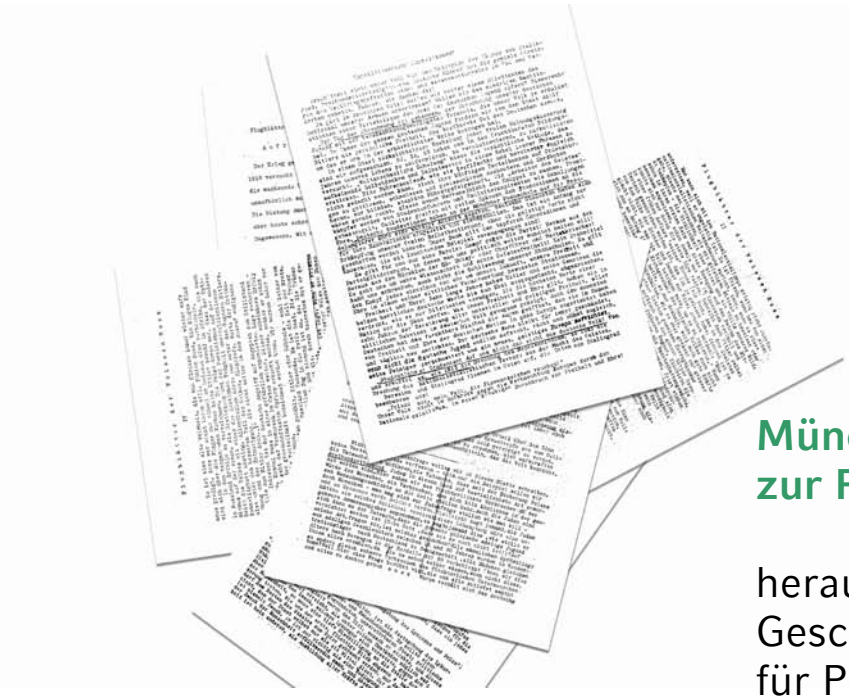
LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

GESCHWISTER-SCHOLL-INSTITUT
FÜR POLITIKWISSENSCHAFT



Münchener Beiträge zur Politikwissenschaft

herausgegeben vom
Geschwister-Scholl-Institut
für Politikwissenschaft

2013

Pascal Pillokeit

Nationale Policies zur Herstellung von Cybersicherheit. Globale Konvergenz oder machtpolitische Pfadabhängigkeit?

Masterarbeit bei
Prof. Dr. Bernhard Zangl
SoSe 2013

Inhaltsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

ANSSI	Agence nationale de la sécurité des systèmes d'information
ARPA	Advanced Research Project Agency
BDI	Bundesverband der Deutschen Industrie
BDK	Bund Deutscher Kriminalbeamter
BelNIS	Belgian Network Information Security Platform
BfV	Bundesamt für Verfassungsschutz
BIPT	Belgian Institute for Postal Services and Telecommunications
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und neue Medien
BKA	Bundeskriminalamt
BMI	Bundesministerium des Inneren
BND	Bundesnachrichtendienst
BPol	Bundespolizei
BSI	Bundesamt für Sicherheit und Informationstechnik
BSI-IT-LZ	IT-Lagezentrum
BVerfG	Bundesverfassungsgericht
CERT	Computer emergency response team
COSSI	Centre d'opération pour la sécurité des systèmes d'information
CSOC	Cyber Security Operations Centre
DARPA	Defense Advanced Research Projects Agency
DIHK	Deutsche Industrie- und Handelskammertag
GAR	Gemeinsames Abwehrzentrum gegen Rechtsextremismus
GASIM	Gemeinsame Analyse- und Strategiezentrum illegale Migration
GCHQ	Government Communications Headquarters
GIZ	Gemeinsame Internet-Zentrum
GTAZ	Gemeinsames Terrorismus-Abwehrzentrum
IKT	Informations- und Kommunikationstechnik
KIS	Information Security Coordination Council
MSCD	Most Similar Cases Design
NCA	National Crime Agency
NCAZ	Nationales Cyber-Abwehrzentrum
NPT	Norwegian Post- and Telecommunication Authority

NSM	National Security Authority
OSCIA	Office of Cyber Security and Information Assurance
SGDSN	Secrétariat général de la défense et de la sécurité nationale
SOCA	Serious Organised Crime Agency

1. Einleitung

Am 4. Oktober 1957 startete die Sowjetunion erfolgreich den ersten künstlichen Erdsatelliten Sputnik 1 und schickte diesen in eine stabile Umlaufbahn um die Erde. Der Start und die dahinter stehende technische Leistung kam für die westlichen Staaten, allen voran die USA, überraschend. Die demonstrierte Leistungsfähigkeit sowjetischer Raketen gab Anlass zur Sorge, denn diese konnten nun theoretisch als nuklear bestückte Interkontinentalraketen US-amerikanisches Territorium erreichen. Der sogenannte Sputnikschock löste vor allem aber eine Krise in der Selbstwahrnehmung der US-Amerikaner aus, da ihr technologischer Vorsprung und der bis dahin sicher geglaubte Überlegenheitsanspruch in Frage gestellt wurde. Als Reaktion wurde der „Wettlauf ins All“ ausgerufen und die Anstrengungen für die Entwicklung von Militär- und Raumfahrttechnologien intensiviert. Zur Koordination und finanziellen Unterstützung wissenschaftlicher Projekte wurde schon im Februar 1958 die *Advanced Research Project Agency* (ARPA) ins Leben gerufen. Dem Psychologen und Computerwissenschaftlicher J.C.R Licklider wurde die Leitung von Projekten zur computerbasierten Unterstützung des Militärs übertragen. Licklider war der Überzeugung, dass Computer nicht nur einfache Rechenmaschinen seien, sondern dass der Mensch durch verstärkte Interaktion mit diesen eines Tages in der Lage wäre seine natürlichen Fähigkeiten zu erweitern. Er formulierte als erster die Vorstellung eines globalen Computernetzwerkes (*Intergalactic Computer Network*), wie wir es heute in Form des Internets kennen. Auf Lickliders Initiative entstand 1966 innerhalb der ARPA das *Information Processing Techniques Office* (IPTO). Dessen Leiter Bob Taylor verfolgte Lickliders Idee weiter und hatte den Plan entwickelt, die Computer verschiedener akademischer Forschungszentren in den USA mittels eines Netzwerkes miteinander zu verbinden. Dadurch sollten Ressourcen wie Rechenkapazitäten und Informationen effektiver gemeinsam nutzbar gemacht werden. Zusammen mit Lickliders Nachfolger, Ivan Sutherland und Forschern des *Massachusetts Institute of Technology* wurde in den Folgejahren daran geforscht die Datenübertragung durch mittels Paketvermittlung anstelle der (bis dahin) üblichen Leitungsvermittlung ,wie beispielsweise im Telefonnetz, umzusetzen. Im September 1969 war es schließlich soweit: Erstmals wurde eine Verbindung zwischen einem Computer der UCLA und der ARPA hergestellt. Das ARPANET war geboren – der Vorgänger des modernen Internet. Etwa zur selben Zeit gab es in andern Ländern ähnliche Projekte, wie z.B. das *National Physical Laboratory* (NPL) in Großbritannien und CYCLADES in Frankreich, welche ebenfalls auf lokaler Ebene Computernetzwerke gebildet hatten. Die Forschungsarbeiten von ARPA zur

Datenübertragung und das ARPANET waren zu diesem Zeitpunkt jedoch bereits richtungsweisend. Die verschiedenen lokalen und nationalen Computernetzwerke konnten nicht miteinander verbunden werden, da diese unterschiedliche Protokolle, d.h. unterschiedliche Kommunikationsregeln, verwendeten. Zu diesem Zwecke entwickelte die zwischenzeitlich unbenannte *Defense Advanced Research Projects Agency* (DARPA) das TCP/IP-Protokoll, welches universell und unabhängig vom Betriebssystem von jedem Netzwerk genutzt werden konnte. Die von der (D)ARPA entwickelten Paketübermittlungsverfahren und TCP/IP-Protokolle bilden noch heute das Rückgrat des Internets (Internet Society 2012). Dieser historische Überblick zeigt, dass ein Ereignis wie der Sputnikschock, eine Reihe von Folgeereignissen auslösen kann, welche am Ende nur noch lose mit dem ursprünglichen Auslöser in Verbindung stehen. Möglicherweise wäre das Internet auch ohne den Sputnikschock, vielleicht sogar in einem anderen Land, entstanden. Aber die Basis des Internets, wie wir es heute kennen, ist entscheidend von Lickliders Vision des *Intergalactic Computer Network* geprägt worden (ComputerWeekly.com 2009). Diese legte den Pfad für die Folgearbeiten seiner Kollegen, welche mit ihren Innovationen die Rolle der ARPA als wegweisende Forschungseinrichtung begründeten und später die technischen Grundlagen für das moderne Internet legten. Ohne den Sputnikschock und die darauffolgende starke Forschungsfinanzierung in den USA würde das Internet in der heutigen Form nicht existieren.

