AIPA 1/2017

Arbeitspapiere zur Internationalen Politik
und Außenpolitik

Stephan Steller

Die Cyber-Sicherheitsstrategie für Deutschland

Lehrstuhl Internationale Politik
Universität zu Köln

ISSN 1611-0072

AIPA 1/2017

Arbeitspapiere zur Internationalen Politik
und Außenpolitik

Stephan Steller

Die Cyber-Sicherheitsstrategie für Deutschland

ISSN 1611-0072

Lehrstuhl Internationale Politik
Universität zu Köln, Gottfried-Keller-Str. 6, 50931 Köln

Redaktionelle Bearbeitung: Nicole Aranibar, Christian Merten

Köln 2017

Abstract

In dieser Arbeit wird die Cyber-Sicherheitsstrategie für Deutschland einer strategischen Analyse unterzogen. Vorfälle wie der NSA-Skandal oder die Veröffentlichung der Panama Papers haben deutlich gezeigt, dass mit der Digitalisierung, neben den vielen Vorteilen, die sie mit sich bringt, auch unzählige Sicherheitsrisiken entstehen. Die jederzeit mögliche Nutzung von Internetdiensten und die weltweite Vernetzung haben einen grundlegenden Wandel in allen gesellschaftlichen Bereichen mit sich gebracht. Um diesen Herausforderungen angemessen begegnen zu können, müssen bei der Ausarbeitung einer Strategie Ziel-Mittel-Umwelt-Kalkulationen berücksichtigt werden, damit die strategischen Zusammenhänge erkannt werden. Durch die vorliegende Analyse wird allerdings deutlich, dass sich die Cyber-Sicherheitsstrategie für Deutschland in ihrer Ausgestaltung eher als Programm denn als Strategie charakterisieren lässt. Die im Bezugsrahmen formulierten Anforderungen, die eine Strategie erfüllen muss, werden nur in einigen Ausnahmen erfüllt. Der Programmcharakter der Strategie wird deutlich durch die starke administrative Ausrichtung und durch die zehn strategischen Bereiche, die hauptsächlich als individuelle Problemfelder begriffen, aber nicht in Beziehung zueinander gesetzt werden. Eine Strategie für die Sicherheit im Cyber-Raum sollte jedoch umfassender konzipiert werden und die internationalen Kontextbedingungen näher betrachten. Für die Konzipierung von zukünftigen Strategien sollten Mitwirkungsinstrumente geschaffen werden, die es der Zivilgesellschaft erlauben, aktiv an der Ausgestaltung von zukünftigen Strategien teilzunehmen.

Keywords: Cyber Security, Strategieanalyse, Sicherheitspolitik, IT-Sicherheit, Cyberkriminalität, Cyberterrorismus, Kritische Infrastrukturen

Stephan Steller

hat Politikwissenschaft an der Universität zu Köln studiert.

Kontakt: stephan-steller@outlook.com

Inhalt

Abbildungsverzeichnis

1 Einleitung

Am 14. Juni 2016 wurde von den VerteidigungsministerInnen der NATO-Mitgliedsländer beschlossen, den Cyber-Raum als offizielles Operationsgebiet anzuerkennen. Damit werden Ereignisse im Cyber-Raum so behandelt wie Angriffe in den bereits existierenden Gebieten Luft, Wasser und Land. Dadurch wird die Bedeutung des digitalen Raums auf eine neue Stufe gehoben, da ein Cyber-Angriff den Bündnisfall nach Artikel 5 des Nordatlantikvertrages auslösen könnte. Die Sicherheit des Cyber-Raums hat somit höchste Priorität, was bedeutet, dass Maßnahmen der Cyber-Abwehr künftig in alle strategischen und militärischen Planungen miteinbezogen werden müssen.

Aber nicht nur in politischen und militärischen Angelegenheiten, sondern auch in fast allen Bereichen des täglichen Lebens nimmt der Einfluss des Cyber-Raums stetig zu. Sinnbildlich dafür stehen der NSA-Skandal, die Luxemburg Leaks, Cablegate und die Panama Papers. Veröffentlichungen von geheimen Daten, diplomatischen Berichten und zweifelhaften politischen Praktiken werden in diesem Ausmaß durch den digitalen Cyber-Raum überhaupt erst durchführbar.

Die Digitalisierung macht es möglich, gewaltige Datenmengen zu entwenden und per Mausklick an Dritte weiterzugeben. Vorfälle dieser Art zeigen deutlich, dass mit der Digitalisierung, neben den vielen Vorteilen, die sie mit sich bringt, auch unzählige Sicherheitsrisiken entstehen. Die jederzeit mögliche Nutzung von Internetdiensten und die weltweite Vernetzung haben einen grundlegenden Wandel in allen gesellschaftlichen Bereichen mit sich gebracht. Durch den Modernisierungsschub entstanden neue Wirtschaftsbereiche und das Kommunikationsverhalten änderte sich grundlegend. Mit diesen Chancen wurden jedoch Sicherheitslücken geschaffen, die von Kriminellen, Terroristen, Hackern, aber auch Geheimdiensten genutzt werden können. Kreditkartenbetrug, Industriespionage und Identitätsdiebstahl sind mit den Möglichkeiten des Cyber-Raums um ein Vielfaches einfacher geworden, während Cybermobbing, Angriffe auf Kritische Infrastrukturen und Mas-

senüberwachung dadurch überhaupt erst möglich wurden (vgl. BSI 2015, S. 6-7). Als Folge der weltweiten Vernetzung entstehen hierbei neue Unsicherheiten, die vom Staat reduziert werden müssen, um Sicherheit im täglichen Leben zu gewährleisten.Dafür wurde 2011 die Cyber-Sicherheitsstrategie für Deutschland vom Bundesministerium des Innern ausgearbeitet, welche den Nationalen Plan zum Schutz der Informationsinfrastrukturen (NPSI)[1] ersetzt.

Im Rahmen dieser Arbeit soll die Cyber-Sicherheitsstrategie für Deutschland aus strategischer Perspektive analysiert werden. Erkenntnisziel der vorliegenden Untersuchung ist es, herauszufinden, ob die deutsche Cyber-Sicherheitsstrategie die Anforderungen erfüllt, die an eine politische Strategie gestellt werden. Dabei werden die Stärken, Schwächen und Leerstellen des Sicherheits-Konzepts einer strategiespezifischen Evaluation unterzogen. Für die Evaluation der Strategie wird der von Ralf Tils (2005) konzeptualisierte *approach* der politischen Strategieanalyse verwendet.

Angeleitet durch den Titel *Cyber-Sicherheitsstrategie* wird das methodische Vorgehen dieser Arbeit an den drei Begriffen ausgerichtet und unterteilt. Nach der Einleitung werden in Kapitel 2 zunächst die Eigenschaften beschrieben, die den Cyber-Raum charakterisieren (2.1) und anschließend die unterschiedlichen Gefahren und Bedrohungen im virtuellen Raum für ein besseres Verständnis klassifiziert (2.2). Die verschiedenen Angriffsmittel und -methoden werden vorgestellt, damit ein umfassendes Bild der allgemeinen Cyber-Bedrohungslage entsteht.

Das dritte Kapitel beschäftigt sich mit dem Konzept der Sicherheit. Es wird dargelegt, was unter dem Zustand der Sicherheit zu verstehen ist und was es bedeutet, wenn dieser Zustand im Cyber-Raum hergestellt werden soll (3.1). Dabei wird veranschaulicht, dass eine simple Übertragung des Sicherheitsbegriffs auf den Cyber-Raum nicht genügt, sondern dass im digitalen Raum andere Gesetzmäßigkeiten gelten, die Regierungen vor neue Herausforderungen stellen. Des Weiteren werden die Bedeutung der kritischen Infrastrukturen für die Cyber-Sicherheit auf-

[1] Der Lesbarkeit halber im Folgenden als NPSI abgekürzt.

gezeigt und demokratiepraktische Probleme (3.2) angesprochen, die durch Maßnahmen im Cyber-Raum entstehen.

Im Zentrum des vierten Kapitels wird der von Tils (2005) entwickelte analytische Bezugsrahmen vorgestellt. Die elf verschiedenen Kriterien werden als Evaluationsraster verwendet und es werden Ergänzungen und Modifikationen vorgenommen, damit der für den Cyber-Raum wichtige internationale Kontext politischer Gestaltung in die Analyse mit einbezogen wird.

In Kapitel 5 wird die Cyber-Sicherheitsstrategie mithilfe des analytischen Bezugsrahmens einer kritischen Analyse unterzogen. Zu analysieren ist, ob die Strategie im *Policy*-Feld verharrt oder ob auch *Politics*-Gesichtspunkte bei der Ausgestaltung der Konzeption berücksichtigt wurden. Es wird also gefragt, ob nur auf inhaltlicher Ebene Empfehlungen und Entwürfe vorgelegt werden oder ob diese auch darauf ausgelegt sind, im politischen, wirtschaftlichen und gesellschaftlichen System von Institutionen ausgeführt zu werden.

Die Cyber-Sicherheitsstrategie wird in dieser Arbeit einer genauer untersucht, da das Leben in modernen Gesellschaften mittlerweile kaum noch ohne die technischen Innovationen des virtuellen Raumes vorstellbar ist. In den kommenden Jahren wird sich der Einfluss des Cyber-Raums noch weiter ausdehnen und sich vor allem die *Cloud*-Nutzung weiter verstärken (vgl. BSI 2015, S. 9). Damit steigt zum einen die Abhängigkeit der Gesellschaft von einem funktionierenden Cyber-Raum und durch die „Abhängigkeiten zwischen einzelnen Sektoren oder Branchen wird das Risiko von Ausfällen noch verstärkt“ (BSI 2015, S. 42).

Eine effektive Cyber-Strategie ist somit erforderlich, um die Gefahren des Cyber-Raums einzudämmen und die Innovationen im digitalen Raum zu unterstützen. Eine Analyse der Strategie kann einen realpolitischen Ertrag liefern und gleichzeitig Optimierungspotenziale für die Strategiebildung aufzeigen.

2 Cyber

Der Begriff Cyber ist laut Duden ein Präfix und wird als Wortbildungselement verwendet, wenn von der durch Computer erzeugten virtuellen Scheinwelt gesprochen wird. Das Wort wird abgeleitet vom englischen Begriff *cybernetics*, der die wissenschaftliche Forschungsrichtung bezeichnet, bei der die Steuerung und Regelung von Maschinen untersucht wird (Duden 2016). Cyberspace ist eine Wortschöpfung, die durch die Kombination der Wörter *cybernetics* und *space* entsteht. Die Raum *(space)* - Metapher wurde von Autor William Gibson (1984) geprägt und später von John Perry Barlow (1990), der 1990 die Electronic Frontier Foundation gründete, in den politischen Bereich eingeführt. Damit sollte deutlich gemacht werden, dass mit der Entwicklung von Computern ein neuer Ort entstand, der in Anspielung auf die *western frontier*, unerforscht und frei von sozialen Einschränkungen ist (Dunn Cavelty 2013, S. 107). Dies ist eine von vielen Möglichkeiten, wie das Konstrukt *Cyber-Raum* verstanden und dargestellt werden kann.

Bruce Sterling und John Barlow erfassen den Cyber-Raum vor allem als einen digitalen Raum, der sich zwischen den einzelnen Netzwerkkomponenten konstituiert und in dem kommuniziert wird. Für Sterling (1994, S. 9) ist es „der unbestimmte Ort dort draußen […] der Raum zwischen den Telefonen“, wo sich Menschen treffen und kommunizieren). In der Unabhängigkeitserklärung des Cyberspace beschreibt Barlow, dass die virtuelle Welt aus Transaktionen und Beziehungen besteht. Weiter schreibt er, „dass es eine Welt ist, die zugleich überall und nirgends ist“ – „die neue Heimat des Geistes“ (Barlow 1996). Deibert und Rohozinski (2010, S. 16) beschreiben den Cyberspace ebenfalls als virtuellen Raum, verweisen aber ebenso darauf, dass es einen materiellen Bereich gibt. Ohne diese physische Infrastruktur könnte der Cyber-Raum nicht existieren. Sie verstehen den Cyber-Raum folglich als einen Raum, der aus verschiedenen Ebenen besteht, einer physischen Ebene und einer Informationsebene.

Der Cyber-Raum lässt sich aber auch als Ökosystem begreifen. In wissenschaftlichen Arbeiten der Computer- und Informationswissenschaften wird der Cyber-Raum häufig mit einem Ökosystem verglichen, um die Verflechtungen und wechselseitigen Abhängigkeiten in einem bestimmten Rahmen darzustellen und besser begreifbar zu machen. Das Ökosystem, welches Lebensraum für unterschiedliche Spezies bietet, wird dem Cyber-Raum gleichgesetzt, in dem sich spezifische Technologien gegenseitig beeinflussen, weiterentwickeln und sich entweder an die neue Umgebung anpassen oder eventuell obsolet werden (Adomavicius et al. 2004; Dhamdhere und Dovrolis 2011; Grunwald 2012). Diese Metapher verdeutlicht die Komplexität des Cyber-Raums und wie die unterschiedlichen Einflussfaktoren das Gesamtsystem ständig verändern, erneuern und weiterentwickeln.

Das U. S. Department of Homeland Security spricht in einem White Paper über Eigenschaften, die nötig sind für ein gesundes und widerstandsfähiges Cyber-Ökosystem. Beim Umgang mit Angriffen und der Gefahrenabwehr vergleicht das U. S. Department den Cyber-Raum mit dem menschlichen Immunsystem. In einem komplexen System mit einer mehrstufigen Verteidigung sollen Angriffe erkannt, abgewehrt und Gegenmaßnahmen eingeleitet werden (Department of Homeland Security 2011).

Moore, Parrott und Karas sowie auch Lapointe beschreiben in ihren Arbeiten weitere Metaphern, mit denen versucht wird, den Cyber-Raum besser erklären zu können, indem man ihn mit anderen Systemen vergleicht. So wird der Cyber-Raum unter anderem mit dem öffentlichen Gesundheitssystem verglichen, mit einem Schlachtfeld, einem öffentlichen Gut oder einem freien Markt (Moore et al. 2008; Lapointe 2011).

Metaphern werden verwendet, da sie ein wesentlicher Bestandteil menschlichen Denkens und der Kommunikation sind (Moore et al. 2008, S. 34). Mithilfe von diesen Metaphern kann die Komplexität des Cyber-Raums verständlicher gemacht und Diskussionen können zielgerichteter geführt werden. Wenn Metaphern verwendet werden, kann dies somit sehr hilfreich sein, um abstrakte Themen zugängli-

cher zu machen. Jedoch besteht dadurch auch die Gefahr, dass sich der Blick auf das gesamte System eingeschränkt, da mit Metaphern die Diskussionen in bestimmte Richtungen gelenkt werden und dadurch eine differenzierte Herangehensweise vermieden wird. Die vereinfachte Sichtweise kann also negative Auswirkungen haben, weil der Gesamtkontext aus dem Blick gerät. Es kann sogar dazu führen, dass der eigene Standpunkt nicht mehr in Frage gestellt wird, was dazu führt, dass eine Metapher nicht mehr zu einer konstruktiven Debatte beiträgt, sondern den Diskurs möglicherweise verkompliziert (Lapointe 2011, S. 18). Wenn ein Dialog über den Cyber-Raum stattfindet, die Teilnehmer aber unterschiedliche Metaphern des Cyber-Raums als Diskussionsgrundlage verwenden, wird es wesentlich schwieriger, gemeinsame Lösungen zu finden. Wird der Cyber-Raum als Schlachtfeld, Ökosystem oder öffentliches Gut dargestellt, so wird der Begriff sofort mit spezifischen Attributen assoziiert. Dies hat zur Folge, dass es bei Diskussionen um den Cyber-Raum häufig darum geht, wie dieser virtuelle Raum entweder eingegrenzt und dominiert werden kann, oder wie die Offenheit und der dezentrale Charakter des Internets beibehalten werden können (Dunn Cavelty 2013, S. 107-108).

Die Art und Weise, wie über den Cyber-Raum nachgedacht wird und welche Metaphern verwendet werden, um die Diskussion zu führen, hat demzufolge Konsequenzen auf das anschließende Vorgehen und auf die Ausarbeitung der Strategie (Betz und Stevens 2011, S. 36). Wenn beispielsweise der Cyber-Raum als rechtsfreier Raum dargestellt wird, der frei von Regeln und Zwängen ist, dann kann leichter für restriktive Mittel argumentiert werden, um dadurch Sicherheit herzustellen und zu gewährleisten. Wird hingegen der Cyber-Raum als Plattform für Informationsaustausch dargestellt, werden die Vorteile der Digitalisierung in den Vordergrund gerückt und es wird deutlich gemacht, dass die Offenheit des Internets ein zu schützendes Gut ist. Dementsprechend werden dann die Strategien freiheitlicher ausgelegt, um die Innovationskraft des Cyber-Raums nicht zu beschränken.

Für die Analyse der Cybersicherheitsstrategie für Deutschland ist es folglich von wesentlicher Bedeutung, wie der Cyber-Raum in der Strategie definiert wird

und ob bestimmte Metaphern verwendet werden, die die Auseinandersetzung mit dem Cyber-Raum beeinflussen und die Diskussion in eine spezielle Richtung lenken.

2.1 Cyber-Raum

Unter Zuhilfenahme von Metaphern wird versucht, den Cyber-Raum bildlicher darzustellen, um dieses komplexe Konstrukt besser begreifbar zu machen. Wodurch wird der Cyber-Raum jedoch begrenzt und welches sind die charakteristischen Merkmale, die den Cyber-Raum definieren?
Das U. S. Verteidigungsministerium definiert den Cyber-Raum wie folgt:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Department of Defense 2010, S. 58)

Diese Definition verdeutlicht, dass das Internet nicht mit dem Cyber-Raum gleichzusetzen ist, sondern das Internet nur einen Teil des Cyber-Raums ausmacht. Es werden folglich auch Technologien mit eingebunden, die auf den ersten Blick nichts mit dem Internet zu tun haben. Desweiteren zeigt der Begriff *Domain*, dass der Cyber-Raum mehr umfasst als nur den materiellen Raum. Immaterielle Dinge wie die virtuelle Realität und Ideen sind auch Teil des Cyber-Raums (Deibert und Rohozinski 2010a, S. 15).

Bedeutende Merkmale des Cyber-Raums sind insbesondere die transnationale Organisation und dass der Cyber-Raum ein Kommunikationsnetzwerk ist. Die dezentrale Organisation wird nicht durch institutionelle staatliche Strukturen bestimmt. Vielmehr sind es unzählige, über die ganze Welt verstreute, kleinere Netzwerke, die verbunden miteinander den Cyber-Raum ergeben. Dieses besondere Strukturmerkmal bedeutet natürlich auch, dass kein einzelner Staat den Cyber-Raum kontrollieren kann und es somit keine zentrale Steuerung und auch keine Instanz gibt, die den Informationsfluss reguliert (Dutton und Peltu 2007, S. 71). Vie-

le unterschiedliche Institutionen wie die Internet Corporation for Assigned Names and Numbers (ICANN), die Internet Society (ISOC) oder die Internet Engineering Task Force (IETF) haben bestimmte Befugnisse. Jede dieser Institutionen hat einen spezifischen Aufgabenbereich, für den sie verantwortlich ist, aber keine davon ist in der Position, die Strategie des Cyber-Raums im Gesamten zu steuern.

Das Kommunikationsnetzwerk wird hauptsächlich verwendet, um Informationen auszutauschen und miteinander zu kommunizieren. Dabei sind verschiedene Kommunikationsformen zu unterscheiden. Menschen können mit anderen Menschen in Kontakt treten (Mensch-Mensch), Menschen können mit Systemen kommunizieren (Mensch-Maschine) oder im Falle der elektronischen Kommunikation kontaktieren Maschinen andere Maschinen (Maschine-Maschine). Des Weiteren lassen sich auch Kommunikationsinhalte in verschiedene Teilbereiche einordnen (z. B. grundrechtsrelevante Kommunikation oder kriminelle Kommunikation) (Bötticher 2015, S. 74).

Diese global miteinander verbundene Informationsinfrastruktur zeichnet sich durch Offenheit und Interoperabilität aus. Die Fähigkeit zu einer reibungslosen Zusammenarbeit zwischen verschiedenen Systemen trägt dazu bei, dass sich eine Person mit einem geeigneten Gerät jederzeit und überall Zugang zu dem Netzwerk verschaffen kann (WSIS 2005). Eine Strategie sollte demnach die dezentrale Organisation des Cyber-Raums beachten und die Zusammenarbeit zwischen heterogenen Systemen gewährleisten, damit die Kommunikation zwischen den global miteinander verbundenen Netzwerken weiterhin sichergestellt ist.

Ein weiteres kennzeichnendes Merkmal ist die Netzwerkstruktur des Cyber-Raums. Der Raum setzt sich zusammen aus unzähligen privaten und öffentlichen Netzwerken. Komponenten der Kommunikationsinfrastruktur, wie z. B. Unterseeglasfaserkabel oder auch Satelliten, sind zum Teil in staatlicher Hand. Andere Komponenten der Infrastruktur liegen jedoch in privater Hand. Die Internetknotenpunkte, die als Austauschpunkte für den Datenverkehr dienen, werden von privaten Unternehmen betrieben, genau wie die Internetdienstanbieter, die an diesen

Netzknoten miteinander verbunden sind. Der Cyber-Raum wird folglich charakterisiert durch einen Mix an staatlicher und privater Infrastruktur und öffentlichen und privaten Netzwerken, was eine zentrale Steuerung des Systems praktisch unmöglich macht. Im Falle der Cyber-Sicherheitspolitik führt dies zu „einer politischen Struktur [...], die auf den Prinzipien Kooperation, Koordination und Kooptation basiert und keinen dominanten einheitlichen Akteur kennt, der ihre Funktionslogik maßgeblich beeinflussen würde“ (Bendiek 2012, S. 24). Eine Strategie für den Cyber-Raum ist somit auf Kooperation zwischen den zahlreichen heterogenen Akteuren angewiesen. Desweiteren müssen Maßnahmen aufgrund der transnationalen Organisation koordiniert werden, um effektiv wirken zu können und durch Kooptation müssen Stakeholder, die eine bedeutende Stellung im Cyber-Raum einnehmen, nachträglich eingebunden werden, um an Entscheidungsprozessen teilnehmen zu können. Dafür eine Basis zu schaffen, ist die Aufgabe einer Strategie.

Ein zusätzliches Merkmal des Cyber-Raums ist es, dass er – im Gegensatz zu den Bereichen Luft, Wasser, Land und Weltraum – von Menschen erschaffen wurde. Diese virtuelle Umwelt wird ständig neu strukturiert. Grundsätzlich wird der Raum also nur begrenzt von der Partizipation der NutzerInnen und deren Einfallsreichtum (Nissenbaum 1998, S. 576). Das Ende-zu-Ende-Prinzip macht es einzelnen NutzerInnenn möglich, neue Technologien, Codes oder Programme in den Cyber-Raum einzuführen. Jede Person mit Zugang zum Cyber-Raum kann demnach neue Ideen im Cyber-Raum verbreiten oder schon bestehende weiterentwickeln. Durch die Vielzahl an heterogenen NutzerInnen entstehen somit konstant neue Innovationen, die den ständigen Wandel des Cyber-Raums vorantreiben. Diese sehr hohe Innovationsfrequenz führt „einerseits zu Wohlstand und Wachstum, andererseits können Innovationen des IKT-Bereichs neue Sicherheitslagen darstellen“ (Bötticher 2015, S. 71-72). Jeder Nutzer kann folglich nicht nur hilfreiche Innovationen in den Cyber-Raum einführen, sondern auch Schadprogramme verbreiten und sich illegal Zugang zu Daten verschaffen. Dies stellt ein massives Problem für Regulierungsbehörden dar, da sich der Cyber-Raum in einer ständigen Transformation befindet

und sich somit die Sicherheitslagen auch fortwährend ändern (Deibert und Rohozinski 2010, S. 16). Eine Strategie sollte demnach präzise genug gefasst sein, um bestehende Gefahrenquellen zu bekämpfen. Gleichzeitig sollte die Strategie aber auch flexibel genug sein, um auf die ständig wechselnden Gefahrenlagen angemessen reagieren zu können.

