Critical Information Infrastructure Protection (CIIP): Eine sicherheitspolitische Herausforderung

von Andreas Wenger, Jan Metzger und Myriam Dunn

Einleitung

Die heute immer schneller fortschreitende „Informationsrevolution" wird dadurch charakterisiert, dass sowohl die Generierung, die Verwaltung als auch die Verwertung von Information in unserer Gesellschaft einen immer höheren Stellenwert einnehmen.[1] Was aber als grosse Chance der heutigen Zeit erkannt und genutzt wird, birgt auch neuartige, kaum erforschte Risiken in sich. Industrienationen stellen hochgradig vernetzte Systeme dar, welche in ihrer Leistungserbringung stark abhängig sind vom reibungslosen Funktionieren der eingesetzten Informations- und Telekommunikationstechnologien.[2] Durch diese Abhängigkeit moderner Gesellschaften von sogenannten „kritischen" Infrastrukturen im allgemeinen und „kritischen" Informationsinfrastrukturen im Speziellen wird die Informationsgesellschaft zur verletzlichen „Risikogesellschaft" oder gar zur „Weltrisikogesellschaft".[3]

Es stellt sich die Frage: Entwickeln wir uns langfristig hin zu robusten Gesellschaften, oder steigt mit zunehmender Vernetzung durch Informationsinfrastrukturen die Unberechenbarkeit negativer Kettenreaktionen, die grosse Teile einer Gesellschaft über längere Zeit lahm legen können?[4] Dabei gilt es zu beachten, dass sowohl die Risiken als auch die Komplexität ambivalenter Natur sind: Erstens sind Risiken verstanden als Herausforderungen seit jeher ein elementarer Bestandteil der kulturellen und gesellschaftlichen Weiterentwicklung; zweitens sind markt-

1 Vgl. z.B. ALBERTS, David S./PAPP Daniel S. (Hrsg.). *The Information Age: An Anthology of Its Impacts and Consequences.* Washington D.C.: NDU Press, 1997. URL http://www.ndu.edu/inss/books/anthology1/.

2 Vgl. THE SWEDISH COMMISSION ON VULNERABILITY AND SECURITY. *Vulnerability and Security in a New Era – A Summary. Stockholm*: Swedish Official Government Reports, 2001, S. 41–42.

3 Begriffe geprägt vom Soziologen Ulrich Beck. BECK, Ulrich. *Die Risikogesellschaft*. Frankfurt a.M.: Suhrkamp, 1986; ders. *Weltrisikogesellschaft, Weltöffentlichkeit und globale Subpolitik*. Wien: Picus, 1997.

4 LUIJF, Eric. *In Bits and Pieces. Vulnerability of the Netherlands ICT-Infrastructure and Consequences for the Information Society*. Issue Paper. März 2000. URL http://www.tno.nl/instit/fel/refs/pub2000/luiijf_bitbreuk_english.doc, S. 5–6. Übersetzung des holländischen Infodrome-Essays: „BITBREUK, de kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij".

wirtschaftlich-individualistische, demokratisch-dezentrale Gesellschaften besser in der Lage, mit auftretenden Krisen fertig zu werden als autoritär-zentrale.[5]

Der Schutz kritischer Infrastrukturen (*Critical Infrastructure Protection*, CIP) ist kein neues Konzept und beschäftigt Staaten bereits seit längerem.[6] Im Informationszeitalter präsentiert sich die Lage aufgrund von Vernetzung, Komplexität und Interdependenzen jedoch grundlegend anders als früher. Der Schutz kritischer Informations- und Kommunikationsinfrastrukturen (*Critical Information Infrastructure Protection*, CIIP) rückt in den Vordergrund. CIP als Überbegriff erstreckt sich auf die Sektoren Information und Kommunikation; Banken- und Finanzwesen; Elektrizität-, Gas- und Ölversorgung; Verkehr und Transport; Wasserversorgung; Notfalldienste sowie die Systeme der Regierung und Verwaltung.[7]

Kritische Informations- und Telekommunikationsinfrastrukturen sind aus zweierlei Gründen besonders bedeutsam: Erstens stellen sie als Wirtschaftsektor einen wichtigen Bestandteil der ökonomischen Wertschöpfung dar; zweitens sind sie das vernetzende Führungselement zwischen anderen Elementarbereichen. Sie sind die Grundvoraussetzung für das Funktionieren *aller* anderen Infrastrukturen. Aus diesem Grunde stehen die Informationsflüsse, welche in diesen Netzwerken transportiert werden, sowie die Dienstleistungen, welche dadurch ermöglicht werden, im Zentrum des gesamtgesellschaftlichen Schutzinteresses.[8]

Der 11. September 2001 hat den Schutz kritischer Infrastrukturen nicht nur in den USA weit oben auf die politische Agenda gesetzt. Der Einsatz von Verkehrsflugzeugen zur Zerstörung des World Trade Centers hat die Verletzlichkeit der Infrastruktur moderner Gesellschaften drastisch vor Augen geführt. Die Entwicklungen nach den Terrorakten in New York und in Washington machen zudem eines deutlich: Die Politik hat sich zurückgemeldet. Der Staat, von manchen bereits totgesagt, gewinnt wieder an Bedeutung und Einfluss.[9] In einem internationalen

---

5 HUTTER, Reinhard. Angriffe auf Informationstechnik und Infrastrukturen – Realität oder Science Fiction? In: *Aus Politik und Zeitgeschichte* 41–42 (2000), S. 36.

6 Vielmehr war der wirtschaftlich-gesellschaftliche Rückraum eines Gegners seit jeher ein lockendes militärisches Angriffsziel. Vgl. RATHMELL, Andrew. International CIP Policy: Problems and Prospects. In: *Information Security Technical Report* 4 (1999), Nr. 3, S. 31.

7 Vgl. Definition der Sektoren in der ersten zentralen amerikanischen Publikation zum Thema: PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION. *Critical Foundations. Protecting America's Infrastructures*. Washington D.C., 13. Oktober 1997, S. 3–4. URL http://www.ciao.gov/PCCIP/report_index.htm. Nachfolgend zitiert als PCCIP Report.

8 Vgl. hierzu vor allem das Fazit des Expertenworkshops „Critical Infrastructure Protection in Europe – Lessons Learned and Steps Ahead", vom 9.–10. November 2001 in Zürich. URL http://www.isn.ethz.ch/crn/issueareas/index.cfm?service=cybersecurity&menu=1.

9 Vgl. die Extrempositionen um sog. Modernisten wie Peter Drucker oder Alvin Toffler. Zum Beispiel DRUCKER, Peter F. *The New Realities: In Government and Politics, in Economics and Business, in Society and*

System, das geprägt ist durch transnationale Risiken, Vernetzung, Interdependenz und Verwundbarkeit, ist der Staat als Anbieter des Kollektivguts Sicherheit nach wie vor unentbehrlich. Sein Einsatz ist unerlässlich, wenn es beispielsweise darum geht zu bestimmen, welche Sicherheitsstandards eingehalten werden sollen; wann nationale Interessen über die Freiheiten des Einzelnen zu setzen sind; oder wer die Kräfte des Marktes reguliert, wenn die Selbstregulierung versagt.[10] Der Diskurs über den adäquaten Schutz von Informationsinfrastrukturen ist somit eng verknüpft mit dem Diskurs über die Rolle des Staates in einer durch die Informationsrevolution grundlegend veränderten Welt.

Als zentrale Frage kristallisiert sich damit heraus, welche Rolle der Staat beim Schutz kritischer Informationsinfrastrukturen wahrnehmen kann und muss. Bei ihrer Beantwortung stösst man jedoch auf ein Problem: Die akademische Auseinandersetzung mit den sicherheitspolitischen Aspekten der Thematik steht ganz am Anfang. In dieser sehr jungen Phase der internationalen CIIP-Forschung hat sich noch keine stabile wissenschaftliche und methodische Basis herausgebildet.[11] Folglich geht es vorerst darum, wichtige Themenkreise zu identifizieren, auf die sich die zukünftige Forschung konzentrieren soll.

Ziel dieses Artikels ist es denn auch nicht Resultate und Antworten zu liefern, sondern vielmehr einige elementare Fragen aufzuwerfen und einen Überblick über richtungsweisende Entwicklungen zu geben. Anhand des Beispiels USA soll aufgezeigt werden, welche Rolle dort der Staat heute im Bereich CIP/CIIP wahrnimmt und welche Herausforderungen für die Sicherheitspolitik im allgemeinen erkennbar sind. In einem ersten Teil werden die Auswirkungen der Informationsrevolution auf die Rolle des Staates umrissen. Anschliessend wird den Ursprüngen der sicherheitspolitischen CIIP-Debatte nachgegangen, wobei wegweisende Entwicklungen in den USA im Zentrum der Ausführungen stehen. Diese dienen als analytische Grundlage für den dritten Teil des Artikels, in dem die wichtigsten Herausforderungen dargelegt werden, die sich in diesem neuen Problemkreis der Sicherheitspolitik gegenwärtig abzeichnen.

World View. New York: Harper Collins, 1989. Oder TOFFLER, Alvin. *Third Wave*. New York: Bantam Books, 1980.).