Das Internet hat seit seiner Entstehungsphase als akademisches Netzwerk verschiedene Entwicklungsphasen durchlaufen: Von der Institutionalisierung, und der Internationalisierung, bis zur Kommerzialisierung und dem Dotcom-Boom am Ende des 20. Jahrhunderts. Das Internet ist dabei stetig gewachsen und hat vor allem seit der Jahrtausendwende massiv an Bedeutung für Privatpersonen, die Wirtschaft und die Staaten zugenommen. Während die Anzahl der Internetnutzer im Jahr 2000 noch bei sieben Prozent lag, ist diese bis 2013 auf knapp 40 Prozent der Weltbevölkerung und 77 Prozent der Bewohner der entwickelten Welt gestiegen (International Telecommunications Union 2013: 2). Auch die Bedeutung des elektronischen Handels für die Wirtschaft hat rasant zugenommen. 2012 überstieg das Gesamtvolumen erstmals die Marke von einer Billion US-Dollar. Innerhalb der G-20 Länder machte die Internetwirtschaft 2010 mit 2,3 Billionen US-Dollar bereits 4,1 Prozent der gesamten Bruttoinlandsprodukte aus. Mittlerweile wird das Internet als unverzichtbarer Antreiber ökonomischen Wachstums gesehen (eMarketer 2013; bcg.perspectives 2012).

Die Nationalstaaten haben die Entwicklung des Internets lange Zeit aus der Ferne betrachtet. In den Demokratien der westlichen Welt wurde die Regulierung des Internets in den Anfangsjahren überwiegend sich selbst überlassen. Dies brachte mit der Zeit jedoch nicht nur Vorteile mit sich, sondern auch neue Möglichkeiten für Kriminalität und andere illegale Aktivitäten. In dem Maße in dem die Abhängigkeit vom Internet stieg, nahm auch das Schadenspotential für die Nutzer zu. Bedrohungen aus dem Internet, oder weiter gefasst aus dem Cyberspace gehen heute von einer Reihe unterschiedlicher Akteure aus. Dies können einzelne Individuen, kriminell oder ideologisch motivierte Gruppierungen, Unternehmen oder staatliche Organisationen sein. Ein Großteil der Angriffe stellt Cyberkriminalität mit dem Ziel der Extraktion von Geld oder Informationen von Individuen oder Unternehmen dar. Andere Angriffe sind ideologisch motiviert, wie die Aktivitäten von Gruppierungen wie *Anonymous*, welche sich in der Regel gegen staatliche Einrichtungen richten. Dazu kamen in den letzten Jahren verstärkt Spionage- und Sabotage-Angriffe seitens Regierungen hinzu, wobei die Sabotage des Kernkraftwerkes Buschehr 2010 im Iran durch Stuxnet am meisten Aufmerksamkeit erzeugt hat.

Regierungen weltweit haben in den letzten Jahren zunehmend begonnen auf diese neuen Bedrohungen zu reagieren. Dazu wurden Strategien entworfen und neue Institutionen, mit dem Ziel kritische Kommunikations- und Informationsinfrastrukturen zu schützen und ausreichend Sicherheit im Cyberspace herzustellen geschaffen. Der externe Anpassungsdruck, d.h. das Maß an Cyberbedrohungen, sowie die Abhängigkeit vom Cyberspace sind für Industriestaaten[1] dabei ähnlich stark ausgeprägt. Dies lässt vermuten, dass die verschiedenen nationalen Policies zur Abwehr von Cyberbedrohungen (im Folgenden mit „Cyber-Policy“ abgekürzt) konvergieren sollten. Ein Blick auf die nationalen Strukturen und Institutionen offenbart jedoch deutliche Unterschiede. So gibt es auf der einen Seite Staaten mit einer stark zentralisierten Cyber-Policy. Dabei koordinieren wenige, mit starken Kompetenzen ausgestattete Sicherheitsbehörden, oft auf hierarchischem Wege, die Aktivitäten der relevanten Akteure. Auf der anderen Seite finden sich Cyber-Policies mit Netzwerk-Charakter: Hier wurden keine oder nur wenige neue Behörden geschaffen. Stattdessen wurden Institutionen zur Kooperation zwischen bereits existierenden Sicherheitsbehörden aufgebaut, deren Zusammenarbeit auf horizontaler Ebene verläuft. Obwohl die westlichen Staaten also demselben externen Druck durch Cyberbedrohungen ausgesetzt sind, ist keine Konvergenz in den verschiedenen nationalen Cyber-Policies auszumachen.

[1] Der Begriff „Industriestaat“ wird hier synonym zum englischen Begriff „developed country“ verwendet und gilt als Abgrenzung zu Schwellen- und Entwicklungsländern.

Diese Beobachtung begründet die Forschungsfrage, welcher diese Arbeit nachgeht: *Warum kann keine Konvergenz bezüglich nationaler Cyber-Policies beobachtet werden? Wie kann die Ausprägung der Cyber-Policies in demokratischen Industriestaaten erklärt werden?* Die hier vertretende Hypothese ist, dass die Entstehung der Cyber-Policy vom politischen System des jeweiligen Landes beeinflusst ist. Je mehr Vetospieler ein politisches System aufweist, desto eher bildet sich eine Cyber-Policy mit Netzwerk-Ansatz heraus. Im Umkehrschluss befördern wenig Vetospieler die Herausbildung einer zentralisierten Cyber-Policy.

Das folgende Kapitel wird sich der Konvergenzthese sowie der Frage, warum eine Konvergenz im Cybersicherheitsbereich zu erwarten sein sollte, widmen. Kapitel drei beleuchtete die Varianz der nationalen Cyber-Policies. Kapitel vier zeigt auf, warum das Vetospielertheorem am besten geeignet ist, um den Untersuchungsgegenstand zu erklären und bietet mit der Pfadabhängigkeit einen kausalen Mechanismus für die Beziehung zwischen Vetospielern und Cyber-Policy an. Nachdem in Kapitel fünf das Untersuchungsdesign dargelegt wurde, folgen in Kapitel sechs die Fallstudien anhand der politischen Entscheidungsprozesse in den Ländern Deutschland und Großbritannien, welche zu den nationalen Cyber-Policies geführt haben. Mit einem Gesamtfazit und einem Ausblick beschließt Kapitel sieben diese Arbeit.

2. Die Konvergenzdebatte: Konzepte und Ursachen

Das folgende Kapitel ist in drei Teile gegliedert: Zunächst werden die Konvergenzthese und die dahinterstehenden Wirkungsmechanismen dargelegt. Danach wird die These auf das Problemfeld der Cybersicherheit übertragen. Abschließend erfolgt eine Verfeinerung der These und die Formulierung der zu widerlegenden Nullhypothese.

In den Politikwissenschaften wurden in den letzten Jahren wieder verstärkt Konvergenzthesen diskutiert. Dabei wird von einer Tendenz zur allmählichen Angleichung nationaler Politiken, Institutionen und Kulturen ausgegangen. Die verschiedenen Ursachen für diese Konvergenz werden generell auf die zunehmende Verflechtung von Staaten und Gesellschaften auf der internationalen Ebene im Zuge der Globalisierung zurückgeführt. Beiträge zur Konvergenzforschung kommen aus unterschiedlichen wissenschaftlichen Disziplinen wie der Ökonomie, der Politikwissenschaft oder der Soziologie. Auch die Untersuchungsgegenstände unterscheiden sich und können Institutionen, Politiken, Praktiken oder Normen umfassen. Statt Konvergenz werden zuweilen auch die Begriffe Diffusion oder Transfer verwendet. Obwohl diese Begriffe konzeptionelle Unterschiede aufweisen und

unterschiedliche analytische Fokusse setzen, haben sie zunächst alle gemein, dass von einer allmählichen Angleichung des Untersuchungsgegenstandes über verschiedene Staaten hinweg ausgegangen wird (Holzinger et al. 2007: 11-16).

