Der Cyber-Krieg, der (so) nicht kommt

Erzählte Katastrophen als (Nicht)Wissenspraxis

MYRIAM DUNN CAVELTY

Gäbe es eine Rangliste für zukünftige Bedrohungen, dann wäre der Cyber-*Krieg* im letzten Jahr auf Platz Nummer eins gerückt. Noch vor kurzem ein Nischenthema für Militärstrategen und wenige Fachexperten, ist die digitale Bedrohung spätestens seit der Entdeckung von und den Spekulationen um Stuxnet, dem Atomanlagen sabotierenden Computerwurm, Dauergast in allen Medien und Diskussionspunkt auf namhaften internationalen Veranstaltungen. Viele Staaten, unter ihnen die Bundesrepublik Deutschland, haben spezifische Cyber-Sicherheitsstrategien entworfen[1] und sehen die Cyber-Bedrohung als eine zukünftige Hauptgefahr für die nationale Sicherheit.

Es ist eine Tatsache, dass heutzutage jeder politische, wirtschaftliche und militärische Konflikt eine Cyber-Komponente aufweist und dass mit Hilfe von Computern politische und wirtschaftliche Spionage auf höchster Ebene betrieben wird. Die Zahl der kriminellen Angriffe scheint zuzunehmen und mit ihr der finanzielle Schaden. Auch das organisierte Verbrechen hat sich längst im virtuellen Raum breit gemacht.[2] Kopfzerbrechen bereiten dabei zum einen die steigende

1 Bundesministerium des Innern: Cyber Sicherheitsstrategie für Deutschland, Berlin 2011.

2 Myriam Dunn Cavelty/Gabriel Brönnimann: „E-mail für Dich", in: Böll Thema 3 (2011), S. 9-10; siehe auch: Internet Crime Complaint Center (Hg.): 2010 Internet Crime Report, Washington DC: The National White Collar Crime Center 2011. Bestehende Statistiken sind jedoch mit genü-

Verwundbarkeit – hauptsächlich aufgrund der zunehmenden Verschmelzung sensibler staatlicher wie unternehmenseigener Infrastrukturen mit dem Internet – zum anderen die zu beobachtende Professionalisierung der „Malware-Branche", mit immer komplexeren, raffinierteren, schwieriger abzuwendenden und höheren Schaden anrichtenden Angriffen.[3] Und nicht zuletzt hat das ausgetüftelte Schadprogramm namens Stuxnet laut gewisser Experten langjährige Schreckensszenarien Wirklichkeit werden lassen: der digitale Erstschlag sei erfolgt und Pandoras Cyber-Kriegs-Büchse geöffnet.[4]

In der Tat birgt diese Art von Angriff alles in sich, was bei Menschen maximale Angst auslöst: Er kommt sozusagen aus dem Nichts, kann jederzeit und überall erfolgen, kann jeden treffen, kann praktisch nicht aufgehalten werden und birgt ultimativ die Gefahr für das Ende der menschlichen Zivilisation in sich.[5] Und doch ist befremdlich, wie in den Medien und unter Experten bereitwillig und flächendeckend alle Register gezogen werden und gleich von Krieg gesprochen wird. Denn bisher hat keines der bekannten Scharmützel im virtuellen Raum je auch nur annähernd eine durch das Wort „Krieg" suggerierte Schwere der Auseinandersetzung mit Gewalt, Zerstörung und Leid auf hoher Stufe erreicht. Auch der Stuxnet-Vorfall, wohl der schwerste beziehungsweise schwerwiegendste in der Geschichte der Cyber/Un/Sicherheit, hat mit Krieg wenig bis nichts zu tun: Zwar ist es vorstellbar, dass die cyber-basierte Manipulation bzw. Zerstörung von Infrastrukturen, die als zentral wichtig für die Sicherheit eines Landes an-

gender Vorsicht zu geniessen, denn die Datenlage ist äusserst unbefriedigend.

3 Melde- und Analysestelle Informationssicherung (MELANI) (Hg.): Informationssicherung – Lage in der Schweiz und International. Halbjahresbericht 2010 (Juli - Dezember), Informatikstrategieorgan Bund: Bern 2011.

4 Vgl. Frank Rieger: „Trojaner ‚Stuxnet': der digitale Erstschlag ist erfolgt", in: FAZ.net vom 22.09.2010.

5 Siehe Forschung zu Risikoperzeptionen: Paul Slovic/Baruch Fischhoff/Sarah Lichtenstein: „Why Study Risk Perception?", in: Risk Analysis 2, 2 (1982), S. 83-93.

gesehen werden, ein zukünftiger Kriegsgrund sein könnte.[6] Aber wenn ein Sabotageakt, dessen konkreten Auswirkungen genauso unklar bleiben werden wie die wirkliche Urheberschaft, so unkritisch zum Krieg hochstilisiert wird, weist das entweder auf die Hilflosigkeit im Umgang mit Cyber-Phänomenen hin – oder kann als (mehr oder weniger) gezielter Versuch der am Diskurs beteiligten Akteure gewertet werden, sich durch die konstante rhetorische Mobilmachung Einfluss (in unterschiedlichen Formen) zu verschaffen.

Dabei ist die Aufregung, die seit der Gleichsetzung von Stuxnet mit Cyber-Krieg herrscht, nur die Krönung in der fast zwanzigjährigen Cyber-Angst-Geschichte. Cyber-Ängste drücken sich *in extremis* in Schreckensszenarien aus, in denen staatliche oder terroristische Attentäter in unsere Computernetzwerke eindringen und uns über die Manipulation oder Zerstörung verschiedener kritischer Infrastrukturen – sehr häufig handelt es sich in den Szenarien um das Stromnetz – in die Knie zwingen oder sogar praktisch in die Steinzeit zurückversetzen.[7] Durch das so herbeigeführte TEOTWAWKI (*The End of the World as We Know It* – das Ende der Welt, wie wir sie kennen) steht nichts Geringeres auf dem Spiel als unsere gesamte Zivilisation und alles, wofür sie steht.[8]

Natürlich kann es in einer hoch technisierten Welt wie der unseren unangenehme, gar fatale Folgen haben, wenn Computer aufgrund von Fehlern ausfallen oder von Übeltätern gezielt manipuliert werden. Doch obwohl die Möglichkeit einer eigentlichen *Super*katastrophe

6 Vgl. z. B. Siobhan Gorman/Julian Barnes: „Cyber Combat: Act of War – Pentagon Sets Stage for U.S. to Respond to Computer Sabotage with Military Force", in: The Wall Street Journal vom 31.05.2011.

7 Diese Art von Schreckensszenarien wurde schon vor Jahren von (amerikanischen) Sicherheitsexperten formuliert und zu Übungszwecken oder als Planungsgrundlage verwendet. Vgl. z. B. John Arquilla: „The Great Cyberwar of 2002", in: Wired 6, 2 (1998); fiktiv: Dan Verton: Black Ice: The Invisible Threat of Cyberterrorism. New York: McGraw Hill 2003. Prominent: Richard Clarke/Robert Knake: Cyber War: The Next Threat to National Security and What to Do About It. New York: Ecco 2010.

8 Diese englische Abkürzung hat vor allem im Zusammenhang mit dem als Y2K bekannten Computerphänomen Prominenz erlangt (und durch einen Song der Gruppe R.E.M) – generell wird es aber von Endzeitgruppierungen aller Art verwendet.

nicht vollständig ausgeschlossen werden kann (auch wenn die Wahrscheinlichkeit verschwindend klein ist!), ist es bezeichnend, dass es in der gesamten Computer-Geschichte noch nie einen wirklich schwerwiegenden Vorfall von großem Ausmaß und mit langfristigen Folgen gegeben hat.[9] Und doch scheinen die Cyber-Schreckensszenarien, gemessen an ihrer Akzeptanz in der breiten Bevölkerung und in politischen Kreisen, eine hohe Glaubwürdigkeit zu haben.

