heute so gestaltet, dass eine spezialisierte Behörde mit ausgewählten privatwirtschaftlichen Partnern (den Betreibern der Infrastrukturen) zusammenarbeitet. Diese Kooperationsart trägt der horizontalen und vertikalen Vernetzung der heutigen Infrastrukturen zu wenig Rechnung. Zum einen sind die meist sektorbezogenen PPP (beispielsweise die ISAC) kaum geeignet, um die Interdependenzen zwischen den verschiedenen Infrastrukturen bzw. Sektoren wirksam zu managen (horizontale Vernetzung). Zum anderen können auch die Grossunternehmen alleine nicht für die Sicherheit der von ihnen betriebenen Infrastrukturen garantieren, denn auch sie sind auf viele verschiedene kleinere Akteure angewiesen (vertikale Vernetzung).

Auch die kleinen und mittleren Unternehmen (KMU) haben ein grosses Bedürfnis nach Unterstützung im Bereich der Informationssicherheit. Sie sind stark von Vorfällen betroffen, verfügen aber nur über wenig Mittel für deren Bekämpfung. Auch aus sicherheitspolitischen Überlegungen ist es deshalb wichtig, Modelle für eine Zusammenarbeit mit KMU zu entwickeln, da die Unterscheidung zwischen kritischen Infrastrukturen und «gewöhnlichen» Unternehmen wegen der immer stärkeren Vernetzung aller Betriebe zunehmend schwieriger wird. Das Aufkommen von so genannten Botnetzen[49] hat zudem deutlich gezeigt, dass ungesicherte Netzwerke unabhängig von ihrem

47 Moteff, John D./Stevens, Gina M. *Critical Infrastructure Information Disclosure and Homeland Security*. Congressional Research Report for Congress, RL31547, 29. Januar 2003. Washington, DC: Congressional Research Service, 2003.

48 Branscomb, Lewis M./Michel-Kerjan, Erwann O. Public-Private Collaboration on a National and International Scale. In: Auerswald/Branscomb/La Porte/Michel-Kerjan, *Seeds of Disaster*, S. 395–404.

49 Der Begriff «Bot» ist von dem Wort «Robot» abgeleitet. Im technischen Umfeld wird der Begriff primär für Fernsteuerprogramme verwendet, über die kompromittierte Systeme von einem Angreifer zentral befehligt werden können. Als Botnetz versteht man einen virtuellen Verbund infizierter *Client*-Systeme, also eine Zusammenschaltung von Bots. Neben *Distributed-Denial-of-Service*-Angriffen (DDoS) ist z.B. auch die Initialverbreitung von neuer *Malware* oder auch der Einsatz von Bots als *Spam-Relay* ein bereits praktiziertes Einsatzszenario (siehe http://cert.uni-stuttgart.de/doc/netsec/bots.php).

Standort eine Gefahr für das Funktionieren der Informationsinfrastruktur darstellen können – was wegen der Interdependenzen auch für alle anderen Sektoren Konsequenzen hat. Deswegen bedarf eine wirksame CIP-Politik der internationalen Kooperation. Terroristische und kriminelle Handlungen sowie Natur- und sonstige Katastrophen machen nicht an Ländergrenzen halt, weshalb Gegenmassnahmen auch international zu koordinieren sind.

Die Notwendigkeit einer besseren horizontalen, vertikalen und internationalen Zusammenarbeit stellt die Regierungen vor grosse Herausforderungen. Die Kooperation in der Form des Austausches sensibler Informationen bedingt ein ausgeprägtes gegenseitiges Vertrauen. Solches Vertrauen ist äusserst schwierig aufzubauen.[50] Das grundlegende Problem besteht darin, dass Vertrauen nur durch Zusammenarbeit entstehen kann, während eine solche Zusammenarbeit wiederum selbst von Vertrauen abhängt. Die Errichtung öffentlich-privater Informationsaustausch-Arrangements ist daher ein Huhn-Ei-Paradox – oder anders ausgedrückt, ein klassisches Kooperationsproblem.[51] Der Informationsaustausch zwischen öffentlichen und privaten Partnern funktioniert deshalb meist nur in einem kleinen Rahmen mit ausgewählten Partnern, zwischen denen bereits ein Vertrauensverhältnis besteht oder ein solches relativ einfach aufgebaut werden kann.

3 EIN ERWEITERTES GOVERNANCE-MODELL FÜR CIP

Obwohl einige der Partnerschaften zum Zweck des Informationsaustausches recht gut zu funktionieren scheinen, sind dem Modell PPP im Bereich CIP enge Grenzen gesetzt. Deshalb stellt sich die Frage nach alternativen Lösungsansätzen. Gesucht wird konkret ein Ansatz, der die Zusammenarbeit zwischen Staat und Privatwirtschaft nicht auf die direkte Partnerschaft (wie im Falle von PPP) reduziert, sondern auch andere Formen der Interaktion be-

50 Frye, Emilie. Information-Sharing Hangups: Is Antitrust Just a Cover? In: *The CIP Report* 1 (2003), Nr. 3, S. 6f.; Prieto, *Information Sharing with the Private Sector*.

51 Vgl. Aviram, Amitai. Network Responses to Network Threats: The Evolution into Private Cyber-Security Associations. In: Grady, Mark F./Parisi, Francesco (Hrsg.). *The Law and Economics of Cybersecurity*. Cambridge: Cambridge University Press, 2006, S. 143–192; Aviram, Amitai/Tor, Avishalom. Overcoming Impediments to Information Sharing. In: *Alabama Law Review* 55 (2004), Nr. 2, S. 231–279.

rücksichtigt. Zur Entwicklung eines solchen Ansatzes greifen wir auf *Governance*-Theorien zurück. Der theoretische Überbau der *Governance*-Theorien besteht in der Abgrenzung zum traditionellen *Government*, wobei die Regierung neu nicht mehr als einziger Akteur im öffentlichen Bereich verstanden wird.[52] *Governance* findet immer dort statt, wo die politische Macht stark fragmentiert ist. Eine Fragmentierung der politischen Macht kann einerseits über eine Dezentralisierung entstehen, wenn die Aufgaben und Kompetenzen der Regierung nach unten (Lokalisierung), nach oben (Supranationalisierung) oder auch seitwärts (Privatisierung) delegiert werden.[53] Andererseits findet sie auch innerhalb der Regierung selbst statt, über die immer stärkere funktionale Differenzierung der Verwaltung.[54]

Innerhalb der *Governance*-Theorie wird vor allem zwischen neoliberalen *Governance*-Theorien und dem Netzwerk-*Governance*-Ansatz unterschieden.[55] Das zentrale Postulat des neoliberalen Ansatzes heisst «weniger *Government* und mehr *Governance*».[56] Das Hauptziel ist die Effizienzerhöhung öffentlicher Verwaltungen, indem die Bürokratie Kompetenzen auf die Privatwirtschaft überträgt. Die im ersten Kapitel beschriebenen Debatten um die Privatisierung, die PPP und auch die Idee des *New Public Management* gehören diesem Ansatz an.[57] Bei CIP geht es jedoch nicht um die Steigerung von Effizienz, sondern um die Erhöhung der Sicherheit. Deshalb ist der neo-

52 Jessop, Bob. The Changing Governance of Welfare: Recent Trends in Primary Functions, Scale and Modes of Coordination. In: *Social Policy and Administration* 33 (1999), Nr. 4, S. 348–359; Krahmann, Elke. Conzeptualizing Security Governance. In: *Cooperation and Conflict* 38 (2003), Nr. 1, S. 6–26; Czempiel, Ernst-Otto/Rosenau, James N. *Governance Without Governement: Order and Change in World Politics*. Cambridge: Cambridge University Press, 1992; Rhodes, Roderick A. W. The New Governance: Governing Without Government. In: *Political Studies* 44 (1996), Nr. 4, S. 652–667.