Die Konvergenzdebatte wird bereits seit den 1970er Jahren geführt und ist stark verknüpft mit der Frage nach den Einflüssen der Globalisierung und der (neuen) Rolle des Staates. Die ersten Hypothesen bezüglich Konvergenz wurden in der Ökonomie aufgestellt. Richard Cooper argumentierte, dass die zunehmende ökonomische Abhängigkeit, genauer die Verflechtung nationaler Märkte, die Effektivität von nationalen Politiken erodieren würde. In Folge dessen wäre die nationale Autonomie hinsichtlich der wirtschaftlichen Selbstbestimmung bedroht und die Rolle des Staates würde geschwächt (Cooper 1968: 164). Verschiedene empirische Arbeiten konnten jedoch zeigen, dass gerade die innerstaatliche Verfasstheit eines Staates kritisch für das Verständnis von länderspezifischen Reaktionen auf äußere ökonomische Herausforderungen ist (Gourevitch 1978; Evans et al. 1985). Im Zuge der späteren Globalisierungsdebatte wurden Coopers Argumente wieder aufgenommen. Eine Reihe von Arbeiten postulieren, dass im Rahmen der zunehmenden Globalisierung ein verstärkter Standortwettbewerb zwischen den Staaten, sowie die sich auflösende Kongruenz von Problembereichen und Einflusssphären des Staates, zu einem massiven Verlust der Effektivität nationaler Politiken führen würde (Zürn 2013: 406). Die bekanntesten Schlagwörter in diesem Zusammenhang sind „race to the bottom“ (Krugman 1995) und „the retreat of the state“ (Ohmae 1995; Strange 1996). Erneut jedoch konnten diese Diagnosen in empirischen Studien keine Bestätigung finden. Stattdessen konnte gezeigt werden, dass unter bestimmten Umständen der externe Druck durch die Globalisierungseffekte den Bedarf an nationaler Regulierung erhöhen kann. So können z.B. nationale Sozialpolitiken die negativen Effekte einer fortschreitenden globalen Marktintegration abfedern (Rodrik 1997). Durch staatliche Intervention kann zudem die Wettbewerbsfähigkeit der einheimischen Wirtschaft gestärkt werden. Die Studien lieferten zudem Belege dafür, dass die institutionellen Gegebenheiten eines Staates und die dahinter stehenden politischen Aushandlungsprozesse, der größte Einflussfaktor sind um die Divergenz nationaler Politiken als Reaktion auf externe Herausforderungen zu verstehen (Zürn 2013: 407). Besonders die verschiedenen Varianten des Kapitalismus (*varieties of capitalism*) wurden als wichtiger Faktor identifiziert um verschiedene nationale Regulierungsformen zu erklären (Hall/Soskice 2001). Zudem konnte keine Konvergenz hinsichtlich einer verstärkten Deregulierung in den 90er Jahren festgestellt werden. Diese Ergebnisse haben jedoch auf inhaltlicher und methodologischer Basis Kritik erfahren. So wurde bemängelt, dass die Globalisierungseffekte sich erst im Laufe der 90er

Jahre entfalten konnten und dass viele der Studien sich daher nur auf einen kurzen relevanten Untersuchungszeitraum stützten. Zudem wurde die Validität der verwendeten Indikatoren kritisiert (Zürn 2013: 407). Befürworter der Konvergenztheorie konnten ihrerseits Belege für ihre Hypothesen präsentieren. So konnten in bestimmten Sektoren wie der Post und Telekommunikation starke Tendenzen hinsichtlich einer zunehmenden Liberalisierung und Deregulierung festgestellt werden. Abschließend lässt sich zur Konvergenzdebatte festhalten, dass die bisherigen Ergebnisse gezeigt haben, dass sich die Globalisierungseffekte in verschiedenen Policy-Bereichen unterschiedlich auswirken können. Daher scheint eine Ausdifferenzierung der Forschung geboten. Offen bleibt zudem die Frage nach den Bedingungen, unter denen Globalisierungseffekte in manchen Staaten stärker Einfluss entfalten können als in anderen, sowie die Rolle nationaler Strukturen bei der Mediation dieser Globalisierungseffekte in verschiedenen Problemfeldern.

In den wissenschaftlichen Beiträgen zur Konvergenzdebatte werden verschiedene Ursachen für eine Konvergenz nationaler Politiken angeführt. Funktionalistische Erklärungen nehmen an, dass Staaten zunehmend ähnlichen Problemen in Bereichen wie Umwelt, Gesellschaft oder Technik ausgesetzt sind. Da sich die Problemstrukturen ähneln, wird abgeleitet, dass Staaten auch gleichartige Problemlösungen in Form von Politiken entwickeln. Die Reaktion der Staaten geschehen dabei unabhängig voneinander. Eine Konvergenz kommt aufgrund parallelen Problemdrucks, einer ähnlichen Wahrnehmung des Problems und vergleichbaren Rahmenbedingungen zustande (Holzinger et al. 2007: 25). In der Ökonomie wurde früh die These formuliert, dass mit der wachsenden Abhängigkeit nationaler Märkte einzelne nationale Regulierungen nicht länger funktionieren würden. Aufgrund des internationalen, ökonomischen Wettbewerbs stehen die einzelnen Staaten unter einem Anpassungszwang, welcher zu einer Konvergenz der nationalen Regulierungen führt (Cooper 1968). Auch Lern- und Imitationsprozesse können zu Konvergenz führen, wenn erfolgreiche Modelle von anderen Staaten übernommen werden (Rose 1991; Stone 2000). Voraussetzung ist, dass eine transnationale Kommunikation und ein Austausch von Informationen stattfinden können. Ein anderes Beispiel für einen solchen „weichen“ Mechanismus sind Überzeugungsprozesse oder die Diffusion von Ideen in andere Länder über bestimmte gesellschaftliche Gruppen oder Eliten (Holzinger et al. 2007: 28). Eine Angleichung nationaler Politiken kann auch auf internationale Verträge zurückgehen, welche verschiedene Staaten zusammen eingegangen sind, oder eine gemeinsame Mitgliedschaft in supranationalen Organisationen (List/Zangl 2003; Abbott et al. 2000). Die Einhaltung von z.B. EU-Richtlinien oder die *Compliance* mit Internationalem Recht kann Politik-Konvergenz

erklären. Verrechtlichungs- und Harmonisierungsprozesse spielen hier die zentrale Rolle. Zuletzt kann Konvergenz auch direkt durch politische oder wirtschaftliche Konditionalität zustande kommen, wenn andere Staaten oder Organisationen ihren Einfluss durch ihre politischen oder finanziellen Ressourcen geltend machen können. Zwang und Konditionalität spielt im Vergleich mit den anderen Mechanismen jedoch eine untergeordnete Rolle bei der Konvergenz von Politiken (Schimmelfennig et al. 2003).

Die beschriebenen Mechanismen können in ihrer Wirksamkeit durch eine Reihe von intervenierenden Faktoren beeinflusst werden. Generell wird davon ausgegangen, dass je ähnlicher sich zwei Länder sind, desto einfacher Politiken übernommen werden können. Die Schwierigkeit der Implementation von Politiken von einem Land zum anderen hängt davon ab, wie ähnlich sich die politischen Systeme und Institutionen sind. Politische Programme können leichter kopiert werden, wenn sie wenig Anpassung benötigen. Eine gemeinsame Kultur und Sprache zwischen zwei Ländern kann zudem die beschriebenen, „weichen" Diffusionsmechanismen, wie Imitations- oder Lernprozesse, erleichtern. Auch die geografische Nähe und sozio-ökonomische Ähnlichkeiten befördern die Übernahme von Politiken. Diese kann andererseits erschwert werden, wenn Politiken einen stark redistributiven oder symbolhaften Charakter haben. Solchen Programmen sind zumeist Aushandlungsprozesse zwischen nationalen Akteuren vorausgegangen und können daher nicht einfach auf andere Länder mit anderen Akteuren übertragen werden (Holzinger et al. 2007: 31).