Die bereits angeführte Definition des Cyber-Raums von Deibert und Rohozinski beschreibt, dass dieser nicht nur aus einem materiellen Bereich, sondern auch aus einem virtuellen Bereich besteht. Dies ist ein weiteres Merkmal, das verdeutlicht, wie der Cyber-Raum aufgebaut ist. Die Hardware bildet eine Basis für den virtuellen Raum. Die großen Fortschritte in diesem Bereich haben unseren Umgang mit Informationen in den letzten Jahrzehnten wesentlich beeinflusst. Hauptgrund dafür sind ein massiver Preisrückgang was digitalen Speicherplatz betrifft und enorme Fortschritte bei der Rechenleistung (Nissenbaum 1998, S. 576). Diese Entwicklungen bedeuten: a) dass es praktisch keine Grenzen bei der Datenerfassung gibt, b) dass es praktisch keine Begrenzung für den Umfang einer Analyse gibt – nur begrenzt durch menschlichen Einfallsreichtum – und c) dass die Informationen praktisch für immer gespeichert werden können (Nissenbaum 1998, S. 576). Für Institutionen und Unternehmen bedeuten diese Weiterentwicklungen, dass nun riesige Datenmengen leicht zu verwalten sind und mit relativ wenig Aufwand analysiert werden können. Informationen, die bereits seit Jahrzehnten öffentlich sind, können so mithilfe der Digitalisierung in Datenbanken eingepflegt werden und mit speziellen Programmen für bestimmte Zwecke ausgewertet werden. Während einzelne Daten nicht sehr aussagekräftig sind, können viele Metadaten, zusammengesetzt durch ein intelligent programmiertes Analysetool, ein sehr exaktes Bild erstellen. Die neuen Möglichkeiten, große Mengen von Daten zu bearbeiten, stellen eine Herausforderung für den Datenschutz dar. Der Schutz von Daten – von Unternehmen, Institutionen und auch privaten BürgerInnen – sollte bei der Ausarbeitung einer Strategie beachtet werden.

Die Offenheit der Informations- und Kommunikationstechnologien fördert Innovationen und die freie Meinungsäußerung und ist somit eine wichtige Quelle für Wirtschaftswachstum. Durch die Vorteile der Digitalisierung wächst der digitale Wirtschaftssektor, was dazu führt, dass die Wirtschaft sowie die Gesellschaft und die Regierungen zunehmend abhängiger von der digitalen Infrastruktur werden, um ihre wesentlichen Aufgaben durchzuführen (OECD 2012, S. 5). Mit der immer größer werdenden Abhängigkeit vom Cyber-Raum gehen auch Verwundbarkeiten einher. Gleichzeitig wurden durch die Fokussierung auf die wirtschaftlichen Vorteile der Digitalisierung Sicherheitsaspekte lange vernachlässigt (von Heinegg 2015).

Besonders in der Wirtschaft ist eine steigende Abhängigkeit der Unternehmen von der Informationstechnik erkennbar (Bundeskriminalamt 2014, S. 13). Produktionsprozesse werden zunehmend mit einer webbasierten Steuerung durchgeführt und sind damit auf die ständige Verfügbarkeit des Netzes angewiesen. Aus der großen Abhängigkeit resultiert ein sehr hohes Bedrohungspotenzial für die Wirtschaft und Schädigungen der IT-Infrastruktur führen nicht nur zur Störung der Kommunikation, „sondern vielmehr auch zum kompletten Produktionsstillstand, was enorme Verluste für Unternehmen nach sich ziehen würde“ (Bundeskriminalamt 2014, S. 13).

Wenn diese unterschiedlichen Merkmale nun miteinander verbunden werden, wird offensichtlich, welch komplexes Gebilde der Cyber-Raum darstellt. Vernetzte Computer haben die Grenzen des territorialen Nationalstaates aufgelöst und machen es ungleich schwerer, für Sicherheit im Cyber-Raum zu sorgen, da Kriminelle ihre Identität und ihren Standort verschleiern können (Hansen und Nissenbaum 2009, S. 1161).

Durch die hohe Innovationsfrequenz im entgrenzten Cyber-Raum verändern sich die Gegebenheiten ständig. Der globale Aufbau des Cyber-Raums mit seiner dezentralen Organisation und der vorherrschenden Anonymität ist für Kriminelle somit ein willkommenes Umfeld. Der Cyber-Raum wurde vollkommen durch den Menschen erschaffen und folglich spiegelt sich in dieser Umwelt auch das menschli-

che Verhalten wider. Zu erkennen ist, dass bei steigender Nutzerzahl auch ein Anstieg der Kriminalität im Netz feststellbar ist (Bötticher 2015, S. 89). Bedrohungen, die in der realen Welt vorkommen und von Menschen ausgehen, existieren somit auch in der virtuellen Welt. Darüber hinaus schaffen die charakteristischen Merkmale des Cyber-Raums ein Umfeld, welches es ermöglicht, dass nicht nur von Gruppen, sondern auch von einzelnen NutzerInnen eine sehr große Gefahr ausgehen kann.

2.2 Gefahren und Bedrohungen im Cyber-Raum

Die oben beschriebenen Merkmale charakterisieren nicht nur den Cyber-Raum, sondern beeinflussen auch gleichzeitig, welche Methoden für Cyber-Angriffe gewählt werden können und welche Bedrohungslage daraus resultiert. Die unterschiedlichen Merkmale des Cyber-Raums bilden zusammengefügt eine Basis für das künftige Handeln im Cyber-Raum. Ausgehend davon können Schwachstellen im System geschaffen und ausgenutzt werden. Durch die bereits erwähnte hohe Innovationsfrequenz im Cyber-Raum bilden sich auch im Kriminalitätsbereich ständig neue Angriffsmittel und –methoden heraus.

Da der Cyber-Raum eine vom Menschen geschaffene Umwelt ist, existieren in ihm auch die gleichen Bedrohungen wie in der realen Welt. Neben Bedrohungen, die überhaupt erst durch den Cyber-Raum entstehen, kann der Cyber-Raum selbst, also seine physische Komponente, bedroht sein. Das Bundeskriminalamt versteht unter Cybercrime „Straftaten, die unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen werden“ (Bundeskriminalamt 2016). Dabei wird unterschieden zwischen Computerkriminalität, dem Internet als Tatmittel und der Bedrohung der IT-Infrastruktur.

Werden die Gefahren, die im Cyber-Raum allgegenwärtig sind, operationalisiert, so findet eine Transformation von Gefahr zu Risiko statt. Die unterschiedlichen Risikodimensionen überlagern sich in der Regel und lassen sich auf den Cy-

ber-Raum übertragen. Dabei unterscheidet Bötticher zwischen sieben unterschiedlichen Risikodimensionen (Bötticher 2015, S. 83).

Die physische Risikodimension umfasst die Zerstörung von Objekten und kann im digitalen Raum auf die Vernichtung von Daten übertragen werden. Die persönliche Risikodimension, also die Zerstörung von Subjekten, kann mit dem Identitätsdiebstahl im Cyber-Raum verglichen werden. Die Zerstörung der psychischen Gesundheit durch z. B. Cyber-Mobbing ist Teil der psychologischen Risikodimension. Die kohärente Risikodimension umfasst dynamische Risiken, die Prozessleitsysteme mit sich bringen. Ökonomische Risiken entstehen durch die Vernetzung des Cyber-Raums, indem Programmierfehler Schäden im globalen Bankensektor nach sich ziehen können. Die politische Risikodimension wird durch die digital organisierten Revolutionen in Nordafrika deutlich. Und die vitale Risikodimension begreift die virtuelle Welt als ökologisches System, in dem die Informationsgesellschaft vom Cyber-Raum als Infrastruktur abhängig ist (Bötticher 2015, S. 86).

Myriam Dunn Cavelty (2013) entwickelte ein Schema, mit dem die unterschiedlichen Bedrohungen kategorisiert und klassifiziert werden können. Das ausgearbeitete Schema wird in diesem Abschnitt verwendet, um einen Überblick über die verschiedenen Bedrohungsarten zu erhalten und eine Einordnung der Risikodimensionen vorzunehmen. Damit soll deutlich gemacht werden, von wem oder was Bedrohungen ausgehen, wer bedroht wird und wie sich diese Bedrohungen auswirken. Dies zu wissen, ist von wesentlicher Bedeutung bei der Ausgestaltung einer Strategie. Denn nur wenn die Gefahrenlage deutlich ist, kann angemessen und vor allem effektiv darauf reagiert werden. Dies ist essentiell für die Konzeption einer Strategie und somit auch hilfreich bei der Analyse einer Strategie, da sich auf diese Weise die nötigen Schwerpunkte identifizieren lassen, mit der sich eine Cybersicherheitsstrategie befassen muss.

Interessant ist hierbei, dass Fragen zur Cybersicherheit lange keine bedeutende Rolle spielten, obwohl das Internet eine militärische Entwicklung war. Fragen der Sicherheit sind also direkt mit der Entwicklung des Cyber-Raumes verknüpft,

aber dessen ungeachtet wurde auch die Netzpolitik von den Parteien lange Zeit stiefmütterlich behandelt (Bötticher 2015, S. 75; Bendiek 2013). Dabei ist laut BKA (Bundeskriminalamt) eine kontinuierlich steigende Kriminalitätsentwicklung in diesem Bereich zu bilanzieren „was zwangsläufig zu einer Steigerung der Bedrohungslage und damit einhergehend auch zu einer weiter zunehmenden Gefährdung von Privaten, Unternehmen und staatlichen Einrichtungen führt“ (Bundeskriminalamt 2014, S. 12). Alle Sektoren, die den Cyber-Raum verwenden, sind somit auch den Cyberbedrohungen ausgesetzt.

Abb. 1 Die drei Bedrohungsarten

	Technological Cluster	Socio-Political Cluster	Human-Machine Cluster
Threat	Malware Network disruptions Advanced Persistent Threats (Malware)	Hackers (all kinds) Cyber-criminals (Nonstate) Cyber-spies (State) Cyber-terrorists (Nonstate) Cyber-commands (State)	Complexity Disruptions in critical infrastructures Cascading effects (Catastrophic) attacks on critical infrastructures
Threat Representation	Virus Intruders Weapons	Lawlessness Anonymity	Vulnerabilty Unknowability Inevitability

(Quelle: Dunn Cavelty 2013, S. 109)[2]

2.2.1 Technischer Bereich

Die unterschiedlichen, im Cyber-Raum vorzufindenden Bedrohungsarten wurden von Dunn Cavelty in drei Gruppen gegliedert. Die erste Gruppe *Technological Cluster* umfasst Bedrohungen aus dem technischen Bereich. Schadprogramme, Netzwerkunterbrechungen und Advanced Persistent Threats (APTs) stellen in diesem Bereich die Bedrohungen dar (Dunn Cavelty 2013, S. 109). Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sind APTs „zielgerichtete Cyber-Angriffe auf sehr stark eingegrenzte Systeme und Netzwerke“ (BSI 2015, S. 27). Ziel

[2] Eigene Darstellung.

der Angriffe sind vor allem die öffentliche Verwaltung, Forschungseinrichtungen, der Rüstungssektor und Hochtechnologien (Auto-/Schiffsbau, Raumfahrt). In diesen Sektoren werden Netzwerke und Computerprogramme hauptsächlich dafür verwendet, um technische Prozesse zu überwachen und zu steuern. Bei SCADA-Systemen wurde bei der Planungsphase die Informationssicherheit in der Sicherheitsarchitektur oft vernachlässigt oder nicht berücksichtigt, da sie als geschlossene Netze betrieben wurden. Wie im Fall von Stuxnet, als das iranische Atomprogramm mit einem Cyber-Angriff attackiert wurde (Farwell und Rohozinski 2011), können aber durch externe Geräte oder USB-Schnittstellen diese geschlossenen Netze mit Schadprogrammen infiziert werden. Eine weitere Gefahrenquelle für diese Systeme kam mit der Entwicklung hin zum *Internet der Dinge* dazu. Mit der intelligenten Vernetzung von Geräten und Maschinen werden Prozesse durch den Informationsaustausch zwischen den einzelnen Netzwerkkomponenten optimiert. Jedoch steigen damit auch die Anforderungen bei der Sicherheitsarchitektur und ein Ausfall eines solchen Netzwerkes hätte weitreichende Folgen. Der Ausfall eines solchen Systems als Folge eines Cyber-Angriffs kann laut Guus Dekkers, CIO (Chief Information Officer) der Airbus Group, „maßgeblich die Reputation und das Wachstum eines Unternehmens beeinflussen“ (BSI 2016, S. 10). Dieser drohende Imageverlust führt dazu, dass geschädigte Unternehmen Straftaten häufig nicht anzeigen, um im Kundenkreis das Image des sicheren und zuverlässigen Partners zu wahren (Bundeskriminalamt 2014, S. 5). Dies ist ein großes Problem für die Bekämpfung von Cyberkriminalität, da die Strafverfolgungsbehörden die durchgeführten Angriffe analysieren müssen, um die Kriminalitätsbekämpfung zu optimieren. Wird ein Großteil der Angriffe nicht gemeldet, so entsteht kein umfassendes Gesamtbild der Gefahrenlage. Dieses ist aber nötig, denn nur dann können Bekämpfungs- und Präventionsstrategien effektiv entwickelt werden. Für die deutsche Cybersicherheitsstrategie ist es somit unbedingt notwendig, dass Unternehmen und andere Institutionen Informationen weiterleiten, wenn diese Opfer von Cyber-Angriffen wurden. Die Meldung von Cyber-Angriffen muss in einer Weise geregelt werden, dass Unternehmen

keinen Imageverlust fürchten müssen und darüber hinaus auch noch einen Anreiz haben, diese Angriffe zu melden. Wie eine vertrauliche Zusammenarbeit zwischen staatlichen Behörden und privaten Unternehmen geregelt sein muss und welche Anreize notwendig sind, um Angriffe zu melden, sollte in einer Cyber-Sicherheitsstrategie formuliert werden.

In diesem technischen Bereich werden Netzwerke durch Viren und Cyber-Waffen bedroht. Manche dieser Cyber-Waffen sind wie im Fall von Stuxnet hochentwickelte digitale Waffen, die mit einem hohen Personal- und Kostenaufwand für ein bestimmtes Ziel entwickelt wurden. Andere Schadprogramme wie der *Morris Worm* oder der *I-love-you-Virus* wurden von einzelnen NutzerInnen programmiert, verbreiteten sich aber millionenfach und richteten Schäden in Milliardenhöhe an (BSI 2016, S. 30). Der *Morris Worm* wurde 1988 von dem College Studenten Robert Tappan Morris Jr. programmiert und legte große Teile des damaligen Internets lahm (Parrika 2005). Dadurch wurde erstmals klar, welche Auswirkungen ein Virus im Cyber-Raum haben kann. Der *Loveletter-Wurm* richtete weltweit Schäden in Höhe von geschätzten 10 Mrd. US-$ an. An diesem Beispiel wird deutlich, welche Gefahr ein einzelner Nutzer für den gesamten Cyber-Raum darstellen kann. Wird eine Schwachstelle im System erkannt, so kann ein Schadprogramm in beachtlicher Geschwindigkeit Millionen von Rechner rund um den Globus infizieren. Die Vorteile der globalen Vernetzung werden in diesem Fall schonungslos von Schadprogrammen ausgenutzt, um fremde Rechner zu infizieren. Dass ein APT-Angriff wie Stuxnet nicht einmalig ist, sondern auch Betreiber deutscher Industrieanlagen davon betroffen sein können, zeigt der gezielte Angriff auf den Hochofen eines Stahlwerks[3]. Im Lagebericht 2014 des BSI wird beschrieben, dass sich die Angreifer erst Zugriff auf das Büronetz des Stahlwerks verschafft haben und sich dann von dort aus bis in die Produktionsnetze vorarbeiteten. Steuerungskomponenten und ganzen Anlagen wurden durch den Angriff lahmgelegt, was zu einem massiven Schaden des Hochofens führte (BSI 2014, S. 31). APT-Angriffe haben also nicht nur einen vir-

[3] Angaben über Ort, Zeitpunkt und Zeitraum des Angriffs werden im BSI-Bericht nicht genannt.

tuellen Effekt, wie manche Schadprogramme, sondern verursachen auch Schaden in der realen Welt, indem Produktionsprozesse verändert oder gar verhindert werden.

Im technischen Bereich der Cyberbedrohungen werden folglich einerseits Schadprogramme verwendet, um gewisse Objekte mit hohem Aufwand gezielt anzugreifen. Andererseits werden Schadprogramme dazu eingesetzt, um sich virusartig zu verbreiten und möglichst viele Computer zu infizieren. Beide Angriffsmethoden können massiven Schaden anrichten, indem sie die Eigenschaften des Cyber-Raums zu ihrem Vorteil nutzen und somit die Gewährleistung der Cyber-Sicherheit wesentlich erschweren. Dies zeigt, dass Schadprogramme zunehmend als Waffen konzipiert werden, die auf ein spezifisches Ziel gerichtet sind. Dunn Cavelty sieht hier eine Verbindung zum soziopolitischen Bereich der Bedrohungen. Denn wenn Waffen im Cyber-Raum vorhanden sind, dann gibt es folgerichtig auch NutzerInnen im Cyber-Raum mit böswilligen Absichten, die diese Waffen entweder programmieren oder nutzen (Dunn Cavelty 2013, S. 111).

2.2.2 Soziopolitischer Bereich

Der soziopolitische Bereich der Cyber-Bedrohungen wird geprägt durch Anonymität und Gesetzlosigkeit im Cyber-Raum. Die unter 2.1 beschriebene uneinheitliche Gesetzeslage im Cyber-Raum, die durch die Abwesenheit einer zentralen regulierenden Institution zustande kommt, wird von einzelnen NutzerInnen und Gruppen auch für illegale Zwecke ausgenutzt. Nichtstaatliche Cyber-Kriminelle und Cyber-Terroristen sowie staatliche Cyber-Spione und Cyber-Kommandos profitieren von den bestehenden Grauzonen im Cyber-Raum und nutzen verschlüsselte Netzwerkverbindungen, um unerkannt an fremde Daten zu gelangen.

Bendiek merkt an, dass die Abwesenheit einer nationalen oder internationalen Institution, welche alle internetbasierten Angriffe registriert, es wesentlich erschwert, ein genaues Bild der Bedrohungslage zu erstellen (Bendiek 2012, S. 7). Ohne diese Daten wird es auch wesentlich schwieriger, eine passgenaue Strategie für den Cyber-Raum zu konzipieren. Dieses strukturelle Problem manifestiert sich im Zuordnungsproblem. Staatliche Strafverfolgungsinstitutionen können den Aus-

gangspunkt von internetbasierten Angriffen nicht nachverfolgen. Diese Lücken im System werden von Cyber-Kriminellen ausgenutzt und haben zu einem drastischen Anstieg von Cyber-Angriffen geführt, bei denen nicht-staatliche Akteure häufig eine Hauptrolle spielen (Allan 2013, S. 57). Die Täter können oftmals nicht identifiziert werden, da keine Behörde über die rechtlichen Kompetenzen verfügt, alle Datenbewegungen im Cyber-Raum zu registrieren und zu überwachen. Außerdem werden von Cyber-Kriminellen Botnetze und Anonymisierungs- und Hostingdienste verwendet, um die eigene Identität zu verschleiern (Bundeskriminalamt 2014, S. 6). Hinzu kommt, dass die Gesetzeslage bezüglich digitaler Straftaten in den einzelnen Nationalstaaten unterschiedlich ist. Resultierend daraus entsteht die Problematik des *sicheren Hafens*. Das heißt: wenn Cyber-Kriminelle in einem Staat eine Straftat begehen, diese aber aus einem anderen Staat heraus verübt wurde, in dem die strafrechtlichen Bestimmungen und die rechtliche Grundlage für eine Strafverfolgung fehlen, dann können die Täter von den Strafverfolgungsbehörden nicht rechtlich belangt werden (Bendiek 2012, S. 14). Andere Kriminelle werden somit nicht durch eine effektive Strafverfolgung abgeschreckt, sondern das Zuordnungsproblem intensiviert die Probleme bei der Kriminalitätsbekämpfung im Cyber-Raum noch.

Unter dem Deckmantel der Anonymität können so fremde Akteure Attacken durchführen, die dann fälschlicherweise Staaten zugeschrieben werden (Dunn Cavelty 2013, S. 113). Auf der anderen Seite können sich Staaten bei selbst durchgeführten Angriffen diese Argumentation zu Nutze machen, und es wird sogar vermutet, dass Staaten bewusst bestimmte kriminelle Techniken verwenden, um sich von einer Zuschreibung der Tat zu distanzieren und ein Klima der Unsicherheit zu erzeugen (Deibert und Rohozinski 2010b, S. 5).

Laut Bundeskriminalamt handeln die nichtstaatlichen Akteure bei ihren kriminellen Aktivitäten im Cyber-Raum überwiegend aus finanzieller Motivation (Bundeskriminalamt 2014, S. 11). Einzeltäter wie auch Tätergruppierungen haben sich an den Cyber-Raum angepasst und orientieren ihre Methoden am technischen Fortschritt und den bestehenden Abwehrmaßnahmen (BSI 2015, S. 36). Bei Angrif-

fen wird Schadsoftware verwendet, um über Downloads und E-Mail-Spam ungezielt Computer anzugreifen. Laut BSI wurden ungefähr 72 % der festgestellten Angriffe auf diese Weise durchgeführt (BSI 2016, S. 16). Desweiteren verwenden Kriminelle *Phishing-Mails* oder *Social Engineering*, um Identitätsdiebstahl zu begehen oder Onlinekonten zu manipulieren (21 % der festgestellten Angriffe). Unternehmen werden mit *(D)DoS-Attacken* gezielt angegriffen, was dazu führt, dass diese einen massiven wirtschaftlichen Schaden erleiden und, laut Cyber-Sicherheitsumfrage 2015, sogar 46 % der befragten Institutionen ihren Betrieb vorübergehend einstellen mussten (BSI 2016, S. 17). Um diese Straftaten durchführen zu können, hat sich im Cyber-Raum ein Dienstleistungssektor herausgebildet, der es Kriminellen ermöglicht, auf Handelsplattformen die nötige Schadsoftware oder komplette technische Infrastrukturen zu erwerben (Bundeskriminalamt 2014, S. 11). Von dieser Entwicklung profitieren Gruppierungen der Organisierten Kriminalität, die auch im Bereich Cybercrime zunehmend aktiv sind.

Neben nichtstaatlichen Akteuren agieren auch staatliche Akteure im Bereich der Cyber-Kriminalität. Nachrichtendienstliche Angriffe werden ebenfalls durchgeführt, um finanzielle Mittel zu erlangen. Mindestens genauso wichtig ist jedoch die Motivation, an geheime Informationen und Daten von anderen Staaten und Großkonzernen zu gelangen. Um eine genauere Analyse vornehmen zu können, unterteilt das BSI die nachrichtendienstlichen Angriffe in die vier Hauptangriffsvektoren: *Strategische Aufklärung*, *Individuelle Angriffe im Kommunikations- und Cyber-Raum*, *Beeinflussung von Standards und Implementierungen* und *Gezielte Manipulation von IT-Equipment* (BSI 2014, S. 22).

Bei der strategischen Aufklärung werden an Kommunikationsknotenpunkten sehr große Datenmengen abgegriffen und vollautomatisch analysiert. Betroffen davon sind beliebige InternetnutzerInnen, deren Kommunikation abgehört wird.