53 Krahmann, *Conzeptualizing Security Governance*, S. 12.

54 Bevir, Mark/Rhodes, Roderick A. W. *A Decentered Theory of Governance: Rational Choice, Institutionalism, and Interpretation*. Working Papers of the Institute of Governmental Studies, Nr. 10. Berkeley: 2001.

55 Ebd., S. 3–8.

56 Osborne, David/Gaebler, Ted. *Reinventing Government: How the Entrepreneurial Spirit Is Transforming the Public Sector*. Reading, MA: Addison-Wesley, 2001, S. 34.

57 *New Public Management* bildet einen eigenen heterogenen Theoriezweig innerhalb der *Governance*-Ansätze. Ursprünglich wurden auch diese Ideen im anglo-amerikanischen Raum entwickelt, fanden danach aber bald den Weg nach Europa und um die Welt. Die Anfänge der «Wirkungsorientierten Verwaltungsführung», wie NPM in der Schweiz heisst, reichen hierzulande ungefähr ins Jahr 1994 zurück. Die spezifischen Ausprägungen der schweizerischen Diskussion sind hier jedoch nicht von Belang.

liberale Ansatz nur beschränkt als theoretisches Fundament einer CIP-Politik geeignet. Nachfolgend soll versucht werden, mit Hilfe des Ansatzes der Netzwerk-*Governance*, den wir im folgenden Unterkapitel mit dem neoliberalen Ansatz kontrastieren, ein alternatives Modell zu entwickeln. Mit Hilfe des Netzwerk-Ansatzes, der von einem anderen Verständnis der öffentlich-privaten Zusammenarbeit ausgeht, wird in einem zweiten Unterkapitel die neue Rolle der Regierung beschrieben. Im dritten Unterkapitel werden die theoretischen Überlegungen auf CIP angewandt, und es wird gezeigt, wie einige der im vorherigen Kapitel aufgezeigten Probleme dadurch gelöst werden können.

3.1 DER NETZWERK-ANSATZ DER GOVERNANCE-THEORIE

Der wichtigste Unterschied des Netzwerk-Ansatzes zum neoliberalen Verständnis der *Governance*-Theorie besteht darin, dass die Einführung von *Governance*-Strukturen nicht länger als Mittel zur Effizienzsteigerung der öffentlichen Verwaltung betrachtet wird, sondern als Folge der fortschreitenden Spezialisierung in modernen Gesellschaften.[58] Immer häufiger braucht es zur Erfüllung von Aufgaben sehr spezifisches Expertenwissen. Die zunehmende Arbeitsteilung führt zu einer Verwischung der Grenzen zwischen dem öffentlichen und dem privaten Sektor. Viele Aufgaben, welche früher durch den Staat wahrgenommen wurden, werden heute durch spezialisierte Unternehmen erfüllt. Diese Differenzierung der öffentlichen Verwaltung kann dann problematisch werden, wenn es um Angelegenheiten geht, die für das Funktionieren der Gesellschaft essentiell sind. Es stellt sich die Frage, wie der Staat die Erfüllung solcher Aufgaben garantieren kann, wenn er selbst nicht mehr über die notwendigen Mittel und Kompetenzen dazu verfügt.

Bei den neoliberalen Ansätzen wird dieses Problem der Kontrolle dadurch gelöst, dass der Staat die Aufgaben, welche er an Unternehmen delegiert,

58 Kooiman, Jan. Findings, Speculations and Recommendations. In: Kooiman, Jan (Hrsg.). *Modern Governance. New Government-Society Interactions.* London: Sage, 1993, S. 249–262; Stoker, Gerry. Theory and Urban Politics. In: *International Political Science Review* 19 (1998), Nr. 2, S. 119–129; Stoker, Gerry. Governance as Theory: Five Propositions. In: *International Social Science Journal* 50 (1998), Nr. 1, S. 17–28; Bevir/Rhodes, *A Decentred Theory of Governance*, S. 18f.

genau definiert und vertraglich festhält, wie sie zu erfüllen sind. So behält er die Kontrolle und kann korrigierend eingreifen, wenn die Privatwirtschaft die notwendigen Leistungen nicht erbringt. Wenn von einer zunehmenden Spezialisierung ausgegangen wird, kann dies aber nicht mehr gelingen. Der Regierung fehlt schlicht das nötige Expertenwissen, um eine angemessene Kontrolle der ausgelagerten Funktionen und Tätigkeiten sicherzustellen. Gerade am Beispiel CIP manifestiert sich dieser Umstand deutlich: Für die Regierungen ist es kaum möglich, die Qualität von Schutzbestimmungen zu beurteilen, weil ihnen das technische Wissen dazu fehlt. Das schöne Bild der Regierung als Steuermann auf dem Schiff ist überholt; moderne Gesellschaften sind eher mit hochkomplexen Maschinen zu vergleichen, deren Steuerung viel Detailwissen voraussetzt.

Der Netzwerk-Ansatz der *Governance*-Theorie geht deshalb davon aus, dass es in modernen Gesellschaften neue Formen der öffentlichen Verwaltung braucht.[59] Weil die hierarchische Kontrolle durch die Regierung nicht mehr möglich ist, muss die Zusammenarbeit zwischen öffentlichen und privaten Akteuren auf eine neue Basis gestellt werden. Die Regierung kann nicht mehr einfach Anweisungen erteilen und deren Einhaltung kontrollieren, sondern muss die Rahmenbedingungen so gestalten, dass die Zusammenarbeit auch ohne Kontrolle funktioniert. Öffentliche Verwaltung wird so zum Teamsport, in dem Überzeugungsarbeit, Verhandlungen und gegenseitiges Vertrauen wichtiger sind als Kontrolle und Regulation.[60]

Um eine solche neue Art der Zusammenarbeit zu ermöglichen, braucht es kleine, relativ homogene Netzwerke, in denen sich alle Akteure beteiligen, die in ihrem eigenen Interesse einen Beitrag zur Erfüllung einer öffentlichen Aufgabe leisten wollen und können. Diese Akteure, die meist sowohl aus dem öffentlichen als auch aus dem privaten Sektor stammen, sollen sich selbständig untereinander organisieren. Sie selbst setzen die Regeln für das gemeinsame Handeln fest und bestimmen die Verantwortlichkeiten und Verpflich-

59 Peters, Guy B./Pierre John. Governance Without Government? Rethinking Public Administration. In: *Journal of Public Administration Research and Theory* 18 (1998), Nr. 2, S. 223–243.