Der Cyber-Gau oder das apokalyptische Cyber-Geddon ist somit als Teil einer Gruppe moderner Gefahren bzw. Risiken zu verstehen, die eine beachtliche Anzahl von Politikern, Experten und Interessengruppen mobilisieren und zyklisch sehr viel Medienaufmerksamkeit erhalten, obwohl (oder gerade weil?) sie nur in unserer Antizipation existieren. Andere prominente Beispiele für solche Risiken sind der terroristische Einsatz von Massenvernichtungswaffen, die nächste Pandemie, aber auch die Klimakatastrophe. Ganz unabhängig davon, wie die Wahrscheinlichkeit und das Ausmaß solcher Ereignisse eingeschätzt werden, handelt es sich um „erzählte Katastrophen";[10] Katastrophen, die in der Form von Erzählungen bzw. Narrationen existieren. Dabei ist zu beachten, das Katastrophen (auch sich „ereignende") immer der Narrative bedürfen (siehe unten). Spezifisch am Cyber/Un/Sicherheits-Diskurs ist jedoch, dass es historisch gesehen *keine* Präzedenzfälle für Cyber-geddon Szenarien gibt. Alle bisher dagewesenen Cyber-Vorfälle, inklusive Stuxnet, können zwar als apokalyptische Vorboten gelesen, gedeutet und politisch eingesetzt werden – aber gemessen am monetären, symbolischen oder auch physischen Schaden, der durch sie entstanden ist, sind sie bloße Fußnoten im Vergleich zu „wirklichen" und gegenwärtigen Großereignissen wie Naturkatastrophen, Hungersnöten oder Kriegen.

Die Art und Weise, wie unter diesen Umständen die Cyber/Un/Sicherheit im politischen Prozess gedacht und vermittelt wird, lädt zu

9 Ralf Bendrath: „The American Cyber-Angst and the Real World – Any Link?", in: Robert Latham (Hg.), Bombs and Bandwidth. The Emerging Relationship between IT and Security, New York: The New Press 2003, S. 49-73.

10 Willy Viehöver: „Die Klimakatastrophe als ein Mythos der reflexiven Moderne", in: Reiner Keller et al. (Hgg.), Handbuch Sozialwissenschaftliche Diskursanalyse, Band I: Theorien und Methoden, Opladen: Leske + Budrich 2003, S. 249.

einer tiefer gehenden Analyse des Diskurses ein. Konkret untersucht das vorliegende Kapitel narrative Praktiken im Fall der Cyber-Apokalypse. Es geht der Frage nach, welche Methoden und Praktiken bei der Generierung von Narrationen im politischen Prozess angewandt werden, welche inhaltlichen Ausprägungen diese Narrationen im konkreten Fall aufweisen und was die Konsequenzen solcher Praktiken sind. In einem ersten Kapitel wird die Idee der erzählen Katastrophe näher erläutert und auf ihre spezifischen Merkmale eingegangen. Insbesondere wird die Rolle von Nichtwissen hervorgehoben. Im zweiten Kapitel wird konkreter auf die narrative Praxis von wissenschaftlichen und politischen Erkenntnisgemeinschaften eingegangen. Im abschließenden Kapitel werden die Konsequenzen solcher Praktiken diskutiert.

ERZÄHLTE KATASTROPHEN

Zwischen der erzählten Katastrophe und dem Konzept des „Risikos" in der post-industriellen Gesellschaft besteht eine enge Verwandtschaft. Der maßgeblich von Ulrich Beck und Anthony Giddens entwickelte und geprägte (soziologische) Risikobegriff bezeichnet Phänomene, die unklar und diffus sind und deren Folgen sich oft erst mit zeitlicher Verzögerung bemerkbar machen. Sie haben eine Menge unangenehmer Eigenschaften, unter anderem, dass ein eigentlich begrenzter Unfall zum Zusammenbruch des gesamten Systems führen kann[11] oder auch, dass sie unkontrollierbar geworden sind. Diese Risiken vergegenwärtigen einen Weltzustand, den es (noch) nicht gibt – und sie sind immer mit möglichen schwerwiegenden Konsequenzen behaftet. Insgeheim bedeuten sie also immer auch die Antizipation einer möglichen Katastrophe.[12]

Erzählte Katastrophen entfalten ihre institutionelle Wirkung hauptsächlich im Modus der Erzählung oder des „Mythos".[13] Tatsächlich bedarf die Katastrophe – auch die reelle – immer der diskursiven

11 Olivier Godard et al.: Traité des nouveaux risques: précaution, crise, assurance, Collection folio actuel, Paris: Gallimard 2002.

12 Ulrich Beck: Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit. Frankfurt a. M.: Suhrkamp 2007.

13 W. Viehöver: Die Klimakatastrophe als ein Mythos der reflexiven Moderne, S. 248.

Vermittlung; oder, in anderen Worten, es braucht eine intersubjektive „Einigung", was wann eine Krise oder gar Katastrophe ist – und was nicht.[14] Im Falle von erzählten Katastrophen ist die Beschäftigung mit der Rolle der Inszenierung einfach noch offensichtlicher als bei solchen, bei denen (artverwandte) Präzedenzfälle bestimmte Referenzwerte, Ankerpunkte und Erfahrungswerte liefern (und dadurch der diskursiven Vermittlung auch klare Grenzen gesetzt werden).

Bei der Beschäftigung mit erzählten Katastrophen produzieren Experten, politische Akteure und insbesondere auch die Medien Narrationen, in denen das Potentielle mit der (gedachten) Wirklichkeit vermischt wird. Die gesellschaftliche Resonanz und die politisch-institutionelle Wirkung werden von der narrativen Form, in der die Geschichte formuliert wird, also nicht nur mitbestimmt, sondern diese schafft quasi ihre eigene Wirklichkeit, denn diese Narrationen holen die Zukunft in die Gegenwart und machen Handlung erst möglich.

Narrationen vermitteln Weltdeutungen, kulturelle Werte und Handlungsorientierungen und stellen so ein zentrales diskursstrukturierendes Regelsystem dar.[15] Auf die daraus resultierende Möglichkeit der Machtanwendung einzelner Akteure mittels instrumentalisierter Narrationen verweist Foucault, wenn er schreibt, Diskurs sei „dasjenige, worum und womit man kämpft; er ist die Macht, deren man sich zu bemächtigen sucht"[16]. Die Generierung von Narrationen tritt also nie ohne Macht(-wirkung) auf. Wer ein dominantes Interpretations- und Argumentationsmuster zu etablieren versteht, kann die Kontrolle über die Bedeutungszuweisung von Worten erlangen und dadurch „sein" Bild der Welt, das von der Öffentlichkeit aufgenommen und als „normales" Bild akzeptiert wird, etablieren.

Narrationen spielen auch in der neueren sicherheitspolitischen Forschung eine Rolle: Die sogenannte „Kopenhagener Schule" entwi-

14 Jan Metzger: „The Concept of Critical Infrastructure Protection (CIP)", in: Alyson Bailes/Isabelle Frommelt (Hgg.), Business and Security: Public-Private Sector Relationships in a New Security Environment, Oxford: Oxford University Press 2004, S. 197-209.

15 Willy Viehöver: „Diskurse als Narrationen", in: Reiner Keller et al. (Hgg.) Handbuch Sozialwissenschaftliche Diskursanalyse, Band I: Theorien und Methoden. Opladen: Leske + Budrich, 2001, S. 177-206.

16 Michel Foucault: Die Ordnung des Diskurses. Frankfurt a. M.: Suhrkamp 1997, S. 11.

ckelte einen Ansatz, der Sicherheitsprobleme und die damit in Gang gesetzte und als legitim erscheinende Dynamik insbesondere auf der Basis von diskursiven Praktiken untersucht.[17] Die erfolgreiche *Securitization* eines Themas rechtfertigt aufgrund der damit einhergehenden Dringlichkeit den Einsatz aller verfügbaren Mittel – auch jener außerhalb der normalen politischen Spielregeln.[18] Deshalb muss vorrangig eine stark mobilisierende diskursive Rechtfertigung für diesen außerordentlichen Zustand gemacht werden. Dies geschieht vor allem in der narrativen Darstellung der dem Staat oder der Gesellschaft drohenden Gefahr.