2.1 Konvergenz der nationalen Cyber-Policies?

Die beschriebenen funktionalen Bedingungen für eine Konvergenz nationaler Politiken lassen sich im Politikfeld der Cybersicherheit finden. Der externe, parallele Druck, dem die westlichen Staaten ausgesetzt sind, sind dabei die Cyberbedrohungen im und aus dem Cyberspace. Diese können in sechs Kategorien eingeteilt werden: Black Hat Hacking, Hacktivism, Cyberkriminalität, Cyberspionage, Cyberterrorismus und Cyberkrieg (Lachow 2009: 438-442). Diese Kategorien sollen einen Überblick bieten und haben weder den Anspruch vollständig noch sich gegenseitig ausschließend zu sein. Der Begriff „Hacken" bezeichnet heute im Allgemeinen den illegalen Zugriff auf Computersysteme und das Manipulieren derselben. Hacken zum Entdecken und Veröffentlichen von Sicherheitslücken zum Zwecke der Verbesserung dieser Systeme wird als White Hat Hacking bezeichnet. Black Hat Hacking hingegen umfasst jegliche Art von Hacken für den eigenen Nutzen. Die Aktionen werden in der Regel ausgeführt von Individuen oder kleineren Gruppen, nicht selten

allein aus Gründen der Selbstbestätigung oder der Freude am Hacken. Ziele können einzelne Individuen, sowie öffentliche Einrichtungen oder Unternehmen sein. Ein Beispiel ist der 2003 auf das Unternehmen Valve verübte Hack, bei dem der Quellcode eines kurz vor der Veröffentlichung stehenden Spieles gestohlen und ins Internet gestellt wurde. Der dadurch entstandene Schaden wurde auf 250 Millionen US-Dollar geschätzt. Eine einzelne Person hatte den Hack ausgeführt (Poulsen 2008). Hacktivism kann ähnliche Aktivitäten umfassen wie Black Hat Hacking, ist jedoch ideologisch motiviert und richtet sich zumeist gegen Regierungen oder regierungsnahe Einrichtungen. Ziel ist es Missfallen gegenüber einer bestimmten politischen Entscheidung oder Inhalten auszudrücken. Auch patriotisch motiviertes Hacken fällt in diese Kategorie. Ein Beispiel dafür sind die 2007 ausgeführten Attacken auf estnische Regierungsseiten, welche mutmaßlich von Hackergruppierungen aus Russland ausgeführt wurden (Traynor 2007). Die Motivation hinter Cyberkriminalität hingegen ist zumeist ökonomischer Gewinn und dementsprechend zielt diese auf Unternehmen oder Individuen. Allgemein wird jegliche Art von Kriminalität im und mittels Cyberspace als Cyberkriminalität bezeichnet: Beispiele sind das Phishing und Computerbetrug. Cyberkriminalität hat sich zu einem der größten Probleme im Cyberspace entwickelt. Eine Studie von Norton aus dem Jahre 2010 kam zu dem Ergebnis das Zweidrittel aller Internetnutzer bereits Opfer von Cyberkriminalität geworden sind. McAfee schätzte den entstandenen Schaden für die globale Wirtschaft im Jahre 2008 auf eine Billion US-Dollar (Mills 2009). Cyberspionage stellt eine Unterkategorie von Cyberkriminalität dar und meint die widerrechtliche Aneignung geheimer oder vertraulicher Daten mittels Informationstechnologien. Chinas Spionageaktivitäten haben in den letzten Jahren verstärkt an Aufmerksamkeit gewonnen und vor kurzem wurde die Existenz einer militärisch eingebundenen Hackereinheit bekannt (Mandiant 2013). Der Whistleblower Edward Snowden wiederrum enthüllte, dass auch die NSA sich via Hackingangriffe wiederrechtlichen Zugang zu chinesischen Forschungszentren verschafft hatte (Süddeutsche 2013). Neben Nationalstaaten betreiben jedoch auch Unternehmen, Gruppierungen oder einzelne Individuen Spionage über Cyberspace. Ziel dieser Angriffe ist es Wirtschaftsgeheimnisse, Technologisches Know-how, oder Daten von Regierungseinrichtungen zu extrahieren. Sowohl Cyberterror und Cyberkrieg sind Begriffe, welche sowohl häufig in den Medien als und auch in offiziellen Dokumenten Verwendung finden. Jedoch gab es bislang noch keinen Vorfall, welcher eine solche Bezeichnung gerechtfertigt hätte (Lewis 2010: 2). Bisher beschränken sich die Aktivitäten von Terroristen im Cyberspace auf die eigene Organisierung. Echte terroristische Cyberangriffe hat es noch nicht gegeben. Ähnlich verhält

es sich mit Cyberkrieg. Auch bei Stuxnet handelte es sich vielmehr um einen Sabotage-, als um einen Kriegsakt. Zum gegenwärtigen Zeitpunkt sind Cyberterrorismus und Cyberkrieg hypothetische Bedrohungsszenarien, während die anderen beschriebenen Cyberbedrohungen bereits häufig realen Schaden anrichten (Rid 2011). Mit den vielfältigen Cyberbedrohungen ist ein externer Druck entstanden, welcher in gleichem Maße auf die westlichen Industriestaaten wirkt. Cyberkriminelle diskriminieren nicht zwischen verschiedenen Ländern, da ihr Interesse allein ökonomischer Natur ist. Der Gefahr durch Cyberspionage sind alle Unternehmen oder Regierungen der Industriestaaten ausgesetzt, auch wenn es hier graduelle Unterschiede geben mag, je nach politischer Bedeutung des Landes oder Größe der Unternehmen. Einzig ideologisch motivierte Angriffe richten sich zumeist gegen bestimmte Länder, verursachen jedoch von den in diesem Kapitel beschriebenen Kategorien den geringsten Schaden. Ein Blick in die Strategiepapiere und Weißbücher von zahlreichen Staaten verrät, dass Regierungen Cyberbedrohungen als real und schädigend wahrnehmen. Gleichzeitig ist die Bedrohung aber diffus und schwer einzuschätzen, was aufgrund einer hohen Dunkelziffer unbemerkter Angriffe verstärkt wird. Dies bewirkt einen starken Handlungszwang für die Industriestaaten potentielle Worst-Case-Szenarien sowie Lösungsmöglichkeiten präventiv zu entwickeln.

Der Cyberspace verbindet heute zahlreiche Bereiche miteinander, von sozialen Netzwerken über kritischer Infrastruktur bis hin zu öffentlichen und privaten Institutionen in Sektoren wie Nahrungsmittel, Telekommunikation, dem Gesundheitswesen, Energie, Wirtschaft oder der Verteidigung. Die große Abhängigkeit unserer modernen Welt vom Cyberspace zeigt sich darin, dass ein Funktionieren ohne ihn in weiten Teilen nicht mehr möglich wäre. Der Cyberspace wird daher auch als „Nervensystem“ eines Landes bezeichnet (Homeland Security 2003: vii). Es ist diese extreme Dependenz, welche das Schadenspotential von Bedrohungen im Cyberspace begründet und weswegen Staaten zunehmend versuchen sich gegen diese zu rüsten (Clarke/Knake 2010). Diese Abhängigkeitsbeziehung ist bei allen entwickelten Industriestaaten ähnlich stark ausgeprägt. Für Entwicklungs- und Schwellenländer, deren Infrastruktur und Wirtschaft nicht kritisch von modernen Kommunikations- und Informationsnetzwerken abhängt, stellen Cyberbedrohungen kein dringendes Problem dar. Industriestaaten weisen mit der Abhängigkeit vom Cyberspace jedoch die ähnlichen Rahmenbedingungen auf und sehen sich dadurch den gleichen Problemen durch die zunehmenden Cyberbedrohungen ausgesetzt.

Neben dem gleichen Problemdruck und ähnlichen Rahmenbedingungen spricht für eine Konvergenz der Cyber-Policies auch die Tatsache, dass es sich bei Cybersicherheit um

ein neues Problemfeld handelt, indem noch keine gesonderten Institutionen existierten. In bestimmten Problemfeldern, wie z.B. der Umweltverschmutzung, hatten sich bereits auf nationaler Ebene Strukturen gebildet, bevor auf internationaler Ebene aufgrund globaler Umweltprobleme ein gemeinsamer Handslungsdruck entstanden war. Dies führte dazu, dass die Policy-Reaktionen von Staaten auf neue globale Umweltprobleme einerseits durch den Problemdruck bestimmt waren, aber andererseits auch durch die bereits auf nationaler Ebene existierenden Strukturen und Institutionen. Solche einmal etablierten Strukturen können schwer abzuschaffen sein, auch wenn möglicherweise andere institutionelle Designs eine effektivere Problemlösung ermöglichen würden. Der Grund dafür sind Lock-in-Effekte wie z.B. hohe Kosten, welche bei der Abschaffung der Strukturen zu erwarten wären. Diese können finanzieller, aber auch politischer Natur sein. Hinzu kommt, dass bestimmte Gruppierungen und Akteure innerhalb der Staaten von bereits existierenden Strukturen profitieren und sich daher für deren Erhalt oder die Kontrolle über diese Strukturen einsetzen (*vested interests*) (DiMaggio/Powell 1991). Existieren solche Strukturen noch nicht auf nationaler Ebene, wie dies im Problemfeld der Cybersicherheit der Fall war, dann spricht dies dafür, dass der gemeinsame Problemdruck der entscheidende Faktor für die Herausbildung einer Cyber-Policy ist und daher eine Konvergenz über die Industriestaaten hinweg zu beobachten sein sollte.