10 RATHMELL, *International CIP Policy*, S. 28–35.

11 WESTRIN, Peter. Critical Information Infrastructure Protection (CIIP). In: WENGER, Andreas (Hrsg.). *Internet and the Changing Face of International Relations and Security. Information & Security* 7 (2001), S. 67–79.

1 Die Rolle des Staats im Informationszeitalter

Kaum jemand zweifelt daran, dass sich die Rahmenbedingungen der internationalen Politik im vergangenen Jahrzehnt grundlegend und nachhaltig verändert haben. Es herrscht ebenfalls weitgehende Übereinstimmung darüber, dass die Informationsrevolution mit ihren wirtschaftlichen, soziokulturellen, politischen und militärischen Auswirkungen ein wichtiges Element dieses Wandels ist.[12] Die genauen Ausprägungen dieser weiterhin andauernden Entwicklung sind jedoch noch unklar. Für die Fragestellung insbesondere interessant ist die Rolle des Staates und wie sie sich durch die Gegebenheiten der Informationsrevolution verändert. Nachfolgend wird in drei Kapiteln dargelegt, welche Herausforderungen sich dem modernen Staat als Anbieter des Kollektivguts Sicherheit stellen.

1.1 Verlust des staatlichen Machtmonopols...

Wird heute das internationale System charakterisiert, dann dürfen zwei Merkmale nicht fehlen: anhaltender Wandel sowie steigende Komplexität.[13] Im Vergleich dazu erscheint im Rückblick die bipolare Ordnung des Kalten Krieges als erstaunlich stabiles System. Die klassische Trennung der Innenpolitik von der Aussenpolitik macht im Angesicht der steigenden Bedeutung internationaler wirtschaftlicher Vernetzung und einem sich verändernden Machtverständnis immer weniger Sinn. Auf der einen Seite werden Güter, Dienstleistungen, Ideen und Kapital heute zunehmend global ausgetauscht. Auf der anderen Seite steht das Bewusstsein des Gemeinschaftlich-Vertrauten respektiv des Lokalen weiterhin in hohem Kurs – man denke hier beispielsweise an die anhaltende Renaissance des Mediums Lokalradio. Teilweise ist es gerade die moderne Informationstechnologie, welche es erlaubt, sich aus einem breiten gesellschaftlich-globalen Diskurs zu lösen und durch ein gemeinschaftlich-konspiratives *Community Building* gegenüber aussen abzuschotten. Auch wirtschaftlich betrachtet behalten lokale Standortfaktoren wie der Bildungsstand, die Infrastruktur, die rechtlichen, kulturellen und politischen Rahmenbedingungen nach wie vor einen wichtigen Einfluss. Vor diesem Hinter-

12 Vgl. Spillmann, Kurt R./Wenger, Andreas/Libiszewski, Stephan/Schedler, Patrik. Informationsgesellschaft und schweizerische Sicherheitspolitik. In: Forschungsstelle für Sicherheitspolitik und Konfliktanalyse(Hrsg.). *Zürcher Beiträge zur Sicherheitspolitik und Konfliktforschung*. Nr. 53 (1999). URL http://www.fsk.ethz.ch/documents/beitraege/zu_53/zu53_con.htm.

13 Rosenau, James. Global Affairs in an Epochal Transformation. In: Henry, C. Ryan/Peartree, Edward C. (Hrsg.). *Information Revolution and International Security.* Washington, D.C.: Center for Strategic and International Studies, 1998, S. 33–57.

grund fragt die internationale Politik nach dem Zusammenspiel zwischen globalen und lokalen Faktoren respektive der Konstitution des „globalen Dorfes".[14]

Die Einheit Staat, Gesellschaft und Wirtschaft ist in ihrem traditionellen Verständnis nicht mehr gegeben: Die geographischen Landesgrenzen haben an Bedeutung verloren, die Grenzen zwischen politischen Räumen verschwimmen zunehmend. Macht und Einfluss in der Informationsgesellschaft leitet sich nicht mehr ausschliesslich von „harten" Faktoren wie Territorium, militärischer Macht und natürlichen Ressourcen ab, sondern wird vermehrt von „sanften" Faktoren wie Information, Technologie und flexible Institutionen beeinflusst.[15] Die Computervernetzung ist durch ihren raumüberwindenden Charakter eine zentrale Voraussetzung und Antriebskraft der sozio-ökonomischen Globalisierung. Ihre Bedeutung und Unersetzlichkeit prädestinieren sie als potentielles Angriffsziel.[16]

In einem Umfeld, welches von dezentralen Netzwerken und „weichen" Machtstrukturen geprägt scheint, wurde viel vom Niedergang des Staates gesprochen. Tatsächlich scheint durch den Aufbau transnationaler, nur schwer kontrollierbarer Netzwerke den Staaten Konkurrenz durch multinationale Wirtschaftsunternehmen, internationale Organisationen und Nicht-Regierungsorganisationen (NGOs) zu erwachsen. Gleichzeitig scheinen flach und flexibel organisierte Netzwerkstrukturen dank grösserer Flexibilität die Oberhand über hierarchische Organisationen zu erlangen, welche sich den dynamischen Veränderungen wegen ihrer institutionellen Trägheit nicht genügend schnell anzupassen vermögen.[17] Es ist daher ein Stück weit richtig, dass der Staat sein Monopol als Akteur der internationalen Beziehungen eingebüsst sowie einen Teil der traditionellen staatlichen Souveränität im internationalen Verkehr verloren hat.

Gleichwohl sind Staaten aus verschiedenen Gründen die wichtigsten Akteure in der internationalen Politik geblieben: Auch wenn man eine Umverteilung von „Macht" auf eine grössere Anzahl Akteure oder eine Diversifizierung von Machtmitteln hin zu Faktoren wie Ideen und Technologie beobachten kann, so ist es doch unumgänglich festzuhalten, dass die drei traditionellen Pfeiler der Macht – wirt-

14 Ibid., S. 33–37; Rosenau schlägt Wortneuschöpfungen vor wie „Glocalization" (= Globalization and Localization) und „Fragmegration" (= Fragmentation and Integration), um die Widersprüchlichkeit der Entwicklungen zu beschreiben.

15 Vgl. zur *Soft power*- Diskussion: KEOHANE, Robert O./NYE, Joseph S. Jr. Power and Interdependence in the Information Age. In: *Foreign Affairs* 77 (1998), Nr. 5, September/Oktober, S. 81–94. NYE, Joseph S. Jr./OWENS, William A. America's Information Edge. In: *Foreign Affairs*, (1996) März/April, S. 20–36.

16 Vgl. SPILLMANN et. al. *Informationsgesellschaft und schweizerische Sicherheitspolitik*.

17 ROTHKOPF, David J. Cyberpolitik: The Changing Nature of Power in the Information Age. In: *Journal of International Affairs* 51 (1998), Nr. 2, S. 325–60.

schaftliche, militärische und politische Macht – immer noch bestehen.[18] In den politischen Wissenschaften mag man sich streiten, welcher dieser Pfeiler nun der wichtigste ist. Niemand ausser dem Staat verfügt jedoch über mehr Ressourcen im Ernstfall und ist mit einer ganzen Palette von Reaktionsmöglichkeiten handlungsfähig.

1.2 ... und Reorientierung

Regierungen sehen sich dennoch gezwungen, ihre Rolle neu zu definieren und sich den veränderten Umständen des Informationszeitalters anzupassen. Teilweise sind bereits Ansätze einer Reorientierung erkennbar: Beispiele sind die Gründung von *E-government*-Einrichtungen,[19] Versuche, *Virtual Diplomacy*-Kapazitäten aufzubauen,[20] oder durch sogenannte *Global Public Policy Networks* – Allianzen von Regierungsinstitutionen, Internationalen Organisationen und Teilen der Zivilgesellschaft – den Einfluss in der Politik auszuweiten.[21]

Vergleicht man die USA mit Europa, entwickeln sich die Debatten zur Rolle des Staates in einem sehr unterschiedlichen politischen und kulturellen Umfeld. Das amerikanische Umfeld ist stark geprägt von einer *winner takes all*-Mentalität, von grossem Vertrauen in die Kräfte des Marktes und privater Initiative an der Basis des Marktes. Die Europäer legen grösseres Gewicht auf sozial-verträgliche und nachhaltige Lösungen, räumen dem Staat mehr Spielraum ein und planen meist eher *top down* als *bottom up*. Die Folge davon ist, dass die Informationsrevolution auch in Zukunft in Europa langsamer voranschreiten wird als in den USA. Dies muss allerdings nicht unbedingt ein Nachteil sein, erlaubt es doch auch von den Entwicklungen in den USA zu lernen und Fehlentwicklungen zu vermeiden.

Speziell auch in der Sicherheitspolitik ist aufgrund der aufgezeigten Veränderungen eine Neupositionierung notwendig, die in den letzten Jahren den meisten Staaten zumindest ansatzweise gelungen ist. Eine modern verstandene Sicherheitspolitik hat neben einer militärischen auch eine wirtschaftliche, eine soziale und eine ökologische Dimension. Das Ziel staatlicher Sicherheitspolitik kann denn

18 Rothkopf, David J. Cyberpolitik: The Changing Nature of Power in the Information Age. In: *Journal of International Affairs* 51 (1998), Nr. 2, S. 325–26.