Aufgrund der sich hinter diesem Prozess befindenden Logik, die zum großen Teil auf Dringlichkeit und imminenter Bedrohung beruht, funktioniert die Securitization bei Risiken, die *per definitionem* als „Möglichkeiten" mit Hilfe von Wahrscheinlichkeiten dargestellt werden, und bei denen der Zeitpunkt und das Ausmaß des möglichen Eintretens ungewiss sind, meistens nicht.[19] Interessanterweise gewinnt diese Logik im Falle der erzählten (Super-)Katastrophe aber wieder an Gewicht. Denn obwohl diese in einer ungewissen Zukunft liegen, werden sie im politischen Prozess häufig als imminent dargestellt – und werden dadurch aus dem Bereich der unsicheren Zukunft quasi als reelle Bedrohung in die Gegenwart geholt. Da es für sie wenig oder sogar keine Erfahrungswerte oder Präzedenzfälle gibt, muss die Gefahr – unter Rückgriff auf Anekdoten, die das potentiell Schreckliche veranschaulichen – als unmittelbar bevorstehend und grauenhaft dargestellt werden, um überhaupt Gehör zu finden. Das erklärt die Fixation der Erzählungen auf apokalyptische „Worst-Case" Szenarien und spekta-

17 Grundlegend: Barry Buzan/Ole Wæver/Jaap de Wilde: Security: A New Framework for Analysis, Boulder: Lynne Rienner 1998.

18 *Securitization* bedeutet die Summe der Darstellung eines Sachverhalts, einer Person oder einer Entwicklung als Gefahr für die militärische, politische, wirtschaftliche, ökologische und/oder gesellschaftliche Sicherheit eines Kollektivs und der Akzeptanz dieser Darstellung durch den jeweils angesprochenen politischen Adressaten.

19 Michael J. Williams: „(In)Security Studies, Reflexive Modernization and the Risk Society", in: Cooperation and Conflict 43, 1 (2008), S. 57-79 und Mark Daniel Jäger: „The Psychology of Securitization Pragmatics of Risks, Threats, and Socially Shared Cognition". Unveröffentlichtes Konferenzpapier, Zürich 2011.

kuläre, sich rasch zuspitzende Unglücksfälle, die in ihrer dramaturgischen Darstellung über den Vorteil szenischer Eindringlichkeit verfügen. Erzählte Katastrophen werden so quasi automatisch und immer zu sicherheitspolitischen Problemen, weil sie die Grenzen des „Normalen" sprengen.

Die Vergangenheit hat gezeigt, dass dadurch unter gewissen Umständen ein absichtlich unsauber auf sicherheitspolitische Belange angewandtes Vorsorgeprinzip legitimiert werden kann.[20] Das aus dem Umweltbereich bekannte Prinzip lässt zu, dass die Rechtsanwendung handeln darf, obwohl nicht sicher ist, dass die Handlung dem Schutzgut tatsächlich dient, weil die Wissensbasis unvollständig ist.[21] Die möglichen zukünftigen Schäden werden aber als so potenziell gravierend oder sogar irreversibel angesehen, dass dringender Handlungsbedarf abgeleitet werden kann. Dies führt sogar so weit, dass nicht mehr das eigentliche primäre Risiko die Hauptbedrohung darstellt, sondern vielmehr das Nicht-Handeln in der Gegenwart. Die Art der zu ergreifenden Maßnahmen wird im politischen Planungsprozess mit Hilfe von bildhaften Vorstellungen, wie die Zukunft sein könnte, bestimmt.[22] Genau wie diese Zukunft in Form von Szenarien gedacht wird, spielt daher eine zentrale Rolle im Umgang mit diesen Gefahren.

Auf das unheimliche Zusammenspiel zwischen dem Modellieren der Zukunft und der dadurch teilweise erst bedingten Konstruktion von Gefahren hat Baudrillard bereits in den 1970ern hingewiesen. Gemäß seiner Überlegungen wird unser Zeitalter dominiert durch „Simulationen", Bilder der Wirklichkeit, die vor allem über die Massenmedien vermittelt werden, die wichtiger und wirklichkeitsmächtiger geworden sind als die Wirklichkeit selbst und die ein Verschwinden der Grenzen zwischen wahr und falsch, zwischen Fiktion und Realität ermögli-

20 Z. B. Craig McLean/Alan Patterson/John Williams: „Risk Assessment, Policy-Making and the Limits of Knowledge: The Precautionary Principle and International Relations", in: International Relations 23, 4 (2009), S. 548-566.

21 „Vorsorgeprinzip", Zusammenfassung der EU Gesetzgebung, *http://europa.eu/legislation_summaries/consumers/consumer_safety/l32042_de.htm*.

22 Marieke de Goede: „Beyond Risk. Premeditation and the Post-9/11 Security Imagination", in: Security Dialogue, 39, 2-3 (2008) S. 155-176.

chen.[23] Die von Experten erzeugten Szenarien (und Narrationen) geraten so in den Verdacht, die Gefahren, vor denen sie warnen, teilweise erst (mit) zu konstruieren und auch zu konstituieren.

Ganz zentral beim (richtigen oder falschen) Vorsorgeprinzip ist, dass die verfügbaren wissenschaftlichen Daten aufgrund hoher Ungewissheit eine umfassende Risikobewertung nicht zulassen. Dabei sind (Sicherheits-)Experten bei der Generierung von Planungsgrundlagen im Falle von erzählten Katastrophen mit zwei Sorten von Unwissen bzw. Nichtwissen konfrontiert:[24] Bei der ersten Sorte Nichtwissen wird angenommen, dass das Problem mit mehr Forschung und dadurch generierten zusätzlichen Daten fassbar gemacht werden kann. Es handelt sich also nur um zeitlich limitiertes Nichtwissen. Diese Art wird als *spezifisches* Nichtwissen bezeichnet: man weiß, dass und was man (noch) nicht weiß; deshalb kann man gezielten Wissenserwerb betreiben, um die identifizierte Lücke zu schließen. Die zweite Sorte Nichtwissen hingegen bezeichnet den Umstand, dass man gewisse Dinge nicht und nie wissen kann. Dieses sogenannte *unspezifische* Nichtwissen bezeichnet einen Bereich kategorisch unverfügbaren Wissens, von dem man nicht sagen kann, was und sogar dass (noch) nicht gewusst wird, sondern der sich als ganzer der Beobachtung entzieht.

Bei erzählten Katastrophen wird durch die oben beschriebene Praktik, sie quasi als Bedrohungen – und daher als imminent und sicher – darzustellen, eine aktive Vertuschung von spezifischem Nichtwissen vorgenommen, wie in der folgenden Fallstudie gezeigt werden wird. Wissen, das für sicher gehalten wird und als sicher dargestellt wird, kann zu einer unguten Verzerrung der Ausgangslage bzw. Planungsgrundlage führen und nicht intendierte Nebeneffekte haben, denn potentielle Katastrophen werden auch durch wissenschaftlich spezifiziertes Nichtwissen, also kontroversem Expertenwissen, (mit) produ-

23 Jean Baudrillard: L'échange symbolique et la mort, Paris: Gallimard 1976, S. 114.

24 Klaus P. Japp: „Zur Soziologie der Katastrophe", in: Lars Clausen/Elke M. Geenen/Elisio Macamo (Hgg.), Entsetzliche soziale Prozesse: Theorie und Empirie der Katastrophen, (Konflikte, Krisen und Katastrophen – in sozialer und kultureller Sicht, Bd. 1), Münster: LIT Verlag 2003, S. 77-90.

ziert.[25] Darüber hinaus führt diese Praxis dazu, dass vollständige „Intransparenz durch […] wahrscheinlichkeitsbezogenes (und damit nur relativ unsicheres) Expertenwissen“[26] substituiert wird. Das unspezifizierte Nichtwissen kann so zu katastrophischen Risikokonstruktionen führen, also Konstruktionen, die im Luhmannschen Sinn zu einem „Totalschaden“ führen[27] bzw. durch die übersteigerte Darstellung des Katastrophischen die eigentliche Katastrophe in einem ganz anderen Bereich erst schaffen.