Hier stellt sich nun die Frage *was* für eine Konvergenz zu beobachten sein sollte, d.h. in welche Richtung die Angleichung der Cyber-Policies geht. Mit Bezug auf die verschiedenen Governance-Modi, durch welche die Steuerung von Organisationen erfolgen kann, kann vermutet werden, dass eine Konvergenz in Richtung hierarchischer Strukturen im Cybersicherheitsbereich zu beobachten sein sollte. Prinzipiell bevorzugt der Staat hierarchische Verwaltungsstrukturen. Dadurch gewährleistet er seine Handlungsfähigkeit und kann durch Arbeitsteilung auch komplexe Problemfelder bearbeiten. Durch ein hohes Maß an Kontrolle kann der Staat die Macht der ausführenden Einheiten begrenzen. Zudem ist dieser bei einer hierarchischen Steuerungsform nicht gezwungen sich mit anderen Akteuren abzustimmen, was es ihm erleichtert auf veränderte Gegebenheiten im Problemfeld z.B. mittels Reformen zu reagieren (Benz/Dose 2004: 260, 261). Dies trifft insbesondere auf den Sicherheitsbereich zu, welcher eine traditionelle Domäne des Staates ist. Auf andere (kooperativere) Governance-Formen lässt der Staat sich möglicherweise zu einem späteren Zeitpunkt aus funktionalen Erwägungen oder Effizienz-Gründen ein. Dies kann z.B. der Fall sein, wenn die Kongruenz zwischen Problembereich und seinem Einflussbereich nicht länger gegeben ist, oder ein freier Wettbewerb eine höhere Effizienz der Problembewältigung

verspricht. Nur dann wird der Verlust an Kontrolle und Einfluss vom Staat in Kauf genommen. Im Internet ist jedoch mit den zunehmenden Cyberbedrohungen eine Art „Governance-Lücke“ entstanden, welche durch keinen anderen Akteur gefüllt werden konnte. Mit der Entstehung des Internets wurde früh die Hoffnung verknüpft, eine non-hierarchische Steuerung durch private und gesellschaftliche Akteure ohne Beteiligung bzw. ohne Regulierung des Staates verwirklichen zu können (Johnson/Post 1996; Gibbons 1997). Aufgrund der steten Zunahme von Cyberkriminalität und der Unfähigkeit andere Akteure jenseits des Staates mit diesem Problem umzugehen, wurde diese Position in den letzten Jahren kritisiert. Der Staat wird zunehmend in der Verantwortung gesehen Sicherheit im Cyberspace herzustellen, da er als einziger verbliebener Akteur über die Möglichkeiten dazu verfüge (Netanel 2000; Lewis 2009). Da zudem keine institutionelle Pfadabhängigkeit durch bereits existierende Strukturen im Problemfeld existiert, sollte der Staat in der Lage sein die präferierten hierarchischen Strukturen zur Problembewältigung aufzubauen. Zusammenfassend lässt sich folgende Nullhypothese formulieren, die es zu widerlegen gilt: *Die Cyber-Policies von Industriestaaten weisen eine Konvergenz in Richtung hierarchischer Steuerung auf, verursacht durch einen parallelen Problemdruck durch Cyber-Bedrohungen und ähnlichen strukturellen Abhängigkeiten vom Cyberspace.*

3. Staatliche Politiken zur Herstellung von Cybersicherheit

Dieses Kapitel widmet sich der Beschreibung und Kategorisierung der Varianz von nationalen Cyber-Policies. Dadurch soll das Explanandum als Forschungsvariable nutzbar gemacht werden. Bevor aber die Cyber-Policies thematisiert werden, soll zunächst geklärt werden, was mit Cyberspace und Sicherheit in diesem Kontext gemeint ist.

3.1 Cyperspace und Sicherheit

Die Begriffe „Cyberspace“, „World Wide Web“ (WWW) und „Internet“ werden oft synonym miteinander verwendet, haben jedoch einen unterschiedlichen Bedeutungsumfang. Eine einheitliche Definition des Cyberspace existiert nicht. In Forschungsarbeiten und offiziellen Dokumenten wird der Begriff auf unterschiedliche Art und Weise verwendet und besitzt unterschiedliche Reichweiten. Der Cyberspace wird dabei nicht immer klar vom WWW oder vom Internet abgegrenzt. Die beiden letzteren Begriffe stellen jedoch nur eine Teilmenge, wenn auch die bedeutendste, des Cyberspace dar. Beim Internet handelt es sich um ein weltweites Netzwerk von Rechnern, welche mittels standardisierter Protokolle miteinander kommunizieren können. Das Internet bezeichnet also in erster Linie die verwendete Hardware

und die Protokolle. Das WWW ist eine von mehreren Internetdiensten, welche auf Basis dieser Infrastruktur funktionieren. Dabei handelt es sich um ein System von elektronischen Hypertext-Dokumenten, die mittels Hyperlinks abgerufen werden können. Andere Internetdienste, wie z.B. E-Mail, oder Dateiübertragungsverfahren (File Transfer Protocol (FTP)), sind nicht Teil des WWW. Daniel T. Kuehls Definition von Cyberspace hebt die wichtigsten Merkmale hervor:

> "...cyberspace is a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies." (Kuehl 2009: 28).

Diese Definition beinhaltet die drei Ebenen des Cyberspace: 1. Die physische Ebene, welche die Hardware und die Infrastruktur umfasst und das Fundament des Cyberspace bildet. Dies sind z.B. Prozessoren, Speicher, Kabel- und Funkverbindungen, Router, sowie die gesendeten Signale. 2. Die syntaktische Ebene, welche im Wesentlichen jegliche Art von geschriebenem Code umfasst. Dies können Programme, aber auch Protokolle, Formate, Dateisysteme oder Adressen sein. 3. Die Ebene der Semantik, welche alle Arten von beinhalteten Informationen umfasst (Libicki 2007: 8, 236f.). Der Cyberspace wird oft als ein neuer, vierter Raum neben den traditionellen Räumen Land, See und Luft angesehen; beziehungsweise bei Mitbeachten des Weltraums als fünfter. Ebenso wie bei den traditionellen Räumen handelt es sich beim Cyberspace um einen globalen Raum, welcher mittels Technologie weiträumig zugänglich geworden ist. Es ist zudem ein operativer Raum, indem zahlreiche menschliche Aktivitäten in Bereichen wie Wirtschaft, Unterhaltung, Militär, Politik bis zur Kriminalität ablaufen. Einige Besonderheiten unterscheiden den Cyberspace jedoch von den anderen Räumen. Die Tatsache, dass das Fundament des Cyberspace durch die Hardware und die Nutzung des elektromagnetischen Spektrums gebildet wird, bringt zwei wichtige Eigenschaften mit sich. Zum einen ist der Cyberspace im Unterschied zu den anderen Räumen menschengemacht. Dies bedeutet, dass der Raum konstruiert, verändert, kopiert, repariert oder temporär verschwinden kann. Cyberspace hat nicht den einzigartigen Charakter der traditionellen Räume. Mit den Worten von Martin C. Libicki: „Cyberspace, by contrast, is built, not born." (Libicki 2007: 5). Die Nutzung des elektromagnetischen Spektrums führt zudem dazu, dass die Interaktion im Cyberspace in Millisekunden verläuft. Ursache und Wirkung fallen zeitlich extrem nah zusammen. Als Folge dessen haben räumliche Distanzen im Cyberspace nahezu

keine Relevanz. Entscheidend ist vielmehr die Verbindungsgeschwindigkeit, welche sich im Zuge der technologischen Entwicklung stetig verbessert (Betz 2011: 39). Kuehls Definition macht uns noch auf zwei weitere Aspekte des Cyberspace aufmerksam: Zum einen auf die besondere Rolle von Informationen, zum anderen auf die Verknüpfung interdependenter Netzwerke. Der Cyberspace wird durch den Austausch von Informationen konstituiert. Die syntaktische Ebene macht den Cyberspace überhaupt erst zugänglich für die Nutzer. Durch das Senden von Informationen bei der Nutzung einer Schnittstelle verschafft man sich Zutritt zum Cyberspace und „existiert" dort. Jede Aktion im Cyberspace beinhaltet das Senden oder Empfangen von Information. Egal ob Programme oder Datenbanken genutzt werden, oder Bilder und Musik getauscht wird – alle Informationen werden in Bytes gespeichert und in Bits übertragen.