19 Vgl. A Survey of Government and the Internet: The Next Revolution. In: *The Economist*, 24. Juni 2000.

20 Brown, Sheryl J./Studemeister, Margarita S. Virtual Diplomacy: Rethinking Foreign Policy Practice in the Information Age. In: Wenger, Andreas (Hrsg.). *Internet and the Changing Face of International Relations and Security. Information & Security* 7 (2001), S. 28–44.

21 Vgl. Reinicke, Wolfgang. H. The Other World Wide Web: Global Public Policy Networks. In: *Foreign Policy* 117 (Winter 1999–2000), S. 44–56.

auch nicht mehr auf den Schutz der territorialen Integrität des Staates reduziert werden.[22] Nicht erst seit dem 11. September ist man sich einer Reihe von neuen Risiken und Gefahren bewusst, deren Abwehr und Bewältigung eine zusätzliche Neuausrichtung verlangen. So wird seit einigen Jahren ausgehend von den USA auch in Europa und der Schweiz vermehrt nach der sicherheitspolitischen Dimension von CIIP gefragt. Ein Grund dafür ist die Erkenntnis, dass teilweise bestehende Lösungen auf der rein technischen oder rein physischen Ebene allein nicht ausreichen, um den modernen „Cyberrisiken" effizient entgegenzutreten.

1.3 Der Staat als Anbieter von Sicherheit im Spannungsfeld zwischen Wirtschaft und Gesellschaft

Im CIIP-Bereich muss sich der Staat in Spannungsfeldern zwischen Staat, Wirtschaft und Gesellschaft positionieren. Im ersten Spannungsfeld zwischen Staat und Wirtschaft gilt es, eine Politik zur Sicherung der kritischen Infrastrukturen zu formulieren, welche die negativen Konsequenzen der Liberalisierung, Privatisierung und Globalisierung aus Sicht der Sicherheitspolitik auffängt, ohne die positiven Effekte zu verhindern. Dabei gilt es zu beachten, dass es mehrere marktbedingte Hindernisse für Informationssicherheit gibt: Sicherheit ergibt keine direkt sichtbaren Renditen. Harter Konkurrenzkampf und sehr schnelle Innovationszyklen von IT-Systemen sind hinderlich für die Einführung von Sicherheitsmassnahmen; denn sie wirklich sicher zu machen, dauert häufig länger als die Entwicklung der IT-Nachfolgegeneration selbst, so dass der erstrebte Sicherheitsstandard nie erreicht wird. Zudem haben Sicherheitsstandards oft einen negativen Effekt auf die Funktionalität und Benutzerfreundlichkeit. Sicherheit ist also nur in den seltensten Fällen ein Kriterium, das sich unmittelbar in Umsatz, Gewinn oder sonstige positive Erfolgsfaktoren umsetzen lässt.[23]

Daraus ergibt sich ein Dilemma zwischen grösstmöglicher Kapazität und grösstmöglichen Marktanteilen auf der einen Seite und einer Tendenz zu reduzierter Qualität und Sicherheit der Dienstleistungen auf der anderen Seite. Wie kann der Markt, der zudem mit dem Problem von Quasimonopolen konfrontiert ist, so reguliert werden, dass eine optimale Balance zwischen Sicherheit und Funktionalität entsteht? Wie können Anreize zu mehr Sicherheitsverpflichtung für Anbieter

22 Vgl. Sicherheit durch Kooperation. Bericht des Bundesrates an die Bundesversammlung über die Sicherheitspolitik der Schweiz (SIPOL B 2000) vom 7. Juni 1999 (Sonderdruck).

23 Vgl. Projekt *Kosten und Nutzen der IT-Sicherheit*. Projekt im Auftrag des Bundesamt für Sicherheit in der Informationstechnik (BSI). URL http://www.uimc.de/BSI/BSIproj.htm, oder NÄF, Michael. Ubiquitous Insecurity? How to „Hack" IT Systems. In: WENGER, Andreas (Hrsg.). *Internet and the Changing Face of International Relations and Security. Information & Security* 7 (2001), S. 104–18.

von Dienstleistungen geschaffen werden? Wie können die Nutzer dahingehend sensibilisiert werden, dass sie ein Mehr an Funktionalität nicht länger vor Sicherheitsdenken setzen? Wie können die (globalen) rechtlichen Rahmenbedingungen für Aktivitäten im virtuellen Raum angeglichen werden, um der Gefahr von „Schlupflöchern" und dem Vorrang von billigen Lösungen entgegenzuwirken? Wie kann Vertrauen zwischen Wirtschaft und Staat geschaffen werden? Klar ist, dass der Staat auf die Kooperation mit dem Privatsektor angewiesen ist. Doch welche Informationen und Kompetenzen braucht es hierzu, wann und von wem?

Eine noch grössere Schwierigkeit ergibt sich im Hinblick auf das Spannungsfeld zwischen (nationaler) Sicherheit und Datenschutz.[24] Eine Gruppe aus den Reihen der privaten Wirtschaft und der Datenschützer wendet sich generell dagegen, überhaupt staatliche Regelungen im Bereich der Informationssicherheit zuzulassen. Verschiedene gesetzliche Entwicklungen in den USA nach den Terroranschlägen geben zudem zu neuen Bedenken Anlass – insbesondere die im *USA Patriot Act*[25] festgehaltenen Bestimmungen für erweiterte Abhörmöglichkeiten für Internet- und Telefonkommunikation.[26] Hinzu kommen Befürchtungen aus verschiedenen Lagern, dass die Legitimation von Internetüberwachungssystemen wie *Carnivore* und *Echelon* nach dem 11. September 2001 nicht mehr genügend hinterfragt wird.[27] Ebenfalls erneut diskutiert werden verschärfte Exportkontrollen von Verschlüsselungstechnologien, die von zahlreichen Vertretern als unerlässlich für die private Internetsicherheit und die Zukunft von *E-Commerce* und *E-Business* angesehen werden.[28] Wie lässt sich eine sinnvolle Grenze in diesem Bereich finden?

Geht man nun den Ursprüngen der CIIP-Debatte in den USA nach, dann lassen sich zusätzliche Schwierigkeiten sowie Kernelemente einer nachhaltigen CIIP-Politik identifizieren. Die Analyse der amerikanischen Lösungsansätze zum Schutz kritischer Informationsinfrastrukturen im nächsten Kapitel dient dazu, bei-

---

24 Siehe hierzu z.B. CHARNEY, Scott. The Internet, Law Enforcement And Security. Internet Policy Institute (IPI). Ohne Datum. URL http://www.internetpolicy.org/briefing/charney.html.

25 Die Abkürzung steht für: *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*.

26 USA Patriot Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act), H.R. 3162, 26. Oktober 2001. Text siehe URL http://www.cdt.org/security/usapatriot/011026usa-patriot.pdf; für eine Sammlung von Analysen des USA Patriot Act siehe Center for Democracy and Technology, URL http://www.cdt.org/security/usapatriot/analysis.shtml.

27 Vgl. dazu die andauernde Diskussion zu Carnivore und Echelon. Siehe z.B. Electronic Privacy Information Center (EPIC), URL http://www.epic.org/privacy/carnivore/.

28 RATHMELL, I*nternational CIP Policy*; ELECTRONIC PRIVACY INFORMATION CENTER (EPIC). *Cryptography and Liberty 2000 – An International Survey of Encryption Policy*. URL http://www2.epic.org/reports/crypto2000/.

spielhaft die Rolle des Staates im Bereich CIP/CIIP zu analysieren und aufzuzeigen, welche Probleme im allgemeinen absehbar sind.

2 Ursprünge der CIIP-Debatte in den Vereinigten Staaten

In der amerikanischen Gesellschaft manifestieren sich unterschiedliche politische Interpretationen der neuen Risiken im Bereich der kritischen Informationsinfrastrukturen. Ursprünglich war die Debatte stark militärstrategisch ausgerichtet und orientierte sich an Ideen der asymmetrischen und unkonventionellen Kriegführung. Aufgrund der Popularität von Begriffen wie „elektronisches Pearl Harbor", „Informationskrieg" und anderen militärischer Metaphern wäre die Zuständigkeit des Verteidigungsministeriums in Belangen der neuen „Cyberrisiken" zu erwarten gewesen. Warum sich schlussendlich aber ein ziviler Ansatz überwiegend durchsetzte, soll nachfolgend aufgezeigt werden.

2.1 Der militärische Ansatz bis 1995

In der ersten Hälfte der 90er Jahre begannen sich Warnungen zu häufen, dass die nationale Sicherheit durch mögliche Cyber-Attacken auf Kraftwerke, Banken, Flugsicherung oder Streitkräfte zunehmend bedroht sei.[29] Diese Ängste wurden zusammengefasst unter dem oft geäusserten Schlagwort *Electronic Pearl Harbor*.[30] Der Begriff suggeriert das Schreckensbild eines überraschenden elektronischen Angriffs auf wesentliche und kritische Teile der amerikanischen Computersysteme durch einen Gegner, der sich ausserhalb der USA befindet und eine Bedrohung für die nationale Sicherheit darstellt.