60 Salamon Lester M. The Tools Approach and the New Governance: Conclusion and Implications. In: Salamon Lester M. (Hrsg.). *The Tools of Government: A Guide to the New Governance*. Oxford: Oxford University Press, 2002, S. 600–610.

tungen der einzelnen Partner.[61] Die verschiedenen Netzwerke kontrollieren sich auch selbst, weil nur innerhalb eines Netzwerks genügend Wissen vorhanden ist, um zu überprüfen, ob alle ihren Verpflichtungen nachkommen. Die Selbstkontrolle in diesen Netzwerken ist möglich, weil sich die Akteure auf der Basis einer gemeinsamen Absicht zusammenschliessen. Akteure, die nicht dieselben Grundinteressen haben, werden nicht Teil des Netzwerks.

Die öffentlichen Aufgaben werden also durch zahlreiche unabhängige, sich selbst regulierende und organisierende Netzwerke wahrgenommen. Auch die Regierungen sind typischerweise in diesen Netzwerken durch die jeweils zuständigen Behörden vertreten. Dabei ist es wichtig, dass diese Behörden innerhalb des Netzwerks keine Sonderstellung innehaben. Sie vertreten zwar die Interessen der Regierung, üben aber sozusagen als *primi inter pares* keine Autorität aus, weil das Netzwerk nur dann funktionieren kann, wenn die Entscheidungen in gleichberechtigten Verhandlungen getroffen werden. Die Unabhängigkeit der Netzwerke von der Regierung ist das entscheidende Element des *Governance*-Konzepts. In der Literatur wird deshalb auch oft auf die Idee der «*Governance* ohne *Government*» verwiesen.[62]

3.2 DIE NEUE ROLLE DER REGIERUNG: META-GOVERNANCE

Die Rolle der Regierung ist ein entscheidendes Unterscheidungsmerkmal zwischen den verschiedenen *Governance*-Theorien. Während sie in der traditionellen Verwaltung alle öffentlichen Aufgaben selbst ausführt, sollte sie gemäss dem neoliberalen Ansatz zwar Aufgaben an die Privatwirtschaft auslagern, die Kontrolle aber stets behalten. Im Netzwerk-Ansatz nehmen die Regierungen nun eine neue Rolle ein. Statt die Aufträge zu erteilen und deren Erfüllung zu kontrollieren, übernehmen die Regierungen die Funktion des Koordinators und Stimulators von Netzwerken. Die Regierungen müssen sicherstellen, dass die öffentlichen Aufgaben durch sich selber regulierende

61 Rhodes, *The New Governance*, S. 658f.

62 Siehe u.a.: Czempiel/Rosenau, *Governance Without Government*; Rhodes, *The New Governance*; Peters/Pierre, *Governance Without Government*.

Netzwerke wahrgenommen werden. Diese indirekte Steuerung wird als «Organisation der Selbstorganisation» oder als «Meta-*Governance*» bezeichnet.[63]

Zu dieser Meta-*Governance* gehört zunächst die Schaffung von Rahmenbedingungen, die es den Netzwerken ermöglichen, sich selbst zu organisieren. Scharpf und Mayntz weisen darauf hin, dass Selbstregulation nur im «Schatten der Hierarchie» funktionieren kann, weil sich auch die internen Regeln und Abmachungen zwischen den Akteuren eines Netzwerks schlussendlich auf die zentralstaatlichen Institutionen und Gesetze beziehen.[64] Neben der Schaffung der Rahmenbedingungen bedeutet Meta-*Governance* aber vor allem Koordination und Promotion. Die Regierungen müssen – wo nötig – neue Netzwerke aktivieren und die bestehenden orchestrieren und modulieren.[65] Konkret bedeutet dies, dass die Regierungen die öffentlichen Aufgaben zunächst definieren und dann überprüfen, ob sie bereits in ausreichendem Masse wahrgenommen werden. Wird eine Aufgabe nicht ausreichend wahrgenommen, müssen die Regierungen neue Netzwerke schaffen oder bestehende Netzwerke dazu bewegen, die Aufgabe zu übernehmen.

Die Wahl der richtigen Instrumente zur Förderung der spezialisierten Netzwerke ist die entscheidende Aufgabe der Regierungen. Die direkte Partnerschaft zwischen öffentlichen und privaten Akteuren ist ein mögliches Instrument. Dabei versuchen die Behörden durch ihr Engagement innerhalb des Netzwerks dazu beizutragen, dass öffentliche Aufgaben erfüllt werden. Daneben stehen den Regierungen zahlreiche andere Instrumente zur Verfügung. Die Palette reicht von regulativen Massnahmen (beispielsweise die Verpflichtung von Firmen zur Mitgliedschaft in Zweckverbänden) über das Setzen von Anreizen bis hin zur simplen Unterstützung von Netzwerken durch Pro-

63 Siehe u.a.: Jessop, Bob. The Rise of Governance and the Risk of Failure: The Case of Economic Development. In: *International Social Science Journal* 50 (1998), Nr. 155, S. 29–46; Sorensen, Eva. MetaGovernance: The Changing Role of Politicians in Processes of Democratic Governance. In: *The American Review of Public Administration* 36 (2006), Nr. 98, S. 98–114.

64 Scharpf, Fritz. Die Handlungsfähigkeit des Staates am Ende des zwanzigsten Jahrhunderts. In: *Politische Vierteljahresschrift* 32 (1991), Nr. 4, S. 621–634; Mayntz, Renate/Scharpf, Fritz. Steuerung und Selbstorganisation in staatsnahen Sektoren. In: Mayntz Renate/Scharpf Fritz (Hrsg.). *Gesellschaftliche Selbstregulierung und politische Steuerung*. Frankfurt/New York: Campus, 1995, S. 9–38.

65 Salamon, Lester M. The New Governance and the Tools of Public Action: An Introduction. In: Salamon, Lester M. (Hrsg.). *The Tools of Government: A Guide to the New Governance*. Oxford: Oxford University Press, 2002, S. 1–47.

motion oder Beratung. Weitere mögliche Instrumente sind soziale und ökonomische Regulationen, die Definitionen der Haftbarkeit, das Abschliessen von Verträgen zwischen öffentlichen und privaten Partnern, Subventionen, Kreditvergaben, Defizitgarantien, die Vergabe von Lizenzen und Konzessionen, die Einrichtung staatlicher Versicherungen, Steuererleichterungen oder auch Bussen.[66] Die Wahl des geeigneten Instrumentes ist deshalb entscheidend, weil die Art der Förderung der Netzwerke durch die Regierung auch die interne Struktur des Netzwerks verändern kann. Obwohl es oft nötig ist, die Netzwerke von aussen zur Erfüllung einer Aufgabe zu motivieren, dürfen dabei die Selbstregulierungs-Mechanismen des Netzwerks nicht untergraben werden, denn sonst fiele die Kontrollfunktion an die Regierung zurück.