Sicherheit im Cyberspace, oder kurz Cybersicherheit wird zumeist wage als Abwesenheit von Cyberbedrohungen definiert. Dabei kann zwischen engen und weiten Definitionen unterschieden werden. Enge Definition fokussieren auf den Schutz von Informationstechnologien (PCs, Netzwerken, Smartphones, usw.) und der dazugehörigen Informationsinfrastruktur (Provider, Leitungen) vor schädigenden Angriffen durch Hacker oder Viren. Die enge Definition wird zumeist von Unternehmen verwendet, welche am Schutz ihrer IT-Systeme interessiert sind, und wird dementsprechend auch als IT- oder Informationssicherheit bezeichnet. Staatliche Behörden erweitern diese Definition um externe Komponenten. Hier werden auch Gefahren *aus* dem Cyberspace für Infrastrukturen, welche nicht zum IT-Sektor gehören, mit einbezogen. Dabei wird die bereits beschriebene Abhängigkeit von kritischen Infrastrukturen wie Energienetze oder Verkehrsleitsysteme vom Cyberspace betont und die Möglichkeit der Manipulation derselben durch Hacking-Angriffe. Weite Definition von Cybersicherheit stellen die Aktivitäten der Nutzer (Individuen, Unternehmen, oder Staaten) im Cyberspace in den Vordergrund. Hierbei wird die positive Wirkung vom Cyberspace betont, z.B. auf das Wirtschaftswachstum oder generell die Informationsbereitstellung für die Gesellschaft. Cybersicherheit bedeutet dann, dass die Aktivitäten der Nutzer, wie Onlinebanking, eTrade, Emails, usw., gefahrenfrei ablaufen können. Auch die weite Definition gewinnt eine externe Komponente, wenn die negativen Konsequenzen von Cyberspace-Aktivitäten für die „reelle" Welt miteinbezogen werden. Beispiele dafür sind Cyber-Mobbing oder illegales Filesharing, was Schaden an Personen oder Unternehmen vor allem außerhalb des Cyberspace verursacht. Die Unterscheidungen zwischen enger und weiter Definition, sowie internen und externen Komponenten sind nicht trennscharf, sondern überlappen sich. Sie helfen aber als analytische Unterscheidungen zur

Bestimmung der Reichweite des Begriffes Cybersicherheit in unterschiedlichen Dokumenten. Tendenziell verwendeten Unternehmen eher die enge Definition, während Staaten in offiziellen Dokumenten zu der weiten Definition mit externen Komponenten tendieren.

3.2 Nationale Cyber-Policies

Bevor die Untersuchung der verschiedenen nationalen Cyber-Policies begonnen werden soll, müssen die Kriterien für die Fallauswahl erläutert werden. Diese ist erstens auf entwickelte Industriestaaten beschränkt, da nur diese, wie bereits beschrieben, im vergleichbaren Maße dem Druck durch Cyberbedrohungen ausgesetzt sind und ähnliche Rahmenbedingungen aufweisen. Zudem müssen zum Aufbau von Strukturen zur Cyberabwehr ausreichende Ressourcen vorhanden sein. Diese Ressourcen umfassen in erster Linie Geld und Know-how. Der Aufbau von Organisationen, Equipment, Forschungsprogramme und die Einstellung von Personal – all dies benötigt substantielle finanzielle Ressourcen, welche entwickelte Staaten in der Tendenz eher in der Lage sind bereitzustellen als Schwellen- und Entwicklungsländer. Als entwickelte Industriestaaten sollen jene Länder angesehen werden, welche von der Weltbank in die Kategorie „High-income OECD members“ eingeordnet werden (World Bank 2013). Zweitens werden nur demokratische Staaten berücksichtigt. Die Aussparung von autokratischen Systemen hat zunächst pragmatische Gründe, da sich der Zugriff auf Daten bezüglich deren Cyber-Policies aufgrund mangelnder Transparenz als problematisch erweist. Schwerer wiegt jedoch, dass Demokratien und Autokratien grundlegend unterschiedliche politische Systeme und politische Kulturen aufweisen. Bei der Suche nach einer Erklärung von Cyber-Policies müsste daher eine größere Anzahl von möglichen Variablen berücksichtigt werden. Hinzu kommt ein stärkeres „Hintergrundrauschen“ durch den Einfluss von möglichen Drittvariablen, welches bei einem Vergleich von ausschließlich demokratischen Ländern besser kontrolliert werden kann. Erste Beobachtungen legen zudem nahe, dass die Entwicklung von Cyber-Policies in autokratischen Staaten einer anderen Motivation als in demokratischen Industriestaaten folgt. Cyber-Policies in z.B. Russland und China weisen einen stärkeren militärischen Schwerpunkt auf. Auch Internetzensur und die staatliche Kontrolle über die Informationsinfrastruktur spielt in Ländern wie Saudi Arabien, den Vereinigten Arabischen Emiraten, oder Weißrussland eine stärkere Rolle. Aus diesem Grund sollen auch ostmitteleuropäische Länder (Polen und Tschechische Republik) sowie Chile, obwohl formal demokratisch, ausgeklammert werden. Die politischen Systeme dieser Transitionsländer verfügen noch nicht über genügend gefestigte Strukturen und institutionelle Stabilität, wie z.B. stabile Parteistrukturen (vgl. Abromeit/Stoiber 2006: 75). Chile stellt in

noch stärkerem Maße ein demokratisches Schwellenland dar, da erst 2005 die letzten autokratischen Elemente aus der Verfassung entfernt wurden. Drittens werden nur Staaten ins Sample miteinbezogen, welche bereits Strategiepapiere bezüglich Cyber-Sicherheit veröffentlicht haben. Ist noch kein Strategiepapier vorhanden, wird dies so gedeutet, dass noch keine Entscheidung hinsichtlich der Richtung der Cyber-Policy gefällt wurde. Dies bedeutet nicht, dass diese Länder keine Abwehrmechanismen gegen Cyberbedrohungen besitzen. Jedoch sind die relevanten Ministerien und Sektoren in der Regel für sich selbst verantwortlich und es findet keine institutionalisierte Koordination oder Informationsaustausch zwischen ihnen statt. Der Trend geht aber eindeutig zur Schaffung gesonderter Strukturen. Es ist also davon auszugehen, dass sich diese Staaten bezüglich der Entwicklung ihrer Cyber-Policy noch in einem Anfangsstadium befinden, weswegen sie in dieser Arbeit ausgeklammert werden. Dies betrifft die Länder Dänemark, Finnland, Griechenland, Irland, Israel, Italien, Portugal, Schweden, Spanien und Südkorea. Unter Berücksichtigung dieser Auswahlkriterien wird die Fallauswahl durch die Staaten Australien, Belgien, Deutschland, Frankreich, Großbritannien, Japan, Kanada, USA, Neuseeland, Niederlande, Norwegen, Schweiz und Österreich gebildet.

Cyber-Policy meint die politischen Inhalte, welche in Strategiepapieren, Gesetzen, Verordnungen, Programmen und Einzelentscheidungen zum Ausdruck kommen und sich auf die Herstellung von nationaler Cybersicherheit beziehen. Der Fokus liegt dabei auf den geschaffenen Governance-Strukturen und Steuerungsformen. Dazu erfolgt die Untersuchung der Cyber-Policies anhand von vier Kategorien.

1. *Aufsicht/Kontrolle*: Welche politische Institution übt die Kontrolle über die Cyber-Policy aus? Wo liegt die Letztverantwortung? Wem sind die Sicherheitsbehörden gegenüber rechenschaftspflichtig?
2. *Policy-Formulierung*: Welche Organisation ist für die strategische Ausrichtung der Cyber-Policy verantwortlich? Wer identifiziert Probleme, setzt Prioritäten und entwickelt Strategiepapiere?
3. *Steuerung*: Durch welche Behörde/Einrichtung erfolgt die Steuerung im Cybersicherheitsbereich?
4. *Implementation*: Welche Behörde obliegt die Umsetzung der strategischen Leitlinien? Wer ist für die exekutiven Maßnahmen zur Herstellung von Cybersicherheit zuständig? Wem obliegt die operative Arbeit?
5. *Governancemodus*: Basiert die Zusammenarbeit/Steuerung auf einem hierarchischen oder auf einem horizontalen Verhältnis zwischen den relevanten Behörden?

Die Unterscheidung wird aus analytischen Zwecken vorgenommen, findet sich jedoch in den meisten Cyber-Policies wieder. Es ist aber nicht ausgeschlossen, dass sich die Ebenen zuweilen überschneiden und Behörden mehrere Verantwortungsbereiche übernehmen. Anhand dieser Ebenen lässt sich für die Fallauswahl folgende Übersichtstabelle erstellen.