Beim zweiten Angriffsvektor werden IT-Systeme von interessanten Personen und Institutionen mit gezielten Cyber-Angriffen attackiert, um die NutzerInnen „von jedem Ort der Welt aus in Echtzeit“ zu überwachen (BSI 2014, S. 22). Nachrich-

tendienste bedienen sich hier auch illegalen Handelsplattformen und kaufen unveröffentlichte Schwachstellen hinzu, um die Computer einzelner Nutzer mit spezifisch adaptierten Angriffen zu manipulieren.

Die Beeinflussung von Standards und Implementierungen wird von Nachrichtendiensten verwendet, um kryptografische Standards zu implementieren, damit Sicherheitsmaßnahmen systematisch geschwächt werden (BSI 2015, S. 35). Das BSI bemängelt, dass die „international standardisierten, starken Kryptoalgorithmen“ mit „schwachen Zufallsgeneratoren kombiniert werden und damit keinen ausreichenden Schutz der Vertraulichkeit mehr bieten“ (BSI 2014, S. 22).

Der letzte Angriffsvektor beschreibt die gezielte Manipulation von IT-Equipment. Das heißt, es werden Hintertüren eingebaut und technische Sicherheitseigenschaften geschwächt, um digitale Geräte zu manipulieren und Cyber-Sabotage zu betreiben.

Neben den Angriffen, die von nationalen Geheimdiensten durchgeführt werden, gibt es mittlerweile auch hochprofessionelle, staatlich geförderte Cyber-Söldner, die effektive Cyber-Waffen entwickeln können und beauftragt werden, um sensible Aufträge auszuführen (Dunn Cavelty 2013, S. 112).

Im Allgemeinen ist eine Professionalisierung bei der Cyber-Kriminalität zu erkennen. Nichtstaatliche wie auch staatliche Akteure verwenden Angriffsmittel und –methoden, um individuelle Nutzer, Unternehmen und auch staatliche Institutionen auszuspionieren und zu erpressen. Das Zuordnungsproblem lässt ein Bedrohungsszenario entstehen, das geprägt ist von Unberechenbarkeit und der Angst vor möglichen Angriffen. Das führt dazu, dass Nationalstaaten viel in die Entwicklung von Cyber-Fähigkeiten investieren und neben Cyber-Waffen für den Angriff auch Mittel für die Cyber-Abschreckung ausbilden.

2.2.3 Mensch und Maschine

Der dritte Bedrohungsbereich befasst sich mit der Komplexität des Cyber-Raums. Die zahlreichen, global miteinander verbundenen Netzwerke bilden ein komplexes System, mit dem wichtige Teile des täglichen Lebens geregelt werden. „Physikali-

sche Objekte wie elektrische Transformatoren, Züge, Pipelinepumpen, Chemiefässer und Radare“ werden von Computernetzwerken kontrolliert (The National Strategy 2003, S. 6). Die zunehmende Abhängigkeit vom Cyber-Raum und von digitalen Techniken machen gesellschaftliche Systeme verwundbarer und durch die Komplexität entsteht eine Unerkennbarkeit und Unvermeidbarkeit von Fehlern, die Teile der Infrastruktur lahmlegen können (Dunn Cavelty 2013, S. 109). Durch katastrophale Attacken auf Infrastrukturen oder Fehlprogrammierungen können Kettenreaktionen ausgelöst werden.

Ein Beispiel für eine Kettenreaktion im Cyber-Raum ist der *Corrupted blood*-Vorfall, der sich 2005 im Computerspiel World of Warcraft ereignete. Dieser digitale Virus verbreitete sich, entgegen der Annahmen der ProgrammiererInnen, schnell weiter und WissenschaftlerInnen erkannten überraschende Ähnlichkeiten mit Epidemien in der realen Welt (Balicer 2007, S. 260). Diese virtuelle Plage wurde von den ProgrammiererInnen nicht geplant und geriet, aufgrund der komplexen Spielewelt von World of Warcraft, schnell außer Kontrolle.

Eben diese Komplexität der realen Umweltbedingungen, in Verbindung mit dem komplexen Cyber-Raum, stellt eine Gefahr dar im Hinblick auf die Geschwindigkeit und Heftigkeit, mit denen sich Störungen zu großen Katastrophen entwickeln können (Dillon 2005, S. 3). Lokale Risiken können so durch die Vernetzung zu Systemrisiken werden. Kaskadeneffekte erzeugen eine Abfolge von unerwarteten Ereignissen und durch Interaktionen zwischen den Akteuren entstehen Überraschungseffekte (Dunn Cavelty 2013, S. 114). Betroffen von solchen Kettenreaktionen können auch die vorhin schon erwähnten Prozessleitsysteme (SCADA-Systeme) sein. Eine Störung dieser Industriekontrollsysteme kann ganze Industrieanlagen und technische Infrastrukturen lahmlegen. Damit würden digitale Effekte auch direkte Auswirkungen auf das reale Leben haben. Ein Fehler in der Software, die Marktkurse bestimmt, kann den globalen Finanzsektor negativ beeinflussen und zeigt, dass die ökonomischen Risiken des Cyber-Raums systemisch sein können

(Bötticher 2015, S. 85). Desweiteren können Netzwerkstörungen die Stromversorgung unterbrechen und den Transport und die Schifffahrt stören (CSTB[4] 2002, S. 6).

Die Selbstverbreitung von Viren im Cyber-Raum lässt sich durch die globale Vernetzung und die schnelle Datenübertragung kaum noch prognostizieren. Der Cyber-Terrorismus und die Cyber-Spionage profitieren von diesen Gegebenheiten und durch die Eigenschaften des Cyber-Raums wird es immer schwieriger, solche Ereignisse nachzuvollziehen. Die ohnehin schon komplexen Vorgänge in einer globalisierten Welt werden durch die typischen Eigenschaften des Cyber-Raums noch verstärkt (Platt 2011, S. 156).

Diese Bedrohungskategorie hat somit die Eigenschaft, dass es im Cyber-Raum keinen Ort gibt, der vor einer Attacke sicher ist, wodurch ein Gefühl erschaffen wird, dass Katastrophen jederzeit ausbrechen können (Graham 2006, S. 258). Während terroristische Angriffe spätestens seit dem 11. September eine ständige Bedrohung darstellen, wird diese Bedrohung durch die Verlagerung in den digitalen Raum noch ungreifbarer und trotzdem allgegenwärtig (Platt 2011, S. 157). Zusammen ergeben die beiden Konzepte *Cyber* und *Terrorismus* eine einschüchternde Kombination.

3 Sicherheit

Im vorherigen Kapitel wurden Gefahren und Bedrohungen beschrieben, die im Cyber-Raum vorherrschen. Gefahren sind mögliche Ereignisse, die eine Schadensfolge nach sich ziehen. Risiken werden dann als Produkt der operationalisierten Gefahr verstanden. Nach Bötticher ist Sicherheit somit ein Zustand, bei dem Risiken auf ein Niveau minimiert wurden, welches unter dem von der Gesellschaft als akzeptabel definierten Schwellenwert liegt (Bötticher 2013, S. 3-4). Während Gefahren unbekannt für Gesellschaften bleiben können, basieren Risiken auf der Wahrnehmung von Gefahren, und Sicherheit wird auf die empfundenen Gefahren gerichtet und ist

[4] Computer Science and Telecommunications Board.

damit Gegenstand der gesellschaftlichen Diskussion. Das Konzept der Sicherheit unterliegt somit dem Wandel der Zeit, ist abhängig von der sozialpolitischen Entwicklung und folglich dynamisch (Bötticher 2013, S. 4). Durch ständig neue Gefahrenlagen und Diskussionen hat sich der Begriff der Sicherheit erweitert. Sicherheit ist demnach ein Kulturprodukt, da „gesellschaftliche Kommunikationsprozesse einen erheblichen Anteil daran haben, was als zu Sicherndes gut wahrgenommen wird, und durch diese Prozesse auch Schwellen der Risikoakzeptanz festgelegt werden“ (Bötticher 2015, S. 77).

Die Sicherheitsdebatte nimmt eine zentrale Stellung im öffentlichen Meinungsaustausch ein, da Sicherheit eine notwendige Basis für ein geregeltes Leben bereitstellt und „eine der wesentlichen Voraussetzungen aller Bereiche des öffentlichen Lebens sowie Grundbedarf aller natürlichen und sozialen Systeme“ ist (Endreß und Petersen 2012). Diese Sicherheit zu gewährleisten ist eine zentrale Aufgabe der Politik. Der Staat wird als Institution angesehen, „die ihre rechtlichen Möglichkeiten dazu einsetzt, Sicherheit zu gewährleisten“ (Singelnstein und Stolle 2012, S. 156).

Kommt der Staat den Anforderungen nicht nach, die Sicherheit zu gewährleisten und Sicherheitsbedürfnisse der Gesellschaft zu befriedigen, dann verliert er seine Legitimationsgrundlage (Daase 2010, S. 9). Es ist also Aufgabe des Staates, Unsicherheiten zu reduzieren. Bedrohungen gehen heutzutage aber nicht mehr nur von anderen Staaten aus, sondern auch von transnationalen und nichtstaatlichen Akteuren, die die Globalisierung nutzen und sich so sensibles Wissen illegal aneignen können. Somit steht die grenzüberschreitende Politik nichtstaatlicher Akteure „in einem Spannungsverhältnis zur nationalstaatlichen Souveränität“ (Freudenberg 2014, S. 282). Dies lässt die einstige Trennung von äußerer und innerer Sicherheit hinfällig werden. Die klare Trennung der Forschungsgebiete von äußerer und innerer Sicherheit in der Wissenschaft kann der Komplexität einer globalisierten Welt im Informationszeitalter nicht gerecht werden. Die einzelnen Sicherheitsbereiche verschmelzen miteinander und kreieren so neue Herausforderungen, denen sich die Nationalstaaten stellen müssen. Deshalb legen viele Staaten „ihrer Sicherheitspolitik

inzwischen einen erweiterten Sicherheitsbegriff zugrunde“, der neben militärischen Bedrohungen auch andere Konfliktursachen wie „Armut und Massenelend, Umweltzerstörung, ethnisch und religiös motivierte Gewalt“ in den Blick nimmt (Bredow 2006). Sicherheit hat sich zu einem der zentralen Wertebegriffe demokratischer Gesellschaften entwickelt und spielt bei der Ausarbeitung von poltischen Strategien eine prägende Rolle. Die Fortentwicklung des Sicherheitsbegriffs und die „daraus resultierende sich wandelnde Wahrnehmung politischer Probleme hat auch maßgeblich zu einem Wandel der Sicherheitskultur geführt“ (Endreß und Petersen 2012).

Münkler unterscheidet zwischen Sicherheitskulturen und Kulturen des Risikos. Letztere versuchen nicht, die Gefahren und Bedrohungen auszusperren, sondern wollen die Risiken kalkulieren und trauen sich so mehr zu als Welten der Sicherheit (Münkler 2010, S. 12). Sicherheitskulturen versuchen dagegen Gefahren und Bedrohungen auszugrenzen um damit sichere Räume zu schaffen. Da Welten der Sicherheit Gefahren gänzlich beseitigen wollen, und somit implizit eine sichere Welt versprechen, werden sie an diesen hohen Erwartungen gemessen. Ständig neue Sicherheitslücken erfordern jedoch einen immer höheren Ressourceneinsatz um das Ziel einer umfassenden Sicherheit doch noch zu erreichen. Das relative Niveau der Sicherheit kann zwar dadurch möglicherweise erhöht werden, aber diese Strategien der Sicherung führen zu einem Dilemma, dass „weder durch Strategiewechsel noch durch erhöhten Ressourceneinsatz aufgelöst werden“ kann (Münkler 2010, S. 12). Denn neben dem Bedürfnis nach Sicherheit wird ein Gefühl der Unsicherheit hervorgebracht, welches sich verstärkt, je höher die Sicherheitszusagen sind. Dies hat mit dazu geführt, dass Nationalstaaten oft nicht mehr in der Lage sind, alle Sicherheitsbedürfnisse zu befriedigen. Private Sicherheitsfirmen übernehmen dann die Aufgaben des Staates, was zu einer Privatisierung der Sicherheit führt, mit dem Resultat, dass „Sicherheit vermehrt primär dort hergestellt“ wird, „wo einflussreich danach verlangt wird bzw. wo für sie gezahlt werden kann, also immer weniger unter Gemeinwohlaspekten“ (Stegmaier und Feltes 2008, S. 305).

3.1 Cyber-Sicherheit

In der Cyber-Sicherheitsstrategie für Deutschland wird der Begriff Cyber-Sicherheit in drei Kategorien unterteilt. Im Strategiepapier wird unterschieden zwischen der globalen Cyber-Sicherheit, der zivilen sowie der militärischen Cyber-Sicherheit. Das Bundesministerium des Innern definiert die Bereiche wie folgt:

> (Globale) Cyber-Sicherheit ist der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des globalen Cyber-Raums auf ein tragbares Maß reduziert sind.
> Cyber-Sicherheit in Deutschland ist demnach der anzustrebende Zustand der IT-Sicherheitslage, in welchem die Risiken des deutschen Cyber-Raums auf ein tragbares Maß reduziert sind. Cyber-Sicherheit (in Deutschland) entsteht durch die Summe von geeigneten und angemessenen Maßnahmen.
> Zivile Cyber-Sicherheit betrachtet die Menge der zivil genutzten IT-Systeme des deutschen Cyber-Raums. Militärische Cyber-Sicherheit betrachtet die Menge der militärisch genutzten IT-Systeme des deutschen Cyber-Raums. (BMI 2011, S. 15)

Dass der Begriff der Sicherheit einem dynamischen Prozess unterliegt und unter anderem von sozialpolitischen Entwicklungen abhängig ist, wird in der Definition deutlich durch die Formulierung, dass die Risiken *auf ein tragbares Maß reduziert* werden sollen. Das heißt, es ist kein genauer Zielkorridor vorgegeben, sondern die Sicherheitslage kann sich stetig ändern und wird abhängig von den Umweltbedingungen bewertet. Auch die Risiken verändern sich fortwährend und verändern somit wieder die Ausgansposition der Sicherheitslage. Anhand von diesen Umwelteinflüssen wird auch entschieden, welche Maßnahmen geeignet und angemessen sind, um den Zustand der Cyber-Sicherheit in Deutschland zu erreichen. Jedoch kann der deutsche Cyber-Raum nicht vollkommen losgelöst von Sicherheitskulturen und Kulturen des Risikos insgesamt betrachtet werden, da der digitale Raum keine nationalen Grenzen kennt.

Das bereits beschriebene Sicherheitsdilemma wird im Informationszeitalter durch die Eigenschaften des Cyber-Raums weiter verstärkt. Durch die hohe Innovationsfrequenz und die intensivierte Nutzung von Kommunikationsmitteln bilden täglich auftretende neue Sicherheitslücken und Schwachstellen frische Bedrohungen für die Nutzer und lösen neue Unsicherheiten aus. Des Weiteren ist der digitale Raum transnational organisiert und mit technischen Mitteln und dem nötigen Fachwissen ist es möglich, Daten abzugreifen, die auf Servern in anderen Ländern gespeichert werden. Darum ist im Feld der Cyber-Sicherheit eine getrennte Betrachtungsweise von innerer und äußerer Sicherheit nicht zielführend. Um eine Sicherheitsanalyse im digitalen Raum durchführen zu können, müssen beide Bereiche miteinander verbunden und Sicherheit als Prozess verstanden und interdisziplinär betrachtet werden (Endreß und Petersen 2012). So ist zum Beispiel eine Veränderung der Schadensszenarien und der Bedrohungen erkennbar, die durch die zunehmende Komplexität entstehen. Wie unter 2.2.3 beschrieben, können durch die komplexen Netzwerksysteme Kaskadeneffekte entstehen, die komplette Regionen vom Strom abschneiden, den Schiffsverkehr lahm- oder das Börsensystem stilllegen können.

Auch wenn die Cyber-Sicherheit noch ein junges Subfeld der Sicherheitspolitik ist (Bötticher 2015, S. 73), so erfährt dieser Sektor zunehmend mehr Aufmerksamkeit und wird, laut BSI, zu einer vorrangig staatlichen Aufgabe. Der Staat muss, laut dem Bundesamt, „immer stärker auch den zivilen, präventiven Bereich berücksichtigen, muss Rahmenbedingungen schaffen, Standards setzen und aktiv Hilfestellung geben“ (BSI 2016, S. 28), um die Bedrohungen zu bekämpfen und zu mindern. Der Staat wird in die Pflicht genommen und kann wie im Politikfeld der Inneren Sicherheit mit Steuerungsmaßnahmen (Ge- und Verbote) operieren. Bei der Herstellung von Cyber-Sicherheit sind jedoch auch regelverändernde politische Maßnahmen (konstitutierende *policies*) erkennbar, da die Cyber-Sicherheit ein noch nicht voll etabliertes Politikfeld ist (Bötticher 2015, S. 73). Das bedeutet, Regierungen können mit regelverändernden Maßnahmen das Feld der Cyber-Sicherheit wesent-

lich mitbestimmen und gestalten. Wenn sich ein neues Subfeld bildet, dann sind noch keine festen Strukturen vorhanden. Es gibt noch keine klaren Handlungsabläufe und Zuständigkeiten. Deshalb konstituieren sich in solchen Umbruchsituationen „neue Verhandlungsthemen und Aushandlungsarenen", „bis dahin unbekannte (oder unbedeutende) Akteure" (Dolata 2001, S. 46) betreten das Feld und alte Akteure müssen sich repositionieren. Im Bereich der deutschen Cyber-Sicherheit sind die Kompetenzen möglicherweise noch nicht vollständig den Akteuren zugeteilt und die Institutionen müssen sich durch Machtkämpfe erst ihre Position in diesem Politikfeld erarbeiten. Auch private Unternehmen, die im Bereich der Computersicherheit tätig sind, versuchen ihren Einfluss in diesem Politikbereich zu vergrößern.

Das Konzept der Sicherheit ist mit dem Einzug des digitalen Zeitalters noch komplexer geworden, da die Souveränität von Nationalstaaten nicht mehr nur an territorialen Gebietsüberschreitungen festgemacht wird, sondern auch an Angriffen, die im Cyber-Raum durchgeführt werden, da der digitale Raum neben dem Land, dem maritimen Bereich, dem Lauftraum und dem Weltraum mittlerweile als fünfter operativer Bereich von Staaten betrachtet wird (vgl. Welch 2011, Hayden 2011). Dabei gibt Larry Welch, ehemaliger Stabschef der U.S. Air Force, zu bedenken, dass es unmöglich ist, den Cyber-Raum jederzeit zu überwachen, genauso wie sich der Luftraum und der Meeresraum einer vollständigen Kontrolle entziehen (Welch 2011, S. 2).

Mit den neuen Herausforderungen, die der Cyber-Raum mit sich bringt, müssen sich die Institutionen den veränderten Bedingungen anpassen, geeignete Mittel auswählen oder erst entwickeln und ihr Instrumentarium modifizieren, um einen Zustand der Sicherheit erreichen zu können (Stegmaier und Feltes 2008, S. 306). Ist es der Politikwissenschaft bisher nicht gelungen „eine abschließende bzw. wirklich zufriedenstellende Definition des Terminus Sicherheit zu finden" (Endreß und Petersen 2012), so wird die Übertragung des Konzepts auf den Cyber-Raum umso schwieriger. Die menschengemachte Domäne des digitalen Raums folgt keinen naturwissenschaftlichen Gesetzen, sondern im Cyber-Raum ist alles mach-

bar, was die technischen Mittel ermöglichen und wozu Menschen fähig sind. Somit werden Aussagen über mögliche Gefahren im Cyber-Raum noch schwieriger.

3.2 Kritische Infrastrukturen und demokratiepraktische Probleme

Die kritischen Infrastrukturen regeln wesentliche Bereiche der Daseinsvorsorge, sind in den Cyber-Raum integriert und bilden somit die Grundlage für die Organisation von modernen Gesellschaften. Das Bundesinnenministerium definiert die kritischen Infrastrukturen als „Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden“ (BMI 2011, S. 15). Dies führt dazu, dass das Wohlbefinden der Gesellschaft mit der Integrität der Computersysteme verbunden ist. Nach dieser Logik wäre jede Bedrohung für Computer und Netzwerke auch eine Bedrohung für die wesentlichen Funktionen des gesellschaftlichen Lebens und ein Angriff könnte verheerende Folgen haben (Nissenbaum et al. 2001, S. 11). Gerade hier wird die Verschmelzung der inneren und äußeren Sicherheit deutlich. Denn durch die Einbettung in den Cyber-Raum, lassen sich die kritischen Infrastrukturen nicht vor Attacken bewahren, „wenn nur außenpolitische oder nur innenpolitische Maßnahmen ergriffen werden“ (Bendiek 2012, S. 20).

Neben möglichen katastrophalen Angriffen auf die Infrastruktur haben sich durch die Digitalisierung auch noch andere Probleme für die Öffentlichkeit ergeben. Die OECD sieht es als eine Schlüsselfrage an, ob die Regierungen den Schutz der Offenheit des Cyber-Raums als einen integralen Bestandteil von Cyber-Sicherheit ansehen und wie dies umgesetzt wird (OECD 2012, S. 13). Denn mit der Digitalisierung haben sich demokratiepraktische Probleme entwickelt, die durch die Technisierung überhaupt erst möglich wurden. In informellen Zirkeln ist eine „autonome Selbststeuerung von Technisierung“ (Bötticher 2015, S. 91) feststellbar und die Grenzen zwischen der Privatwirtschaft, der Polizei und privaten Firmen verwi-

schen. In diesen informellen Zirkeln wie auch zwischen Institutionen auf EU-Ebene findet ein Informationsaustausch statt, der kaum noch aufschlüsselbar ist und sich der demokratischen Kontrolle entzieht (Bötticher 2015, S. 91). Bendiek identifiziert im Bezug auf die europäische Cybersicherheitspolitik drei demokratiepraktische Probleme.

Die Zuständigkeitsbereiche der Innen- und Außenpolitik verschwimmen zunehmend, da sich die Gefahrenquellen kaum mehr eindeutig zuordnen lassen und sich somit innere Strukturprobleme „als Verwundbarkeiten gegenüber Bedrohungen von außen" entpuppen (Bendiek 2012, S. 21).

Ein weiteres Problem ist die Versicherheitlichung auf nationaler und auch auf EU-Ebene. Es ist erkennbar, dass sich die politische Schwerpunktsetzung zunehmend von der Freiheit zur Sicherheit verschiebt. Dabei sollten „das Streben nach mehr innerer Sicherheit und der Schutz der Grundrechte [..] im Sinne einer Doppelstrategie Hand in Hand gehen" (Busuioc und Curtin 2011, S. 15). Dass dies nicht der Fall ist, zeigt eine Mitteilung der Europäischen Kommission, in der sie auf das Stockholmer Programm des Europäischen Rates reagiert. In dieser Mitteilung geht die Kommission ausführlich auf die sicherheitspolitischen Herausforderungen ein, betont jedoch nicht, „dass parallel ein umfassendes Regelwerk geschaffen werden müsste, das die informationellen Grundrechte der Bürger gegenüber expansiven staatlichen Eingriffen schützt" (Bendiek 2012, S. 21).

Durch den vermehrten Einfluss von privaten Sicherheitsunternehmen in der Cyber-Sicherheitspolitik verliert die Trennung zwischen privat und öffentlich in den politischen Strukturen zunehmend an Bedeutung. Einerseits ist das technologische Know-how dieser Unternehmen notwendig um die relevanten Gefahren angemessen zu identifizieren, andererseits sollte der Einfluss von privaten Unternehmen begrenzt werden, denn in Demokratien sollten „Parlamente der Ort sein, an dem das Verhältnis von Sicherheit und Freiheit definiert wird, gerade auch was Cybersicherheitspolitik anbelangt" (Bendiek 2012, S. 6).