3.3 NETZWERK-GOVERNANCE IM FALLE VON CIP

Nachfolgend zeigen wir, wie die meisten in Kapitel 2.3 identifizierten Schwierigkeiten mit Hilfe des Netzwerk-Ansatzes gelöst oder zumindest abgeschwächt werden können. Wenn sorgfältiger zwischen den verschiedenen Optionen der öffentlich-privaten Zusammenarbeit unterschieden und die jeweils am besten geeignete ausgewählt und angewendet wird, kann dies zur besseren Bewältigung der Herausforderungen im Bereich CIP beitragen.

Problem 1: Der Staat hat keine Möglichkeit zu kontrollieren, ob die privaten Unternehmen ihre Aufgabe im Bereich CIP wahrnehmen.

Der Verlust der Kontrollfunktion der Regierung ist ein zentrales Argument für einen Netzwerk-Ansatz in der CIP-Politik. Bei einem Informationsaustausch ist es schwierig zu beurteilen, ob die Unternehmen die relevanten Informationen auch tatsächlich weitergeben. Die Lösung des Problems besteht in der Selbstregulation und Selbstkontrolle der Netzwerke. Die Partner in Netzwerken kennen sich gegenseitig gut und können deshalb am ehesten einschätzen, ob ausreichend kooperiert wird. Während Unternehmen beispielsweise gegenüber der Regierung ihre Schwachstellen und Verletzbarkei-

66 Salamon, *Introduction*, S. 21; Sorensen, *MetaGovernance*, S. 100–103.

ten leicht beschönigen können, fällt ihnen dies gegenüber anderen Fachleuten schwerer. Die Lösung für das erste Problem besteht also darin, Teilaufgaben im Bereich CIP der Kontrolle von gut strukturierten, sich selbst organisierenden Netzwerken zu überlassen. So wurde beispielsweise in den USA die Aufgabe der Minderung der Verletzlichkeiten der Informationssysteme der Finanzindustrie weitgehend den bereits vorhandenen Netzwerken in diesem Sektor überlassen.[67]

Problem 2: Die öffentlich-private Zusammenarbeit erweist sich auf Grund der divergierenden Interessen oft als schwierig.

Das Problem der divergierenden Interessen entsteht, wenn Partner zu einer Kooperation gezwungen werden. Netzwerke können nur auf der Basis eines ausreichend grossen gemeinsamen Nenners erfolgreich sein. Eine direkte Partnerschaft zwischen Unternehmen und Behörden aus dem Bereich der Sicherheitspolitik ist schwierig, weil die Partner völlig unterschiedliche Hintergründe haben. Eine solche Partnerschaft ist nur dann von Nutzen, wenn die Regierung einen wesentlichen Beitrag zur Funktionalität des Netzwerks leisten kann. Dies kann im Bereich der CIP durchaus der Fall sein, beispielsweise wenn die Regierungen den Unternehmen helfen können, die Bedrohungslage besser einzuschätzen.[68] Weil den Sicherheitsbehörden jedoch oft das Verständnis für die spezifischen Bedürfnisse der Privatwirtschaft fehlt, kann es notwendig sein, neue Netzwerke für die Zusammenarbeit zu schaffen. Häufig sind diese Netzwerke an Schnittstellen das, was als PPP im Bereich CIP bezeichnet wird. Sie können dann funktionieren, wenn die involvierten Akteure auf die gemeinsamen Interessen fokussieren und sich gegenseitig vertrauen. In der Schweiz gibt es mit der Melde- und Analysestelle Informationssicherung (MELANI) ein Beispiel für eine funktionierende Partnerschaft

67 The Financial Service Information Sharing and Analysis Center (FS-ISAC). *Financial Service Information Sharing and Analysis Center: Making the Financial Services Sector Stronger and Safer*. Oktober 2007. http://www.fsisac.com/files/FS-ISAC_Overview_2007_04_10.pdf.

68 Suter, *A Generic National Framework for Critical Information Infrastructure Protection*.

an der Schnittstelle zwischen den Netzwerken der Sicherheitspolitik und der Privatwirtschaft.[69]

Problem 3: PPP sind nur mit ausgewählten Firmen möglich. Sie müssen klein sein, da sie auf gegenseitigem Vertrauen basieren, und es können nicht beliebig viele PPP geschaffen werden, weil dies die Ressourcen der Regierung übersteigen würde.

Das Problem der begrenzten Anzahl möglicher Partner in PPP besteht nur dann, wenn davon ausgegangen wird, dass die Regierung zwingend direkt mit der Privatwirtschaft zusammenarbeiten muss. Dabei wird die Möglichkeit von sich selbst regulierenden Netzwerken ausser Acht gelassen. Die Unternehmen haben selbst ein Interesse an Sicherheit und engagieren sich teilweise bereits in Teilbereichen von CIP. Die Regierung kann sich darum häufig darauf beschränken, bestehende Netzwerke mit ähnlichen Aufgaben zu fördern oder die Entstehung von neuen Netzwerken im Bereich CIP mit Promotionsmassnahmen zu unterstützen.[70] Ein solches Vorgehen hat beispielsweise die britische Regierung im Bereich der Informationssicherheit gewählt, indem sie den Informationsaustausch zwischen KMU in so genannten *Warning Advice and Reporting Points* (WARPs) fördert, ohne sich selbst direkt daran zu beteiligen.[71]

Problem 4: Wegen der intensiven Einbindung der Regierung sind PPP nicht geeignet, um die internationale Zusammenarbeit zu fördern.

Die internationale Zusammenarbeit wird durch ein direktes Engagement von Regierungen oft eher erschwert. Die Grossunternehmen, welche kritische Infrastrukturen betreiben, sind international in der Regel bereits gut vernetzt. Unter diesen Spezialisten kann sich deshalb eine Zusammenarbeit relativ leicht ergeben. Die Unabhängigkeit von Regierungen ist dabei oft eine

69 Melde und Analysestelle Informationssicherung (MELANI). *Über MELANI*. Juni 2008. http://www.melani.admin.ch/org/index.html?lang=de.

70 Aviram, *Network Responses to Network Threats*, S. 185.

71 Warning Advice and Reporting Point (WARP). *WARPs Introduction*. März 2007. http://www.warp.gov.uk/Index/indexintroduction.htm.

Voraussetzung für eine erfolgreiche Zusammenarbeit. Ein Beispiel für ein internationales Netzwerk, das sich unabhängig von den Regierungen herausgebildet hat, ist das *Forum of Incident Response and Security Teams* (FIRST), in welchem sich Fachleute gegenseitig austauschen.[72]

Problem 5: Es existiert eine Dissonanz zwischen der Sicherheitslogik und der PPP-Logik. Die Kernaufgabe des Staates kann nicht ausgelagert werden.