Tabelle 1: Nationale Cyber-Policies

	Australien	***Belgien***	***Deutschland***	***Frankreich***	***Großbritannien***
Aufsicht/ Kontrolle	• Attorney-General's Department	• Federal Ministry of the Interior (IBZ)	• Bundesministerium des Inneren	• Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN)	• Cabinet Office
Policy-Formulierung	• Attorney-General's Department	• Federal Ministry of the Interior (IBZ) • Ministerial Committee for Intelligence and Security	• Nationaler Cybersicherheitsrat	• Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN)	• Office of Cyber Security and Information Assurance (OSCIA)
Steuerung	• Cyber Security Policy and Coordination (CSPC)	• Belgian Network Information Security Platform (BelNIS) • Belgian Institute for Postal Services and Telecommunications (BIPT) • Belgian Cyber Crime Centre	• Nationales Cyberabwehrzentrum (NCAZ) • Nationaler Cybersicherheitsrat • Umsetzungsplan KRITIS	• Agence nationale de la sécurité des systèmes d'information (ANSSI)	• Office of Cyber Security and Information Assurance (OSCIA) • Centre for the Protection of the National Infrastructure (CPNI)
Implementation	• Cyber Security Operations Centre (CSOC) • Australian Cyber Security Centre (ACSC) • CERT Australia	• Federal Computer Crime Unit (FCCU) (Bundesebene) • Regionale Computer Crime Units (RCCU) (Regionalebenen) • CERT.be	• BSI • BfV • BKA • BND • Bundesamt für Bevölkerungsschutz (BBK) • Bundespolizei • Bundeswehr • Zollkriminalamt	• ANSSI via Centre d'opération pour la sécurité des systèmes d'information (COSSI) • Office Central de Lutte contre la Criminalité liée aux Technologies de l"Information (OCLCTIC) • Haut Fonctionnaire de Défense et de Sécurité (HFDS)	• Government Communications Headquarters (GCHQ) mit dem angeschlossenem Cyber Security Operations Centre (CSOC) • National Cyber Crime Unit
Governance-Modus	• Hierarchie: Das Attorney-General's Department sitzt dem CSPC vor. CERT Australia ist zudem Teil des Departments.	• Netzwerk: Kompetenzen der beteiligten Akteure bleiben erhalten	• Netzwerk: Das NCAZ ist keine eigenständige Behörde, sondern eine Kooperations-einrichtung. Die Kompetenzen der beteiligten Akteure bleiben erhalten	• Hierarchie: ANSSI hat starke Befugnisse bzgl. der Überwachung der nationalen Informations-systeme und um die Einhaltung der nationalen Richtlinien zu kontrollieren	• Hierarchie: OSCIA kontrolliert das CSOC, dem der Großteil des von der Regierung zur Verfügung gestellten Budgets zur Herstellung von Cybersicherheit zukommt

(Quellen: Attorney-General's Department 2009; ENISA 2011; BMI 2011; ANSSI,2011; Cabinet Office 2011)

Fortsetzung Tabelle 1

	Japan	***Kanada***	***USA***	***Neuseeland***
Aufsicht/ Kontrolle	• Cabinet Secretariat • National Information Security Center (NISC)	• Public Safety Canada	• White House Cybersecurity Office • Department of Homeland Security (DHS) • Department of Defense	• Department of the Prime Minister and Cabinet
Policy-Formulierung	• Information Security Policy Council (ISPC)	• Public Safety Canada • Department of National Defence (DND) • Treasury Board Secretariat (TBS)	• White House Cybersecurity Office • Department of Homeland Security (DHS) • Department of Defense	• National Cyber Policy Office (NCPO)
Steuerung	• National Information Security Center (NISC) • Information Security Policy Council (ISPC)	• Canadian Cyber Incident Response Centre (CCIRC)	• Information and Communications Infrastructure Interagency Policy Committee	• National Cyber Policy Office (NCPO)
Implementation	• Ministry of Internal Affairs and Communication (MIC) • Ministry of Economy, Trade, and Industry (METI) • National Police Agency (NPA) • Ministry of Defense (MOD)	• Communications Security Establishment Canada (CSEC) • Royal Canadian Mounted Police (RCMP) • Canadian Security Intelligence Service (CSIS) • Department of National Defence (DND)	• Electronic Crimes Task Forces (ECTFs) • National Cybersecurity and Communications Integration Center (NCCIC) • United States Strategic Command (USSTRATCOM) • United States Cyber Command (USCYBERCOM) • FBI: National Cyber Investigative Joint Task Force	• Ministry of Economic Development • Department of Internal Affairs • Government Communications Security Bureau • Centre for Critical Infrastructure Protection • NetSafe • New Zealand Police • New Zealand Security Intelligence Service
Governance-Modus	• Hierarchie: Das NISC überwacht die Aktivitäten der Ministerien hinsichtlich der Umsetzung der Cyberstrategie und gibt die strategische Ausrichtung vor	• Hierarchie: Public Safety Canada und das CCIRC koordinieren die kanadische Cyberabwehr	• Netzwerk: „Currently, no single individual or entity has the responsibility to coordinate Federal government cybersecurity-related activities“ (White House 2009: 7)	• Hierarchie: NCPO zuständig für Entwicklung, Koordinierung und Implementation der Cyber-Policy

(Quellen: Yamada et al. 2010; Public Safety Canada, 2010; White House 2009; Ministry for Communications and Information Technology 2011)

Fortsetzung Tabelle 1

	Niederlande	***Norwegen***	***Schweiz***	***Österreich***
Aufsicht/ Kontrolle	• Ministry of Security and Justice	• Auf vier verschiedene Ministerien verteilt • Im Krisenfall sektor-spezifisch	• Bundesverwaltung • Auf sechs weitere Ministerien verteilt	• Bundeskanzleramt
Policy-Formulierung	• Cyber Security Council	• In Zusammenarbeit verschiedener Ministerien	• Je nach zuständigem Department	• Bundeskanzleramt • Cyber Sicherheit Steuerungsgruppe • Österreichische Cyber Sicherheit Plattform
Steuerung	• National Cyber Security Centre	• Information Security Coordination Council (KIS) (Öffentlicher Sektor) • Norwegian Post- and Telecommunication Authority (NPT) (Privatem Sektor)	• Informatiksteuerungsorgan des Bundes (ISB)	• Cyber Sicherheit Steuerungsgruppe • Lagebild Cyber Sicherheit
Implementation	• Defence Computer Emergency Response Team (DefCERT) • Defence Intelligence & Security Service (DISS) • General Intelligence and Security Service • National Police Services Agency	• NorCERT • Im Krisenfall Sektor-spezifisch	• Melde- und Analysestelle Informationssicherung (MELANI) • Bundeskriminalpolizei • Koordinationsstelle zur Bekämpfung der Internetkriminalität (KOBIK) • Nachrichtendienst des Bundes (NDB) • Bundesamt für Informatik und Telekommunikation (BIT)	• Bundesministerium für Landesverteidigung und Sport • Bundesministerium für Inneres • Bundeskriminalamt • Cyber Crime Competence Center
Governance-Modus	• Netzwerk: Die niederländische Regierung verfolgt eine „network-centred form of collaboration“ (Ministry of Security and Justice 2011: 9)	• Netzwerk: Starke Selbstverantwortung der einzelnen Sektoren bei gleichzeitig gemeinsamer Policy-Entwicklung	• Netzwerk: Die Strukturen zur Bewältigung von Cyber-Risiken sind bisher dezentral organisiert.	• Netzwerk: Die Steuerungsgruppe besteht aus Vertretern der Ministerien und Länder. Es hat keine Weisungsbefugnis, sondern berichtet der Regierung bezüglich der Umsetzung der Cyberstrategie

(Quellen: Ministry of Security and Justice 2011, Norwegian Ministries 2012; Eidgenössisches Departement VBS 2012, Bundeskanzleramt 2013)