Eine Strategie sollte somit nicht nur die Gefahren bekämpfen und eindämmen, sondern gleichzeitig auch die Grundrechte der BürgerInnen schützen und sich an Kriterien wie Rechtsstaatlichkeit, Partizipation, Rechenschaftspflicht und Transparenz ausrichten.

4 Bezugsrahmen der Strategieanalyse

In diesem Kapitel wird der von Ralf Tils generierte analytische Bezugsrahmen vorgestellt. Dieser Bezugsrahmen bildet ein Evaluationsraster, mit dem anschließend die Cyber-Sicherheitsstrategie für Deutschland analysiert werden kann. Der Bezugsrahmen wurde von Tils entwickelt um die Strategiequalität von politischen Strategien zu untersuchen, indem die Prozessdimension und die Ausgestaltung der Strategie analysiert werden. Gegenstand der Analyse waren bei Tils der umweltpolitische Strategieansatz von Martin Jänicke und die deutsche Nachhaltigkeitsstrategie. Diese strategischen Konzepte haben ihren Schwerpunkt im nationalen Kontext und dementsprechend wurde die strategische Evaluation der politischen Strategien vorrangig für die nationale Ebene konzeptualisiert (Tils 2005, S. 21). Da die dezentrale Organisation und die globale Vernetzung wesentliche Merkmale des Cyber-Raums sind, werden für den analytischen Bezugsrahmen Ergänzungen und Modifikationen vorgenommen bezüglich des internationalen Kontextes politischer Gestaltung. Eine Strategie für den Cyber-Raum muss einerseits den nationalen Kontext Deutschlands berücksichtigen, andererseits aber auch die internationalen Zusammenhänge in die Ausgestaltung miteinbeziehen um praxistauglich zu sein.

4.1 Strategiebegriff

Bei der Analyse des Strategiebegriffs wird untersucht, welche Bedeutung dem Begriff der Strategie zukommt. Wird dem Begriff viel Einfluss zugeschrieben und wirkt sich dies auf die Gestaltung des Gesamtkonzepts aus, oder wird der Begriff Strategie nur plakativ verwendet, um andere Kennzeichnungen wie Programm oder

Plan zu vermeiden? Dies wird ausführlich mit den folgenden spezifischeren Kriterien betrachtet, allerdings werden oft schon „auf der Ebene des Strategiebegriffs Mängel erkennbar“ (Tils 2005, S. 103).

Politische Strategien basieren auf situationsübergreifenden, erfolgsorientierten und dynamischen Ziel-Mittel-Umwelt-Kalkulationen. Aus diesen Einzelelementen setzt sich der Strategiebegriff zusammen. In diesem Zusammenhang meint *situationsübergreifend* eine längerfristige Orientierung, die eine Mehrzahl von Situationen umfasst. Der Zeitrahmen für eine Strategie ist von den einzelnen strategischen Einheiten abhängig, welche kurz-, mittel- oder langfristig angelegt sein können, und geht über den Augenblick hinaus. In diesem Fall wird strategisches Verhalten klar abgegrenzt zu taktischem Verhalten, welches kurzfristig orientiert ist und ein positives Ergebnis in möglichst kurzer Zeit erreichen will.

Strategische Kalkulationen werden, im Bezug auf ihre Erfolgsorientierung, danach beurteilt „inwieweit das politische Handeln zur Zielerreichung beiträgt“ (Tils 2005, S. 27). Strategische Politik sollte in diesem Zusammenhang wertende und zweckorientierte Überlegungen miteinander verbinden.

Eine Strategie, die sich mit dem Cyber-Raum befasst, muss sich in besonderer Weise mit den ständig ändernden Umweltbedingungen beschäftigen, damit eine Zielerreichung weiterhin möglich bleibt. Eine dynamische Strategieausformung ermöglicht die Anpassung an neue Ausgangslagen, analysiert fortwährend, wo es einen Anpassungsbedarf gibt (Ziele, Mittel, Akteure etc.) und auf welche Art Anpassungen vorgenommen werden sollen. Für Strategien ist es von großer Bedeutung, dynamisch auf Veränderungen der Umweltbedingungen reagieren zu können, um Gelegenheiten zu nutzen, die die Aussicht auf die Zielerreichung vergrößern (Ganz 2005, S. 214).

Für die Umsetzung der strategischen Kalkulationen muss deutlich gemacht werden, für welche Adressaten die Handlungsanweisungen und Verpflichtungen gelten. Die Mittel, mit denen die anvisierten Ziele erreicht werden sollen, müssen die strategisch-relevante Umwelt als Kontext mit einbeziehen.

Für die Evaluation ist interessant, ob in dem Strategiepapier eine explizite Strategiedefinition vorgestellt, der Strategiebegriff näher erläutert und umrissen oder dem Strategiebegriff keine tiefergehende Bedeutung beigemessen wird.

4.2 Akteure strategischer Politik

In einer Strategie sind Kollektivakteure notwendig, um die Ziel-Mittel-Umwelt-Kalkulationen umzusetzen, da der politische Prozess in Industriegesellschaften durch Kollektivakteure geprägt wird (Benz 2001, S. 155). Im Strategiepapier müssen deshalb die Kollektivakteure gekennzeichnet werden, die für die Verwirklichung der Strategie zentral sind. Hierbei muss getrennt werden zwischen Strategen und strategischen Akteuren. Strategen sind für die Konzeption der Strategie verantwortlich, während die strategischen Akteure bestimmte Funktionen zugeschrieben bekommen, die ausgeführt werden sollen, um die gewünschten Ziele zu erreichen. Um diese Aufgaben erfüllen zu können, müssen Anforderungsprofile formuliert und Kollektivakteuren bestimmte Rollen zugeschrieben werden. Eine klare Aufgabenverteilung und die Kennzeichnung der relevanten Strategieakteure sind wichtig für eine effektive Umsetzung der Strategie (Tils 2005, S. 104). Bei der Ausarbeitung sollte von Strategen beachtet werden, dass Gruppen wie ProduzentInnen, VerbraucherInnen oder ganz allgemein BürgerInnen nicht notwendigerweise über eine kollektive Akteurqualität verfügen und somit auch nicht als strategische Akteure einbezogen werden können. Konkretes Aufzeigen der Handlungsmöglichkeiten und die Erstellung von Schnittstellen zwischen *Top-down* und *Bottom-up* Prozessen sind erforderlich, um Kollektivakteure in den Gestaltungsprozess einzubinden. Neben den Fertigkeiten des Strategieakteurs hängen die Erfolgsaussichten von Strategien „auch vom Handeln anderer beteiligter Akteure und sonstigen äußeren Einflüssen ab, die vom Strategieakteur nicht unmittelbar steuerbar sind“ (Tils 2005, S. 105). Diese externen Bedingungskomplexe, die das Handlungsumfeld der Akteure beeinflussen, müssen bei den strategischen Kalkulationen mit einbezogen werden, um die politischen Prozesse auf die Zielerreichung hin auszurichten.

Für eine Cyber-Sicherheitsstrategie ist die internationale Handlungsebene gleichermaßen von Bedeutung wie die nationale Ebene. Auch für die internationale Handlungsebene müssen, in Verbindung zum globalen Handlungskontext, strategische Akteure identifiziert und ihnen Handlungsaufträge zugeschrieben werden. Ob eine Strategie erfolgreich ist, hängt somit zum einen von den Fertigkeiten der Strategieakteure ab, zum anderen von den äußeren Einflussfaktoren (Tils 2005, S. 105).

Bei der Analyse von Akteuren liegt der Fokus auf den Kollektivakteuren, da das Handeln von individuellen Akteuren im Außenverhältnis als Handeln des Kollektivakteurs wahrgenommen wird (Tils 2005, S. 105). Desweiteren bilden öffentliche und private Kollektivakteure zusammen ein dezentrales Netzwerk, in dem zusammengearbeitet und der politische Prozess gemeinsam geprägt wird (Teubner 1999, S. 346). Für einen Kollektivakteur besteht die Herausforderung darin, die unterschiedlichen und teilweise gegenläufigen Handlungen der individuellen Akteure miteinander zu verbinden, um nach außen hin eine kollektive Realität zu erzeugen.

Für die strategische Evaluation ist es demnach wichtig, ob die zentralen strategischen Akteure im Entwurf benannt wurden und ob die Strategen bei der Ausgestaltung die Schwächen und Stärken der Strategieakteure berücksichtigt und mit den nachfolgenden Kriterien abgeglichen haben.

4.3 Strategische Ziele

Strategische Ziele können unterteilt werden in übergeordnet angestrebte Zustände und darunter liegende Teilziele. Ziele helfen dabei herauszufinden, welche Maßnahmen notwendig sind, um die angestrebten Zustände zu erreichen. Durch die strategischen Ziele werden die strategischen Mittel bestimmt, mit denen versucht wird, die gewünschten Zustände zu erreichen. Ziele geben folglich die Richtung des strategischen Handelns vor. Tils unterscheidet zwischen den Begriffen *Ziel* und *Zweck* und hebt hervor, dass „der Zielbegriff die Möglichkeit letztendlicher Zielerreichung hervorhebt“ (Tils 2005, S. 106).

Bei den Zielarten lässt sich zwischen quantitativen und qualitativen Zielen unterscheiden. Quantitative Ziele können durch Messbarkeit überprüft werden (z. B. Senkung der Arbeitslosigkeit um 2 %), während qualitative Ziele nicht messbar sind, aber dennoch überprüfbare Zustände beschreiben (z. B. dauerhaft niedrige Neuverschuldung).

Bevor die strategischen Ziele in das Konzept integriert werden, wird die Operationalisierbarkeit der Ziele überprüft, das Zielsystem analysiert und somit kritisch reflektiert, ob die angestrebten strategischen Ziele in die Strategie aufgenommen werden sollen. Sind die vorgegebenen Ziele nicht operationalisierbar, so kann auch nicht überprüft werden, ob die strategischen Kalkulationen die gewünschten Änderungen gebracht haben und die Ziele erreicht wurden (Tils 2005, S. 108). Es sind also zum einen keine Rückschlüsse möglich, ob die gesetzten strategischen Ziele erreicht wurden, zum anderen kann nicht überprüft werden, ob die eingesetzten strategischen Mittel passend ausgewählt oder richtig angewendet wurden.

Da Strategien meist nicht nur ein Ziel verfolgen, hängt die Bedeutung der einzelnen Ziele von den Intentionen der Strategen und strategischen Akteuren ab, und es kann zu Zielkonflikten kommen. Diese können bei einer umfassenden Strategie nicht ausgeschlossen werden, jedoch sollten mögliche Zielkonflikte aufgezeigt und Vermittlungsvorschläge erarbeitet werden, damit klare Strukturen für eine Problemlösung vorhanden sind.

Neben qualitativen und quantitativen Zielen unterscheidet Raschke außerdem auch zwischen Machtzielen (*Politics*-Ziele) und Gestaltungszielen (*Policy*-Ziele) (Raschke 2002, S. 210). Machtziele können der Machtgewinnung und dem Machterhalt dienen, aber auch Ausgangspositionen bilden, um die angestrebten Gestaltungsziele durchzusetzen. Mit Gestaltungszielen sind die angestrebten Lösungen gemeint, die sich inhaltlich mit spezifischen Problemen befassen. Macht- und Gestaltungsziele sind daher beide notwendig um Strategien ausführen zu können und müssen deshalb beim Strategieentwurf beachtet werden. Werden beide in einen

inneren Zusammenhang gebracht und miteinander verknüpft, so kann verhindert werden, dass Strategien für Manipulationen und Machtzwecke missbraucht werden (Raschke und Tils 2008, S. 24).

4.4 Strategische Mittel

Für eine erfolgreiche Zielerreichung ist eine systematische Verknüpfung von Zielen und Mitteln von großer Bedeutung. Tils definiert strategische Mittel „als intentional, rational und erfolgsorientiert ausgewählte Handlungsalternativen und Maßnahmen [..], die zum Erreichen der anvisierten strategischen Ziele führen sollen“ (Tils 2005, S. 108). Um die von den Strategen festgelegten Ziele zu erreichen, verwenden die strategischen Akteure unterschiedliche, ihnen zur Verfügung stehende Mittel.

Dabei kann, wie bei den strategischen Zielen, zwischen strategischen *Policy*-Mitteln und Politics-Mitteln unterschieden werden. Mit *Policy*-Mitteln sollen sachliche Problemlösungen erreicht werden, indem Handlungsalternativen und Maßnahmen empfohlen werden, die auf inhaltliche Gestaltungsziele ausgerichtet sind. *Politics*-Mittel dagegen dienen zur Durchsetzung bestimmter Machtziele in politischen Entscheidungsverfahren. Die Aufteilung von *Politics*-Mitteln in politikfeldbezogene und politikfeldübergreifende *Politics*-Mittel ist hilfreich bei der strategischen Evaluation des Konzeptes (Tils 2005, S. 109). Politikfeldbezogene *Politics*-Mittel werden verwendet für die Schaffung einer Machtbasis innerhalb eines oder mehrerer Politikfelder, um die angestrebten inhaltlichen Gestaltungsziele zu erreichen. Mit politikfeldübergreifenden *Politics*-Mitteln versuchen Kollektivakteure, Macht- und Gestaltungspositionen außerhalb eines spezifischen Politikbereichs zu erreichen.

Die zur Verfügung stehenden Mittel können von den strategischen Akteuren auf unterschiedliche Weise angewendet werden und somit verschiedene Zwecke erfüllen. Tils beschreibt dies am Beispiel von strategischen Bündnissen. Diese können entweder als politikfeldbezogene *Politics*-Mittel verwendet werden, indem der eigene Handlungsspielraum für eine größere Machtbasis ausgeweitet werden soll,

oder aber als *Policy*-Mittel, um mithilfe von Kooperationen konkrete Probleme zu lösen (Tils 2005, S. 109). Werden strategische Bündnisse geschlossen, dann setzen strategische Akteure politikfeldübergreifende Politics-Mittel ein, um die Mehrheitsfähigkeit zu sichern und somit Machterhaltungsziele erreichbar zu machen. Die Machtgewinnung steht hierbei an erster Stelle, während die inhaltliche Auseinandersetzung über ein gemeinsames Programm erst später folgt.

Durch die Trennung der unterschiedlichen Mittel werden Differenzen und Wechselbeziehungen besser darstellbar. Für Strategien sind im Besonderen die politikfeldübergreifenden *Politics*-Mittel bedeutend, da eine breite Machtbasis die Erfolgspotenziale von Strategien signifikant erhöhen.

4.5 Strategiefähigkeit

Auch wenn individuelle Akteure die Fähigkeit besitzen, Strategien zu entwickeln, sagt dies nichts über die Fähigkeit der Akteure aus, diese auch durchzusetzen. Ebenso lässt sich nicht von individueller Strategiefähigkeit auf die Strategiefähigkeit eines Kollektivakteurs schließen. Kollektivakteure (Regierungen, Parteien, Interessenverbände) sind die politisch relevanten Betrachtungseinheiten, auf deren Strategiefähigkeit es ankommt (Raschke 2002, S. 213). Während innerhalb der Kollektivakteure einzelne Individuen das strategische Verhalten definieren, ist es anschließend maßgeblich, ob der Kollektivakteur die Fähigkeit besitzt, die Strategie durchzusetzen. Um strategiefähig zu sein, müssen Strategieakteure an erster Stelle Kompetenzen aufbauen und diese dann auch fortwährend weiterentwickeln, um strategiefähig zu bleiben. Um zielgerichtet und einheitlich strategisch zu Handeln müssen Kollektivakteure über strategische Selbststeuerungskompetenz verfügen (Tils 2005, S. 111). Das heißt, die Handlungen der individuellen Akteure müssen koordiniert werden, damit im Außenverhältnis der Kollektivakteur zu einer handlungsfähigen Einheit wird. Wie bereits unter 4.2 erwähnt, müssen die internen unterschiedlichen Präferenzen und Interessen zusammengeführt werden, um gemeinsame Zielvorstellungen zu erarbeiten. Damit erreicht der Kollektivakteur eine kollektive Handlungs-

fähigkeit und wird somit erst strategiefähig. Kollektive Handlungsfähigkeit ist notwendig für die Ausarbeitung einer Strategie, sowie für den internen Entscheidungsprozess und die spätere Organisation des strategischen Handelns. Für diese Arbeit ist es zweitrangig, wie über die Strategie entschieden und abgestimmt wurde. Deutlich wichtiger für die strategische Evaluation ist, dass die akteursinterne Ausarbeitung und spätere Durchsetzung und Organisation der Strategie angemessen reflektiert wird.

Die strategische Selbststeuerungskompetenz ist eine notwendige Voraussetzung für die Strategiefähigkeit eines Kollektivakteurs und von inneren Strukturmerkmalen abhängig. Der interne Aufbau eines kollektiven Akteurs und die vorherrschenden Verfahrensweisen können Strategiefähigkeit fördern oder behindern. Koordination unter den individuellen Mitgliedern, interne Kommunikation, die administrative Umsetzung getroffener Entscheidungen und leistungsfähige Organisationsstrukturen tragen zur Entwicklung von Strategiefähigkeit bei (Tils 2005, S. 111). Personelle, finanzielle und informationelle Ressourcen gehören zur Grundlage, damit Selbststeuerungskompetenz aufgebaut werden kann. Die Ressourcen, die einem Akteur zur Verfügung stehen, beeinflussen seine Arbeitsweise mit und begrenzen seinen Wirkungsradius. Während eine Basisausstattung an Ressourcen Startvorteile gewährt, kann dadurch nicht zwangsläufig auf die Strategiefähigkeit des Akteurs geschlossen werden. Klare interne Organisationsstrukturen sind erforderlich, damit der Kollektivakteur sich strategisch positionieren und nach außen hin als Gesamtheit agieren kann. Dadurch wird auch zielgerichtetes Handeln möglich. Für Strategen ist es vorteilhaft *Strength*- und *Weakness*-Profile der strategischen Akteure zu erarbeiten, da es wenig erfolgversprechend scheint, Akteuren mit mangelhafter Selbststeuerungskompetenz eine große Bedeutung zuzumessen (Tils 2005, S. 112). Bei Strategien müssen die Kalkulationen mit dem Handlungsumfeld abgeglichen werden, ebenso sollten akteursinterne Merkmale mit einer Umweltperspektive verknüpft werden. Erst dann wird deutlich, ob die Kompetenzen des Akteurs in Verbindung mit den Umweltbedingungen den Akteur strategiefähig machen.

Des Weiteren bedeuten gute interne Strukturen und eine hohe Selbststeuerungskompetenz nicht, dass der strategische Akteur auch ein großes Einflusspotenzial in den Umweltbeziehungen besitzt. Vielmehr wird die externe Strategiefähigkeit durch Macht- und Interaktionsverhältnisse zu anderen Akteuren und den Rahmenbedingungen bestimmt. Für die relevanten strategischen Akteure ist es wichtig, dass sie Strategiefähigkeit besitzen und ihre Stärken erkennen und effektiv einsetzen.

4.6 Strategische Kontexte

Das Kriterium *Strategische Kontexte* behandelt die Akteur-Umwelt-Beziehungen der relevanten Akteure. Damit ist die mittelfristig relevante Handlungsumgebung gemeint, „die über die zeitlich begrenztere einzelne Situation hinausragt“ (Tils 2005, S. 113). Während mit einem Aktionsplan auf aktuelle Gegebenheiten reagiert wird, um kurzfristige Änderungen herbeizuführen, so werden mit einer Strategie längerfristige Ziele verfolgt. Der Kontext darf also nicht nur als Momentaufnahme betrachtet werden, sondern das Handlungsumfeld und die Rahmenbedingungen müssen auch auf mittelfristige Sicht analytisch beschrieben und abgeschätzt werden. Wenn sich eine Strategie nur nach den aktuellen Rahmenbedingungen richtet, zukünftig absehbare Änderungen dieser Rahmenbedingungen aber außer Acht lässt, dann sind die Aussichten der Strategie wenig erfolgsträchtig. Ohne Kontextanalyse können von den Strategen zwar Ziele formuliert werden, allerdings lassen sich dann keine Aussagen über Lösungswege machen, da sich das Handlungsumfeld, vor allem im digitalen Raum, ständig verändert (Tils 2005, S. 113). Eine Kontextanalyse umfasst auch den politischen Gelegenheitskontext, in dem sich ein Akteur bewegt, den er beeinflussen kann, der ihm Handlungsmöglichkeiten, aber auch Restriktionen bereithält. Die externen Bedingungskomplexe formen den Handlungskorridor der Akteure. Um den strategischen Kontext zu bestimmen, wird unterteilt in politisch-institutionelle, sozio-ökonomische und politisch-kulturelle Gelegenheitskontexte.

Der politisch-institutionelle Gelegenheitskontext wird bestimmt durch das Regierungssystem, das Rechtssystem, Vetospieler und die Willensbildungs- und Entscheidungsverfahren. Diese Merkmale des politisch-administrativen Systems sind Grundlage für stabile Bedingungen. Institutionelle Vetospieler, wie der Bundesrat oder das Bundesverfassungsgericht, können sich durch ihre Vetooptionen einerseits als Hemmnisse erweisen, andererseits aber auch von den Akteuren für Vorteile (z. B. strategische Bündnisse) verwendet werden (Tsebelis 2002). Die institutionelle Ausgestaltung ist für den Optionsspielraum der Akteure von wesentlicher Bedeutung und beeinflusst somit den Handlungsspielraum. Dies ist ausschlaggebend bei der Durchsetzung von Entscheidungen und ob diese schnell durchgeführt werden können. Die politisch-institutionellen Rahmenbedingungen können zwar geändert werden, aber nur mit einem großen Aufwand und der Unterstützung von anderen Akteuren. Primär müssen sich die Strategen bei ihrer Ausarbeitung an die gegebenen Kontextbedingungen halten, da eine Änderung des kontextuellen Rahmens mit einem großen Aufwand verbunden wäre und möglicherweise neue unvorhersehbare Hindernisse entstehen könnten (Tils 2005, S. 115).

Der sozio-ökonomische Gelegenheitskontext umfasst die Bereiche Wirtschaft, Gesellschaft, ökonomische Sektoren, sowie Wandlungsprozesse, das Wohlstandsniveau und die Marktverhältnisse. Bei der Ausarbeitung der Strategie sollte beachtet werden, welche Bedingungen und Konsequenzen daraus für den Politikprozess und die Politikgestaltung entstehen. Strategieakteure müssen auf Veränderungen in diesen Bereichen reagieren und deshalb müssen Strategien auch dynamisch konzipiert werden, damit auf Umgestaltungen schnell und angemessen reagiert werden kann (Tils 2005, S. 115). Um diesen Wandlungsprozessen angemessen entgegenzutreten, ist die Einbindung von Großgruppen (Kooptation) sinnvoll (Bendiek 2012, S. 24). Mit sozioökonomischen Parametern lassen sich diese potenziellen Träger von politischen Strategien identifizieren und es ergeben sich Beurteilungskriterien für Strategiepfade.