AUF DEN SPUREN DER CYBER-APOKALYPSE

Die Cyber-Katastrophe gehört am ehesten in den Bereich der Technikkatastrophen. Technikkatastrophen sind definitionsgemäß menschengemacht und setzen meist auch eine Art von politischem Versagen voraus.[28] In der Gesellschaftstheorie blieb Technik lange ein relativ unbeachteter Faktor: Der Erfolg des Begriffs „Risikogesellschaft“ änderte dies in den 1980er Jahren, als sich die durch Ulrich Beck geprägte Denkrichtung für den Umgang moderner Gesellschaften mit unintendierten Folgen technologischen Fortschritts beziehungsweise der Antizipation möglicher Folgen von Technologie zu beschäftigen begann.[29] Eine solche Betrachtungsweise spiegelt einen grundlegenden Wandel der Rolle von Technik im Rationalisierungsprozess wider: von einem verlässlichen Mittel wird sie zum Unsicherheitsfaktor, indem sie Zwecke gefährdet und sogar destruktive Gefährdungen erst hervorbringt.[30]

---

25 Ulrich Beck: Die Erfindung des Politischen. Zu einer Theorie reflexiver Modernisierung. Frankfurt a. M.: Suhrkamp 1993.

26 K. Japp: Zur Soziologie der Katastrophe, S. 80.

27 Niklas Luhmann: Beobachtungen der Moderne. Opladen: Westdeutscher Verlag 1992.

28 Vgl. Charles Perrow: Normal Accidents: Living with High-Risk Technologies, New York: Basic Books 1984.

29 Ulrich Beck: Risikogesellschaft. Auf dem Weg in eine andere Moderne. Frankfurt a. Main: Suhrkamp 1986.

30 Gerhard Panzer: Kairos der „Risikogesellschaft“: wie gesellschaftstheoretische Zeitdiagnosen mit technischer Unsicherheit umgehen, Kassel: Kassel University Press 2001.

In der Cyber-Debatte wird die Technik selbst zur zielgerichteten Waffe und durch die den Technologien eigene Unsicherheit zur Achillesferse moderner Gesellschaften.[31] Kritische Infrastrukturen sind in der Cyber-Kriegs-Ära zum Sinnbild für die Verwundbarkeit der liberalen, offenen Gesellschaft und deren Schutzbedürfnis geworden. Sie sind Brennpunkt in einer politischen Debatte, in der schleichende Angst vor allgegenwärtiger Verwundbarkeit und eine unbestimmte Angst vor der Zukunft signifikante Merkmale sind und in der das Prinzip der willentlichen Ausnützung von Verwundbarkeiten moderner Gesellschaften das Prinzip von Wandel und Unfall nicht ersetzt, aber doch zumindest teilweise abgelöst hat.

In den nächsten drei Unterkapiteln werden die Voraussetzungen für die Konstruktion der Cyber-Katastrophe aufgefächert und ihre Ausprägungen beschrieben. Erstens wird beschrieben, worauf die Konstruktion der Katastrophe beruht, und es wird auf die Inhalte gängiger Cyber-Katastrophen-Narrationen eingegangen. Diese Narrationen entstehen häufig nicht ausschließlich in Regierungs- bzw. Verwaltungskreisen, sondern sind stark von den Medien und externen Experten geprägt. Es geht aber weniger um die Frage, wer die Charakteristiken dieser Risiken aufzuzeigen vermag (also um die Machtfrage), sondern darum, in welcher Form dies geschieht. In einem zweiten Unterkapitel wird explizit auf die Kategorie des spezifischen Nichtwissens in diesem Prozess eingegangen. In einem dritten auf den Umgang mit unspezifischem Nichtwissen.[32]

DIE ERZÄHLUNG VON DER ALLUMFASSENDEN VERWUNDBARKEIT

In den 1980ern wurde die Cyber-Gefahr noch als vor allem Regierungsnetzwerke betreffend angesehen und die Debatte war auf Cyber-Spionage fixiert. Erst in den späteren 1990ern ist eine qualitative Ver-

31 Vgl. Robert Deibert/Rafal Rohozinski: „Risking Security: Policies and Paradoxes of Cyberspace Security“, in: International Political Sociology 4 (2010), S. 15-32.

32 Wobei angemerkt sei, dass die Identifikation dieser Kategorie mit empirischen Schwierigkeiten besetzt ist – sind doch alle im Prozess identifizierten Wissenslücken bereits zu spezifischem Nichtwissen geworden.

änderung der Bedrohungswahrnehmung zu beobachten. Vermehrt wurden in (amerikanischen) Dokumenten eine Verknüpfung zwischen Computern (oder Informationsinfrastrukturen) und sogenannt kritischen Infrastrukturen hergestellt.[33]

Die Ausgangslage sieht demnach wie folgt aus: Die moderne technologisierte Gesellschaft ist auf das zuverlässige Funktionieren von *Infrastrukturen* angewiesen. Unter dem Begriff Infrastrukturen – bestehend aus den beiden Wörtern Infra („unterhalb") und Struktur („Gefüge, Bau, Aufbau") – versteht man Anlagen, Einrichtungen, Organisationen, aber auch Prozesse, Produkte, Dienstleistungen und Informationsflüsse, die den „Unterbau" für das reibungslose Funktionieren der Gesellschaft, der Wirtschaft und des Staates bilden.[34] Als kritisch werden jene Infrastrukturen bezeichnet, die bei einem Ausfall zu gravierenden politischen oder wirtschaftlichen Schäden führen können. In diese Kategorie fallen gemeinhin die Energieversorgung, die Kommunikation, das Gesundheitswesen, der Verkehr oder die öffentliche Sicherheit.[35]

So wichtig sie sind, so verletzlich scheinen sie: Zum einen bilden *Informations*infrastrukturen, die als inhärent unsicher gelten, häufig die Grundvoraussetzung für das Funktionieren aller anderen Infrastrukturen. Diese Debatte bedeutend mitgeprägt hat das US Militär, das in den frühen 1990er Jahren verstärkt über asymmetrische Bedrohungen nachzudenken begann. Es schien unumgänglich, dass zukünftige Gegner der absolut überlegenen militärischen Macht nur noch asymmetrisch begegnen konnten.[36] Die damals in Schwung kommende

33 Myriam Dunn Cavelty: „Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate", Journal of Information Technology and Politics 4, 1 (2007), S. 19-36.

34 President's Commission on Critical Infrastructure Protection: Critical Foundations: Protecting America's Infrastructures, Washington, DC: US Government Printing Office 1997.

35 Myriam Dunn Cavelty/Kristian Søby Kristensen: „Introduction: Securing the Homeland – Critical Infrastructure, Risk, and (In)Security", in: dies. (Hgg), The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation, London: Routledge 2008, S. 1-14.

36 Neal A. Pollard: „Indications and Warning of Infrastructure Attack", in: Lars Nicander/Magnus Ranstorp (Hgg.), Terrorism in the Information Age: New Frontiers?, Stockholm: National Defence College 2004, S. 43.