Ursprünglich kam es zu einer Sensibilisierung für eine neue Gefährdung durch die sicherheitspolitische Neuorientierung nach dem Zusammenbruch der Sowjetunion, als man in den USA begann, den Blick verstärkt auf nichtstaatliche Akteure zu lenken, die mit terroristischen Anschlägen eine Bedrohung für amerikanische

29 BENDRATH, Ralf. Elektronisches Pearl Harbor oder Computerkriminalität? Die Reformulierung der Sicherheitspolitik in Zeiten globaler Datennetze. In: *S+F. Vierteljahresschrift für Sicherheit und Frieden* (2000), Nr. 2, S. 135–44. URL http://userpage.fu-berlin.de/~bendrath/SuF_2000.rtf; BENDRATH, Ralf. The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection. In: WENGER, Andreas (Hrsg.). *Internet and the Changing Face of International Relations and Security. Information & Security* 7 (2001), S. 80–103.

30 Ausdruck geprägt von Winn Schwartau, der ihn erstmals im Juni 1991 in einer Anhörung des US-Kongresses benutzte. SCHWARTAU, Winn. Electronic Civil Defense. In: Ders. (Hrsg.). *Information Warfare. Chaos on the Electronic Superhighway.* New York: Thunder's Mouth Press, 1994, S. 43.

Staatsbürger darstellen könnten.[31] Bezeichnend und beunruhigend war, dass der „neue Gegner" nicht mehr klar identifiziert werden konnte. Als Folge davon gingen Unsicherheitsabschätzungen verstärkt von der potentiellen Gefährlichkeit der Mittel aus, welche möglichen Gegnern der USA zur Verfügung stehen könnten. Dabei wurden neben Massenvernichtungswaffen auch Bedrohungen in Erwägung gezogen, die auf der offenen Struktur der amerikanischen Datensysteme, der unkontrollierbaren Software-Proliferation sowie dem breit vorhandenen *Hacker-Know-How* basierten.[32]

Die sich häufenden Warnungen, dass die nationale Sicherheit durch mögliche Cyber-Attacken auf kritische Einrichtungen bedroht sei, fielen zusammen mit einer wachsenden Sorge über die Verwundbarkeit der US-Streitkräfte. Dies war auch gar nicht so abwegig – insbesondere vor dem Hintergrund des militärischen Ursprungs des Internet. Zunächst war die Diskussion über die *Revolution in Military Affairs* und die Computerisierung der Streitkräfte von grosser Euphorie geprägt.[33] Seit Mitte der neunziger Jahre ist ein Umschwung zu beobachten, nach dem den möglichen Risiken stärkere Beachtung geschenkt wird.[34] Die Formulierung von Strategien, die nicht mehr nur auf die Kräfte des Gegners, sondern direkt auch auf seine Informationsflüsse zielen,[35] rückte die vergleichsweise hohe Verwundbarkeit der elektronisch stark vernetzten amerikanischen Truppen ins Blickfeld. Je weiter die Diskussion über Angriffe auf die Informationssysteme möglicher Gegner voranschritt, desto intensiver wurden mögliche Gefahren der eigenen militärischen und zivilen Datennetze thematisiert.[36]

Aufgrund der stark militärisch geprägten Debatte schien die Zuständigkeit des Verteidigungsministeriums für die Bedrohung der kritischen Informations- und Kommunikationsinfrastruktur beschlossene Sache. Die Schwierigkeiten, mit territorial nicht mehr begrenzten und auf keine identifizierbaren Akteure mehr festlegbaren Bedrohungen umzugehen, warfen aber schnell grundlegende Fragen über

31 COHEN, William S. *The Report of the Quadrennial Defense Review*. Washington D.C.: Department of Defense, May 1997. Section II: The Global Security Environment. URL http://www.defenselink.mil/pubs/qdr/.

32 PCCIP Report, S. 14.

33 Vgl. z.B. CAMPEN, A.D. (Hrsg.). *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War*. Fairfax: AFCEA Press, 1992. Oder COHEN, Eliot. A Revolution in Military Affairs. In: *Foreign Affairs 75 (1996)*, Nr. 2, S. 37–54.

34 Vgl. z.B. HUNDLEY, Richard O./ANDERSON, Robert H. Emerging Challenge: Security and Safety in Cyberspace. In: ARQUILLA, John/RONFELDT, David (Hrsg.). *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: RAND, 1997, S. 231–52.

35 Vgl. z.B. JOINT CHIEFS OF STAFF. *Joint Doctrine for Command and Control Warfare (C2W)*. Joint Publication 3–13.1. Washington: Joint Chiefs of Staff, 7. Februar 1996.

36 ANDERSON, R. et. al. *Securing the U.S. Defense Information Infrastructure: A Proposed Approach*. Santa Monica: RAND, 1999. URL http://www.rand.org/publications/MR/MR993.

Kompetenzaufteilungen, gesetzliche Regelungen und politische sowie technische Strategien einer neuen Sicherheitspolitik auf. Gleichzeitig erweckte die Natur der neuen Bedrohung Unbehagen beim Militär selber: Der Charakter von Informationsoperationen führt dazu, dass die Grenzen zwischen innerer und äusserer Sicherheit, zwischen Aufgaben der Streitkräfte und jenen der Polizei mehr und mehr verschwinden.[37] Ein weiteres Indiz für das Unbehagen des Militärs gegenüber der Thematik ist, dass die neuen Informationskriegskonzepte bis anhing nur zögerlich in die Praxis umgesetzt wurden.[38] Bezeichnend für die rechtliche Unsicherheit ist die Warnung der Rechtsabteilung des Pentagon vor völkerrechtlichen Problemen für den Fall, dass die US-Streitkräfte digitale Angriffe auf andere Staaten durchführen würden.[39]

Aufgrund der sich abzeichnenden unkontrollierbaren rechtlichen und politischen Risiken von Cyberkriegen hob die US-Regierung das Thema aus dem militärischen Kontext heraus und etablierte es in einer zivilen Umgebung. Diese Entwicklung nahm ihren Anfang, als im April 1995 eine interministerielle Arbeitsgruppe als Reaktion auf den Bombenanschlag in Oklahoma eingesetzt wurde, welche Amerikas Verwundbarkeit durch den Terrorismus umfassend untersuchen sollte.[40] Als Folge davon zögerte man im Pentagon mit der Einrichtung operativer Abteilungen zur Verteidigung möglicher Cyberattacken und kümmerte sich zunächst vor allem um den Schutz der eigenen militärischen Computernetze.

2.2 Der zivile Ansatz setzt sich durch

Rückblickend zeichnete sich bereits 1995 ab, dass CIIP eher als polizeiliche denn als militärische Aufgabe behandelt werden sollte. Die Leitung der ersten Arbeitsgruppe mit dem Namen *Critical Infrastructure Working Group (CIWG)*, in der Mitglieder aus Strafverfolgung, Militär, Spionage und dem Nationalen Sicherheitsrat vertreten waren, wurde nämlich dem Justizministerium übertragen. Daraus wird ersichtlich, dass der Schutz kritischer Infrastrukturen als eine Verbundaufgabe der äusseren und inneren Sicherheit angegangen werden sollte, und dass der Fokus längerfristig eher auf Computerkriminalität als auf *Cyberwar* gerichtet war.

37 Dunn, Myriam. *Information Age Conflicts. A Study on the Information Revolution and a Changing International Operating Environment*. Liz. Universität Zürich, 2001, (im Erscheinen).

38 Ibid.

39 Department of Defense, Office of General Counsel. *An Assessment of International Legal Issues in Information Operations.* Washington D.C., May 1999.

40 White House. *Presidential Decision Directive 39: U.S. Policy on Counterterrorism,* 21. Juni 1995. URL http://www.fas.org/irp/offdocs/pdd39.htm.

Aufgrund einer Empfehlung der CWIG wurde im Sommer 1996 die *Presidential Commission on Critical Infrastructure Protection* (PCCIP) eingesetzt, um einen umfassenden Bericht über die Sicherheit von Infrastruktursystemen der USA zu erstellen. Der Schwerpunkt der Untersuchung lag auf Cyberrisiken, da die Thematik im Gegensatz zu der schon länger etablierten Auseinandersetzung mit traditionelleren Infrastrukturen neu war, und weil man die Gefahr der informationsinfrastrukturellen Abhängigkeiten und die Folge möglicher Interdependenzen als gravierend erkannte.[41] Durch die Wahl der Mitglieder der PCCIP wurde die zivile Lösung endgültig gefestigt: Die Kommission setzte sich nicht mehr nur aus Vertretern des sicherheitspolitischen Apparates, sondern aus allen wichtigen Ministerien zusammen. In die Diskussion mit einbezogen wurden sogar auch private Infrastrukturbetreiber. Damit wurde der Versuch unternommen, Verantwortung in einem sicherheitspolitischen Bereich zu teilen, in dem sich der Staat ausserstande sah, alleine für Sicherheit zu garantieren.[42]

Der Bericht der PCCIP mit dem Namen *Critical Foundations: Protecting America's Infrastructures* wurde im Herbst 1997 vorgelegt.[43] Präsident Clinton folgte im Mai 1998 mit den *Presidential Decision Directives 62* und *63* (PDD 62, PDD 63) weitgehend den darin formulierten Empfehlungen, auf welche hier nicht im Detail eingegangen wird.[44] Interessant ist insbesondere die klare Stellungnahme, dass die mit der PCCIP begonnene Praxis der Kooperation mit der Privatwirtschaft verstärkt fortgeführt werden sollte. Für die Sicherheit einzelner Sektoren der Infrastruktur wurden unterschiedliche Ministerien als *Lead Agencies* zur Kooperation mit den Betreibern bestimmt. Dabei erkennbar wird eine Art „Selbsthilfe-System", in dem der Staat in Belangen der privaten Sicherheitsaktivitäten als blosser Moderator fungiert, seine repressive Rolle als Strafverfolger in allen Bereichen aber nach wie vor wahrnimmt. Auf die sich hieraus ergebenden Probleme der Kooperation mit der Privatwirtschaft wird an späterer Stelle noch eingegangen.