Beim politisch-kulturellen Gelegenheitskontext wird darauf geachtet, wie sich die Mitglieder einer Gesellschaft bezüglich eines politischen Prozesses orientieren. Die Wahl der strategischen Mittel zur Zielerreichung sollte sich im Möglichkeitsspektrum bewegen, da die strategischen Akteure sonst ihre Legitimationsbasis aufs Spiel setzen. Die Grenzen politisch akzeptierter Verhaltensweisen müssen bei der Strategieplanung wie auch der Umsetzung eingehalten werden. In diesem Kontext soll laut Tils Politische Kultur „hier längerfristige Meinungen, Vorstellungen, Einstellungen, Bewertungen und Wertüberzeugungen kennzeichnen, die sich an politisches Handeln richten und von einem großen Teil der Gesellschaft geteilt werden“ (Tils 2005, S. 116). Politische Kultur ist ein wichtiger Kontext im Hinblick auf die Wahl der politisch-strategischen Handlungsoptionen und gibt vor, was sich Regierungen erlauben können, wo die Grenzen ihres Zuständigkeitsbereichs sind und wofür die Bevölkerung Verständnis hat. Denn nicht alle Maßnahmen, die eine Regierung rein rechtlich durchführen dürfte, werden auch von der Gesellschaft unterstützt. Die Handlungsoptionen der Strategieakteure werden somit durch die politisch-kulturellen Gelegenheitskontexte begrenzt. Strategien sollten folglich im Einklang mit den politisch-kulturellen Überzeugungen sein, damit sie mit gesellschaftlicher Unterstützung rechnen können (Tils 2005, S. 116). Ebenfalls Rücksicht sollte auf die unterschiedlichen *opportunities* und *threats* gegeben werden, die sich aus den spezifischen Kontexten für die strategischen Akteure ergeben. Diese grenzen mögliche Strategiepfade ein, schaffen also einen Möglichkeitsrahmen, der eingehalten werden sollte, damit die Strategie Erfolgsaussichten bietet. Günstige Gelegenheitskontexte können somit ein Vorteil bei der Realisierung der Strategie sein.

4.7 Strategische Optionen

Die strategischen Optionen werden bestimmt durch die strategiefähigen strategischen Akteure und den strategischen Kontexten. Auf dieser Grundlage können dann strategische Optionen entwickelt und eine Ausarbeitung erstellt werden, die dann verschiedene Handlungsmöglichkeiten anbietet. Aus diesen Optionen kann

dann eine Strategie entwickelt werden. Wichtig für den analytischen Bezugsrahmen ist, ob die gewonnenen Erkenntnisse aus der Kontextanalyse und der Strategiefähigkeit der strategischen Akteure in die strategischen Optionen integriert wurden oder ob die Wahl der strategischen Mittel zur Zielerreichung unabhängig von diesen Erkenntnissen stattfand (Tils 2005, S. 117). Durch strategische Optionen werden erfolgsversprechende Handlungsrichtungen (Möglichkeitsräume) eröffnet, die aber keine erfolgreiche Umsetzung der Strategie garantieren. Die Schwächen und Stärken der Strategieakteure, ebenso wie die Kontextbedingungen, müssen in die Kalkulationen einbezogen werden. Durch die Ausarbeitung von strategischen Potenzialen und strategischen Szenarien kann dieses Kriterium operationalisiert werden.

Strategische Potenziale befassen sich mit den Fähigkeiten und Kapazitäten von Akteuren und ob Akteure damit mögliche zukünftige Probleme effektiv bearbeiten können. Erst die operative Tätigkeit zeigt jedoch, ob die Strategieakteure ihr Handlungspotenzial auch verwirklichen können (Tils 2005, S. 118). Mit strategischen Szenarien werden mögliche Entwicklungsverläufe skizziert, indem die momentane Ausgangssituation mit Hilfe von Parametern so verändert wird, um künftige Entwicklungen antizipieren zu können. Strategische Szenarien können so den strategischen Kontexten und der Strategiefähigkeit der strategischen Akteure gegenübergestellt werden. Beide Wege des Operationalisierens setzen Umwelt und Akteure in ein gegenseitiges Bezugsverhältnis. Dabei werden denkbare Wege und wählbare Mittel aufgezeigt und Optionen können mit Stärken/Schwächen der Akteure auf ihre Erfolgschancen analysiert werden.

4.8 Strategische Orientierungen

Das Kriterium *Strategische Orientierungen* betrachtet Kollektivakteure und wie deren Handeln von den Bedingungen und Erfordernissen verschiedener Politikfelder beeinflusst wird. Bei der Verwirklichung einer Strategie sind Kollektivakteure in mehreren Politikfeldern tätig. Deshalb dürfen Kollektivakteure bei der Strategiekonzeption nicht nur auf ihre Rolle innerhalb eines Politikfeldes begrenzt werden. *Policy-*

Akteure können als *multiple selves* konzeptualisiert werden, da sie sich nicht nur an einem Politikfeld orientieren müssen (Jansen 1997, S. 213). Ebenso werden die strategischen Kontexte nicht nur durch ein Politikfeld bestimmt. Intern bestehen Kollektivakteure aus individuellen Akteuren und sind „Multiple Selbst" (Wiesenthal 1990, S. 90-91). Diese individuellen Akteure vertreten unterschiedliche Weltsichten, Orientierungen und Werte. Der Kollektivakteur muss dies tolerieren, sich damit auseinandersetzen und dabei handlungsfähig bleiben. Nach außen ist dies ein Vorteil für den Kollektivakteur, da er dadurch mit mehrdeutigen Umwelten umgehen kann. Die intern koexistierenden unterschiedlichen Referenzsysteme leiten nach außen hin das kollektive Handeln des Akteurs. Da Handlungskontexte divergieren und die Rahmenbedingungen stets unterschiedlich sind, ist die Kopräsenz von mehreren Referenzsystemen von Vorteil. Die Entscheidungskalkulationen der Kollektivakteure bilden verschiedene *cognitive maps*, mit denen im Anschluss relevante Handlungssituationen ausgearbeitet und Annahmen über die Absichten anderer Akteure analysiert werden können (Weick und Bougon 1986).

Die multiplen Orientierungen eines Akteurs können für ein besseres Verständnis in interteilsystemische und intrateilsystemische Orientierungen unterteilt werden. Bei interteilsystemischen Differenzen wandelt sich die Orientierung, je nachdem, in welchem Referenzsystem sich der Akteur befindet (ökonomisch, politisch, wissenschaftlich). In diesen Referenzsystemen gelten jeweils andere spezifische Logiken, aus denen dann andere Kalkulationen für erfolgreiches Handeln resultieren. Abhängig vom Kontext „variieren die normativen („Sollen"), kognitiven („Können") und evaluativen („Wollen") Orientierungen der teilsystemisch handelnden Akteure" (Tils 2005, S. 120). In einer Gesamtbetrachtung muss also evaluiert werden, was gemacht werden soll, was gemacht werden kann, was der Kontext zulässt und was die Akteure aufgrund ihrer Orientierungen durchsetzen wollen.

Bei multiplen intrateilsystemischen Orientierungen können individuelle Akteure als Repräsentanten des Kollektivakteurs die strategischen Orientierungen je nach Kontext wechseln. Gründe dafür können der politische Durchsetzungserfolg

sein, eine gewollt abweichende Positionierung von der Konkurrenz, die mediale Wirkung, eine problembezogene Sichtweise oder Verhaltensanforderungen, die aus der thematischen Debatte zu diesem Problemfeld resultieren (Tils 2005, S. 120). Es wird deutlich, dass die Verhaltenskalkulationen je nach Kontext variieren und deshalb unterschiedliche Orientierungen koordiniert werden müssen. Lösungsstrategien für Konflikte zwischen verschiedenen Orientierungen müssen entwickelt werden und für die Evaluation stellt sich die Frage, ob die Mehrdimensionalität von Akteursorientierungen in den Strategien berücksichtigt wird. In einem Kollektivakteur existieren multiple handlungsleitende Rationalitäten und bei der Strategiebildung muss berücksichtigt werden, dass sich die Orientierungen der beteiligten Akteure je nach Ausgangslage und Kontextbedingungen verändern.

4.9 Strategische Zeitdimensionen

Zeitliche Aspekte müssen bei der strategischen Zielerreichung eingeplant werden, da Strategien Lösungsansätze sind, die über den Augenblick hinausgehen. Ein Zeitrahmen ist wichtig, damit eine zeitlich sinnvolle Abfolge der Maßnahmen geplant und später entsprechend ausgeführt werden kann. Eine Unterteilung der Zeitdimensionen in *Policy*- und *Politics*-Perspektive ist hilfreich. Während Strategien meist auf einen langfristigen Zeitraum angelegt werden, durchschneiden Wahlen in relativ kurzen Abständen die politischen Gestaltungszeiträume. Der Logik demokratischer Systeme folgend, benötigen politische Akteure Legitimation um ihre Gestaltungsmacht ausüben zu können und diese Legitimation muss immer wieder neu errungen werden (Müller 1998, S. 300). Dadurch können Probleme bei der zeitlichen Ausgestaltung einer Strategie entstehen. Der Cyber-Raum wird zwar einerseits durch eine hohe Innovationsfrequenz geprägt, andererseits müssen Institutionen und Regelwerke aber auf langfristige Sicht ausgelegt werden. Großunternehmen und Behörden benötigen längere Zeit sich an neue Regelwerke anzupassen und brauchen Planungssicherheit. Programmatische Kurswechsel nach jeder Wahl würden sich negativ auf das Wirtschaftsklima auswirken. Es muss also ein Spagat zwi-

schen der Schnelllebigkeit des Cyber-Raums und der Trägheit von Bürokratie geschaffen werden.

Sach- und fachpolitische Dringlichkeit von politischen Maßnahmen ist aber nur einer der Entscheidungsparameter. Politische Akteure müssen auch politische Forderungen und Stimmungen bei der Strategiebildung mit einbeziehen, da sich manche Maßnahmen wegen des Sanktionspotenzials der WählerInnen als nicht durchführbar erweisen (Tils 2005, S. 121).

Erfolgt die Planung für einen langfristigen Zeitraum, so besteht die Gefahr, dass die eingesetzten Mittel nach einiger Zeit nicht mehr geeignet sind für die Zielerreichung (Wiesenthal 1990, S. 58). Denn über eine längere Zeitspanne hinweg können sich die Realisationsbedingungen in unvorhersehbarer Weise verändern und „mit der Länge des Planungszeitraumes nimmt die Planungsadäquanz exponentiell ab“ (Wiesenthal 1990, S. 33). Gewählte Problemlösungspfade sind dann möglicherweise nicht mehr zielführend und speziell bei einer Cybersicherheitsstrategie kann dies zutreffen, da der Cyber-Raum einem steten Wandel unterliegt.

Eine Strategie zu planen, ohne die Mittel festzulegen und einen zeitlichen Rahmen vorzugeben, ist nicht strategisch, wenig zielführend und verzichtet „auf die möglichen Erträge der strategischen Akteurkompetenz, [denn] Handeln gemäß den situativen Präferenzen simuliert nur den Prozess der natürlichen Evolution“ (Wiesenthal 1990, S. 34). Somit ist kein einheitliches Problemlösungsschema erkennbar und vieles wird dem Zufall überlassen.

Hinzu kommt, dass politische Akteure aufgrund von Zeitknappheit und fehlender Zeitsouveränität oft mehr reaktiv als proaktiv agieren. Getrieben von einem eng geplanten Terminkalender müssen Akteure politische Zeitfenster schaffen, damit dadurch Gelegenheiten entstehen, politische Maßnahmen durchsetzen zu können (Müller 1998, S. 299).

Das rationale Verhalten von politischen Akteuren Probleme situativ zu lösen kann kaum geändert werden (Tils 2005, S. 122). Um dieses Verhalten zu unterbinden, können sich Akteure, „die ihre Kurzsichtigkeit kennen und den Nachteilen

eines (ex Ante) ungewollten Präferenzwandels entgehen möchten“ (Wiesenthal 1990, S. 34), Restriktionen selbst auferlegen.

Die Ausführungen verdeutlichen, dass Strategiekonzepte auf unterschiedliche strategische Zeitdimensionen reagieren. Für die Evaluation ist es bedeutsam, ob die unterschiedlichen Zeithorizonte der strategischen Akteure thematisiert werden und ob bei der Zielerreichung eine systematische Verknüpfung der zeitlichen Perspektiven gewährleistet wird.

4.10 Strategische Bündnisse

Unter Bündnissen werden Kooperationen zwischen zwei oder mehreren Akteuren verstanden, die zeitlich begrenzt sind und zur Durchsetzung bestimmter Ziele dienen. Bündnisse gelten als strategisch, wenn sie intentional, zielgerichtet und aus rationalen Erwägungen über einen längeren Zeitraum erfolgen (Tils 2005, S. 123). Akteure gehen Bündnisse ein, da durch die Koordination ihres Handelns und die Kombination von Mitteln ihre Erfolgschancen verbessert werden. Bündnisse sind ein preiswertes Verfahren um die eigene Machtposition zu verbessern und um „die Gewichte auf dem Spielfeld“ zu verschieben, damit neue Handlungschancen gegenüber Gegenspielern eröffnet werden (Sofsky und Paris 1991, S. 187).

Sofsky und Paris merken an, dass sich mitunter auch Partner zusammentun, „von denen kaum jemand ahnen konnte, dass sie irgendetwas gemeinsam hätten“ (Sofsky und Paris 1991, S. 187). Dies verdeutlicht, dass eine Interessenübereinstimmung zwischen den Bündnispartnern nicht vorausgesetzt wird. Einigkeit über ein gemeinsames Ziel reicht, um die Partnerschaft zu begründen und es wird unterschieden zwischen Zielen der Partner und Zielen des Bündnisses. Die autonomen Akteure des Bündnisses haben unterschiedliche Ziele, sind aber wechselseitig voneinander abhängig. Dieses Spannungsverhältnis muss von den Bündnispartnern ausbalanciert werden, um gemeinsam handlungsfähig zu sein. Mögliche Bündnisse können zwischen politischen Kollektivakteuren (Parteikoalition), zwischen gesellschaftlichen Kollektivakteuren (Branchendialog) oder zwischen politischen und

gesellschaftlichen Kollektivakteuren (Bündnis für Arbeit) geschlossen werden (Tils 2005, S. 124).

Damit Bündnisse überhaupt möglich sind, müssen Akteure die Kompetenz besitzen, strategische Bündnisse auszugestalten und einzugehen. Die Fähigkeit, tragfähige Bündnisse aufzubauen, ist somit eine wesentliche Strategiekompetenz, die notwendig ist, um strategische Handlungsfähigkeit zu erreichen (Raschke und Tils 2008, S. 18). Diese Fähigkeit wäre nur dann verzichtbar, wenn ein Akteur genug Macht hätte, um Entscheidungen eigenhändig durchzusetzen. Allerdings würde der Akteur mit solch einem Vorgehen über längere Zeit seine Legitimationsbasis verlieren. Das bedeutet, staatliche und nichtstaatliche Akteure benötigen für eine erfolgreiche Implementierung von Strategien Kooperationsfähigkeit. Sind Kollektivakteure nicht bündnisfähig, sind sie auch nicht strategisch handlungsfähig.

Beim Kriterium strategischer Bündnisse wird somit danach gefragt, ob die Notwendigkeit strategischer Bündnisse anerkannt, die Bündniskompetenz von Akteuren thematisiert wird und ob sinnvolle Ideen für strategische Kooperationen entwickelt wurden.

4.11 Strategische Kommunikation

Der strategischen Kommunikation kommt zentrale Bedeutung zu, da öffentliche und veröffentlichte Meinung einen großen Einfluss auf den politischen Prozess haben.

Die zunehmende Komplexität der Gesellschaft erschwert es den Parteien, die soziale Legitimation für ihr Handeln zu erhalten (Schmitt-Beck 2002, S. 110). Deshalb müssen strategische Akteure die öffentliche Kommunikation als Instrument verwenden, um die Darstellung der politischen Prozesse beeinflussen zu können. Durch die strategische Öffentlichkeitsarbeit können politische Entscheidungen begründet und erklärt und somit eine Legitimitätsgrundlage geschaffen werden (Schmitt-Beck 2002, S. 111). Dabei findet eine Verschmelzung zwischen Politikherstellung und Politikdarstellung statt (Sarcinelli 1987, S. 66) und das politische Han-

deln nimmt die Züge einer permanenten Kampagne an (Schmitt-Beck 2002, S. 111). Die Kompetenz zu strategischer Kommunikation ist somit eine Voraussetzung für die Strategiefähigkeit strategischer Akteure (Tils 2005, S. 125).

Tils definiert die strategische Kommunikation als den „Versuch der gezielten Einflussnahme auf die politische Agenda und die öffentliche Meinung durch mediale Kommunikationsangebote von politischen Akteuren" (Tils 2005, S. 125). Mit der politischen Agenda sind Themen gemeint, die in der Öffentlichkeit diskutiert und als wichtig erachtet werden. *Issues* sind die politischen Probleme, die einer Lösung zugeführt werden sollen. Im Sinne der strategischen Kommunikation versuchen die Strategieakteure durch Agenda-Building, die für sie vorteilhaften Themen in der Öffentlichkeit zu etablieren. Um dies planen zu können, müssen zu Beginn die Kommunikationsziele festgelegt werden. Desweiteren müssen die Kontextbedingungen analysiert, Handlungsmöglichkeiten ausgearbeitet und strategische Optionen abgeschätzt werden.

Bei der strategischen Kommunikation muss zusätzlich beachtet werden, dass die Massenmedien und die BürgerInnen, als Adressaten von Botschaften, getrennt voneinander zu betrachten sind. Außerdem müssen die Akteure einplanen, dass in der öffentlichen Kommunikation das gesendete kommunikative Ausgangssignal meist nicht identisch mit dem ankommenden Eingangssignal ist (Tils 2005, S. 126). Für die Kollektivakteure bedeutet dies, je mehr Wissen sie über die individuellen Filter besitzen und wie mit Medien umzugehen ist, desto erfolgsversprechender ist die strategische Kommunikationssteuerung.

Kollektivakteure müssen dementsprechend strategische Kommunikationskompetenz aufbauen, indem im Innenverhältnis Klarheit über die Kommunikationsziele herrscht und es ihnen gelingt, eine einheitliche Position nach außen zu vermitteln. Durch das Mediensystem haben sich neue Möglichkeiten in der Politik ergeben. Die zunehmende Personalisierung hat es ermöglicht, dass einzelne Personen in Spitzenpositionen eine ganze Partei strategisch steuern können „und so einen

erheblichen Teil der Implementation von Strategien selbst […] übernehmen" (Raschke 2002, S. 225).

Die verschiedenen politischen Akteure verfügen im Wettbewerb um Aufmerksamkeit über unterschiedliche Ausgangspositionen und Handlungschancen. Die Regierung befindet sich in der besten Ausgangslage und kann aktiv politische Prioritäten setzen, während die Opposition durch Abgrenzungsstrategien gegenüber den Regierenden öffentliche Aufmerksamkeit erregen will (Tils 2005, S. 128). Für Akteure reicht es jedoch nicht, nur Themen in der Öffentlichkeit zu platzieren, sondern die öffentliche Darstellung von Politik in bewusst gewählten Präsentationskontexten (*framing*) ist von ebenso großer Bedeutung (Kaase 1998, S. 49). Mit diesen Mitteln kann zwar keine erfolgreiche Kommunikationssteuerung garantiert werden, da einzelne Akteure die Öffentlichkeit nicht steuern können, aber dennoch ist die strategische Kommunikation ein unverzichtbarer Bestandteil heutiger Politik.

Beim Kriterium strategischer Kommunikation wird untersucht, ob die Kommunikationskompetenz der wichtigen Akteure behandelt wird und ob Kommunikationsstrategien entwickelt wurden.

5 Strategische Evaluation

Die strategische Evaluation der Cybersicherheitsstrategie für Deutschland betrachtet nicht die Art und Weise der Strategieentwicklung, sondern analysiert das ausgearbeitete Strategiepapier, also das Endprodukt. Der Entstehungszusammenhang kann hilfreich sein, um strategische Defizite einordnen zu können, jedoch wird nicht nach einer optimalen Strategiebildung gefragt. Entscheidend ist vielmehr, ob die veröffentlichte Strategie strategisch angelegt ist, wie diese ausgestaltet und ob die nachfolgende strategische Steuerung bei der Konzeptumsetzung mit einbezogen wurde. Dabei „entscheidet nicht der Komplexitätsgrad über die Qualität einer Strategie, sondern die Auswahl der berücksichtigten Aspekte" (Tils 2005, S. 16). Die ausgearbeiteten Kategorien des analytischen Bezugsrahmens zeigen bei der Evaluation, ob

die Strategie Bezug auf die einzelnen Aspekte nimmt. Desweiteren kann ausgehend vom Umfang der Strategie nicht auf ihre Qualität geschlossen werden. Vielmehr kommt es darauf an, die Begriffsdefinitionen präzise zu formulieren, die strategischen Ziele, Mittel und Akteure klar zu benennen und in der strategischen Umwelt zu verordnen, damit eine erfolgversprechende Strategie daraus resultiert.

5.1 Strategiebegriff

Wie bereits dargestellt, basieren politische Strategien auf situationsübergreifenden, erfolgsorientierten und dynamischen Ziel-Mittel-Umwelt-Kalkulationen. Im Strategiepapier „Cyber-Sicherheitsstrategie für Deutschland“ vom Bundesministerium des Innern (BMI) ist zwar keine explizite Strategiedefinition enthalten, jedoch finden sich im Text einige Konkretisierungen, die verdeutlichen sollen, wie der Strategiebegriff im Sinne der Strategen zu verstehen ist.

Strategie bedeutet im Zusammenhang mit dem Cyber-Raum, dass diese Rahmenbedingungen schafft, um die Cyber-Sicherheit zu verbessern (BMI 2011, S. 5) und nur dann erfolgreich sein kann, „wenn alle Akteure gemeinsam und partnerschaftlich ihre jeweilige Aufgabe wahrnehmen. Gleiches gilt im internationalen Kontext” (BMI 2011, S. 6). Desweiteren kann Cyber-Sicherheit „nur in einem umfassenden Ansatz verfolgt werden“, was eine „Vernetzung unter außen- und sicherheitspolitischen Gesichtspunkten unverzichtbar“ werden lässt (BMI 2011, S. 7). Diese Merkmale einer politischen Strategie bilden die Leitlinie der Cyber-Sicherheitsstrategie und somit eine Handlungsanleitung für die strategischen Ziele und Maßnahmen. Durch Maßnahmen in zehn strategischen Bereichen will die Bundesregierung ihre Strukturen an die Gefährdungslage anpassen. Eine Operationalisierung des Strategiebegriffs in zehn strategische Bereiche ist jedoch nicht ausreichend, solange Adressaten und Verpflichtungsgrad der Anweisungen nicht weiter spezifiziert werden.

Deutlich wird die mangelhafte Operationalisierung am Merkmal der Erfolgsorientierung. Das Papier weist darauf hin, dass eine Strategie nur durch Ko-

operation erfolgreich sein kann, aber durch fehlende Zielkorridore kann dies nicht überprüft werden. Diese Gradmesser sind jedoch erforderlich, damit bewertet werden kann, ob die Mittel zur Erreichung der Ziele richtig gewählt wurden.

Die Notwendigkeit von Ziel-Mittel-Umwelt-Kalkulationen wird im Strategiepapier deutlich gemacht durch die Erläuterungen, dass Cyber-Sicherheit nur durch die Vernetzung von unterschiedlichen Politikbereichen möglich ist. Unterschiedliche Bereiche müssen integriert werden und „nur eine Mischung aus innen- und außenpolitischen Maßnahmen kann der Dimension der Problematik gerecht werden“ (BMI 2011, S. 6). Durch die angesprochene Politikfeldintegration wird gezeigt, dass Sicherheit nur durch Zusammenarbeit möglich ist, jedoch werden kulturelle und ökonomische Kontexte nicht angesprochen und mögliche Zielkonflikte der strategischen Akteure werden nicht aufgezeigt. Gerade bei der für den Cyber-Raum wichtigen internationalen Zusammenarbeit ist von unterschiedlichen Interessen auszugehen und eine Strategie sollte mögliche Lösungswege für diese Konflikte aufzeigen.