Dieses Problem lässt sich mit einem Netzwerk-Ansatz *nicht* lösen. Die Auslagerung von essentiellen Aufgaben im Bereich CIP an sich selbst regulierende, nicht durch den Staat zu kontrollierende Netzwerke ist aus sicherheitspolitischer Sicht sogar problematisch. Im Vergleich zum Konzept der PPP, bei welchen der Staat die Kompetenzen zwar auch privaten Akteuren überlässt, gleichzeitig aber die Kontrolle über die Erfüllung der Aufgaben behält, akzentuiert sich das Problem der Verantwortung in einer Netzwerk-*Governance*, weil der Staat sich auf die Koordination von Netzwerken beschränkt. Dieses Problem der unklaren Zuordnung der Verantwortlichkeiten wird in der allgemeinen *Governance*-Literatur breit diskutiert.[73] Diese Dissonanz zwischen der Logik der Sicherheitspolitik und der Logik der öffentlich-privaten Zusammenarbeit bedarf einer offenen Debatte über die Möglichkeiten und Grenzen staatlicher Kontrolle im Bereich CIP.

4 CIP IN DER SCHWEIZ AUS DER NETZWERK-GOVERNANCE-PERSPEKTIVE

Was bedeuten die in den vorangegangen Kapiteln gewonnenen Erkenntnisse für die Schweiz? Im Vergleich zu anderen Ländern hat die Schweiz geringere Probleme mit bereits bestehenden PPP. Auch die Ausgangslage für Netzwerk-

72 Forum of Incident Response and Security Teams (FIRST). *About FIRST*. Juni 2008. http://www.first.org/about/.

73 Vertreter des Netzwerk-Ansatzes argumentieren, dass die Regierung für die Koordination und Stimulation der Netzwerke, nicht aber für die direkte Erfüllung öffentlicher Aufgaben verantwortlich ist. Viele Autoren weisen aber darauf hin, dass die Erwartungen an den Staat in der Realität oft höher sind. Zur Debatte um die Zuteilung von Verantwortlichkeiten in der Netzwerk-*Governance* siehe: Posner, Paul L. Accountability Challenges of Third-Party Government. In: Salamon, *The Tools of Government,* S. 523–551.

Governance ist besser: Dank des stark verbreiteten Milizgedankens und des Föderalismus besteht in der Schweiz eine lange Tradition der vielfältigen Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor. Im Bereich CIP stellen die bereits funktionierenden, kleinen und homogenen Netzwerke eine günstige Ausgangslage dar, die wir in einem ersten Unterkapitel beschreiben. Weitere Anstrengungen sollten sich auf Meta-*Governance* konzentrieren, wie im zweiten Unterkapitel dargelegt wird. Die Bestrebungen zur besseren Koordination dieser Netzwerke können mit Hilfe des Netzwerk-Ansatzes klarer und zielgerichteter gestaltet werden. Um die Bemühungen der Bundesverwaltung zur Erarbeitung einer schweizerischen CIP-Strategie zu unterstützen, entwerfen wir im dritten Kapitel eine *Roadmap*, in welcher ein schrittweises Vorgehen hin zu einer CIP-Meta-*Governance* in der Schweiz skizziert wird.

4.1 BESTEHENDE NETZWERKE: DER EFFEKT DES FÖDERALISMUS UND DES MILIZSYSTEMS

Auch in der Schweiz ist die Debatte über den Schutz kritischer Infrastrukturen eng verknüpft mit der zunehmenden Abhängigkeit der Wirtschaft von Informations- und Kommunikationstechnologien. Obwohl der (physische) Objektschutz eine lange Tradition hat, kann die Strategische Führungsübung 1997 (SFU 97) als Startschuss für die schweizerische CIP-Politik gelten. Im damals durchgespielten Übungsszenario wurde die schweizerische Informationsinfrastruktur verschiedenen elektronischen Attacken ausgesetzt. Als Folge davon wurde dem Bundesrat als dringliche Massnahme vorgeschlagen, einen Sonderstab Informationssicherheit für die Krisenbewältigung auf Stufe Bund zu schaffen. Im Juni 2001 wurde die Nachfolgeübung INFORMO durchgeführt, die sich mit der Thematik von durch Störungen in der Informationsinfrastruktur ausgelösten Krisen beschäftigte. Dabei wurde auch die Funktionsweise des neu geschaffenen Sonderstabs *Information Assurance* (Sonderstab Informationssicherung, SONIA) getestet, der sich aus Vertretern der Bundesverwaltung und der Wirtschaft zusammengesetzt ist.

Der im August 1998 veröffentlichte «Bericht Brunner»[74] thematisierte ebenfalls Störungen im Informatikbereich. Die Kommission Brunner sah diese Problematik als gemeinsame Aufgabe von Behörden und Privatwirtschaft und empfahl die Errichtung eines nationalen Alarmsystems und eine Initiative zur Förderung der Forschung und der Zusammenarbeit im Kampf gegen die absichtliche Störung von Informatiknetzen.[75] Die wenige Jahre später gegründete *Melde- und Analysestelle Informationssicherung* (MELANI), eine gut funktionierende PPP, nimmt sich inzwischen eines Grossteils der damals angesprochenen Herausforderungen an.

Alle diese Organisationen, die sich mit dem Schutz kritischer (Informations-)Infrastrukturen befassen, funktionieren als Netzwerke. Sie umfassen spezialisierte Akteure aus der Privatwirtschaft und aus dem öffentlichen Sektor, die sich im gemeinsamen Interesse eines Teilbereichs des CIP annehmen. Wie bereits angetönt, ist in der Schweiz die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor relativ gut entwickelt. Im Gegensatz zu starken Zentralstaaten ist hier die politische Macht aufgrund des Föderalismus schon seit jeher stark fragmentiert. Die Zusammenarbeit in Netzwerken hat im Föderalismus daher eine lange Tradition und ist nicht erst mit der zunehmenden Spezialisierung der modernen Gesellschaften nötig geworden. Ein zweiter Faktor, der die Entstehung funktionierender Netzwerke begünstigt, ist das Milizsystem. Viele öffentliche Aufgaben werden in der Schweiz nebenamtlich durch private Akteure wahrgenommen. Die Trennung zwischen dem öffentlichen und dem privaten Sektor ist deshalb weniger stark ausgeprägt als anderswo.[76] Die Zusammenarbeit ist in vielen Bereichen selbstverständlich und die Regierung muss zur Umsetzung eines *Governance*-Ansatzes zum Schutz kritischer Infrastrukturen ihre Rolle nicht komplett neu definieren, sondern sie kann auf bestehende Strukturen zurückgreifen.