„Informationsrevolution" schien diese Möglichkeit noch zu verstärken. In den Augen von Sicherheitsexperten führte sie dazu, dass die Gesellschaft von einer Vielfalt von nationalen und internationalen Informationsinfrastrukturen abhängig – und deshalb verwundbar – wurde. Nicht nur gelten Informationsinfrastrukturen aufgrund technischer Unzulänglichkeiten als sehr unsicher, auch werden sie als besonders anfällig für asymmetrische Maßnahmen seitens staatlicher und nichtstaatlicher Organisationen oder Einzeltäter angesehen, denn diese können durch die Nutzung weiterverbreiteter und kostengünstiger digitaler Angriffsmöglichkeiten maximalen Schaden anrichten.[37]

In Cyber-Katastrophen-Narrationen[38] wird die drohende Gefahr immer als sehr vielseitig und gleichzeitig als sehr vage dargestellt. Vor allem das Ungewisse und Unbekannte macht Angst: Wie bei der klassischen Gespenstergeschichte ist die Angst dann am größten, wenn man eine Gefahr erwartet, aber nicht genau weiß, in welcher Form und wann sie auftreten wird. Zu den zahlreichen Risiken und Gefahren, welchen kritische Infrastrukturen ausgesetzt sein sollen, werden eine große Anzahl struktureller Gefahren wie auch akteurspezifische Bedrohungen gezählt. Das Spektrum möglicher Angreifer ist weit gespannt und reicht vom gelangweilten Teenager über verärgerte oder unzufriedene Mitarbeiter, Industriespione, organisiertes Verbrechen, Fanatiker und Terroreinheiten bis hin zu feindlichen Staaten. Das Spektrum der Angriffsoptionen reicht von Hackerangriffen bis zur physischen Zerstörung ziviler oder militärischer Einrichtungen. Gera-

37 Als Teil des Stuxnet-Mythos gilt, dass die Programmierung dieses Wurms teuer und komplex gewesen sei – und dass das auf einen (oder mehrere) Staaten als Urheber schließen lasse. Im Vergleich zu konventionellen Waffensystemen oder Nuklearwaffen ist die geschätzten Summe (es sind Zahlen zwischen drei bis zehn Millionen Dollar im Umlauf) aber ein Klacks, so dass auch zukünftige Cyber-„Waffen" im Vergleich dazu als asymmetrisch angesehen werden dürften.

38 Details dieser Narrationen finden sich z. B. in: Maura Conway: „Media, Fear and the Hyperreal. The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures", in: Myriam Dunn Cavelty/ Kristian Søby Kristensen (Hgg.), Securing the Homeland: Critical Infrastructure, Risk, and (In)Security, London: Routledge 2008, S. 109-129 und Myriam Dunn Cavelty: Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, London: Routledge 2008.

de aufgrund dieser langen Liste ist die genaue Ausprägung der Gefahr in Bezug auf Zeitpunkt, Akteur, Motivation und Ausmaß sehr unsicher.

Darüber hinaus werden in den Cyber-Narrationen zwei zentrale menschliche Ängste miteinander verknüpft: die Angst vor der Technik und die Angst vor dem Terrorismus.[39] Da beide vor allem mit Ungewissheit und Unsicherheit im Zusammenhang stehen, vermag die Kombination von Technik und Terrorismus besonders stark zu mobilisieren.[40] Der Terrorismus – ganz gemäß terroristischem Kalkül – wird gefürchtet, weil er unverstehbar und unkontrollierbar erscheint und weil er das Sicherheitsgefühl eines jeden Menschen untergräbt. Informationstechnologie wiederum ist gefürchtet, weil ihr Einfluss auf das Individuum als komplex, abstrakt und arkan angesehen wird. Diese Angst hängt mit drohendem „Kontrollverlust" zusammen[41]: Insbesondere im Zeitalter von weltumspannenden (Daten-)Netzwerken verliert der Mensch die Kontrolle über die Funktionen, die von Computern gesteuert werden.[42] Die Superkatastrophe im Bereich von kritischen Infrastrukturen ist auch immer konzipiert als interdependente Katastrophe: Die Interdependenzen zwischen Systemen und Menschen und die Wahrscheinlichkeit von sogenannten kaskadischen Dominoeffekten, also Effekten, die außerhalb unserer Kontrolle liegen, potenzieren die möglichen Auswirkungen um ein Vielfaches. Cyber-Szenarien erwecken zudem den Eindruck, dass der nächste spektakuläre Terroran-

39 Walter Laqueur: The New Terrorism: Fanaticism and the Arms of Mass Destruction. Oxford: Oxford University Press 1999, S. 254.

40 Ayn Embar-Seddon: „Cyberterrorism: Are we Under Siege?", in: American Behavioral Scientist 45, 6 (2002). Dabei muss offen gelassen werden, ob diese Ängste tatsächlich in der breiten Bevölkerung existieren – oder ob sie nicht eher auf politischer Ebene angenommen werden; und dann aufgrund solcher Annahmen gehandelt wird.

41 Vgl. auch Langdon Winner: „Trust and Terror: The Vulnerability of Complex Socio-technical Systems", in: Science as Culture 13, 2 (2004), S. 155-172 und Lee Clarke: Worst Cases. Terror and Catastrophe in the Popular Imagination, Chicago u. a.: University of Chicago Press 2006.

42 Mark M. Pollitt: „Cyberterrorism: Fact or Fancy?", in: Computer Fraud and Security 2 (1998), S. 8; Barry Sandwell: „Monsters in Cyberspace: Cyberphobia and Cultural Panic in the Information Age", in: Information, Communication & Society 9, 1 (2006), S. 47.

schlag durch den Gebrauch des Internets als Waffe gleichzeitig überall und nirgends stattfinden wird.[43]

Durch die unheilvolle Kombination von Verwundbarkeit, Komplexität auf technischer Ebene und Akteuren mit apokalyptischen Absichten scheint eine Superkatastrophe vorprogrammiert. Eine in praktischer und theoretischer Hinsicht überwältigende Komplexität auf der Ebene der technischen Systeme hält konstant die drohende Wahrscheinlichkeit eines „normalen Unfalls" vor Augen. Obwohl das Leben in westlichen Wohlstandsgesellschaften dank des technischen Fortschritts eigentlich immer sicherer erscheint, wird die Menschheit mit immer mehr und immer größeren, immer umfassenderen Risiken konfrontiert. Auch die durch terroristische Akteure über kritische Infrastrukturen hervorgebrachte Superkatastrophe ist konzipiert als „integraler Unfall"[44], der sich künftig, im Gegensatz zu bisherigen Unfällen, die in ihren Wirkungen und Ausmaßen beschränkt waren, auf die ganze Welt auswirken wird.

Cyber-Narrationen sind voll von Metaphern, bei denen es um die Auflösung von sicheren Zuständen durch neue, unberechenbare und auch unvorhersehbare Gefahren geht. Die Narrationen sind also geprägt von Macht- und Kontrollverlust; Nichtwissen an und für sich wird als Gefahr dargestellt, denn Nichtwissen führt zu Ungewissheit in Bezug auf Zeitpunkt, Akteure, Ziele und Motivationen. Die „Ohnmacht", die aus diesem Nichtwissen entsteht, wird im politischen Prozess häufig dahingehend instrumentalisiert, dass aufgrund der unklaren Gefahrenlage schnelles und effektives Handeln im Bereich der Schutzmaßnahmen nötig sei, was natürlich häufig auch einen Ruf nach zusätzlichen Ressourcen nach sich zieht.

43 François Debrix: „Cyberterror and Media-induced Fears: The Production of Emergency Culture", in: Strategies 14, 1 (2001), S. 156 und François Debrix/Alexander D. Barder: „Nothing to Fear but Fear: Governmentality and the Biopolitical Production of Terror", International Political Sociology 3, 4 (2009), S. 398-413.