Im Bereich der internationalen Zusammenarbeit werden politische Institutionen, wie die EU, der Europarat und die NATO genannt, allerdings werden wirtschaftliche und gesellschaftliche Organisationen in der Strategie nicht konkret angeführt. Eine Einbindung der Wirtschaft und der Zivilgesellschaft würde eine breite Basis für eine Strategieumsetzung bilden.

Den ständigen Veränderungen der Rahmenbedingungen im Cyber-Raum wird mit einer dynamischen Strategieausformung begegnet. So soll die Bedrohungslage regelmäßig geprüft werden um „geeignete Schutzmaßnahmen ergreifen“ (BMI 2011, S. 12) zu können und die Bundesregierung wird die „Erreichung der Ziele der Cyber-Sicherheitsstrategie unter Federführung des Nationalen Cyber-Sicherheitsrates in regelmäßigem Abstand überprüfen und die verfolgten Strategien und Maßnahmen den aktuellen Erfordernissen und Rahmenbedingungen anpassen“ (BMI 2011, S. 13). Damit wird darauf hingewiesen, dass eine Strategie an die Prioritäten der Zeit angepasst werden muss. Allerdings wird nicht konkretisiert, in

welchen Abständen diese Überprüfungen stattfinden sollen, wo sich möglicherweise Anpassungsbedarf ergeben könnte und wie diese Anpassungen durchgeführt werden sollen. Dies sollte nicht unbedingt durch konkrete Verfahrensweisen festgelegt werden, aber durch spezifischere Aussagen könnten beliebige Abwandlungen und kurzfristige Problemlösungen vermieden werden.

5.2 Akteure strategischer Politik

Das Evaluationskriterium *Akteure strategischer Politik* befasst sich mit den Kollektivakteuren, die notwendig sind, um die Ziel-Mittel-Umwelt-Kalkulationen umzusetzen und die Strategie zu verwirklichen.

Zu Beginn der Strategie werden Staat, Wirtschaft und Gesellschaft als die zentralen Akteure identifiziert, die für die Gewährleistung von Cyber-Sicherheit zuständig sind. Zugleich sind diese drei Akteure auch Opfer von „gezielt herbeigeführten oder auch zufällig eintretenden IT-Ausfällen“ (BMI 2011, S. 3). Auf der nationalen Ebene verbleibt die Strategie jedoch weitestgehend bei dieser abstrakten Benennung der Kollektivakteure. Dies ist allerdings problematisch, da *die Wirtschaft* und *die Gesellschaft* sehr heterogene Akteure sind, mit unterschiedlichsten Orientierungen. Damit sind diese nur *agierende soziale Gesamtheiten*, die nicht über eine kollektive Akteurqualität verfügen, sondern in Einzelakteure zerfallen (Tils 2005, S. 240). Die Strategie müsste hier, sofern eine Zusammenarbeit mit verschiedenen Akteursgruppen angestrebt wird, aufzeigen, wie eine kollektive Einbindung gelingen kann. Teilgruppen aus der Gesellschaft müssen konkret benannt und die Akteurqualität dieser Gesellschaftsmitglieder muss thematisiert werden. Durch konkrete Rollenzuschreibungen für einzelne Akteursgruppen können Anforderungsprofile formuliert werden. In der Strategie ist jedoch nur die Rede davon, dass die Akteure „ihre jeweilige Aufgabe wahrnehmen sollen“ (BMI 2011, S. 4) und somit wird es verpasst die Verantwortung der einzelnen Akteure zu spezifizieren. Daraus können aber keine konkreten Handlungsanweisungen abgeleitet werden.

Im Bereich der kritischen Infrastrukturen beruft sich die Strategie auf den *Umsetzungsplan KRITIS* als Basis der Zusammenarbeit. Damit ist ein Rahmen gesetzt, wie die Kooperation zwischen Staat und diesem Wirtschaftsbereich aussehen soll. Allerdings wird hinzugefügt, dass die Zusammenarbeit auch systematisch ausgebaut werden soll, aber es wird nicht konkretisiert, wie diese vertiefte Kooperation ausgestaltet wird und welche Rolle die Betreiber der Kritischen Infrastrukturen dabei einnehmen. Andere Kollektivakteure der Wirtschaft, neben den kritischen Infrastrukturen, werden von der Strategie nicht spezifisch benannt (BMI 2011, S. 6-7).

Auf der nationalen Ebene sieht die Bundesregierung eine Zusammenarbeit mit gesellschaftlichen Gruppen vor um „für eine zielgerichtete Bündelung von Informations- und Beratungsangeboten“ zu sorgen (BMI 2011, S. 7). Der Nationale Cyber-Sicherheitsrat[5] (NCS), bestehend aus Vertretern mehrerer Ministerien, Wirtschaftsvertretern und bei Bedarf Vertretern der Wissenschaft, soll als Schnittstelle zwischen Staat und Wirtschaft dienen. Während die teilnehmenden Ministerien genannt werden, gibt es keine Konkretisierungen, welche Wirtschaftsvertreter als assoziierte Mitglieder eingeladen werden, wann der Bedarf besteht, Vertreter aus der Wissenschaft hinzuzuziehen und welche Aufgaben diese Vertreter dann übernehmen sollen. Ob diese Vertreter über eine kollektive Akteurqualität verfügen und damit eine kollektive Einbindung in die Strategieumsetzung gelingen kann, wird ebenfalls nicht weiter ausgeführt.

Die Schnittstelle für eine operative Zusammenarbeit zwischen den Behörden und zwischen Bund und Ländern soll das neu gegründete Nationale-Cyber-Abwehrzentrum[6] (NCAZ) bilden. Die Zusammensetzung des Abwehrzentrums wird konkret benannt und der Aufgabenbereich grob umrissen. Das NCAZ „hat zur Aufgabe, IT-Sicherheitsvorfälle schnell und umfassend zu bewerten und abgestimmte Handlungsempfehlungen zu erarbeiten“ (BSI 2011). Allerdings sollen diese Aufgaben von nur zehn Personen geleistet werden. Führende IT-SicherheitsexpertInnen kritisierten schon früh, dass mindestens das Zehnfache not-

[5] Der Lesbarkeit halber im Folgenden als NCS abgekürzt.
[6] Der Lesbarkeit halber im Folgenden als NCAZ abgekürzt.

wendig sei, um Cyber-Attacken abwehren zu können (Süddeutsche 2011). Noch deutlicher wurden die fehlenden Investitionen in die Akteurqualität des NCAZ, als 2014 ein vertraulicher Bericht des Bundesrechnungshofs, der sich mit dem Bonner Zentrum beschäftigt, von mehreren Medien veröffentlicht wurde. Der Bundesrechnungshof urteilte darin, dass das NCAZ nicht geeignet sei, „die über die Behördenlandschaft verteilten Zuständigkeiten und Fähigkeiten bei der Abwehr von Angriffen aus dem Cyber-Raum zu bündeln“ (Süddeutsche 2014). Gründe dafür sind die zu geringe personelle Ausstattung und ein unklarer Aufgabenbereich. Das führt dazu, dass dem NCAZ Handlungskompetenzen fehlen und es sich nicht gegen andere Institutionen mit einem ähnlichen Aufgabenbereich behaupten kann. Die fehlende Auseinandersetzung, ob der NCAZ die ihm übertragenen Aufgaben überhaupt leisten kann, zeigt, dass die Strategen die Akteurqualität des NCAZ innerhalb des Handlungsumfeldes nicht ausreichend thematisiert haben.

Für den internationalen Handlungskontext werden die Europäische Union und die NATO als wichtige Kooperationspartner für die Gewährleistung von Cyber-Sicherheit identifiziert. Es ist zwar nicht notwendig, die kollektive Akteurqualität dieser beiden Akteure in der Strategie zu thematisieren, allerdings sollte genauer dargestellt werden, wie eine Zusammenarbeit aussehen könnte. Für eine Zusammenarbeit mit der EU beruft sich die Strategie auf die EU-Strategie der Inneren Sicherheit. Auf Basis dieser Strategie soll ein Kodex für staatliches Verhalten im Cyber-Raum ausgearbeitet werden. Allerdings kann diese Vorgehensweise nicht überzeugen, da von den Staaten bisher noch kein Kodex verabschiedet wurde und mit dem Verweis auf die bereits bestehende Strategie auch keine neuen Anreize geschaffen werden. Die Kooperation wird folglich nicht verändert und somit können auch keine Änderungen erwartet werden.

5.3 Strategische Ziele

Mit den strategischen Zielen soll angezeigt werden, in welche Richtung der Stratege die Entwicklung treiben will. In dieser Kategorie wird somit analysiert, ob in der

Strategie die übergeordnet angestrebten Zustände und die darunter liegenden Teilziele gekennzeichnet werden.

Im Strategiepapier formuliert die Bundesregierung eine Leitlinie der Cyber-Sicherheitsstrategie. Demnach ist die Gewährleistung der Sicherheit im Cyber-Raum das übergeordnete Ziel. Die Bundesregierung betrachtet die Cyber-Sicherheit als Teil gesamtstaatlicher Sicherheitsvorsorge und setzt es sich als Ziel einen „signifikanten Beitrag für einen sicheren Cyber-Raum zu leisten" (BMI 2011, S. 4). Um diesen übergeordnet angestrebten Zustand zu erreichen, ist eine enge Kooperation der Strafverfolgungsbehörden notwendig. Gemeinsame Mindestregelungen *(Code of conduct)* mit Verbündeten und Partnern sollen getroffen werden und eine Intensivierung der Koordinierung und des Informationsaustausches ist erforderlich. Im Abschnitt *Strategische Ziele und Maßnahmen* werden die darunter liegenden Teilziele in 10 Punkte aufgeteilt. Erkennbar in diesem Abschnitt ist die deutliche *Policy*-Orientierung der Strategie und das Ziele und Maßnahmen häufig gleichgesetzt werden.

Unter Punkt 1 wird die zentrale Bedeutung der kritischen Informationsinfrastrukturen hervorgehoben. Der Schutz dieser Einrichtungen steht, laut Strategie, im Kern der Cyber-Sicherheit. Eine Operationalisierung dieses Zieles wird jedoch nicht bereitgestellt. Die zentrale Bedeutung dieser Infrastrukturen wird gewürdigt, jedoch kein Sicherheitsniveau festgelegt, an dem gemessen oder überprüft werden könnte, ob das strategische Ziel erreicht wurde. Der systematische Ausbau der Zusammenarbeit ist in diesem Punkt Maßnahme und Ziel zugleich und da keine klare Zielformulierung vorliegt, ist eine letztendliche Zielerreichung auch nicht möglich. Desweiteren besteht noch immenser Klärungsbedarf „ob und an welchen Stellen Schutzmaßnahmen vorgegeben werden müssen und ob und an welchen Stellen bei konkreten Bedrohungen zusätzliche Befugnisse erforderlich sind" (BMI 2011, S. 7). Eine lückenhafte Ausarbeitung und fehlende Zielsetzungen für geeignete Schutzmaßnahmen und Befugnisse stehen in einem klaren Widerspruch zu der zuvor deutlich betonten Wichtigkeit der kritischen Informationsinfrastrukturen. Gerade

im digitalen Bereich, wo täglich neue Bedrohungen entstehen, ist eine schnelle Reaktionsfähigkeit der Behörden notwendig und klar getrennte Aufgabenbereiche verbessern die Zusammenarbeit innerhalb der Akteure und zwischen Akteuren.

Punkt 2 befasst sich mit der Sicherheit von IT-Systemen von BürgerInnen sowie von kleinen und mittelständischen Unternehmen. Die Strategie lässt auch hier klare Zielvorgaben vermissen und will lediglich ein „sicherheitsbewusstes Verhalten im Cyber-Raum" erreichen (BMI 2011, S. 7). Klare Zielformulierungen zu einem beabsichtigten Sicherheitsniveau sind schwierig, wie die Ausführungen zum Sicherheitsverständnis in Abschnitt 3 deutlich gemacht haben. Jedoch könnten beispielsweise Studien herangezogen werden, die Hinweise darauf geben, wie viele Nutzer sichere IT-Systeme verwenden und über Gefahren im Cyber-Raum aufgeklärt sind. Auf dieser wissenschaftlichen Basis könnten dann klare Zielvorstellungen formuliert werden.

Defizite bei der klaren Ausarbeitung von strategischen Zielen sind auch bei der Kriminalitätsbekämpfung im Cyber-Raum erkennbar. Die steigende Cyber-Kriminalität wird zwar als Problem erkannt, jedoch sind simple Appelle, wie die Stärkung der Fähigkeiten von Strafverfolgungsbehörden, um der global agierenden Cyber-Kriminalität entgegenzutreten, nicht spezifisch genug, damit strategische Akteure klare Handlungsanweisungen erhalten und somit für bestimmte Maßnahmen verpflichtet werden. Vorstellbar wären quantitative Ziele, wie die Senkung der Cyber-Kriminalität um 10 % oder qualitative Ziele, wie ein generell hohes Sicherheitsniveau im zivilen Datenverkehr. Eine Auseinandersetzung in der Ausarbeitungsphase der Strategie mit diesen klar definierten Zielen würde zum einen Aussagen über die Erreichbarkeit der Ziele liefern, und zum anderen Erkenntnisse hervorbringen, mit welchen strategischen Mitteln diese Ziele erreicht werden könnten. Behörden wie das BSI oder das Bundeskriminalamt weisen in ihren Berichten darauf hin, dass die große Dunkelziffer bei der Erfassung von Cyber-Delikten ein enormes Problem darstellt. Wären bei der Strategiekonzeption quantitative Ziele

diskutiert worden, dann hätten Strategen dieses doch wesentliche Problem der Strafverfolgung erkannt und Problemlösungen erarbeitet werden können.

Eine Politics-Perspektive der Strategen ist in der Strategie nicht zu erkennen. Mögliche nationale oder internationale Bündnisse, um die eigene Machtposition zu stärken oder den geforderten Cyber-Kodex durchzusetzen, werden, wenn überhaupt, nur kurz erwähnt. In Zusammenarbeit mit internationalen Organisationen soll ein Cyber-Kodex etabliert werden, allerdings wird nicht weiter spezifiziert, was genau solch ein Kodex beinhalten soll und welches Ziel damit verfolgt wird. Das bei den soziopolitischen Bedrohungen angesprochene Problem des sicheren Hafens wäre ein solches Problem, dass mit einem internationalen Cyber-Kodex angegangen werden könnte. Dieses wird jedoch in der gesamten Strategie nicht erwähnt.

Ein Resultat der ungenügend ausgearbeiteten Zielformulierungen ist, dass mögliche Zielkonflikte zwischen strategischen Akteuren nicht in der Strategie aufgelistet wurden. Auf diese Zielkonflikte folgen Interessenkonflikte der Verlierer und Gewinner, die antizipiert werden müssen. Strategen müssen hierfür Dialogstrategien entwickeln, damit die Umsetzung der Strategie nicht gefährdet wird.

5.4 Strategische Mittel

Mit dem Evaluationskriterium *Strategische Mittel* wird analysiert, wie es der Strategie gelingt, die formulierten Ziele mit *Policy*- und *Politics*-Mitteln zu verbinden. Dabei wird unterschieden zwischen *Policy*-Mitteln, politikfeldbezogenen *Politics*-Mitteln und politikfeldübergreifenden *Politics*-Mitteln. Bei der Analyse wird vor allem darauf geachtet, ob spezifizierte Handlungsalternativen und –maßnahmen vorgesehen sind oder ob hauptsächlich auf alte Instrumente zurückgegriffen wird. Denn „Strategiekonzeptionen ohne ausführliche Konkretisierungen der Mittelwahl und neue Ideen können hier kaum Erfolge versprechen“ (Tils 2005, S. 247).
Auf nationaler Ebene sind Initiativen mit gesellschaftlichen Gruppen geplant um BürgerInnen über Cyber-Sicherheit aufzuklären. Dieses politikfeldübergreifende Politics-Mittel wird eingesetzt, um auf ziviler Ebene die eigene Machtbasis zu stär-

ken und auf dieser Grundlage dann das strategische Ziel zu verfolgen. Allerdings werden keine spezifizierten Handlungsalternativen und –maßnahmen genannt, die näher beschreiben, wie die Kooperation mit den gesellschaftlichen Gruppen ausgestaltet werden soll. Welche gesellschaftlichen Gruppen sollen mit eingebunden werden und von wem sollen die Beratungsangebote durchgeführt werden? Wer bestimmt den Inhalt der Informationsangebote und stellt damit sicher, dass strategische Mittel und Ziele konzeptionell miteinander verzahnt sind? Das gleiche Problem ist erkennbar wenn es um die Förderung staatlich zertifizierter Basissicherheitsfunktionen geht. Durch „gezielte Anreize" sollen diese Funktionen zur Massennutzung gebracht werden (BMI 2011: 7). Wie diese Anreize konkret aussehen und ob damit z.B. steuerliche Vorteile oder Subventionen gemeint sind, wird nicht weiter ausgeführt. Diese unkonkrete Ausgestaltung der strategischen Mittel ist wenig erfolgsversprechend, da aufgrund der fehlenden Handlungsmaßnahmen kurzfristige Problemlösungen begünstigt werden.

Auf der Ebene der Politics-Mittel setzt die Strategie vor allem auf die Einrichtung von neuen Institutionen wie dem Nationalen Cyber-Abwehrzentrum und dem Nationalen Cyber-Sicherheitsrat. Diese Behörden sollen vor allem die Zusammenarbeit innerhalb der Bundesregierung und zwischen Staat und Wirtschaft verbessern. Nach der Gründung haben diese Institutionen dann die Aufgabe mit Policy-Mitteln, die ihnen zugewiesenen Problemfelder zu bearbeiten. Gerade beineu gegründeten Institutionen, die sich in einem politischen und wirtschaftlichen System gegen etablierte Akteure durchsetzen müssen, sind klare Rollenzuschreibungen und Handlungsanweisungen notwendig. Ansonsten verfügt der neue Akteur nicht über eine ausreichende Machtbasis, auf deren Grundlage er effektiv handeln kann. Dies wurde am Beispiel des NCAZ deutlich. Etablierte Akteure wie das Zollkriminalamt oder Einrichtungen der Bundeswehr sind zu Lagebesprechungen des Abwehrzentrums überhaupt nicht erschienen (Süddeutsche 2014).

Die große Bedeutung der internationalen Ebene wird mehrfach in der Strategie erwähnt. Auf globaler Ebene will sich die Bundesregierung für eine Harmoni-

sierung des Strafrechts einsetzen, gibt aber keine konkreten Handlungsmaßnahmen vor, wie dieses Ziel erreicht werden soll. Dabei soll das Übereinkommen des Europarates als Grundlage verwendet werden, aber mögliche Bündnisse oder Maßnahmen, die zu einer Durchsetzung beitragen könnten, werden nicht aufgezeigt. Auch beim angestrebten Cyber-Kodex wird deutlich, dass es keine klaren Aussagen zu den strategischen Mitteln gibt und somit keine Verbindung zu den strategischen Zielen hergestellt werden kann. Noch offensichtlicher wird die ungenügende Verzahnung zwischen strategischen Mitteln und Zielen in der Antwort auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN über die Cyber-Strategie und Cyber-Außenpolitik der Bundesregierung. Darin wird gefragt, welche Maßnahmen bisher unternommen wurden und welche geplant sind, um die Transparenz im militärischen und nachrichtendienstlichen Bereich zwischen Staaten zu verbessern. In ihrer Antwort bringt die Regierung zum Ausdruck, dass solche Übereinkommen nur mit komplexen Verhandlungsprozessen erreicht werden können und „kurz- bzw. mittelfristig und im großen Rahmen kaum realisierbar" erscheinen (Bundesregierung der BRD 2011, S. 6). Genau diese Problemstellungen müssen jedoch von einer Strategie durch situationsübergreifende und erfolgsorientierte Kalkulationen bearbeitet werden, um dann mögliche Handlungsmaßnahmen für ein weiteres Vorgehen aufzuzeigen.

5.5 Strategiefähigkeit

Das Evaluationskriterium der Strategiefähigkeit betrachtet die strategische Selbststeuerungskompetenz und bezieht sich dabei auf die Innenverhältnisse von Kollektivakteuren. Dabei ist es nicht notwendig eine konkrete Analyse der Strategieeignung einzelner strategischer Akteure vorzunehmen, jedoch müssen die Leistungsanforderungen zu ihren spezifischen Fähigkeiten passen. Die Strategieakteure müssen die Kapazitäten vorweisen können, die erforderlich sind um die Aufgabenzuweisungen umsetzen zu können.

Mit dem NCAZ und dem NCS wurden von der Bundesregierung im Zuge der Cyber-Sicherheitsstrategie zwei Institutionen gegründet, die wesentliche Aufgaben bei der Gewährleistung der Cyber-Sicherheit übernommen sollen. Im NCS sind das Bundeskanzleramt und verschiedene Ministerien mit jeweils einem Staatssekretär vertreten. Die Besetzung des NCS mit Staatsekretären zeigt, dass die Institution mit den notwendigen Kapazitäten und Kompetenzen ausgestattet wurde, um ihre Funktion als Koordinations- und Organisationsstelle angemessen ausfüllen zu können. Desweiteren wird die Arbeit des NCS von bereits bestehenden Gremien wie dem IT-Planungsrat unterstützt, womit der NCS auf bereits bestehendes Wissen zurückgreifen kann.

Gegensätzlich sieht die Situation beim Nationalen Cyber-Abwehrzentrum aus. Mit zehn Mitarbeitern soll das NCAZ IT-Vorfälle analysieren, Handlungsempfehlungen geben und dabei die Interessen der Wirtschaft berücksichtigen. Die Mitarbeiter kommen von verschiedenen Behörden (BSI, BfV, BBK, BKA, etc.) und jeder „leitet aus der gemeinsam erstellten nationalen Cyber-Sicherheitslage die von ihm zu ergreifenden Maßnahmen ab“ (BMI 2011, S. 8). Hier ist zu erkennen, dass dem NCAZ Aufgaben zugewiesen wurden, ohne Bezug zu den bestehenden Kapazitäten und Kompetenzen. Anders ist die Fülle an Aufgaben für den NCAZ nicht zu erklären, der mit seinen Ressourcen diese ihm zugewiesene Rolle nicht zu leisten vermag. Die unterschiedlichen MitarbeiterInnen müssen sich mit ihrer Behörde abstimmen, mindestens genauso wichtig ist jedoch eine funktionierende Kommunikation unter den MitarbeiterInnen, damit der NCAZ eine interne Strategiefähigkeit aufbauen kann. Diese interne Strategiefähigkeit ist offensichtlich nicht gegeben und schon im August 2011 wurden von der Opposition Zweifel geäußert, ob das NCAZ geeignet ist, um die Sicherheit des Cyber-Raums in Deutschland zu verbessern (Deutscher Bundestag 2011, S. 1). Durch die spätere Untersuchung des Bundesrechnungshofs wurden diese Zweifel bestätigt. Bei einer genaueren Analyse und einem Abgleich der Leistungsanforderungen mit den Ressourcen des neu gegründeten Akteurs hätten diese Fehler vermieden werden können.

Für eine effektive Umsetzung der Strategie ist zu fragen, ob nicht das Bundeskanzleramt der passende Ort wäre für eine institutionelle Verankerung der Cyber-Sicherheitsstrategie, da dort eine politikfeldübergreifende Koordination möglich ist. Als Koordinationsstelle könnte das Bundeskanzleramt durch die zentrale Organisation von Synergieeffekten profitieren und gleichzeitig würde die Verortung dort die Bedeutung der Cyber-Sicherheitsstrategie hervorheben.