In den letzten Jahren hat jedoch eine gewisse Verschiebung in der Art und Weise stattgefunden, wie CIP hierzulande verstanden wird. Dadurch wurde

74 Bericht der Studienkommission für strategische Fragen (Kommission Brunner). Bern, 26. Februar 1998.

75 **Wigert, Isabelle. Der Schutz kritischer Informationsinfrastrukturen in der Schweiz: Eine Analyse** von Akteuren und Herausforderungen. In: *Bulletin 2005 zur schweizerischen Sicherheitspolitik*. Zürich: Forschungsstelle für Sicherheitspolitik, 2005, S. 97–121.

76 Siehe Suter/Brunner, *CIIP Handbook 2008*.

die Ausgangslage komplizierter. Wie auch in anderen Staaten lag der Fokus der ersten schweizerischen CIP-Aktivitäten fast ausschliesslich im Bereich der Informationsinfrastrukturen und der Informationssicherheit. Dieser Fokus erschien einigen Vertretern der Bundesverwaltung zu Recht als zu limitiert. 2004 wurde auf Lücken hinsichtlich eines gemeinsamen Grundverständnisses und der Definition von Schutzzielen und auf den sich daraus ergebenden Handlungsbedarf im Bereich CIP hingewiesen. Daraufhin beauftragte der Bundesrat im Jahr 2005 das Bundesamt für Bevölkerungsschutz (BABS) damit, die Koordination der Arbeiten zum Thema «Schutz Kritischer Infrastrukturen» zu übernehmen und zusammen mit den beteiligten Departementen den Handlungsbedarf im Bereich CIP zu konkretisieren und adäquate Massnahmen auszuarbeiten.[77]

4.2 ERSTE SCHRITTE ZU EINER META-GOVERNANCE

Durch die Ausweitung des CIP-Verständnisses rückten neu weitere, heterogene und nicht koordinierte Netzwerke aus dem CIP-Bereich ins Blickfeld. In der Schweiz beschäftigen sich auf Bundesebene eine Vielzahl von Verwaltungsstellen mit CIP, so dass nicht immer auf den ersten Blick ersichtlich ist, welcher Akteur sich mit welchen Aspekten beschäftigt. Die Verantwortlichkeiten überschneiden sich teilweise, wodurch Unklarheiten über die jeweiligen Zuständigkeiten entstehen. Die angedachte Koordination der bestehenden Aktivitäten wird somit zu Recht als eine der Hauptherausforderungen auf dem Weg zu einer nationalen Strategie angesehen.

Um das gemeinsame Verständnis für CIP innerhalb der Bundesverwaltung zu fördern und die angestrebte nationale Strategie zum Schutz kritischer Infrastrukturen auszuarbeiten, wurde eine «Arbeitsgruppe Schutz Kritischer Infrastrukturen» (AG SKI) gebildet. In dieser sind 23 Bundesstellen vertreten.[78] In einem ersten Bericht an den Bundesrat vom 20. Juni 2007 wurden die gemeinsam erarbeiteten Begriffsdefinitionen und Schutzziele vorgestellt und die Aufgaben und Verantwortlichkeiten der beteiligten Ak-

77 Bundesamt für Bevölkerungsschutz. *Schutz von Kritischen Infrastrukturen verbessern*. 4.7.2007. http://www.news.admin.ch/message/index.html?lang=de&msg-id=13516.

78 BABS, *Erster Bericht an den Bundesrat zum Schutz kritischer Infrastrukturen*, S. 3.

teure skizziert.[79] Die anvisierte nationale Strategie, die bis 2012 vorliegen soll, will «den Dialog und die Zusammenarbeit zwischen diesen Stellen fördern, Synergien nutzen sowie den Austausch von Wissen und Erfahrungen institutionalisiert vorantreiben.» Solche Aussagen sind *grosso modo* mit den theoretischen Vorgaben der Netzwerk-Theorie kompatibel. Die bestehenden und angedachten Bemühungen zu einer besseren Koordination könnten jedoch mit Hilfe der theoretischen Überlegungen zur Meta-*Governance* noch zielorientierter gestaltet und dabei auch sinnvoll «verschlankt» werden. Der Ansatz hilft ebenfalls dabei, Klarheit darüber zu erlangen, wie und wann welche Art von Partner – z.B. die Kantone und die Privatwirtschaft – in den Prozess eingebunden werden sollen und worauf bei dieser Koordination vor allem zu achten ist. Im Folgenden soll ein Vorschlag zu einer strukturierten und prozessorientierten Vorgehensweise der Koordination in der schweizerischen CIP-Politik gemacht werden.

4.3 ROADMAP FÜR CIP-META-GOVERNANCE IN DER SCHWEIZ

Schritt 1: Die zentrale Grundidee der Meta-*Governance* ist, dass die Regierung verschiedene bereits bestehende Netzwerke so aufeinander abstimmt, dass eine Aufgabe möglichst vollständig in ihrem Sinne erfüllt wird. Dafür ist es zentral, dass die Regierung ihre Erwartungen und Absichten von Anfang an deutlich kommuniziert. Die Koordination der verschiedenen Netzwerke ist nur möglich, wenn klar ist, welches Ziel verfolgt wird. Der erste Schritt ist also eine klare Definition der Ziele und Prioritäten. Dies ist ein inhärent politischer Prozess und kann nur durch die Politik vorgenommen werden. Wenn die Ziele und Prioritäten feststehen, gilt es, sie den bestehenden Netzwerken zu kommunizieren. Gemäss Meta-*Governance* kann eine optimale Kommunikation von Seiten der Regierung in Bezug auf die Wichtigkeit einer Aufgabe und den damit einhergehenden Erwartungen substantiell dazu beitragen, dass bestehende Netzwerke sich (freiwillig) um diese Aufgabe kümmern. Denn indem sie das Problem eindeutig definiert und die Prioritäten festlegt, hilft sie, die Kohärenz der Aktivitäten der verschiedenen

79 BABS, *Erster Bericht an den Bundesrat zum Schutz kritischer Infrastrukturen*.

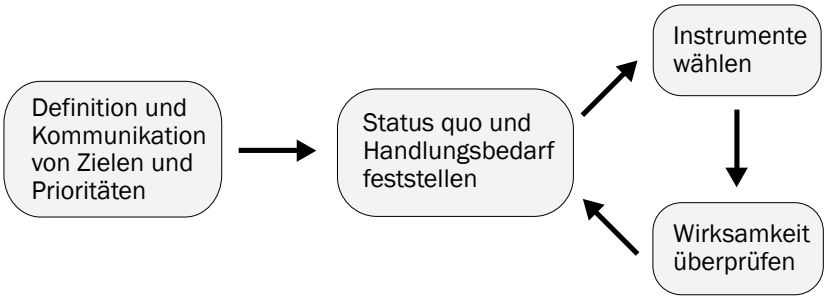
Netzwerke zu verbessern.[80] Je klarer dabei die Prioritäten und Erwartungen definiert sind, desto leichter werden die nächsten Schritte sein.