44 Paul Virilio: Original Accident, Cambridge: Polity Press 2007.

UMGANG MIT SPEZIFISCHEM NICHTWISSEN

Die Basis für alle Maßnahmenplanungen im Bereich von kritischen Infrastrukturen sind Risikoanalysen. Das klassische (technische) Risikomodell berechnet das Risiko (R) als das Produkt aus Schadenshöhe (S) und Eintrittswahrscheinlichkeit (W), also R = S * W. Ein Risiko lässt sich demzufolge als Wert in einer Risikomatrix darstellen und auch mit anderen Risiken vergleichen. Im sicherheitspolitischen Prozess spricht man dabei oftmals von Gefährdungsanalyse. Zweck einer solchen ist die Planung der Prävention zur Verringerung der Verletzlichkeit sowie die Planung der Vorsorge zur Bewältigung von Katastrophen und Notlagen. Das Gefährdungspotential berechnet sich analog zur Risikoanalyse aus der Größe des zu erwartenden Schadens einerseits und der Wahrscheinlichkeit des Eintretens des Schadens andererseits. Mit der der Gefährdungsanalyse nachfolgenden Risikobewertung wird festgelegt, welche Schutzziele gelten sollen, d. h. was noch akzeptabel ist und was Maßnahmen erfordert.

Eine solche Analyse beruht immer auf der Annahme, dass Gefahren sowie Wahrscheinlichkeiten objektiv messbar sind. Dabei bleiben die wichtigsten Aspekte der Gefährdung im Grunde genommen unerschlossen. Erstens besteht große Ungewissheit in Bezug auf was wirklich kritisch ist und wie diese Kritikalität zu eruieren ist.[45] Zweitens gibt es Ungewissheit über diverse Aspekte der zu schützenden Infrastruktursysteme.[46] Insbesondere die Interdependenzen zwischen Infrastrukturen stellen Praktiker vor große technische, aber auch analytische Probleme, denn solche Interdependenzen zu erfassen ist für klassische Analysemethoden praktisch unmöglich; ausgeschlossen hiervon sind wohl einzig hochkomplexe Simulationen auf Basis von Agent-Based-Modeling.[47] Der Versuch, mit immer komplexeren Algo-

45 Myriam Dunn: „The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)“, in: International Journal for Critical Infrastructure Protection, 1, 2, 3 (2005), S. 58-68.

46 James A. Lewis: Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Washington D.C.: Center for Strategic and International Studies 2002.

47 Myriam Dunn: The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP).

rithmen zusätzliches Wissen zu generieren ist ein Paradebeispiel für den Umgang mit spezifischem Nichtwissen.

Drittens gibt es nur marginales Wissen bezüglich Akteuren und ihren Fähigkeiten, so dass es unklar bleibt, wie die Gefahr einer großen Cyber-Attacke einzuschätzen ist. Was wir wissen: In den letzten zehn Jahren haben mehrere Mächte mit globalen Ambitionen begonnen, den Cyberspace in ihre nationale Verteidigungsstrategie zu integrieren und mehr oder weniger laut über den offensiven Cyber-Krieg nachzudenken. Ganz allgemein bleibt das Wissen über Cyber-Waffen und deren Einsatz aber höchst spekulativ. Die Geheimdienste verwenden laut eigener Angaben verschiedenste „weiche" Indikatoren als Hinweis auf mögliche offensive Cyber-Kriegsmittel anderer Staaten.[48]

Es liegt in der Natur der Sache, dass die Evaluierung fremder Kapazitäten immer spekulativ bleiben muss. Denn anders als im Bereich der Nuklearwaffen lassen sich sowohl die Herstellung, das Testen wie auch die „Lagerung" von Cyber-Waffen optimal verbergen. Gewissheit über ihre Existenz ist unmöglich, denn eine solche würde das Scannen aller Computer und Speichermedien, einschliesslich klassifizierter Systeme, bedingen.[49] Sogar im Fall eines Angriffs ist es ungemein schwierig, die Urheberschaft nachzuweisen, wenn diese verborgen bleiben will (Stuxnet ist ein schönes Beispiel dafür). Wenn, dann dauert eine solche „Attribution" im besten Fall Monate.

Was wir also nicht wissen: Wer Cyber-Waffen hat, wer sie entwickeln will und wird und vor allem, wer sie auch wirklich einsetzen wird. Amerikanische Experten substituieren dieses spezifische Nichtwissen um Akteure und ihre Fähigkeiten durch eine willentliche Verschiebung des Augenmerks auf neue, besser fassbare Kategorien – und unter aktiver Vertuschung des Nichtwissens. Aus diesem Grund wird in der Cyber-Debatte der Fokus nicht auf Akteure und deren Motivation, sondern hauptsächlich auf Verwundbarkeiten von kritischen Infrastruktursystemen gelegt. Darüber hinaus ist die Praxis der Szenarien-

48 CRS Report for Congress: Information Operations, Electronic Warfare and Cyberwar: Capabilities and Related Policy Issues, Washington DC: Congressional Research Service, Updated 5 June 2007.

49 Dorothy E. Denning: „Obstacles and Options for Cyber Arms Controls", (unveröffentlichtes) Konferenzpapier, 22. Juni 2001, Arms Control in Cyberspace, Heinrich Böll Foundation Berlin, *http://faculty.nps.edu/dedennin/publications/berlin.pdf*.

entwicklung ein typisches Beispiel für den Umgang mit spezifischem Nichtwissen: Szenarien werden als unabdingbar für das Risikomanagement angesehen, da sie mögliche Ereignisse oder Entwicklungen beschreiben und somit die Ungewissheiten der Realität scheinbar vermindern.

Europäische Experten hingegen ersetzen Nichtwissen durch bereits bestehende (amerikanische) Narrationen, inklusive der ihnen innewohnenden strategischen Logik, mit eher zweifelhafter Anwendbarkeit im europäischen Umfeld. Denn viele der Annahmen, deren man sich in der Cyber-Kriegs-Debatte bedient, sind die Ängste einer militärischen Supermacht. Die von den USA mit besonderem Argwohn beäugten Cyber-Kapazitäten sind diejenige ihrer Rivalen, der aufsteigenden Macht China und der absteigenden Macht Russland. Die diesbezüglichen Überlegungen folgen einer konventionell-strategischen Logik, was sich auch im Sprachgebrauch niederschlägt: Man bedient sich des Vokabulars der Nuklearstrategie und weitet diese auf die Cyber-Domäne aus. Die Hauptfrage dabei ist, ob die Cyber-Komponente das gegenwärtige internationale Machtgefüge zu Ungunsten der USA verändern könnte, sei es als ‚Streitkräfte-Verstärker' oder als generelles Abschreckungsmittel.[50]

Im europäischen Kontext wird durch diesen Umgang mit Nichtwissen die Möglichkeit einer breiteren Debatte über Sinn und Unsinn solcher Gefahrenperzeptionen verunmöglicht oder zumindest stark erschwert. Dabei sollte jeder Staat, der den gegen ihn gerichteten bewaffneten Konflikt als unwahrscheinlich erachtet, guten Gewissens den Cyber-Krieg ebenfalls als unwahrscheinlich ansehen; sei es als Kernelement einer lang angelegten militärischen Operation oder in Form eines gegnerischen Angriffs auf Datennetzwerke oder Infrastrukturen.

NICHT-UMGANG MIT UNSPEZIFISCHEM NICHTWISSEN

In der hier betrachteten Generierung von Narrationen durch Sicherheitsexperten wird die zweite Kategorie von Nichtwissen negiert – beziehungsweise befindet sich gewissermaßen selber in der Domäne des

50 Martin C. Libicki: Cyberdeterrence and Cyberwar, Santa Monica: RAND Corporation 2009.

unspezifischen Nichtwissens. Dies ist erklärbar vor dem Hintergrund eines Bedürfnisses nach gesichertem Wissen, welches die Experten bereitstellen sollen und auch wollen. Die Negierung des unspezifischen Nichtwissens ist tatsächlich bereits in die Grundidee einer Risiko- oder Gefährdungsanalyse eingebaut: Zum einen besteht der Anspruch an die Risikoanalyse, dass Resultate geliefert werden, aufgrund derer die als höchstes Risiko eingeschätzten Gebiete eruiert und Pläne zum optimalen Schutz entwickelt werden können. Zum anderen werden so die Ergebnisse in einer Art und Weise aufbereitet, die das Bild einer durch Risikomanagementstrategien bewältigbaren Welt zeichnen.