Der Bericht der PCCIP beschäftigte sich mit Grundlagenfragen und umfasste dementsprechend keine Sicherheitsstrategie für die kritischen Informationssysteme. Verschiedene Ministerien, Behörden und Ausschüsse arbeiteten deswegen von 1998 bis 2000 an der Entwicklung einer umfassenden nationalen Strategie. Diese Anstrengungen mündeten am 7. Januar 2000 in den von Präsident Clinton vor-

41 PCCIP Report, S. vii, x.

42 WHITE HOUSE. *Executive Order 13010: Critical Infrastructure Protection*, 15. Juli 1996. URL http://www.info-sec.com/pccip/web/eo13010.html.

43 PCCIP Report.

44 WHITE HOUSE. *Presidential Decision Directive 62: Protection Against Unconventional Threats to the Homeland and Americans Overseas*, 22. Mai 1998; WHITE HOUSE. *Presidential Decision Directive 63: Critical Infrastructure Protection*, 22. Mai 1998.

gelegten *National Plan for Information Systems Protection*.[45] Darin wurde die grundlegende Annahme der PDDs 62 und 63, dass die Sicherheit der amerikanischen Computersysteme eine geteilte Verantwortung von Regierung und privaten Betreibern bedeutet, bestätigt und verstärkt. Die staatlichen Stellen waren nur noch dafür zuständig, die *eigenen* Datennetze vor Eindringlingen zu schützen.[46]

Mit diesem Vorgehen reagierte die Regierung auf die breite öffentliche Kritik an weitergehenden Ambitionen der Strafverfolgungsbehörden und Geheimdienste und der zunehmenden Sorge vor den Abhörmassnahmen der NSA.[47] Innerhalb der zuständigen Sicherheitsorgane zeichnete sich eine starke Stellung des FBI gegenüber dem Pentagon und den Geheimdiensten ab – bedingt durch inhaltliches *Know-How*, institutionelle, technische und operationelle Erfolge sowie durch die angesprochenen politischen Bedenken.[48] Weiter wurde im Nationalen Plan klar festgehalten, dass die Bundesregierung die kritischen Infrastrukturen der USA allein nicht schützen kann.[49] Als anzustrebendes Ziel wurde eine enge privat-öffentliche Partnerschaft genannt, mit einem stärkeren Einbezug der Regierungen der Bundesstaaten sowie der Kommunalverwaltungen.[50] Die private Wirtschaft zögerte allerdings stark mit der Zusammenarbeit. Wichtige Gründe für die Zurückhaltung waren: Widerwillen, mit den Konkurrenten zu kooperieren, Ängste vor Wirtschaftsspionage und schlechter Publicity sowie grosses Misstrauen vor staatlichen Überwachungsversuchen.[51]

Der 11. September 2001 hat kaum etwas an der bestehenden amerikanischen CIP/CIIP-Politik geändert. Obwohl die Anschläge mit einfachsten technischen Mitteln in die Tat umgesetzt wurden, bleibt die Regierung im CIP-Bereich bei einer starken Fokussierung auf „Cyberrisiken". Seit dem 11. September ist die CIP/CIIP-Politik jedoch zentraler Bestandteil der inneren Sicherheitspolitik und wird dabei stärker in die Gesamtheit der Anti-Terror-Massnahmen eingebettet: Cybersicherheits-Aktivitäten sollen in Zukunft besser mit diesen Bemühungen

45 CLINTON, William. *Defending America's Cyberspace. National Plan for Information Systems Protection, Version 1.0. An Invitation to a Dialogue.* Washington, D.C.: 7. Januar 2000. URL http://www.ciao.gov/publicaffairs/np1final.pdf.

46 Ibid., S. 39–42.

47 Vgl. die seit 1998 im Europäischen Parlament andauernden Untersuchungen zum Echelon-System, welches das NSA zusammen mit anderen Geheimdiensten betreibt und das weltweit den Telefon-, Email- und Faxverkehr abhört und automatisch auswertet.

48 Vgl. Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime, before the Senate Committee on Appropriations Subcommittee for the Departments of Commerce, Justice, State, the Judiciary, and Related Agencies. Washington, D.C, 16. Februar 2000. URL http://www.fbi.gov/congress/congress00/cyber021600.htm.

49 CLINTON, *Defending America's Cyberspace*, S. 104.

50 Ibid., S. 106.

51 BENDRATH, *The Cyberwar Debate*.

koordiniert und Forschung und Entwicklung im Bereich der Informationssicherheit besser mit ihnen verbunden werden.[52]

Die Bush Administration hat in diesem Zusammenhang zwei relevante *Executive Orders* (EO) verabschiedet: EO 13228, am 8. Oktober 2001 unterzeichnet, etablierte das *Office of Homeland Security*, welches alle US-Anstrengungen zum Schutz kritischer Infrastruktur vor den Konsequenzen von Terroranschlägen zu koordinieren hat.[53] EO 13231, vom 16. Oktober, hält die anzustrebende Politik und die Ziele der Bush Administration im Zusammenhang mit dem Schutz kritischer Infrastrukturen fest. Diese sind beinahe deckungsgleich mit jenen des PDD-63 und die Weiterführung der Mehrzahl der Aktivitäten des PDD-63 wird explizit festgehalten. Auch EO 13231 richtet ein spezielles Augenmerk auf Informationssysteme als Rückgrat der modernen Gesellschaft. Gleichzeitig wird im EO 13231 das *President's Critical Infrastructure Protection Board* ins Leben gerufen. Aufgabe des Ausschusses ist es, Programme vorzuschlagen und zu koordinieren, welche Informationssysteme kritischer Infrastrukturen schützen sollen.[54]

Zusammenfassend lassen sich folgende Schlüsselelemente der amerikanischen CIIP-Politik erkennen: Aus der Sicht des Staates steht zuoberst, dass er *sich selbst* schützen kann. Dazu werden die Kräfte interdepartemental gebündelt. Innerhalb des staatlichen Sicherheitsapparates haben sich vor allem das FBI aufgrund seiner institutionellen Vorleistungen und die NSA aufgrund des technischen Vorsprungs durchgesetzt. Als entscheidend zum Erfolg werden Partnerschaften zwischen dem Staat und dem privaten Sektor eingeschätzt. Die bedeutende Rolle, die den privaten Infrastrukturbetreibern in der Umsetzung und sogar der Definition der CIIP-Politik zukommt, hat zur Folge, dass in den letzten Jahren eine Abkehr vom Konzept der territorialen Verteidigung gegen Bedrohungen und eine Hinwendung zur funktionalen Sicherung gegen Risiken zu beobachten ist. Während der Staat eine nationale Schutzstrategie anstrebt, geht es den Infrastrukturbetreibern um die Sicherheit der technischen Systeme und damit um lokal begrenzte Sicherungsmassnahmen.[55] Daraus wird ersichtlich, dass der Staat die Möglichkeit für Sicherheit zu sorgen und Verwundbarkeiten entgegenzutreten teilweise an die Wirtschaft

52 Vgl. KNEZO, Genevieve J. *Federal R&D for Counterterrorism: Organization, Funding and Options.* Washington D.C.: Congressional Research Service, aktualisiert am 3. Januar 2002. URL http://www.ieeeusa.org/forum/PAPERS/CRSterrorismresearch.pdf.

53 WHITE HOUSE. *Executive Order EO 13228: Establishing the Office of Homeland Security and the Homeland Security Council,* 8. Oktober 2001. URL http://www.fas.org/irp/offdocs/eo/eo-13228.htm.

54 WHITE HOUSE. *Executive Order EO 13231: Critical Infrastructure Protection in the Information Age,* 16. Oktober 2001. URL http://www.ncs.gov/Image-Files/eo-13231.htm.

55 Ibid.

verliert und seine Rolle im Informationszeitalter einer Neubeurteilung unterwerfen muss.