Schritt 2: Der zweite Schritt der Meta-*Governance* besteht in der Analyse des Status quo und in der Bestimmung des Handlungsbedarfs. Es gilt zu untersuchen, welche Netzwerke vorhanden sind, ob sie sich bereits bei der Erfüllung der in Schritt 1 definierten Aufgabe engagieren und wie sie allenfalls motiviert werden können, weitere Anstrengungen zu unternehmen. Daneben muss die Zusammenarbeit zwischen den verschiedenen Netzwerken überprüft und der Koordinationsbedarf eruiert werden.

Schritt 3: Wenn ein Handlungsbedarf festgestellt wird, müssen als dritter Schritt geeignete Instrumente der Meta-*Governance* identifiziert werden. Dies ist der schwierigste Schritt im Meta-*Governance*-Prozess. Er ist deswegen heikel, weil die immanente Gefahr besteht, durch die Wahl zu massiv eingreifender Instrumente den Selbstregulierungs-Mechanismus der Netzwerke zu untergraben. Je besser die Prioritäten zuvor festgelegt wurden und je genauer der Status quo beschrieben werden kann, desto geringer wird diese Gefahr. Im Idealfall ergibt sich die Wahl der Instrumente automatisch aus der Differenz zwischen den Zielen und dem Status quo. In der Realität wird aber auch die Wahl der Instrumente stets durch politische Prozesse beeinflusst.[81]

Schritt 4: Als vierter und letzter Schritt wird die Wirksamkeit der Massnahmen analysiert. Eine Behördenstelle prüft, ob die Netzwerke nach der Anwendung der gewählten *Governance*-Instrumente die Aufgabe nun so erfüllen, dass die definierten Ziele und Prioritäten erreicht werden. Dies führt automatisch wieder zurück zur Überprüfung des Status quo. Wie die Abbildung zeigt, ist die Meta-*Governance* deshalb als kontinuierlicher Prozess zu verstehen.

80 Sorensen, *MetaGovernance*, S. 101.
81 Peters, Guy P. The Politics of Tool Choice. In: Salamon, *The Tools of Government*, S. 552–564.



Darstellung 1: Der Prozess der Meta-Governance

Um diese vier Schritte praktisch zu veranschaulichen, möchten wir nachfolgend spezifischer auf den laufenden CIP-Strategiefindungsprozess in der Schweiz eingehen:

1) Ziele und Prioritäten formulieren und kommunizieren: Die Ziele und Prioritäten müssen in einen grösseren (sicherheits-)politischen, aber auch wirtschafts- und gesellschaftspolitischen Kontext eingepasst sein. Ein internationaler Vergleich zeigt: die Definition von «kritischen» Infrastrukturen und das Festlegen von Schutzzielen ist inhärent politisch, da es dabei immer um Priorisierung und Ressourcenverteilung geht. Die Definition sollte im politischen Prozess deshalb auch möglichst hoch angesiedelt werden. In der Schweiz wäre dies eine Aufgabe, die der Sicherheitsausschuss des Bundesrats oder die Lenkungsgruppe Sicherheit wahrnehmen sollte. Gegenwärtig werden aber sowohl die Bestimmung, welche Infrastrukturen überhaupt als «kritisch» zu betrachten sind, als auch die Schutzziele in einem *Bottom-up*-Prozess in der AG SKI erarbeitet. Die Prioritäten lassen sich aber nur schwer in Zusammenarbeit mit allen Akteuren festlegen, da alle Beteiligten versuchen werden, ihre partikulären Interessen durchzusetzen. Auch wenn dies inhaltlich gesehen sinnvolle Resultate ergeben kann, entsteht dadurch die Gefahr, dass spätestens im Schritt 3 aufgrund mangelnder Legitimität und politischer Verankerung Probleme auftauchen.

2) Analyse des Status quo: Bisher hat die AG SKI unter der Leitung des BABS die zentralen Begriffe definiert und die Ziele der Schweizer CIP-Politik aus-

gearbeitet. Auch die zentralen Akteure im Bereich der Bundesverwaltung wurden identifiziert. Dies sind wichtige erste Schritte auf dem Weg zu einer funktionierenden Meta-*Governance*. Die Analyse sollte darüber hinaus aber auch eine möglichst detaillierte Bewertung der bestehenden Aktivitäten enthalten, um den nächsten Schritt zu ermöglichen. Das für die Schweiz relevante *Mapping* der bestehenden Netzwerke muss auch die Aktivitäten der Kantone und natürlich der Privatwirtschaft enthalten. Klare, politisch abgestützte und anwendbare Definitionen und Konzepte – was gehört zu CIP, was gehört nicht zu CIP, was will man erreichen, wie sollen funktionierende Netzwerke aussehen, usw. – sind für eine solche Analyse unabdingbar.

3) Instrumente wählen: Die Auswahl der anzuwendenden Instrumente sollte erst nach Klärung von Schritt 1 und 2 und erst aufgrund der fertigen CIP-Strategie erfolgen. Es ist aber sinnvoll, bereits frühzeitig über mögliche Instrumente und ihre Auswirkungen nachzudenken. Dabei ist es wichtig, die gesamte Palette direkter und indirekter Instrumente in Betracht zu ziehen und nicht nur auf der zu limitierten PPP-Idee zu verharren. Ausserdem wird in der Schweiz zurzeit kaum über erweiterte Informationsaustauschprogramme nachgedacht. Die internationalen Entwicklungen zeigen jedoch, dass Partnerschaften im CIP-Bereich in fast allen Fällen auf einen Austausch von Informationen hinauslaufen. Dieser kann sehr unterschiedlich gestaltet werden, so dass eine Prüfung diverser Modelle sinnvoll wäre.

4) Wirksamkeit der Massnahmen überprüfen: Dieser letzte Schritt beinhaltet eine *Monitoring*-Aufgabe, die sinnvollerweise vom BABS als Koordinationsstelle wahrgenommen werden sollte. Die konkreten Ausprägungen dieses *Monitorings* sowie der Interaktionsformen mit den Netzwerken müssten noch genauer geprüft werden. Wichtig ist, dass die fundierte und möglichst genaue Analyse des Status quo auch hier eine zentrale Rolle spielt. Die involvierten Stellen in der Schweiz müssen sich aber bewusst sein, dass sie viele der Netzwerke nicht direkt steuern können und dass ihre Ziele nicht innert kurzer Frist erreicht werden können. Zum Prozessmanagement gehört auch, dass schrittweise vorgegangen wird und von den Partnerschaften nicht kurz nach ihrer Etablierung Wunderdinge erwartet werden.