5.6 Strategische Kontexte

Bei diesem Evaluationskriterium wird analysiert, ob die strategischen Kontexte mit ihren Möglichkeiten und Grenzen für die strategierelevanten Akteure berücksichtigt werden. Dabei wird vor allem darauf geachtet, ob die *opportunities* und *threats* der unterschiedlichen Akteure herausgearbeitet werden und sich daraus Handlungsmöglichkeiten und –grenzen der strategischen Akteure ableiten lassen. Für eine Strategie ist dies wichtig, da „die Charakterisierungen günstigerer und ungünstigerer politisch-institutioneller Rahmenbedingungen für den Strategieerfolg dann für einzelne Strategieelemente (Bündnisse, Kommunikation, etc.) in Modi des strategischen Vorgehens (Konsensstrategie, Kommunikationsstrategie, etc.) transformiert werden“ können (Tils 2005, S. 256). Aus diesen Überlegungen lassen sich dann Einschätzungen zu globalen Möglichkeiten und Bedrohungen treffen.

In der Strategie wird der globale Charakter des Cyber-Raums betont und hervorgehoben, wie wichtig eine funktionierende Informations- und Kommunikationstechnik für alle Bereiche des gesellschaftlichen und wirtschaftlichen Lebens ist. Daraus wird abgeleitet, dass die Gewährleistung der Cyber-Sicherheit zu einer „zentralen gemeinsamen Herausforderung für Staat, Wirtschaft und Gesellschaft im nationalen und internationalen Kontext“ wird (BMI 2011, S. 3). Der Kontext, in dem die Strategie verortet werden soll, wird somit als ein zentraler Faktor identifiziert, den es für die Strategieumsetzung zu beachten gilt.

Betrachtet man die Strategie im Folgenden genauer und prüft dabei die Ausarbeitung der unterschiedlichen Gelegenheitskontexte, dann werden einige Defizite sichtbar, da die strategischen Kontexte meist nur oberflächlich bearbeitet wurden.

Eine systematische Ausarbeitung und Auflistung der *opportunities* und *threats* der relevanten strategischen Akteure hält die Strategie nicht bereit. Der politisch-institutionelle Gelegenheitskontext wird allgemein beschrieben, aber nicht ausführlicher analysiert. Im Vordergrund der Strategie steht die notwendige Problembehandlung von Cyber-Delikten. Welche institutionellen Hürden bei der Durchsetzung von konkreten Maßnahmen auftreten könnten, wird nicht näher erläutert. Parlamentarische Mehrheiten oder Prozessbedingungen spielen bei der politischen Gestaltung eine bedeutende Rolle und liefern wichtige Erkenntnisse für das strategische Vorgehen. Mögliche Vetospieler, wie zum Beispiel das Bundesverfassungsgericht, die eine Hürde für die Strategieumsetzung darstellen könnten, werden nicht erwähnt. Dabei wurde nur ein Jahr zuvor, im März 2010, das Gesetz zur Vorratsdatenspeicherung vom Bundesverfassungsgericht für nichtig erklärt. Mögliche Vetospieler sollten deshalb für die Strategieumsetzung beachtet werden, um mögliche Hindernisse mit einzukalkulieren. Von Beginn an stand das Bundesverfassungsgericht dem Gesetz kritisch gegenüber und der *Arbeitskreis Vorratsdatenspeicherung*, unterstützt von mehr als 30000 BürgerInnen, reichte eine Verfassungsbeschwerde (Tagesschau 2013) ein. Dies zeigt auch, wie wichtig der politisch-kulturelle Kontext für die Ausarbeitung einer Strategie ist. Die öffentliche Meinung zur digitalen Sicherheit liefert für die Strategen Hinweise darauf, für welche Maßnahmen eine breite Unterstützung in der Zivilgesellschaft zu erwarten wäre und welche gesellschaftlichen Gruppen in den Umsetzungsprozess eingebunden werden könnten.

Die Strategie listet die wichtigen internationalen Institutionen auf, mit denen eine Zusammenarbeit notwendig ist, um die weltweite Harmonisierung des Strafrechts zu erreichen oder einen Cyber-Kodex zu etablieren. Vermissen lässt sie aber eine systematische Analyse der Ausgangslage und welche Umweltbedingungen bei der Zielerreichung zu beachten sind. Innerhalb der Vereinten Nationen sind inter-

nationale Abkommen im digitalen Bereich schwer zu erreichen, da Länder wie China und Russland einerseits und die Vereinigten Staaten andererseits, unterschiedliche Vorstellungen haben was die Ausgestaltung betrifft. Dieses grundsätzliche Problem wird in der Strategie nicht angesprochen und es werden auch keine Handlungsmöglichkeiten vorgeschlagen, die zu einer Lösung beitragen könnten.

5.7 Strategische Optionen

Bei den strategischen Optionen wird die innere Verbindung der Voraussetzungen von Strategie (Strategiefähigkeit, strategische Mittel, Kontexte) mit den strategischen Zielen analysiert. Dabei ist entscheidend, welche Ausgangslage vorliegt, welche Mittel eingesetzt werden und auf Basis welcher Kalkulationen mit welchen strategischen Optionen die angestrebten Ziele erreicht werden sollen.

In der Strategie wird die große Bedeutung von Informationsinfrastrukturen hervorgehoben, aber es wird auch betont, dass die Infrastrukturen immer häufiger Opfer von professionalisierten Angriffen sind. Ein vom Cyber-Raum zunehmend abhängiges globales System führt durch gezielte Angriffe zu einer kritischen Cyber-Sicherheitslage. Primäres Mittel, um die Sicherheit im Cyber-Raum zu gewährleisten, ist die nationale und internationale Kooperation, da die „Cyber-Sicherheitsstrategie nur dann erfolgreichist, wenn alle Akteure gemeinsam und partnerschaftlich ihre jeweilige Aufgabe wahrnehmen“ (BMI 2011, S. 4). Um die Kooperation auf staatlicher Ebene zu verbessern, wurden das NCAZ und der NCS gegründet, auf der internationalen Ebene will sich die Bundesregierung für einen gemeinsamen Cyber-Kodex und die weltweite Harmonisierung des Strafrechts einsetzen. Dass vor allem bei der internationalen Kooperation viele Hürden zu überwinden sind, wird von den Strategen beachtet. Der Strategie gelingt es, eine Verbindung zwischen der Ausgangslage und den angestrebten Zielen herzustellen. Die Kontexte, in denen eine Cyber-Sicherheitsstrategie verortet werden muss, werden ebenfalls in groben Zügen dargestellt. Der Hauptmangel liegt bei den nicht explizit genannten strategischen Mitteln, die zur Erreichung der Ziele notwendig sind. Die

Stärken und Schwächen der beteiligten Akteure werden nicht genügend berücksichtigt bei der Wahl der Handlungsvarianten, wodurch die starke *Policy*-Orientierung der Strategie erneut deutlich wird. Um aber Gestaltungsziele erreichen zu können, muss eine ausreichende Machtbasis vorhanden sein. Somit müssen Strategieakteure entweder strategiefähig sein und über die notwendigen Ressourcen verfügen oder sie müssen mit den nötigen Befugnissen und Ressourcen ausgestattet werden. Auf die begrenzten Kapazitäten und Steuerungsmöglichkeiten im internationalen Kontext wird zwar hingewiesen, jedoch findet keine systematische Auseinandersetzung damit statt, was geleistet werden kann, was andere beitragen sollen „und wie die vorhandenen Fähigkeiten prozessual zusammengeführt werden könnten" (Tils 2005, S. 259). Während versucht wird, die kritischen Infrastrukturen in die Strategie mit einzubinden, so sind deutliche Schwächen erkennbar, wenn es um die Mitwirkung gesellschaftlicher Akteure geht. Hier sollten die Aufgabenbeschreibungen für die Zivilgesellschaft konkretisiert werden, ebenso wie die prozessualen Vorstellungen.

5.8 Strategische Orientierungen

Die strategisch relevanten Akteure müssen ihr Handeln mit Ziel-Mittel-Umwelt-Kalkulationen je nach Handlungsumfeld an unterschiedlichen Referenzsystemen ausrichten. Ein bedeutender Faktor ist, ob in der Strategie die multiplen Referenzsysteme der Akteure berücksichtigt und ob dafür Anschlussstellen geschaffen werden. Dabei muss es einer Strategie vor allem gelingen, teilsystemische Akteure zu motivieren, damit diese die Cyber-Sicherheit forcieren.

Dies misslang beim neugegründeten Cyber-Abwehrzentrum. Für die anderen Behörden hätten Anreize geschaffen werden müssen, damit die Zusammenarbeit mit der neuen Behörde reizvoll erscheint und nicht als Zusatzaufwand verbucht wird. Ein allgemeiner Appell, dass die operative Zusammenarbeit zu einer besseren Koordinierung führt und somit zur Cyber-Sicherheit beiträgt, reicht nicht aus, um alle Akteure von einer Kooperation zu überzeugen. Als zentrale Koordinationsstelle

zwischen den staatlichen Behörden und zwischen Staat und Wirtschaft muss sich das NCAZ an multiple Referenzsysteme anpassen, damit das strategische Handeln auf das jeweilige Handlungsumfeld ausgerichtet ist. Mit nur zehn Personen kann dieser enorme Arbeitsaufwand jedoch nicht geleistet werden.

Auch auf der individuellen Akteursebene sollten Profilierungsmöglichkeiten und Problemlösungsinstrumente für politische Akteure aufgezeigt werden, damit diese aktiv die Entwicklung der Cyber-Sicherheit vorantreiben. Wenn der Bereich der Cyber-Sicherheit für politische Akteure reizvoll erscheint, dann können Gestaltungsmaßnahmen aufgrund der breiteren Machtbasis effektiver durchgesetzt werden. Dass in diesem Bereich noch viel Arbeit zu leisten ist, zeigt zum einen ein Blick in die Strategie, in der dieses Problemfeld nicht angesprochen wird. Zum anderen gelten Netzpolitiker in der deutschen Parteienlandschaft noch immer als Exoten. Der fehlende Sachverstand gepaart mit dem fehlenden Interesse an diesem Politikfeld führt dazu, dass Netzpolitik nur ein Randthema der Parteien ist und „die Einflussnahme der Netzpolitiker auf Prozesse des Agendasettings“ nur sehr gering ist (Bötticher 2015, S. 80). Parteipolitische Mitglieder treffen ihre Entscheidungen „je nach Bezugsfeld und Arena auf der Grundlage divergierender öffentlichkeits-, wettbewerbs-, wählerbezogener oder parteiinterner Kalkulationen“ (Tils 2005, S. 264). Deshalb müssen Anschlussstellen geschaffen werden, die die multiplen Referenzsysteme der politischen wie auch der gesellschaftlichen Akteure berücksichtigen.

Im zweiten Kapitel wurde dargestellt, welche Unterschiede bei der Charakterisierung gemacht werden. Der digitale Raum kann als offene Informationsplattform gedacht werden oder aber als gesetzloser Raum. Die Offenheit des Cyber-Raums wird in der deutschen Cyber-Sicherheitsstrategie jedoch vorwiegend als zu bekämpfendes Problem dargestellt (vgl. BMI 2011, S. 3). Für eine erfolgreiche Einbindung von gesellschaftlichen Akteurgruppen ist es dagegen erforderlich, das unterschiedliche Weltsichten integriert werden und auf deren Referenzsysteme Bezug genommen wird, damit diese Akteurgruppen auch aktiviert werden können. Nur so

kann die in der Strategie oft geforderte Einbindung von gesellschaftlichen Gruppen gelingen.

Für die Wirtschaft stellen Cyber-Angriffe ein enormes Problem dar, aber auch gerade deshalb ist ein Aufzeigen von ökonomischen Chancen und Handlungsmöglichkeiten notwendig, damit wirtschaftliche Akteure zur Cyber-Sicherheit beitragen. Vor allem für Unternehmen müssen die Potenziale der Cyber-Sicherheit sichtbar gemacht werden, damit die Akteure sie in ihre Handlungslogik transformieren können.

International sollen mit der deutschen Cyber-Außenpolitik „deutsche Interessen und Vorstellungen in Bezug auf Cyber-Sicherheit in internationalen Organisationen […] koordiniert und gezielt verfolgt werden" (BMI 2011, S. 11). Für den geplanten internationalen Cyber-Kodex müssen von der Bundesregierung ebenfalls multiple Referenzsysteme berücksichtigt werden, da sich andere Staaten mit abweichenden Umweltbedingungen konfrontiert sehen. Hier wäre es nötig, die unterschiedlichen Orientierungen zu koordinieren und in der Strategie zu erörtern, ob es auch sinnvoll sein kann, Cyber-Sicherheit auch nach anderen Orientierungsreferenzen auszurichten.

In der deutschen Cyber-Sicherheitsstrategie werden allerdings unterschiedliche Referenzsysteme kaum diskutiert, während für die Strategieumsetzung hauptsächlich die in der Administration relevanten Maßstäbe und Referenzpunkte angelegt werden. Dies ignoriert die Heterogenität der Akteursgruppen und vernachlässigt, dass Akteure den digitalen Raum auf unterschiedliche Weise begreifen und somit andere Maßstäbe bei der Problemlösung anlegen.

5.9 Strategische Zeitdimensionen

Die strategischen Zeitdimensionen sollten in einer Strategie berücksichtigt werden, da die strategisch relevanten Akteure ihr Handeln nach unterschiedlichen Zeithorizonten ausrichten müssen. Da der Cyber-Raum kurzen Innovationszyklen unterliegt, muss es einer Strategie in diesem Bereich gelingen, kurzfristige mit langfristi-

gen Maßnahmen zu vereinen. Dabei sollte die Strategie einerseits flexibel, andererseits über den Augenblick hinaus ausgerichtet sein, denn „die Besonderheit strategischen Handelns liegt gerade darin, die längerfristige strategische Linie des Gesamtkonzepts im einzelfallbezogenen politischen Handeln zu verwirklichen“ (Tils 2005, S. 265). Die Problematik der Zeithorizonte in den Teilbereichen wird jedoch nur bedingt in der Strategie aufgegriffen.

Das NCAZ setzt sich aus Mitarbeitern unterschiedlicher Behörden zusammen und kann somit seine Arbeit auch nach einem Regierungswechsel fortsetzen. Diese Kontinuität muss gegeben sein, damit in situativen Einzelentscheidungen eine strategische Linienführung erkennbar wird. Deswegen ist die Besetzung von Institutionen quer zur Dauer der Legislaturperioden ein wichtiges strategisches Mittel, um die Strategieumsetzung für die Zeit nach einem Regierungswechsel zu garantieren.

Der Nationale Cyber-Sicherheitsrat setzt sich unter anderem aus Staatssekretären verschiedener Ministerien zusammen, wodurch ein gewisser Grad an Kontinuität, auch nach einem Regierungswechsel, garantiert wird. Allerdings werden keine internen Zeitstrategien für diese Institutionen entworfen, damit auf die Abweichungen zwischen kurzen *Politics*- und langen *Policy*-Zeithorizonten angemessen reagiert werden kann.

Da eine Kooperation zwischen Staat und Wirtschaft beabsichtigt ist, müssen gerade für Unternehmen Zeitstrategien entworfen werden, damit der zukünftige Nutzen von Sicherheitsmaßnahmen über den jetzt anfallenden Kosten steht. Kooperation wird dadurch nicht garantiert, aber die Einbindung von wirtschaftlichen Akteuren kann somit besser geplant werden.

Eine Strategie für den Cyber-Raum ist nur dann effektiv, wenn auch Abkommen auf der internationalen Ebene abgeschlossen werden. Politische Ereignisse wie die Treffen des Europäischen Rats oder die G7-Gipfel können als Gelegenheitsfenster verwendet werden, um diese Abkommen voranzutreiben. Eine schriftliche Fixierung innerhalb der Strategie, ein politisches Treffen für diese Zwecke zu nut-

zen, würde den Verpflichtungsgrad für eine Bundesregierung erhöhen, diesen Zielen auch nachzukommen.

5.10 Strategische Bündnisse

Bestimmte Maßnahmen lassen sich von einzelnen strategischen Akteuren durchführen, für andere jedoch besteht die Notwendigkeit, strategische Bündnisse einzugehen. Mit diesem Evaluationskriterium wird deshalb analysiert, ob in der Strategie Bündnisideen entwickelt werden und ob die Bündniskompetenzen der strategischen Akteure berücksichtigt werden.

Da der Schutz der kritischen Informationsinfrastrukturen im Kern der Cyber-Sicherheit steht, wird eine noch engere Zusammenarbeit zwischen Staat und Wirtschaft als dringend erforderlich angesehen. Neue Bündnisideen werden hingegen nicht entwickelt, sondern die Strategie beruft sich auf den bereits bestehenden „Umsetzungsplan KRITIS“ (BMI 2011, S. 6). Auf dieser Basis soll die Kooperation systematisch ausgebaut werden, neue konzeptionelle Vorschläge werden aber nicht vorgestellt. In Anbetracht der Tatsache, dass der Schutz von Informationsinfrastrukturen höchste Priorität genießt, die Zusammenarbeit jedoch immer noch unzureichend ist, sollten konkrete Möglichkeiten zur Gestaltung von Bündnissen im Strategiekonzept vorgestellt werden.

Damit sich ein sicherheitsbewusstes Verhalten im Cyber-Raum bei den BürgerInnen ausbildet, sollen Initiativen mit gesellschaftlichen Gruppen durchgeführt werden. Insbesondere wenn beabsichtigt ist, gesellschaftliche Gruppen einzubinden, dann muss eine partizipativ orientierte Strategie auch Wege und Verfahren der Teilnahme aufzeigen. Denn diese Gruppen verfügen nicht über eine kollektive Akteurqualität, was bedeutet, dass zivilgesellschaftliches Engagement „auf externe Beratung und Unterstützung bei der Prozess-Koordination angewiesen“ ist (Draschba et al. 2003, S. 9). Die Strategie sollte sich deshalb damit auseinandersetzen, wie sich strategische Bündnisse idealerweise zusammensetzen und ob sektorale oder sektorübergreifende Bündnisse von Vorteil sind. Trifft dies nicht zu, wie in

dieser Strategie, dann wird die Bedeutung der Kooperation der Zivilgesellschaft betont, aber es werden keine Voraussetzungen geschaffen, die gesellschaftlichen Akteure in strategische Bündnisse zu integrieren.

Auf der internationalen Ebene stützt sich die Strategie auf das Übereinkommen des Europarates, um die Computerkriminalität zu bekämpfen. Somit wird die Basis einer gemeinsamen Zusammenarbeit genannt, aber es werden keine Kooperationsinitiativen entwickelt, die zu einer besseren Ausgangslage für ein Übereinkommen beitragen könnten. Für die deutsche Cyber-Außenpolitik wird in der Strategie signalisiert, dass die deutschen Interessen gezielt verfolgt werden sollen (BMI 2011, S. 11). Durch die zahlreichen anderen Staaten mit unterschiedlichen Interessenlagen sind aber Widerstandspotenziale zu erwarten. Deshalb wäre eine Ausarbeitung von möglichen Bündnispartnern hilfreich bei der Durchsetzung der eigenen strategischen Ziele.

5.11 Strategische Kommunikation

Über die Ausarbeitungsphase der deutschen Cyber-Sicherheitsstrategie gibt es nur wenige Informationen. Die Strategie wurde vom Bundesinnenministerium ausgearbeitet, am 23. Februar vom Kabinett beschlossen und anschließend von Bundesinnenminister de Maizière und Bundeswirtschaftsminister Brüderle öffentlich vorgestellt. Das Bundesinnenministerium koordiniert die Umsetzung der Strategie über den Bundesbeauftragten für Informationstechnik. Diese zentrale Rolle des BMI lässt darauf schließen, dass bei der Strategiekonzeption hauptsächlich ExpertInnen dieses Ministeriums beteiligt waren. Über eine Dialog- oder Beteiligungsphase für gesellschaftliche Gruppen in der Entstehungsphase der Strategie gibt es keine Informationen und auch in der Strategie selbst wird nicht auf solche Mitwirkungsinstrumente hingewiesen.

In der Strategie wird zwar ein kommunikativer Austausch als wichtig erachtet, die relevanten wirtschaftlichen und gesellschaftlichen Akteursgruppen wurden jedoch nicht in die Erarbeitungsphase mit eingebunden. Die Bedeutsamkeit der

Mitwirkung von Bürgerinnen und Bürger für die Cyber-Sicherheit wird in der Strategie betont (vgl. BMI 2011, S. 7), die Zielgruppen werden aber nicht deutlich angesprochen. Desweiteren wird nicht konkretisiert, wer auf der administrativen Ebene für die Organisation des gesellschaftlichen Dialogs verantwortlich ist. In der Strategie sind nur allgemeine Formulierungen vorzufinden wie: „wir werden in gemeinsamen Initiativen…" oder „wir wollen durch gezielte Anreize…" (BMI 2011, S. 7). Das Bundesinnenministerium ist jedoch ein komplexer Kollektivakteur, bestehend aus vielen individuellen Akteuren. Damit eine Strategie effektiv umgesetzt werden kann, ist es notwendig, die Zuständigkeiten innerhalb des Kollektivakteurs klar zu kommunizieren.

Die strategische Kommunikation weist somit Unzulänglichkeiten in der Kommunikationsleistung auf. Einerseits wird nicht spezifiziert, wer auf der administrativen Seite als Vermittler auftreten soll, andererseits werden die gesellschaftlichen und wirtschaftlichen Zielgruppen nicht konkret benannt. Somit ist kein Konzept vorhanden, dass mit kommunikativen Maßnahmen zur Etablierung eines Dialogs beitragen könnte.

Aufgrund der kurzen Innovationszyklen im Cyber-Raum wird die Bundesregierung „in regelmäßigem Abstand überprüfen", ob die gewählten Maßnahmen an die neuen Rahmenbedingungen angepasst werden müssen (BMI 2011, S. 13). Berichte zum Umsetzungsstand der Strategie oder zu neuen Anpassungen werden allerdings nicht veröffentlicht. Dies hätte jedoch zwei Vorteile. Durch die öffentliche Kommunikation können gesellschaftliche Gruppen den Umsetzungsprozess verfolgen und dadurch auch aktiv mit Initiativen in den Prozess eingreifen. Desweiteren würden öffentliche Berichte den Verpflichtungsgrad der zuständigen Behörden erhöhen, die selbst gesetzten Ziele in der vorgesehenen Zeit zu erreichen.

Kampagnenkonzepte, mit denen für die eigene Strategie oder um Kooperation von anderen strategischen Akteuren geworben wird, werden in der Strategie nicht angesprochen. Dabei stellen politische Kampagnenkonzepte ein geeignetes Mittel dar, um die strategischen Ziele zu erreichen. Die in der Strategie verwende-

ten Leitbilder und Begriffe sind hauptsächlich für staatliche Behörden und Kritische Informationsinfrastrukturen geeignet. Mitarbeiter dieser Institutionen können durch ihre Expertise auf dem Feld der Cyber-Sicherheit die Auswirkungen der Maßnahmen einschätzen. Sollen gesellschaftliche Gruppen jedoch an der Strategieumsetzung mitwirken, dann sollten die oft abstrakten und komplexen Sachverhalte einfacher dargestellt werden, um eine breite, öffentliche Diskussion zu ermöglichen. Auch für Kooperationen auf der internationalen Ebene ist es sinnvoll zu identifizieren, welche Felder kommunikativ günstig sind und wo sinnvolle Anknüpfungspunkte liegen, um die strategischen Maßnahmen zu unterstützen.

In der Strategie ist keine klare Kommunikationsstrategie erkennbar und die Anforderungen an die moderne gesellschaftliche Kommunikation werden auch nicht gesondert berücksichtigt.

6 Fazit

Durch die Analyse ist auch inhaltlich deutlich geworden, dass die deutsche Cyber-Sicherheitsstrategie den Nationalen Plan zum Schutz der Informationsinfrastrukturen ersetzen soll. Offensichtlich wird dies durch die zentrale Stellung, die der Schutz von Kritischen Informationsinfrastrukturen in der Strategie einnimmt. Eine Strategie für die Sicherheit im Cyber-Raum sollte jedoch umfassender konzipiert werden und auch andere Bereiche konkret in die Strategie mit einbeziehen.