3 Schutz kritischer Informationsinfrastrukturen als neuer Problemkomplex der Sicherheitspolitik

Welches sind nun die wichtigsten Fragen und Themen, die sich in diesem neuen Gegenstand der Sicherheitspolitik abzeichnen? In einem ersten Schritt wird auf grundlegende und weitgehend ungeklärte Fragen des Problemkomplexes eingegangen, deren detaillierte Beantwortung für eine solide CIIP-Politik unumgänglich ist. Allerdings wird die Definition der exakten Rolle des Staates im CIIP-Bereich erschwert durch die Spannungsfelder im Umfeld zwischen Staat, Wirtschaft und Gesellschaft, welche oben bereits angetönt wurden. Zuletzt wird überblicksmässig auf wegweisende CIIP-Ansätze in der Schweiz und in Europa hingewiesen.

3.1 Offene Fragen

Die neuen Verwundbarkeiten der Informationsgesellschaft sind schwierig zu analysieren. Drei Elemente sind besonders hervorzuheben: Erstens können die sogenannten Cyberrisiken nur sehr ungenau in den drei Dimensionen Akteur, Absichten und Möglichkeiten erfasst werden, was eine ganze Reihe von Problemen für die Erfassung und das Verständnis der Risiken nach sich zieht.[56] Zweitens lassen sich in der zunehmend durch Informationssysteme und Datenflüsse vernetzten postmodernen Gesellschaft Dienstleistungsketten kaum mehr voneinander isolieren, was dazu führt, dass traditionelle CIP-Ansätze, die einzelne Sektoren isoliert betrachten, weitgehend obsolet geworden sind.[57] Drittens kommt den Informationsinfrastrukturen als Sektor im Gesamtsystem und gleichzeitig als vernetzende Komponente aller Teilsysteme eine besondere und bis anhin kaum untersuchte Bedeutung zu.

Wie kann vor diesem Hintergrund ein robustes CIIP-Gesamtsystem sichergestellt werden? Dazu braucht es vordringlich bessere Kenntnisse über die Verbindungen zwischen Informationssystemen und Infrastrukturen und zwar, holistisch gesehen, über die funktionalen, personellen, institutionellen, physischen, digitalen und psychologischen Verbindungen. Weiter sind Einsichten über Art und Grad der Komplexität des Gesamtsystems und funktionaler Teilsysteme sowie die Erfor-

56 HUTTER, Reinhard. ‚Cyber-Terror': Risiken im Informationszeitalter. In: *Aus Politik und Zeitgeschichte* (2002) Bd. 10–11, S. 31–39.

57 RATHMELL, *International CIP Policy*, S. 31.

schung neuer Verletzlichkeiten, die sich aus den Interdependenzen im System ergeben, vonnöten.[58] Die Komplexität der Aufgabe, die hier auf die Forschung zukommt, lässt sich zusätzlich mit einigen Gedanken zu den folgenden Fragestellungen veranschaulichen: Was ist überhaupt kritisch? Wie können die neuen Risiken verstanden und gemessen werden? Wie soll geschützt werden? Wer genau muss für den Schutz sorgen?

Wie definiert man „kritisch"? Oder, anders gefragt, wie soll der Prozess aussehen, in dem festgelegt wird, nach welchen Kriterien der Schutz kritischer Informationsinfrastrukturen ausgerichtet werden soll? Schutz und Abwehr sind dabei nur eine Seite der Medaille. Vielmehr ist es notwendig, Rückfallpositionen und Minimallösungen für den Ernstfall zu definieren, sich also zu fragen, welche Infrastrukturen lebenswichtig sind und welche minimale Funktionsfähigkeit im Ernstfall bestehen bleiben muss.[59] Das primäre Schutzziel ist die langfristige Überlebensfähigkeit aller relevanten Netzwerke, also die Sicherung eines robusten CIIP-Gesamtsystems: Unterbrüche der Dienstleistungen, die durch diese Infrastrukturen gewährleistet werden, dürfen nur selten vorkommen, sollten von kurzer Dauer sein und müssen einfach und schnell behoben werden können.[60] Eine Definition von „kritisch" kann nicht im Hinblick auf einzelne Infrastrukturkomponenten gelingen, sondern muss mit Blick auf das Gesamtsystem erfolgen. Dabei hängt das, was als kritisch eingeschätzt wird, von der Perspektive des jeweiligen Akteurs ab. Ausschlaggebend sind also zum Beispiel die Erwartungen der Benutzer, die Ansprüche der Nutzniesser von Dienstleistungsketten sowie die Risikowahrnehmung der jeweiligen Akteure. Nicht ausser Acht lassen kann man im Hinblick auf die Bewältigung allfälliger Krisen zudem die Qualität der an Ort verfügbaren Managementkapazitäten.[61] Erneut stellt sich hier die Rolle des Staates als zentral heraus, weil es ihm als einzigem gelingen könnte, mit Hilfe der einzelnen Infrastrukturbetreiber Kritizität im Hinblick auf das Gesamtsystem zu beurteilen. Unterschiedliche Gesellschaften werden zudem „kritisch" unterschiedlich definieren. Bis anhin hat sich noch kein gemeinsames Vokabular zur Verständigung herausgebildet; wohl aber ein gemeinsames Verständnis der Problematik. Je stärker die Systeme über die Landesgrenzen hinweg voneinander abhängig sind, umso

58 CLINTON, William. *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities*. Washington D.C., Januar 2001. URL http://www.ciao.gov/final.pdf.

59 HUTTER, Cyber-Terror, S. 39.

60 Vgl. Primärziele des amerikanischen CIIP: CLINTON, *Defending America's Cyberspace*, S. 16.

61 Vgl. Fazit des Expertenworkshops „Critical Infrastructure Protection in Europe – Lessons Learned and Steps Ahead", vom 9.–10. November 2001 in Zürich. URL http://www.isn.ethz.ch/crn/extended/workshop_zh/ppt/group4/sld001.htm.

dringender wird ein internationaler Dialog zur Frage, wie Risiken analysiert und miteinander verglichen werden sollen.

Wie lassen sich Cyberrisiken beschreiben und bewerten? Die Frage nach potentiellen Akteuren, ihren Motiven, Absichten, Möglichkeiten und Vorgehensweisen muss neu gestellt werden. Die Akteure können Hacker sein, die ihre Attaken als eine Art Freizeitbeschäftigung betreiben. Es kann sich um Individuen oder organisierte Gruppen von Kriminellen handeln, die sich durch ihre Aktivitäten finanzielle Gewinne erhoffen. Es können terroristische Netzwerke als Täter auftreten, die Aufmerksamkeit und Unterstützung für ihre politischen Zielsetzungen gewinnen wollen. Oder es kann sich um Staaten handeln, die anderen Staaten Schaden zufügen wollen.[62] Das Spektrum der Angriffsoptionen reicht von „Hakkerangriffen" bis zur gezielten Störung oder Zerstörung ziviler oder militärischer Einrichtungen, von physischen über elektronische und logische Bedrohungen bis zu Drohungen gegen Entscheidungsträger einer Organisation. Das grösste Potential geht heute wohl von Staaten aus, die sich logischer Bedrohungen bedienen.[63] Unerlässlich in diesem Zusammenhang ist die Definition von Schwellenwerten: Ab wann handelt es sich tatsächlich um ein sicherheitspolitisches Problem? Wie kann sichergestellt werden, dass allfällige Cyberattacken in einem sinnvollen Zeitrahmen richtig eingeschätzt werden?

Wie soll geschützt werden? Entwicklungen in Amerika zeigen, dass es eine Mischung unterschiedlicher Ansätze auf verschiedenen Ebenen braucht. Sicherheit sollte auf der untersten technischen Stufe möglichst schon in die entstehenden Informationsinfrastrukturen eingebaut werden, ist somit also Sache des Systemdesigns und der Systemimplementation.[64] Weiter braucht es Instrumente, um mögliche Fehlerquellen frühzeitig zu erkennen und zu beseitigen, um Systeme so zu bauen, dass sie Fehler zwar vertragen, jedoch nicht wesentlich an Funktionalität verlieren. Es gilt, den entstandenen Schaden möglichst schnell und ohne signifikanten Verlust wieder zu beheben.[65] Genauso zentral ist aber der Faktor Mensch: Training von Spezialisten sowie eine sorgfältige Sensibilisierung der breiten Bevölkerung für allfällige Gefahren sind unerlässlich. Eine sehr grosse Lücke besteht zudem noch in der Gesetzgebung: Es existiert eine sehr unklare nationale

62 Dennis, Ian. Infrastructure's Dependence and Interdependence on Technology. In: Gunnar, Jervas. (Hrsg.). *New Technology as a Threat and Risk Generator. Can Countermeasures Keep Up with the Pace?* Stockholm: Devision of Defence Analysis, Swedish Defence Research Agency (FOI), 2001. S. 278–79.

63 Clinton, *Defending America's Cyberspace*, S. 6–10.

64 Vgl. Masera, M./Wilikens, M. *Interdependencies with the Information Infrastructure: Dependability and Complexity Issues*. Conference Paper at the 5th International Conference on Technology, Policy, and Innovation, 26.–29. Juni 2001. URL http://www.delft2001.tudelft.nl/paper%20files/paper1168.doc.