Und doch wird auch die perfekteste Cyber-Sicherheitsstrategie der Welt nicht dazu führen, dass der digitale Raum gefahrenfrei wird. Der Schutz kann noch so vielfältig und gut sein, Cyber-Kriminalität wird ein Problem bleiben, wie auch die Cyber-Spionage. 100% Sicherheit kann nicht hergestellt werden. Es lässt sich auch nicht ausschließen, dass es zu größeren Störungen in der kritischen Infrastruktur kommen wird, sei es aufgrund von spontanen technischen Störungen oder aufgrund menschlicher Eingriffe. Die umfassende Gewährleistung von Sicherheit durch den Staat ist angesichts der Vielfalt, der Komplexität und der Unvorhersehbarkeit moderner Risiken ohnehin längst nicht mehr möglich (wenn sie es je war).

Gesellschaften müssen also lernen, in pragmatischer Art und Weise mit dieser Unsicherheit zu leben, während der Staat die Verpflichtung hat, sein Möglichstes und Bestes zu geben, um diese Probleme zum Wohle der Allgemeinheit zu minimieren, aber ebenso lernen muss, die Grenzen des Möglichen zu kommunizieren. Durch die Generierung von Narrationen in der erzählten Katastrophe unter Negierung von Nichtwissen wird im schlimmsten Fall die Wahrscheinlichkeit einer Katastrophe erhöht: Denn eine Situation wird erst zur Katastrophe, wenn die Intransparenz der Gefährdungssituation, ein unspezifisches Nichtwissen, nicht als solches kommuniziert wird.[51]

51 K. Japp: Zur Soziologie der Katastrophe, S. 80.

SCHLUSSFOLGERUNGEN

Selbstverständlich soll und muss sich die Sicherheits- und Verteidigungspolitik auch mit sogenannten Worst-Case-Szenarien, also zum Beispiel dem TEOTWAWKI befassen. Aber Worst-Case-Überlegungen dürfen nie auf Kosten anderer, weitaus wahrscheinlicherer bzw. bereits aktueller Phänomene gehen oder zu einer Verzerrung des Bedrohungsbildes führen. Denn: Falls Worst-Case-Vorfällen, die sich immer durch ein sehr hohes Schadensausmaß auszeichnen, trotz ihrer extrem kleinen Eintrittswahrscheinlichkeit ein zu großes Gewicht beigemessen wird, tritt die Frage nach eben dieser Wahrscheinlichkeit in den Hintergrund und mit ihr auch die Forderung nach Beweisen, dass hinter diesen Szenarien nicht nur Spekulationen, sondern auch reale Bedrohungen stecken.

Dies weist auf die Notwendigkeit eines reflexiven Verständnisses und eines bewussten Umgangs mit Nichtwissen beider Gattungen innerhalb von Expertengruppen (und in der Politik) hin. An Vorsorge orientierte Politik darf sich der Problematik von Nichtwissen nicht entziehen. Neben der Bearbeitung von mehr oder weniger wohldefinierbaren Risiken muss untersucht werden, was nicht gewusst und nicht vorhergesehen wird. Darüber hinaus muss in diesem Prozess die Frage gestellt werden, weshalb es nicht gewusst wird, wie unter Bedingungen des Nichtwissens gehandelt und entschieden werden soll und wie Nichtwissen kommunikativ vermittelt werden kann.[52] Den Inhalten von Katastrophennarrationen kommt vor allem beim letzten Punkt eine wichtige Rolle zu.

In diesem Kapitel wurde aufgezeigt, wie die Problematik des Nichtwissen-Könnens explizit häufig bereits Teil der öffentlichen Cyber-Narrationen ist. Nichtwissen sollte jedoch nie als Katalysator und Beweis für die Notwendigkeit von zusätzlichen Sicherheitsanstrengungen verstanden und eingesetzt werden. Ein Verständnis für die Regeln der Sicherheitspolitik mit Verweis auf bestehende Katastrophennarrationen ist dabei zentral, denn ein solches lässt die Beobachtung

52 Stefan Böschen: „Reflexive Wissenspolitik: Zur Formierung und Strukturierung von Gestaltungsöffentlichkeiten“ in: Bogner, Alexander/Torgersen, Helge (Hgg.), Wozu Experten? Ambivalenzen der Beziehung von Wissenschaft und Politik, Wiesbaden: Verlag für Sozialwissenschaften 2005, S. 241-263.

zu, dass ebendiese Regeln eine Übertreibung der Gefahrenlage begünstigen, gar fördern, aber dass diese Übertreibung der Lösung der Problematik nicht förderlich ist. Durch eine ausbalanciertere Darstellung könnte zum Beispiel dem Umstand entgegengewirkt werden, dass die in den Szenarien beschriebenen apokalyptischen Ereignisse aufgrund ihrer Form und Intensität jegliche Vorsorgeplanung eigentlich von vornherein zum Scheitern verurteilen und dass durch die Darstellung der Katastrophe als überaus schrecklich und allumfassend eine ungesunde Priorität der Prävention ganze Gesellschaften in den Zustand des Konjunktivs versetzt.[53]

Dadurch, dass die Angst vor TEOTWAWKI während Jahren so weit gestreut wurde, befindet sich die Gesellschaft in einem Zustand der abwartenden Daueralarmierung. Jeder Vorfall wird zwar mehr oder weniger stark von den durch die Szenarien geformten Erwartungen in Bezug auf Ausmaß und Schrecklichkeit abweichen, diesem Zustand aber dennoch nicht Abhilfe leisten. Vielmehr werden diese Vorfälle, ganz gemäß der Logik, mit der mit Nichtwissen umgegangen wird, weiterhin dafür verwendet werden, das „es hätte noch viel schlimmer sein können" dem „seht ihr, es ist ja gar nicht so schlimm" vorzuziehen. Die „erzählte Katastrophe" sollte jedoch nicht als Beweis für die Notwendigkeit von außerordentlichen Maßnahmen verstanden werden und als Geldmaschine für eine „Industrie" der Angstmache fungieren können. Vielmehr sollte sie als Bild dafür verwendet werden, dass die Katastrophe eben noch nicht eingetreten ist und jeder Gesellschaft deshalb zahlreiche Handlungsoptionen offen stehen. So wird der gegenwärtige Cyber/Un/Sicherheits-Diskurs nicht mehr vor allem zusätzliche und fortwährende Unsicherheit (mit-)schaffen, sondern Wege aufzeigen können, wie in einer zunehmend komplexen und vernetzten Welt ein gesundes Maß von Sicherheit angestrebt und auch erreicht werden kann.

53 U. Beck: Weltrisikogesellschaft.

LITERATUR

Arquilla, John: „The Great Cyberwar of 2002“, in: Wired 6, 2 (1998). *http://www.wired.com/wired/archive/6.02/cyberwar.html*

Baudrillard, Jean: L'échange symbolique et la mort, Paris: Gallimard 1976.

Beck, Ulrich: Die Erfindung des Politischen. Zu einer Theorie reflexiver Modernisierung, Frankfurt a. M.: Suhrkamp 1993.

Beck, Ulrich: Weltrisikogesellschaft. Auf der Suche nach der verlorenen Sicherheit, Frankfurt a. M.: Suhrkamp 2007.

Böschen, Stefan: „Reflexive Wissenspolitik. Zur Formierung und Strukturierung von Gestaltungsöffentlichkeiten“, in: Alexander Bogner/Helge Torgersen (Hgg.), Wozu Experten? Ambivalenzen der Beziehung von Wissenschaft und Politik, Wiesbaden: Verlag für Sozialwissenschaften 2005, S. 241-263.

Bundesministerium des Innern: Cyber Sicherheitsstrategie für Deutschland, Berlin 2011.