Die Cyber-Sicherheitsstrategie für Deutschland lässt sich somit in ihrer Ausgestaltung eher als Programm charakterisieren denn als Strategie. Die im Bezugsrahmen formulierten Anforderungen, die eine Strategie erfüllen muss, werden nur in einigen Ausnahmen erfüllt. Der Programmcharakter der Strategie wird deutlich durch die starke administrative Ausrichtung und durch die zehn strategischen Bereiche, die hauptsächlich als individuelle Problemfelder begriffen, aber nicht in Beziehung zueinander gesetzt werden.

Abgesehen davon enthält die Cyber-Sicherheitsstrategie für Deutschland auch innovative Elemente. Mit den Neugründungen des Nationalen Cyber-Abwehrzentrums und des Nationalen Cyber-Sicherheitsrats wird versucht, das noch junge Subfeld der Cyber-Sicherheit aktiv mitzugestalten. Die identifizierten zehn strategischen Bereiche vereinfachen die politische Problembearbeitung und können öffentlichkeitswirksam kommuniziert werden, um eine öffentliche Debatte zu initiieren. Gerade am NCAZ wird die starke *Policy*-Orientierung der Strategie deutlich. Einerseits wird der neuen Institution ein großer Aufgabenkatalog zugewiesen, andererseits befasst sich die Strategie nicht näher damit, welche Umweltbedingungen für das NCAZ vorliegen und wie das Abwehrzentrum diese Fülle an Aufgaben bewältigen soll.

Desweiteren werden wesentliche Elemente einer Strategie in dem Konzept nicht aufgegriffen oder nur ungenügend ausgearbeitet. Das situationsübergreifende Element einer Strategie wird als einziges Kriterium erfüllt. Bei der Ausgestaltung der Strategie werden die einzelnen strategischen Einheiten berücksichtigt und somit werden die Maßnahmen und Ziele der Strategie auch über den Augenblick hinaus ausgerichtet. Allerdings muss hier angemerkt werden, dass die später beschlossene Digitale Agenda und das IT-Sicherheitsgesetz weitere Maßnahmen im digitalen Bereich sind, aber in der Strategie nicht konkret angesprochen wurden. Dies zeigt auch, dass von den Strategen kein ganzheitlicher Ansatz ausgearbeitet wurde, der alle Bereiche der Cyber-Sicherheit miteinander in Beziehung setzt. Richtig ist, dass eine längerfristige Orientierung im Bereich der Cyber-Sicherheit durch den dauerhaften Wandel schwierig ist. Dennoch darf die Gewährleistung der Cyber-Sicherheit nicht zu einem Stückwerk verfallen, in dem fortwährend neue Regelwerke geschaffen werden, mit denen situativ auf neue Begebenheiten reagiert wird.

Ziel-Mittel-Umwelt-Kalkulationen, die wichtig sind, um strategische Zusammenhänge zu erkennen, werden in der Strategie nicht explizit herausgearbeitet. Desweiteren werden in der Strategie die strategischen Ziele und Mittel nicht im Zusammenhang mit den relevanten Umweltbedingungen betrachtet. Auch die syste-

matische Verknüpfung von Zielen und Mitteln findet nur in begrenztem Umfang statt. Die Strategen beschränken sich vorwiegend auf die *Policy*-Dimension, jedoch müsste in einer Strategie auch die *Politics*-Dimension der nationalen und internationalen Ebene ausführlicher bearbeitet werden. Es wird zwar erwähnt, dass internationale Abkommen schwierig zu erreichen sind, jedoch findet keine systematische Ausarbeitung zu Vetospielern oder möglichen strategischen Bündnissen statt. Das bloße Ansprechen der schwierigen internationalen Bedingungen ist in erster Linie eine Einschätzung und unterstreicht erneut den Programmcharakter der Konzeption. In einer Strategie sollten jedoch die politischen Kontextbedingungen konkret analysiert werden, um Aussagen über Möglichkeiten der Strategieumsetzung treffen zu können.

Mögliche Hindernisse, die auf nationaler Ebene bei der Strategieumsetzung auftreten könnten, werden im Konzept nur ungenügend bearbeitet. Es wird angemerkt, dass mit der Wirtschaft und der Gesellschaft kooperiert werden muss, jedoch gehen die Strategen nicht näher auf mögliche Konkurrenzperspektiven ein, die eine Kooperation behindern könnten. Hier müsste ein Strategiekonzept die wirtschaftlichen und gesellschaftlichen Prozessbedingungen beachten. Für eine Strategie ist es notwendig, die unterschiedlichen strategischen Orientierungen der gesellschaftlichen Gruppen und der Wirtschaft zu berücksichtigen, damit eine erfolgsversprechende Strategieimplementation möglich gemacht wird. Eine spezifische Ausarbeitung der Mehrdimensionalität von Akteursorientierungen, mit der Lösungsstrategien für mögliche Konflikte entwickelt werden könnten, findet jedoch nicht statt. Auch hier wird die starke *Policy*-Orientierung der Strategie deutlich. Genauso wie die *Policy*-Dimension muss aber auch die *Politics*-Dimension betrachtet werden, die sich mit den Bedingungen der Strategiedurchsetzung befasst. Dieses Defizit kann nicht behoben werden, indem Kollektivakteure ungezielt angesprochen werden und darüber hinaus nur aufgefordert werden, an der Strategie mitzuwirken, ohne dass Möglichkeiten der Mitwirkung vorgestellt werden.

Die Ausgestaltung von zukünftigen Strategien wird zeigen, wie die Bundesregierung mit dem Spannungsverhältnis Freiheit versus Sicherheit im Cyber-Raum umgehen will. Interessant wird zu sehen sein, ob Mitwirkungsinstrumente geschaffen werden, die es der Zivilgesellschaft erlauben,

aktiv an diesem Prozess teilzunehmen. Ebenso wichtig wird es sein, wie sich die Zusammenarbeit in informellen Zirkeln zwischen privaten Cyber-Sicherheitsfirmen und Behörden entwickeln wird und ob dabei demokratische Grundrechte beachtet werden.

7 Literatur und Quellenverzeichnis

Adomavicius, G., Bockstedt, J. C., Gupta, A. & Kauffman, R. J. (2004). An ecosystem model of technology evolution. Carlson School of Management. University of Minnesota. http://misrc.umn.edu/workingpapers/fullpapers/2004/0429_112404.pdf. Zugegriffen: 13. Apr. 2016.

Allan, C. S. (2013). Attribution Issues in Cyberspace. *Chicago-Kent Journal of International and Comparative Law*, *13*(2), 55–83.

Balicer, R. D. (2007). Modeling Infectious Diseases Dissemination through Online Role-Playing Games. *Epidemiology*, *18(*2*)*, 260.

Barlow, J. P. (1990). Crime and Puzzlement. https://w2.eff.org/Misc/Publications/John_Perry_Barlow/crime_and_puzzlement.1.txt. Zugegriffen: 12. Apr. 2016.

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence. Zugegriffen: 12. Apr. 2016.

Betz, D. J. & Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyberpower.* London: The International Institute for Strategic Studies. Abingdon, Oxon: Routledge.

Bendiek, A. (2012). Europaïsche Cybersicherheitspolitik. Berlin: Stiftung Wissenschaft und Politik. http://www.swp-berlin.org/fileadmin/contents/products/studien/2012_S15_bdk.pdf. Zugegriffen: 20. Apr. 2016.

Bendiek, A. (2013). Umstrittene Partnerschaft: Cybersicherheit, Internet Governance und Datenschutz in der transatlantischen Zusammenarbeit. Berlin: Stiftung

Wissenschaft und Politik. https://www.swp-berlin.org/fileadmin/contents/products/studien/2013_S26_bdk.pdf. Zugegriffen: 28. Apr. 2016.

Benz, A. (2001). *Der moderne Staat. Grundlagen der politologischen Analyse*. München/Wien: Oldenburg.

Bundeskriminalamt. (2014). Cybercrime – Bundeslagebild 2014. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2014.html. Zugegriffen: 02. Mai 2016.

Bundeskriminalamt. (2016). Internetkriminalität / Cybercrime. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetKriminalitaet.html. Zugegriffen: 02. Mai 2016.

Bötticher, A. & Mareš, M. (2013). Extremism as a security threat in the Central Europe. German experiences from countering extremist – implications and recommendations for Czech Republic and Slovak Republic and Central European influence towards Germany. CENAA – Centre for European and North Atlantic Affairs. http://cenaa.org/wp-content/uploads/2013/02/German-experiencesCounterMeasuresPDF.pdf. Zugegriffen: 04. Juni 2016.

Bötticher, A. (2015). Die Strukturlandschaft der Inneren Sicherheit der Bundesrepublik Deutschland. In Lange, H.-J. & Bötticher, A (Hrsg.), *Cyber-Sicherheit* (S. 69-102). Wiesbaden: Springer Fachmedien Wiesbaden.

Bredow, W. (2006). Sicherheitspolitik im 21. Jahrhundert-Neue Herausforderungen. Informationen zur politischen Bildung, Heft(291). http://www.bpb.de/izpb/8669/neue-herausforderungen?p=all. Zugegriffen: 05. Juni 2016.

BSI. (2011). Nationales Cyber-Abwehrzentrum nimmt Arbeit auf. https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2011/Cyber-Abwehrzentrum_01042011.html. Zugegriffen: 19. Juni 2016.

BSI. (2014). Die Lage der IT-Sicherheit in Deutschland 2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile. Zugegriffen: 03. Mai 2016.

BSI. (2015). Die Lage der IT-Sicherheit in Deutschland 2015. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf?__blob=publicationFile&v=4. Zugegriffen: 02. Mai .2016.

BSI. (2016). 25 Jahre BSI – Mit Transparenz mehr Sicherheit. BSI Magazin 2016/01. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2016_01.pdf?__blob=publicationFile&v=9. Zugegriffen: 03. Mai .2016.

Bundesregierung der BRD. (2011). Antwort der Bundesregierung – Cyber-Strategie und Cyber-Außenpolitik der Bundesregierung. Deutscher Bundestag. 17. Wahlperiode. Drucksache 17/6971. http://dipbt.bundestag.de/dip21/btd/17/069/1706971.pdf. Zugegriffen: 25. Juni 2016.

Busuioc, M. & Curtin, D. (2011). Die EU-Strategie der inneren Sicherheit, der EU-Politikzyklus und die Rolle der (RSFR-)Agenturen: Perspektiven, Stolpersteine und Auswege. Studie im Auftrag des Europäischen Parlaments, PE453.185. http://edz.bib.uni-mannheim.de/daten/edz-ma/ep/11/EST40730.pdf. Zugegriffen: 06. Juli 2016.

CSTB. (2002). Cybersecurity Today and Tomorrow: Pay Now or Pay Later. Washington, DC: National Academy Press. http://people.eecs.ku.edu/~saiedian/Teaching/Fa10/710/Readings/nrc-security.pdf. Zugegriffen: 02. Juni 2016.

Daase, C. (2010). Wandel der Sicherheitskultur. *Aus Politik und Zeitgeschichte* (*APuZ)*, 50/2010, 9-16.

Deibert, R. & Rohozinski, R. (2010a). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology, 4*(1), 15-32.

Deibert, R. & Rohozinski, R. (2010b). SHADOWS IN THE CLOUD: Investigating Cyber Espionage 2.0. https://de.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0. Zugegriffen: 04. Juni 2016.

Department of Defense. (2010). Department of Defense Dictionary of Military and Associated Terms. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf. Zugegriffen: 19. Apr. 2016).

Department of Homeland Security. (2011). Enabling Distributed Security in Cyberspace - Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action. https://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf. Zugegriffen: 13. Apr. 2016.

Deutscher Bundestag. (2011). Kleine Anfrage der Abgeordneten Agnes Malczak, Omid Nouripour, Dr. Konstantin von Notz, Marielouise Beck (Bremen), Volker Beck (Köln), Viola von Cramon-Taubadel, Thilo Hoppe, Uwe Kekeritz, Katja Keul,Ute Koczy, Kerstin Müller (Köln), Lisa Paus, Claudia Roth (Augsburg), Manuel Sarrazin, Dr. Frithjof Schmidt, Hans-Christian Ströbele und der Fraktion BÜNDNIS 90/DIE GRÜNEN. Cyber-Strategie und Cyber-Außenpolitik der Bundesregierung. Deutscher Bundestag. 17. Wahlperiode.

Drucksache 17/6802.http://dipbt.bundestag.de/dip21/btd/17/068/1706802.pdf. Zugegriffen: 25. Juni 2016.

Dhamdhere, A. & Dovrolis, C. (2011). Ten years in the evolution of the Internet ecosystem. The Pennsylvania State University CiteSeerX Archives. http://www.cc.gatech.edu/~dovrolis/Papers/internet-evolution-imc08.pdf. Zugegriffen: 13. Apr. 2016.

Dillon, M. (2005). Global Security in the 21st Century: Circulation, Complexity and Contingency. *ISP/NSC Briefing Paper 05/02*, Chatham House.

Dolata, U. (2001). Risse im Netz - Macht, Konkurrenz und Kooperation in der Technikentwicklung und –regulierung. In Simonis, G., Martinsen, R. & Saretzki, T. (Hrsg.), *Politik und Technik. Analysen zum Verhältnisvon technologischem, politischem und staatlichem Wandel am Anfang des 21. Jahrhunderts* (S. 37-54). Opladen: Westdeutscher Verlag.

Draschba, S., Heidorn, F. & Zachow, E. (2003). Möglichkeiten zur Erhöhung des Dynamikpotenzials in Nachhaltigkeitsinitiativen. Umweltbundesamt. http://www.umweltbundesamt.de/sites/default/files/medien/publikation/short/k2300.pdf. Zugegriffen: 01. Juli 2016.

Duden. (2016). Stichwort cyber-, Cyber-, http://www.duden.de/rechtschreibung/cyber_. Zugegriffen: 12. Apr. 2016.

Dunn Cavelty, M. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review*, *15*(1), 105-122.

Dutton, W. H. & Peltu, M. (2007). The Emerging Internet Governance Mosaic: Connecting the Pieces. *Information Polity: The International Journal of Government & Democracy in the Information Age*, *12*(1/2), 63–81.

Endreß, C. & Petersen, N. (2012). Die Dimensionen des Sicherheitsbegriffs. Bundeszentrale für Politische Bildung., Dossier Innere Sicherheit. http://www.bpb.de/politik/innenpolitik/innere-sicherheit/76634/dimensionen-des-sicherheitsbegriffs?p=all#footnode5-5. Zugegriffen: 04. Juni 2016.

Farwell, J. P. & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival, 53*(1), 23-40.

Freudenberg, D. (2014). Unternehmenssicherheit und Unternehmenskultur als Bestandteile einer umfassenden Sicherheitspolitik – Plädoyer für einen integrierten Gesamtansatz. In Lange, H. J., Wendekamm, M., Endreß, C. (Hrsg.), *Dimensionen der Sicherheitskultur* (S. 281–300). Wiesbaden: Springer Fachmedien Wiesbaden.

Ganz, M. (2005). Why David sometimes wins: Strategic capacity in social movements. In Messick, D. M. & Kramer, R. M. (Hrsg.), *The psychology of leadership: New perspectives and research* (S.209–238). Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers.

Gibson, W. (1984). *Neuromancer*. New York: Ace.

Goetz, J. & Leyendecker, H. (2014, 7. Juni). Rechnungsprüfer halten Cyber-Abwehrzentrum für "nicht gerechtfertigt". Süddeutsche Zeitung. http://www.sueddeutsche.de/digital/behoerde-in-bonn-rechnungspruefer-halten-cyber-abwehrzentrum-fuer-nicht-gerechtfertigt-1.1989433. Zugegriffen: 19. Juni 2016.

Graham, S. (2006). Cities and the "War on Terror." *International Journal of Urban and Regional Research, 30*(2), 255–276.

Grunwald, D. (2012). The Internet Ecosystem – The Potential for Discrimination. The Pennsylvania State University CiteSeerX Archives.

http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.211.9370. Zugegriffen: 13. Apr. 2016.

Hansen, L. & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, *53*(4), 1155–1175.

Hayden, M. V. (2011). The Future of Things "Cyber". *Strategic Studies Quarterly*, *5*(1), 3-7.

Jansen, D. (1997). Das Problem der Akteurqualität korporativer Akteure. In Benz, A. & Seibl, W. (Hrsg.), *Theorieentwicklung in der Politikwissenschaft – eine Zwischenbilanz* (S. 193–235). Baden-Baden: Nomos.

Kaase, M. (1998). Demokratisches System und die Mediatisierung von Politik. In Sarcinell, U. (Hrsg.), *Politikvermittlung und Demokratie in der Mediengesellschaft. Beiträge zur politischen Kommunikationskultur* (S. 24–51). Bonn: Bundeszentrale für politische Bildung.

Kuhn, J. & Hauck, M. (2011, 17. Juni). Behörden-Sheriffs gegen Hacker-Attacken. Süddeutsche Zeitung. http://www.sueddeutsche.de/digital/nationales-cyber-abwehrzentrum-bei-hackerangriff-ruf-den-minister-1.1109300. Zugegriffen: 19. Juni 2016.

Lapointe, A. (2011). When Good Metaphors Go Bad: The Metaphoric "Branding" of Cyberspace. Center for Strategic and International Studies. http://csis.org/publication/when-good-metaphors-go-bad-metaphoric-branding-cyberspace. Zugegriffen: 14. Apr. 2016.

Moore, J. H., Parrott, L. K. & Karas, T. H. (2008). Metaphors for cyber security. Sandia Report. http://www.evolutionofcomputing.org/Multicellular/Cyberfest%20Report.pdf. Zugegriffen: 14. Apr. 2016.

Müller, E. (1998). Impressionen zum Thema Zeit in der Umweltpolitik. In Jann, W., König, K., Landfried, C. & Wordelmann, P. (Hrsg.), *Politik und Verwaltung auf de Weg in die transindustrielle Gesellschaft* (S. 297–308). Baden-Baden: Nomos.

Münkler, H. (2010). Strategien der Sicherung: Welten der Sicherheit und Kulturen des Risikos. Theoretische Perspektiven. In Münkler, H. ; Bohlender, M. & Meurer, S. (Hrsg.), *Sicherheit und Risiko: über den Umgang mit Gefahr im 21. Jahrhundert* (S. 11–34). Bielefeld: transcript Verlag.

Nissenbaum, H. (1998). Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, *17*(5/6), 559–596.

Nissenbaum, H., Friedman, B. & Felten, E. (2001). COMPUTER SECURITY: COMPETING CONCEPTIONS. http://arxiv.org/html/cs/0110001v2. Zugegriffen: 04. Juli 2016.

OECD. (2012). Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy. OECD Digital Economy Papers, OECD Publishing. http://dx.doi.org/10.1787/5k8zq92vdgtl-en. Zugegriffen: 04. Juli 2016.

Parrika, J. (2005). Digital Monsters, Binary Aliens – Computer Viruses, Capitalism and the Flow of Information. *The Fibreculture Journal*, *2005*(4). http://four.fibreculturejournal.org/fcj-019-digital-monsters-binary-aliens-%E2%80%93-computer-viruses-capitalism-and-the-flow-of-information/. Zugegriffen: 03. Mai 2016.

Platt, V. (2011). Still the Fire-Proof House?: An Analysis of Canada's Cyber Security Strategy. *International Journal*, *67*(1), 155-168.

Raschke, J. (2002). Politische Strategie. Überlegungen zu einem politischen und politologischen Konzept. In Nullmeier, F. & Saretzki, T. (Hrsg.), *Jenseits des Regie-*

rungsalltags. Strategiefähigkeit politischer Parteien (S. 207-241). Frankfurt am Main: Campus.

Raschke, J. & Tils, R. (2008). Politische Strategie. *Forschungsjournal Neue Soziale Bewegungen*, *21*(1), 11-24.

Sarcinelli, U. (1987). *Symbolische Politik: Zur Bedeutung symbolischen Handelns in der Wahlkampfkommunikation der Bundesrepublik Deutschland*. Opladen: Westdeutscher Verlag.

Schmitt-Beck, R. (2002). Laufen, um auf der Stelle zu bleiben: „Postmoderne" Kampagnepolitik in Deutschland. In Nullmeier, F. & Saretzki, T. (Hrsg.), *Jenseits des Regierungsalltags. Strategiefähigkeit politischer Parteien* (S. 109-132). Frankfurt am Main: Campus.

Singelnstein, T. & Stolle, P. (2012). *Die Sicherheitsgesellschaft: Soziale Kontrolle im 21. Jahrhundert.* Wiesbaden: VS Verlag für Sozialwissenschaften.

Sofsky, W. & Paris, R. (1991). *Figurationen sozialer Macht: Autorität - Stellvertretung – Koalition*. Opladen: Leske + Budrich.

Stegmaier, P. & Feltes, T.(2008). Die ganze Vernetzung der inneren Sicherheit: Wissenskrise und Effektivitätsmythos. In Möllers, M. H. W. & Ooyen, R. (Hrsg.), *Jahrbuch Öffentliche Sicherheit 2008/2009* (S.305 – 316). Frankfurt am Main: Verlag für Polizeiwissenschaft.

Sterling, B. (1994). The hacker crackdown: law and disorder on the electronic frontier. United States: Project Gutenberg. http://www.gutenberg.org/etext/101. Zugegriffen: 12. Apr. 2016.

Tagesschau. (2013, 9.Juli). EuGH verhandelt über Vorratsdatenspeicherung - Wer telefoniert wann mit wem?

https://www.tagesschau.de/ausland/vorratsdatenspeicherung192.html. Zugegriffen: 28. Juni 2016.

Teubner, G. (1999). Polykorporatismus: Der Staat als "Netzwerk" öffentlicher und privater Kollektivakteure. In Niesen, P. & Brunkhorst, H. (Hrsg.), *Das Recht der Republik. Festschrift Ingeborg Maus* (S. 346–372). Frankfurt: Suhrkamp.

The National Strategy (2003, Feb.). The National Strategy to Secure Cyberspace. The White House. Washington, DC.. https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf. Zugegriffen: 02. Juni 2016.

Tils, R. (2005). *Politische Strategieanalyse: Konzeptionelle Grundlagen und Anwendung in der Umwelt- und Nachhaltigkeitspolitik*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Tsebelis, G. (2002). *Veto Players: How Political Institutions Work*. Princeton: Princeton University Press.

Von Heinegg, W. H. (2015). Cyber-Bedrohungen aus dem Netz. Informationen zur politischen Bildung (326). http://www.bpb.de/izpb/209667/cyber-bedrohungen-aus-dem-netz?p=all. Zugegriffen: 12. Juli 2016.

Weick, K. E. & Bougon, M. G. (1986). Organizations as Cognitive Maps. Charting Ways to Success and Failure. In Sims, H. P. & Gioia, D. A. (Hrsg.), *The Thinking Organization. Dynamics of Organizational Social Cognition* (S. 102–135). San Francisco: Jossey-Bass.

Welch, L. D. (2011). CYBERSPACE – THE FIFTH OPERATIONAL DOMAIN. https://www.ida.org/~/media/Corporate/Files/Publications/ResearchNotes/RN2011/2011%20Cyberspace%20-%20The%20Fifth%20Operational%20Domain.pdf. Zugegriffen: 06. Juni 2016.

Wiesenthal, H. (1990). *Unsicherheit und Multiple-Self-Identität: Eine Spekulation über die Voraussetzungen strategischen Handelns*. MPIFG discussion paper, 90(2). Max-Planck-Inst. für Gesellschaftsforschung.

WSIS. (2005). World Summit on the Information Society – Tunis Commitment. http://www.itu.int/net/wsis/docs2/tunis/off/7.html.
Zugegriffen: 20. Apr. 2016.