65 Clinton, *Defending America's Cyberspace*, S. 16.

und internationale Rechtsgrundlage im Bereich der Cyberrisiken, insbesondere im Bereich der Prävention.[66] Verbindliche Regeln im Umgang mit Informationstechnologie, Sicherheitsstandards und Verhaltensregeln (*Code of Conduct*) insbesondere zur Nutzung des Internets in internationalen Auseinandersetzungen sind nur auf einer internationalen Ebene wirklich sinnvoll.[67] In der Erarbeitung eines solchen internationalen Cyber-Regelwerks kommt eine schwierige Aufgabe auf die Staatenwelt zu.

Wer muss für den notwendigen Schutz sorgen? Verantwortlichkeiten und Zuständigkeiten für den Schutz von Informations- und Kommunikationstechnologien sind unklar. Der unbestimmte Charakter der neuen Gefahren trägt dazu bei, dass die Grenzen zwischen innerer und äusserer Sicherheit, zwischen Aufgaben der Streitkräfte und der Polizei immer schwieriger auszumachen sind.[68] Klar ist jedoch, dass sich eine nationale und transnationale Verbundlösung aufdrängt: Staaten und internationale Organisationen sind ebenso gefordert wie private und zivile Institutionen. Private Dienstleistungsanbieter und -besitzer sollten Sicherheitsaspekte als einen zentralen Bestandteil ihrer Business-Strategien berücksichtigen; der Staat soll dort nachhelfen, wo das Marktresultat die nationalen Interessen zuwenig widerspiegelt. Um den Schutz gegen Gefahren und Risiken des Alltages – dazu gehören neben Hackerangriffen auch kleinere natürliche Katastrophen – muss der Infrastrukturbetreiber selber bemüht sein. Vom Staat hingegen wird erwartet, dass er Schutz gegen Gefahren der „ausserordentlichen Lage", d.h. einer höheren Eskalationsstufe bieten kann – wie zum Beispiel Angriffe von Terroristen und anderen Staaten. Er ist somit zuständig für die Bewältigung von Ereignissen mit grossen oder als gross wahrgenommenen Wirkungen.[69]

66 Für Ermittlung und Strafverfahren existiert die *Cybercrime Convention* des Europarates (Budapest, 23. November 2001) wobei die Ratifizierung und Umsetzung in nationales Recht noch einige Zeit in Anspruch nehmen dürfte. URL http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm.

67 HUTTER, *Cyber-Terror*, S. 39; RATHMELL, Andrew. Controlling Computer Network Operations. WENGER, Andreas (Hrsg.). *Internet and the Changing Face of International Relations and Security. Information & Security* 7 (2001), S. 121–144; RATHMELL, *International CIP Policy*, S. 39–40

68 Vgl. HUTTER, *Cyber-Terror*, S. 35.

69 RATHMELL, *International CIP Policy*, S. 30–31.

3.2 CIIP-Initiativen in der Schweiz und im europäschen Umfeld

Während es in den USA bereits seit einigen Jahren zahlreiche Initiativen zum Schutz kritischer Infrastrukturen gibt, stehen die Entwicklungen in Europa und in der Schweiz erst am Anfang. Die wenigen Ansätze, die es gibt, werden nachfolgend kurz im Überblick vorgestellt. Vorneweg lässt sich festhalten, dass die Schweiz über eine gut vernetzte *CIIP-Community* verfügt. Im öffentlichen Sektor wurde das Problem erkannt und eine Vielzahl von Verwaltungsstellen beschäftigen sich mit der Thematik:

- Basierend auf der Auswertung der Strategischen Führungsübung SFU 97 im Bereich Risiken und Chancen der Informationsrevolution und auf den entsprechenden Anträgen und Entscheiden des Bundesrates, organisierte die Strategische Führungsausbildung der Bundeskanzlei (SFA) im Juni 2001 die Übung INFORMO, welche einen wichtigen Meilenstein im Bereich der schweizerischen CIIP-Politik darstellt.[70]
- Die Koordinationsgruppe Informationsgesellschaft sorgt für die Koordination auf Stufe Bund; sie legte im Mai 2000 ein erstes Konzept *Information Assurance* vor.[71]
- In enger Partnerschaft zwischen Privatwirtschaft und Verwaltung hat das Informatikstrategieorgan Bund (ISB) einen Sonderstab *Information Assurance* (SONIA) gebildet. Gleichzeitig befindet sich ein nationales Frühwarnsystem gegen Angriffe aus dem Internet im Aufbau.[72]
- Der Bereich ICT-Infrastruktur der wirtschaftlichen Landesversorgung dient als Anlaufstelle für die Privatwirtschaft. Gemäss dem Prinzip der Subsidiarität leistet sie dort Hilfestellungen, wo der private Sektor die Probleme nicht selber lösen kann.[73]

Im internationalen Vergleich setzt die schweizerische Regierung allerdings nur relativ beschränkte Mittel für den Schutz der kritischen Informationsinfrastruktur ein. Oftmals ist zudem unklar, welche Verwaltungseinheit sich mit welchen Aspekten beschäftigt. Der Bedarf nach Information und Koordination ist weiterhin offensichtlich. Im privaten Sektor verfügen grosse Firmen über eigene Einheiten, die sich mit Informationssicherheit auseinandersetzen. Hier stellt sich erneut die zentrale Frage, wie die Informationen zwischen dem öffentlichen Sektor und

70 Information dazu: URL http://www.admin.ch/ch/sfa/d/services/archiv.html.

71 KOORDINATIONSGRUPPE INFORMATIONSGESSELLSCHAFT. *2. Bericht der Koordinationsgruppe Informationsgesellschaft an den Bundesrat*, 5. Juli 2000. URL http://www.isps.ch/ger/stored_documents/WORD/310.doc.

72 KOORDINATIONSGRUPPE INFORMATIONSGESSELLSCHAFT. *3. Bericht der Koordinationsgruppe Informationsgesellschaft an den Bundesrat*, 29. August 2001, S. 54. URL http://www.isps.ch/download/report_ger.doc.

73 Bundesamt für Wirtschaftliche Landesversorgung Website: URL http://www.bwl.admin.ch/.

dem privaten Sektor besser fliessen und wie gemeinsame Aktivitäten koordiniert werden können.

Das Ziel, als Verbindungsstelle zwischen Privatwirtschaft und Verwaltung zu dienen, verfolgt hierzulande die Stiftung *InfoSurance*. Sie wurde als Kompetenzzentrum der Wirtschaft gegründet und auch in erster Linie über die Wirtschaft finanziert, wird aber vom Bund unterstützt. Die Stiftung bezweckt in enger Partnerschaft zwischen dem privaten und dem öffentlichen Sektor organisatorische und infrastrukturseitige Voraussetzungen zu schaffen, damit:

- die mit der zunehmenden Abhängigkeit von Informationstechnologien verbundenen Risiken für die Schweiz erkannt und erfasst werden können,
- Entscheidungsträger und Benützer der Informationstechnologien im privaten und öffentlichen Sektor die Risiken und Gefahren kennen,
- akute Gefahren früh erkannt werden und Massnahmen zur Prävention resp. Schadensminderung und -bewältigung getroffen werden können.[74]

Sie übernimmt also hauptsächlich die Rolle einer zentralen Diskussionsplattform für den Informationsaustausch. Mit ihrem weitverzweigten Kontaktnetz will sie für das Thema sensibilisieren. Ursprüngliche Pläne, sie zu einer unabhängigen Melde- und Frühwarnstelle zu machen, werden mittlerweile nicht mehr weiterverfolgt.

Die Europäische Union hat das Thema unter dem Titel *Information Infrastructure Dependability Development Support Initiative* (DDSI) aufgenommen.[75] Das Ziel der Initiative ist die Etablierung eines transnationalen Netzwerkes, in dem öffentliche und private Organisationen gemeinsam zur Identifizierung und zum Schutz kritischer Informationsinfrastrukturen beitragen können. Die Europäische Kommission beauftragte ein Konsortium mit Partnerorganisationen aus den Niederlanden, Grossbritannien, Deutschland, Schweden, Italien, Portugal, Griechenland und der Schweiz mit der Durchführung des Projektes. Ernst Basler + Partner Ltd. deckt als Schweizer Vertreter den Raum Schweiz und Liechtenstein ab; Infosurance und die Forschungsstelle für Sicherheitspolitik und Konfliktanalyse (FSK) unterstützen die DDSI als Projektpartner. Aktivitäten im Rahmen der DDSI umfassen in erster Linie das Erarbeiten von Definitionen sowie die konzeptionelle Klärung fundamentaler Punkte: Von welchen Infrastrukturen sprechen wir, wo bestehen Abhängigkeiten? Welche Faktoren bestimmen den politischen Kontext der CIIP-Debatte? Als zweites sollen sogenannte *Country Surveys* erarbeitet

74 InfoSurance Website: URL http://www.infosurance.ch/.
75 DDSI Website: URL http://www.ddsi.org/.

werden, die einen Überblick über die nationalen Rahmen der Debatte im sozialen, politischen, wirtschaftlichen und rechtlichen Bereich geben, was die einzelnen Regierungen, was die Industrie, was Private unternehmen und welche Partnerschaften zwischen den öffentlichen und dem privaten Sektor bestehen. Das erarbeitete Wissen soll über eine Website der Gemeinschaft zur Verfügung gestellt werden. Die Initiative ist demnach auch hauptsächlich dem Informationsaustausch und der Sensibilisierung verschrieben.