5 SCHLUSSWORT

Beim Schutz kritischer Infrastrukturen, einem noch relativ neuen Problemkomplex der Sicherheitspolitik, erweist sich die Frage nach der adäquaten Rolle des Staates als ein zentrales Thema. Die zunehmende Globalisierung und die grenzüberschreitende Konzentration auf zahlreiche Märkte haben zur Folge, dass sicherheitspolitisch relevante kritische Infrastrukturen mitunter von grossen, multinationalen Akteuren betrieben werden, die sich dem Einfluss staatlicher Regulierungen und Kontrollen weitgehend entziehen können. Aufgrund der grenzüberschreitenden Art der Risiken aus dem Cyberspace, denen alle kritischen Infrastrukturen ausgesetzt sind, werden zudem auch KMU für eine umfassende Schutzstrategie immer wichtiger. Dass CIP deshalb nur durch die enge Zusammenarbeit von Staat und Wirtschaft überhaupt zu gewährleisten ist, ist längst Allgemeinwissen. Seit mehr als zehn Jahren wird deshalb versucht, eine solche Zusammenarbeit in Form von *Public-Private Partnerships* (PPP) zum Schutz kritischer Infrastrukturen zu errichten. Dabei müssen oft diametral entgegengesetzte Interessenlagen überwunden werden: Denn während der Staat eine umfassende nationale Schutzstrategie anstrebt, kümmert sich die Privatwirtschaft im Wesentlichen um die Eigensicherung in einem räumlich begrenzten Bereich. Eine Zusammenarbeit ist aber nicht nur schwierig, weil mehr Sicherheit die Überwindung von marktbedingten Hindernissen erfordert, sondern auch weil zwischen Privatwirtschaft und Staat viel Misstrauen herrscht und die Bereitschaft zur Kooperation stark von der Art und Weise abhängt, wie der Staat gegenüber dem Privatsektor auftritt.

In diesem Artikel wurden die Nutzen und die Grenzen von PPP für CIP aufgezeigt. Dazu haben wir das Konzept erstens kritisch durchleuchtet und zweitens auf eine solidere theoretische Basis gestellt. Es wurde darauf hingewiesen, dass das Modell der PPP ursprünglich in einem anderen Kontext entwickelt wurde und vor allem dem Zweck der Effizienzsteigerung diente. Fast alle Probleme, die sich bei der Anwendung von PPP für CIP ergeben, sind denn auch darauf zurückzuführen, dass PPP in erster Linie der Erhöhung der Sicherheit und nicht der Steigerung der Effizienz dienen. PPP sind aber nur eine von vielen möglichen Arten der Zusammenarbeit: Werden sie gemäss des *Governance*-Netzwerk-Ansatzes nur als Teil einer viel breiteren

Toolbox verstanden, lässt sich ein befreiender Schritt weg vom die Optionen einschränkenden PPP-Begriff hin zu einem neuen Verständnis der Rolle des Staates in diesem Bereich vollziehen.

Weil der Netzwerk-Ansatz der *Governance*-Theorie von sich selbst regulierenden Netzwerken ausgeht, besteht die Hauptaufgabe des Staates nicht mehr wie unter dem klassischen neoliberalen *Governance*-Verständnis in der Kontrolle der mit ihm zusammenarbeitenden Akteure. Im Zentrum stehen vielmehr die Koordination und die Stimulierung funktionaler Netzwerke, damit diese die vom Staat gewünschten Aufgaben optimal erfüllen. Das bedeutet aber nicht, dass der Staat obsolet wird, im Gegenteil: Der Staat bleibt nach wie vor der wichtigste Akteur der Politik. Nur der Staat kann Politik formulieren und gleichzeitig für deren demokratische Legitimität sorgen. Und niemand ausser dem Staat verfügt im Ernstfall über mehr Ressourcen und ist mit einer breiteren Palette von Reaktionsmöglichkeiten handlungsfähig. Auch als Anbieter des Kollektivguts Sicherheit bleibt der Staat unentbehrlich. Der Netzwerk-Ansatz definiert aber die Rolle des Staates neu: Öffentliche Verwaltung besteht nicht mehr aus dem Erteilen von Aufträgen und der Kontrolle der Ausführenden, sondern in der Schaffung von Rahmenbedingungen, die die Selbstorganisation von Netzwerken ermöglichen. Netzwerke werden nur dort aktiviert, wo die bereits bestehenden Netzwerke versagen bzw. die nötigen Aufgaben nicht erfüllen. Die Aushandlung der *Governance*-Instrumente ist so ein fortdauernder politischer Prozess, der stark von Gefahrenperzeptionen und anderen Faktoren abhängt. In gewissen Fällen werden auch Zwang und Regulierung nötig erscheinen. Je stärker die sicherheitspolitischen Aspekte in gewissen (Teil-)Sektoren betont werden, desto eher sind solche Eingriffe in den Markt zu erwarten, da den negativen Konsequenzen der Globalisierung mehr Beachtung geschenkt wird als den positiven Effekten.

Weil der in diesem Artikel dargestellte Netzwerk-*Governance*-Ansatz für eine neue Rolle des Staates plädiert, bietet er interessante Denkanstösse für die laufenden Arbeiten zur Entwicklung einer CIP-Strategie in der Schweiz. In der Schweiz bestehen dank des Föderalismus und des Milizsystems günstige Voraussetzungen für Netzwerke. Wenn die Regierung ihre Rolle als Koordinatorin der bestehenden Netzwerke verstärkt wahrnimmt, wird in der Schweiz ein erfolgreiches Modell zum Schutz kritischer Infrastrukturen

entstehen. Dafür ist jedoch ein gut strukturiertes Vorgehen im Sinne der Meta-*Governance* notwendig. Zuerst sollten die Ziele und Prioritäten klar definiert werden, dann der Status quo und der Handlungsbedarf analysiert und am Schluss die geeigneten *Governance*-Instrumente bestimmt werden. Die in diesem Artikel skizzierte *Roadmap* für eine CIP-Meta-*Governance* in der Schweiz ist ein konkreter, direkt aus dem Netzwerk-Ansatz abgeleiteter Vorschlag für die weiteren Arbeiten im Bereich CIP in der Schweiz.

Der Netzwerk-Ansatz vermag gewisse Probleme, die bei der Umsetzung von PPP aufgetreten sind, zu umgehen. Andere, wie z.B. Fragen der Verantwortlichkeit im Falle sicherheitspolitischer Aufgaben, bleiben bestehen oder werden sogar noch verstärkt. Und doch ist der Netzwerk-*Governance*-Ansatz in vielerlei Hinsicht «ehrlicher» als herkömmliche *Governance*-Ansätze (inkl. PPP): Anstatt zu suggerieren, dass staatliche Kontrolle sowie die Gewährleistung von Sicherheit jederzeit und absolut möglich sind, akzeptiert der Staat, dass er seine Rolle überdenken muss und dass er auch bei zentralen staatlichen Aufgaben auf die Hilfe nichtstaatlicher Akteure angewiesen ist. Ein solcher Wandel im Selbstverständnis des Staates scheint im Anbetracht der vielen Herausforderungen, die sich im Bereich CIP stellen, viel erfolgversprechender als das Verharren in alten und teilweise nicht mehr aufrechtzuerhaltenden Vorstellungen staatlicher Kontrollmöglichkeiten.