Buzan, Barry/Wæver, Ole/de Wilde, Jaap: Security. A New Framework for Analysis, Boulder: Lynne Rienner 1998.

Clarke, Lee: Worst Cases. Terror and Catastrophe in the Popular Imagination, Chicago: University of Chicago Press 2006.

Clarke, Richard/Knake, Robert: Cyber War. The Next Threat to National Security and What to Do About It, New York: Ecco 2010.

Conway, Maura: „Media, Fear and the Hyperreal. The Construction of Cyberterrorism as the Ultimate Threat to Critical Infrastructures“, in: Myriam Dunn Cavelty/Kristian Søby Kristensen (Hgg.), Securing the Homeland: Critical Infrastructure, Risk, and (In)Security, London: Routledge 2008, S. 109-129.

CRS Report for Congress: Information Operations, Electronic Warfare and Cyberwar. Capabilities and Related Policy Issues, Washington DC: Congressional Research Service, Updated 5 June 2007.

De Goede, Marieke: „Beyond Risk: Premediation and the Post-9/11 Security Imagination“, in: Security Dialogue 39, 2-3 (2008), S. 155-176.

Debrix, François: „Cyberterror and Media-induced Fears: The Production of Emergency Culture“, in: Strategies 14, 1 (2001), S. 149-168.

Debrix, François/Barder, Alexander: „Nothing to Fear but Fear. Governmentality and the Biopolitical Production of Terror“, in: International Political Sociology 3, 4 (2009), S. 398-413.

Deibert, Robert/Rohozinski, Rafal: „Risking Security. Policies and Paradoxes of Cyberspace Security“, in: International Political Sociology 4 (2010), S. 15-32.

Denning, Dorothy E.: „Obstacles and Options for Cyber Arms Controls“, (unveröffentlichtes) Konferenzpapier, 22. Juni 2001, Arms Control in Cyberspace, Heinrich Böll Foundation Berlin, *http://faculty.nps.edu/dedennin/publications/berlin.pdf*.

Dunn Cavelty, Myriam: „Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate“, in: Journal of Information Technology and Politics 4, 1 (2007), S. 19-36.

Dunn Cavelty, Myriam: Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, London: Routledge 2008.

Dunn Cavelty, Myriam/Kristensen, Kristian Soby: „Introduction. Securing the Homeland – Critical Infrastructure, Risk, and (In)Security“, in: dies. (Hgg.), The Politics of Securing the Homeland. Critical Infrastructure, Risk and Securitisation, London: Routledge 2008, S. 1-14.

Dunn Cavelty, Myriam/Brönnimann, Gabriel: „E-mail für Dich“, in: Böll Thema 3 (2011), Grenzenlos illegal – Transnationale organisierte Kriminalität, S. 9-10.

Dunn, Myriam: „The Socio-Political Dimensions of Critical Information Infrastructure Protection (CIIP)“, in: International Journal for Critical Infrastructure Protection 1, 2/3 (2005), S. 58-68.

Embar-Seddon, Ayn: „Cyberterrorism. Are we Under Siege?“, in: American Behavioral Scientist 45, 6 (2002), S. 1033-1043.

Foucault, Michel: Die Ordnung des Diskurses. Frankfurt a. M.: Suhrkamp 1997.

Godard, Olivier et al.: Traité des nouveaux risques: précaution, crise, assurance, Collection folio actuel, Paris: Gallimard 2002.

Gorman, Siobhan/Barnes, Julian: „Cyber Combat“. Act of War – Internet Crime Complaint Center: 2010 Internet Crime Report, Washington DC: The National White Collar Crime Center 2011.

Jaeger, Mark Daniel: „The Psychology of Securitization: Pragmatics of Risks, Threats, and Socially Shared Cognition“, Unveröffentlichtes Konferenzpapier, Zürich 2011.

Japp, Klaus P.: „Zur Soziologie der Katastrophe“, in: Lars Clausen/Elke M. Geenen/Elisio Macamo (Hgg.), Entsetzliche soziale Prozesse. Theorie und Empirie der Katastrophen, (Konflikte, Krisen und Katastrophen – in sozialer und kultureller Sicht, Bd. 1), Münster: LIT Verlag 2003, S. 77-90.

Laqueur, Walter: The New Terrorism: Fanaticism and the Arms of Mass Destruction, Oxford: Oxford University Press 1999.

Lewis, James: Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Washington D.C.: Center for Strategic and International Studies 2002.

Libicki, Martin: Cyberdeterrence and Cyberwar, Santa Monica: RAND Corporation 2009.

McLean, Craig/Patterson, Alan/Williams, John: „Risk Assessment, Policy-Making and the Limits of Knowledge. The Precautionary Principle and International Relations“, in: International Relations 23, 4 (2009), S. 548-566.

Melde- und Analysestelle Informationssicherung (MELANI) (Hg.): Informationssicherung – Lage in der Schweiz und International. Halbjahresbericht 2010 (Juli – Dezember), Informatikstrategieorgan Bund: Bern 2011.

Metzger, Jan: „The Concept of Critical Infrastructure Protection (CIP)“, in: Alyson Bailes/Isabelle Frommelt (Hgg.), Business and Security: Public-Private Sector Relationships in a New Security Environment, Oxford: Oxford University Press 2004, S. 197-209.

Panzer, Gerhard: Kairos der „Risikogesellschaft“. Wie gesellschaftstheoretische Zeitdiagnosen mit technischer Unsicherheit umgehen, Kassel: Kassel University Press 2001.

„Pentagon Sets Stage for U.S. to Respond to Computer Sabotage With Military Force“, in: The Wall Street Journal vom 31.05.2011.

Perrow, Charles: Normal Accidents. Living with High-Risk Technologies, New York: Basic Books 1984.

Pollard, Neal: „Indications and Warning of Infrastructure Attack“, in: Lars Nicander/Magnus Ranstorp (Hgg.), Terrorism in the Information Age. New Frontiers?, Stockholm: National Defence College 2004, S. 41-57.

Pollitt, Mark M.: „Cyberterrorism: Fact or Fancy?“, in: Computer Fraud and Security 2 (1998), S. 8-10.

President's Commission on Critical Infrastructure Protection: Critical Foundations: Protecting America's Infrastructures, Washington, DC: US Government Printing Office 1997.

Rieger, Frank: „Trojaner „Stuxnet": der digitale Erstschlag ist erfolgt", in FAZ.net vom 22.09.2010.

Sandwell, Barry: „Monsters in Cyberspace. Cyberphobia and Cultural Panic in the Information Age", in: Information, Communication & Society 9, 1 (2006), S. 39-61.

Slovic, Paul/Fischhoff, Baruch/Lichtenstein, Sarah: „Why Study Risk Perception?", in: Risk Analysis 2, 2 (1982), S. 83-93.

Verton, Dan: Black Ice. The Invisible Threat of Cyberterrorism, New York: McGraw Hill 2003.

Viehöver, Willy: „Die Klimakatastrophe als ein Mythos der reflexiven Moderne", in: Reiner Keller et al. (Hgg.), Handbuch Sozialwissenschaftliche Diskursanalyse, Band I: Theorien und Methoden, Opladen: Leske + Budrich 2003, S. 247-286.

Viehöver, Willy: „Diskurse als Narrationen", in: Reiner Keller et al. (Hgg.), Handbuch Sozialwissenschaftliche Diskursanalyse, Band I: Theorien und Methoden, Opladen: Leske + Budrich, 2001, S. 177-206.

Virilio, Paul: Original Accident, Cambridge: Polity Press 2007.

Williams, Michael J.: „(In)Security Studies, Reflexive Modernization and the Risk Society", in: Cooperation and Conflict 43, 1 (2008), S. 57-79.

Winner, Langdon: „Trust and Terror: The Vulnerability of Complex Socio-technical Systems", in: Science as Culture 13, 2 (2004), S. 155-172.