An der Forschungsstelle für Sicherheitspolitik und Konfliktanalyse (FSK) beschäftigt sich seit kurzem ein fünfköpfiges Team mit der Risikoanalyse auf nationaler Ebene. Ziel des Projekts ist: Erstens wissenschaftliche Expertise über gegenwärtige und zukünftige Bedrohungen der Schweiz aufzubauen; zweitens das gewonnene Wissen international auszutauschen und zu überprüfen; und drittens die Erarbeitung einer umfassenden Risikoanalyse Schweiz in der Form eines nationalen Risiko- respektive Verwundbarkeits-Profils methodisch und inhaltlich zu unterstützen (Projekt Risikoanalyse XXI). Gegenwärtig bestehen die folgenden thematischen Schwerpunkte:

- Risikoanalytik: Wie können Risiken in ihrer Komplexität analysiert und in ihrer Interdependenz begriffen werden?
- Schutz kritischer Infrastrukturen/*Critical Infrastructure Protection* (CIP): Warum, wann und für wen sind Infrastrukturen „kritisch"? Wie kann eine ganzheitliche Sicherheitspolitik in diesem Bereich formuliert werden?
- Vernetzung und Verwundbarkeit kritischer Informationsinfrastrukturen/*Critical Information Infrastructure Protection* (CIIP): Wie vernetzt sind kritische Informationsinfrastrukturen und wie verwundbar sind wir dadurch?
- Internationaler Terrorismus: Was ist „neu" am sogenannten „neuen Terrorismus"? Wodurch lassen sich politische Gewaltbewegungen (*Political Violence Movements*) als Akteure charakterisieren und wie politische Gegenstrategien formulieren?[76]

Auch in der Forschung stellt sich die Herausforderung der inhaltlich-interdisziplinären Integration des akademischen Fachwissens sowie der Koordination mit dem privaten Sektor. Im Angesicht transnationaler Bedrohungen und Verwundbarkeiten ist ein internationaler Forschungsansatz unumgänglich. Um diesen Dialog zu fördern und einen Überblick über CIIP-Aktivitäten in ausgewählten Ländern zu geben, erarbeitet die Forschungsgruppe zusammen mit Ernst Basler + Partner Ltd.

76 Website des *Comprehensive Risk Analysis and Management Networks* (CRN): URL http://www.isn.ethz.ch/crn.

gegenwärtig das *International Critical Information Infrastructure Protection (CIIP) Handbook*.[77] Hierbei geht es darum, nationale Politiken, Methoden und Modelle zum Schutz kritischer Informations- und Kommunikationsinfrastrukturen zu inventarisieren und miteinander zu vergleichen.

Schlusswort

Der Schutz kritischer Informations- und Kommunikationsinfrastruktur stellt einen neuen Problemkomplex der Sicherheitspolitik dar. Richtungsweisende Entwicklungen sind sowohl in den USA als auch in Europa spürbar. Als übergeordnete und zentrale Frage erweist sich diejenige nach der künftigen Rolle des Staates. Obwohl vor allem in den USA die Debatte vorerst stark militärstrategisch ausgerichtet war, wird CIIP heute in allen Ländern interdepartemental angegangen. Allen uns bekannten nationalen und internationalen Initiativen im CIIP-Bereich ist die Anlage eines Kooperationsprogramms gemeinsam, welches die Partnerschaft von Staat und Privatwirtschaft beinhaltet. Dabei wird dem Faktum Rechnung getragen, dass Einzelmassnahmen auf der technischen Ebene nicht ausreichen, um gegen massive und konzertierte Cyber-Attacken mit kriegerischer bzw. terroristischer Absicht gewappnet zu sein. Darin zeigt sich aber auch, dass der Staat sich ausserstande sieht, alleine für Schutz der kritischen Informationsinfrastrukturen zu sorgen.

Die zunehmende Globalisierung und grenzüberschreitende Konzentration auf zahlreichen Märkten hat zur Folge, dass mitunter grosse multinationale Akteure sicherheitspolitisch relevante kritische Infrastrukturen betreiben, sich gleichzeitig jedoch dem Einfluss staatlicher Regulierung und Kontrolle weitgehend entziehen können. Da sich die wichtigsten Informationsinfrastrukturen in privaten Händen befinden, verliert der Staat einen substantiellen Teil seiner Autorität für das Kollektivgut Sicherheit an die Wirtschaft. Dies ist als ein Indiz dafür zu werten, dass der Staat heute einen Teil seines Machtmonopols verloren hat und sich und seine Funktionen im Informationszeitalter grundlegend überdenken muss. CIIP ist nur durch enge Zusammenarbeit von Staat und Wirtschaft überhaupt zu gewährleisten, wobei es zwei diametrale Interessenlagen zu überwinden gilt: Während das Ziel des Staates eine nationale umfassende Schutzstrategie ist, kümmert sich die Privatwirtschaft im wesentlichen um die Eigensicherung in einem räumlich begrenzten Bereich. Eine solche Zusammenarbeit ist nicht nur schwierig, weil marktbedingte Hindernisse für Informationssicherheit zu überwinden sind, sondern auch,

77 Die acht ausgewählten Länder sind: Kanada, Australien, Deutschland, Schweiz, Niederlande, USA, Schweden, Norwegen. Erscheinungsdatum des *CIIP-Handbooks* ist der Oktober 2002.

weil viel Misstrauen und wenig Bereitschaft zur Kooperation herrscht, wie die Erfahrungen in den USA zeigen.

Damit eine umfassende Schutzpolitik formuliert werden kann, sind aber nicht nur Zusammenarbeit zwischen Privatwirtschaft und Regierung unerlässlich, sondern auch internationale Koalitionen in Politik und Forschung. Bei der Aufgabe CIIP geht es nicht in erster Linie um den Schutz von Objekten der Informationsinfrastruktur. Ein absoluter Schutz unserer Gesellschaft im allgemeinen und unserer kritischer Infrastrukturen im speziellen ist gar nicht möglich. Im Vordergrund muss die Gewährleistung einer gewissen Resistenz oder Robustheit der Systeme stehen. Dies bedingt die Definition und Überprüfung von konkreten Schutzzielen respektive unabdingbaren Funktionsbedürfnissen.

Um eine ganzheitliche Schutzstrategie formulieren zu können, braucht es eine holistische Perspektive von Risiken und Verwundbarkeiten, die physische, digitale, psychologische, institutionelle, personelle und logische Aspekte mit einbezieht und den gesamten Risikoanalyse und -management-Zyklus berücksichtigt. Die eingehende Beschäftigung mit den Akteuren darf im Zusammenhang mit Cyberrisiken ebenfalls nicht fehlen. CIIP ist mehr als blosse Internetsicherheit und als zentraler Teil von CIP zu verstehen, wobei eine sinnvolle Linie zwischen privatwirtschaftlicher Verantwortung und Fragen der nationalen Sicherheit zu ziehen ist.

Mit Hilfe der Forschung müssen nicht nur die Fähigkeiten verbessert werden, um die Absichten zur Ausnutzung der Informationstechnik für feindliche und demokratiegefährdende Aktionen zu erkennen und zu beurteilen, sondern auch Strategien entwickelt werden, um solche Aktionen zu verhindern, und, wenn nötig, aktiv zu bekämpfen. Man ist heute aber weit davon entfernt zu verstehen, welche IT-Strukturen durch realistisch anzunehmende Attacken auf welche Weise verwundbar sind. Die kontinuierliche Bewertung von Verwundbarkeiten und Risiken fehlt genauso wie die gründliche Beschäftigung mit komplexen vernetzten Systemen und insbesondere mit Interdependenzen und Verwundbarkeiten von Informations-Infrastrukturen in einem modernen sicherheitspolitischen Umfeld. Um den Austausch relevanter Informationen unter den Betroffenen zu fördern, braucht es nicht nur einen Grundkonsens unter den potenziell Beteiligten und Betroffenen, sondern auch die Erarbeitung vergleichbarer Methoden und Standards zur Bewertung von Sicherheitsrisiken und zur Einführung eines geeigneten Risiko-Managements.

Isolierte Ansätze in einzelnen Fachrichtungen vermögen diesen Anforderungen kaum mehr zu genügen: Vielmehr ist eine umfassende Risiko- und Verwundbarkeitsanalyse auf nationaler Ebene anzustreben. Eine solche Forschung verlangt

aber eine starke inter- und multidisziplinäre Ausrichtung, die unter anderem technische, politik- und rechtswissenschaftliche Aspekte vereinigt. Nur mit Hilfe eines interdisziplinären Forschungsansatzes kann sichergestellt werden, dass CIIP in einem durch Vernetzung und Interdependenzen, transnationale Risiken und Verwundbarkeiten geprägten internationalen Umfeld zum Herzstück einer modernen, teilweise transnationalen Sicherheitspolitik wird, welche die zentrale Aufgabe zu erfüllen hat, die Robustheit kritischer Dienstleistungen sicherzustellen. Damit eine solche Forschung entstehen kann, braucht es viel Arbeit und Offenheit gegenüber Themen, welche die traditionellen Grenzen gängiger akademischer Forschung sprengen.