Bei der Untersuchung der geschaffenen Strukturen dieser Länder ließen sich zwei Arten von Cyber-Policies erkennen. Diese sollen an den Beispielen Frankreich, Belgien und Norwegen dargestellt werden. In Frankreich wurde die Verantwortung im Bereich Cybersicherheit der *Agence nationale de la sécurité des systèmes d'information* (ANSSI) übertragen. Die Organisation wurde im Juli 2009 gegründet und untersteht dem *Secrétariat général de la défense et de la sécurité nationale* (SGDSN). Für das SGDSN ist der Premierminister verantwortlich, welcher eng mit dem Präsidentenamt und verschiedenen Ministerien zusammen arbeitet. ANSSI kommt die Rolle einer nationalen Planungsstelle zu. Zudem ist die Organisation für die Implementation der strategischen Vorgaben und für die Maßnahmen zur Herstellung von Sicherheit im Cyberspace zuständig. Ihre Aufgabe ist es die Informationssysteme zu überwachen, Gefahren aufzuspüren und gegebenenfalls Gegenmaßnahmen einzuleiten. Dazu werden kritische Regierungsnetzwerke, sowie öffentliche Provider beobachtet. Die Behörde hat die Befugnis weitreichende Verteidigungsmaßnahmen einzuleiten, wie z.B. die Trennung und Isolierung von Netzwerken. Für diese und andere operative Maßnahmen leitet ANSSI das angeschlossene *Centre d'opération pour la sécurité des systèmes d'information* (COSSI). COSSI ist zudem für die Koordination der verschiedenen französischen Ministerien hinsichtlich des Schutzes der nationalen Netzwerke zuständig. Darüber hinaus ist die Behörde an der Entwicklung und Zertifizierung von Sicherheitsprodukten und Dienstleistungen beteiligt (Tromparent 2012: 80). ANSSI nimmt Evaluationen der Sicherheitssysteme von Unternehmen und Organisationen vor und versieht diese bei Bestehen mit Zertifikaten. Die Bewertungen werden von neutralen, akkreditierten Testzentren vorgenommen. Auf diese Weise will ANSSI Anreize für verbesserte Sicherheitsmaßnahmen im Cyberspace beim privaten Sektor schaffen. Provider und andere Telekommunikationsanbieter sind per Anordnung dazu verpflichtet Sicherheitspläne für die von ihnen angebotene Infrastruktur zu erstellen. Diese Pläne werden dann vom *Haut Fonctionnaire de Défense et de Sécurité* (HFDS), dem französischen Ministerium für Wirtschaft, Industrie und Beschäftigung, auf Einhaltung der nationalen Sicherheitsbestimmungen geprüft (ANSSI 2010). Insgesamt ist die Zusammenarbeit mit anderen Sektoren im Bereich Cybersicherheit nicht besonders ausgeprägt.

In Belgien existiert keine zentrale Organisation, welcher die Verantwortung oder Ausführung der exekutiven Maßnahmen im Bereich der Cybersicherheit übertragen wurde. Cyber-Sicherheit ist in den größeren Kontext von Innerer und Äußerer Sicherheit eingebettet. Das belgische Innenministerirum und das *Ministerial Committee for Intelligence and Security* sind für die allgemeine Policy-Formulierung in Sachen der (Inneren) Sicherheit und der

Geheimdienste zuständig. Zur Koordinierung der Verantwortlichkeiten und Kompetenzen im Bereich der Cybersicherheit hat der belgische Ministerrat 2005 die *Belgian Network Information Security Platform* (BelNIS) gegründet. BelNIS hält regelmäßige Treffen ab, auf denen die relevanten Organisationen der Bundesregierung zum Informationsaustausch zusammenkommen. Dies sind unter anderem das Bundesamt für Informations- und Kommunikationstechnologie (Fedict), das Bundesreferat für Computerkriminalität (FCCU), die Telekommunikations- und Internetbehörde (BIPT), die Geheimdienste, sowie Behörden aus den Bereichen Datenschutz und Wirtschaft. Auf Initiative des Bundesjustizministeriums wurde 2011 das *Belgian Cyber Crime Centre* eröffnet. Hier soll Expertise aus Wissenschaft, Industrie und Öffentlich Einrichtungen zusammen kommen. Das Center soll als Kollaborations- und Forschungsplattform dienen und unter anderem Trainingskurse für Beamte aus den Bereichen Justiz und Sicherheit anbieten (ENISA 2011; B-ccentre 2013). Die Zusammenarbeit zwischen dem Öffentlichen Sektor und der Industrie, insbesondere den Telekommunikationsunternehmen verläuft über das BIPT. Bezüglich der Widerstandfähigkeit der Informationsnetzwerke besteht ein Informationsaustausch zwischen dem BIPT und den Providern. Letztere können Informationen jedoch mit Hinweis auf den Datenschutz zurückhalten. In der Regel melden die Provider nur Störfälle, welche an die Öffentlichkeit gelangt sind, an die BIPT. Auch gibt es keine Standardprozeduren oder bestimmte Zeitfenster welche bezüglich der Meldung von Störfällen eingehalten werden müssen. Die exekutiven Maßnahmen erfolgen durch Cybercrime-Abteilungen der bundesstaatlichen und regionalen Polizeiabteilungen (ENISA 2011: 26).

Norwegen verfolgt ebenfalls einen Netzwerk-Ansatz, welcher zudem auf eine starke Eigenverantwortlichkeit der einzelnen Sektoren setzt. Dies bedeutet, dass präventive Maßnahmen, sowie die Reaktion in Krisenfällen zumeist sektorspezifisch erfolgen. Aufgrund dieses Ansatzes sind die Verantwortlichkeiten und Aufgaben auf viele verschiedene öffentliche Akteure verteilt und überschneiden sich teilweise. Die wichtigsten sollen hier kurz umrissen werden. Das *Ministry of Transport and Communications* (MCT) ist verantwortlich für die Sicherheit der elektronischen Kommunikation und Netzwerke und koordiniert die verschiedenen Policies und Regulationen in diesem Bereich. Das *Ministry of Government Administration, Reform and Church Affairs* ist insbesondere für den Bereich der Informations- und Kommunikationstechnik (IKT) zuständig. Ziele sind unter anderem den Zugang zur Informationstechnologie für die Gesellschaft zu garantieren und Innovationen und Wachstum der IKT-Industrie zu fördern. Dem Ministerium ist das *Information Security Coordination Council* (KIS) angeschlossen, welches die relevanten öffentlichen Behörden

miteinander koordinieren soll. KIS bietet eine Plattform zum Austausch über Regulationen, Standards, Best-Practice sowie Sicherheitslücken. Die Organisation spricht zudem Empfehlungen aus und agiert als Berater zur Implementation der nationalen Strategie im Bereich der Informationssicherheit. Das norwegische Justizministerium und das Verteidigungsministerium sind zuständig für den Schutz der kritischen Infrastruktur und der Koordinierung der nationalen Sicherheits- und Verteidigungspolitik. Ihnen wird von der *National Security Authority* (NSM) Bericht erstattet. NSM ist verantwortlich für präventive Maßnahmen zum Schutz der nationalen Sicherheit, sowie der Sicherheit im IKT-Bereich. Dazu ist der Behörde NorCERT angeschlossen, das norwegische Computer Emergency Response Team, welches bei IT-Sicherheitsvorfällen Hilfestellung leistet. Die *Norwegian Post- and Telecommunication Authority* (NPT) ist zuständig für die Kooperation mit dem privaten Sektor, insbesondere den Energieversorgern und den Telekommunikationsanbietern. Dabei werden Informationen über kritische Infrastrukturen und Abhängigkeiten zwischen dem Stromnetz und dem Internet zum Zwecke der Notfallvorsorge ausgetauscht. Um die Vorsorge- und Krisenmaßnahmen bewerten zu können veranstaltet die NPT alle zwei Jahre Übungen mit erwähnten Unternehmen und anderen relevanten Akteuren. Dazu werden Übungen auf regionaler Ebene abgehalten um die Kooperation zwischen den lokalen Behörden und den Energieversorgern und den Telekommunikationsanbietern zu stärken (ENISA 2011b; Norwegian Ministries 2012).

Frankreichs Cyber-Policy stellt ein Beispiel für einen zentralisierten Ansatz dar. Dieser ist dadurch gekennzeichnet, dass eine oder wenige zentrale Sicherheitsbehörden mit starken Ressourcen und Befugnissen gegenüber anderen Akteuren geschaffen werden. Die Koordination anderer Behörden erfolgt daher oft durch hierarchische Steuerung. Die Kontrolle über die zentralen Cybersicherheitsbehörden ist oft auf einer hohen politischen Ebene angesiedelt. Diese Cyber-Policy soll nach dem vorherrschenden Governance-Modus als „Hierarchie“ gelabelt werden. Belgiens und Norwegens Cyber-Policy hingegen stellen Beispiele für einen Ansatz mit Netzwerk-Charakter dar. Hierbei werden Kooperationszentren geschaffen, in denen die relevanten Behörden im Sicherheitsbereich zwecks der Herstellung von Cybersicherheit zusammenkommen. Die Kooperation zwischen den Akteuren erfolgt dabei zumeist durch eine horizontale Steuerung. Die Kontrolle ist auf Ministerialebene angesiedelt und oft auf verschiedene Ministerien verteilt. Diese Art der Cyber-Policy wird mit „Netzwerk“ gelabelt.[2]

[2] Für eine Auflistung verschiedener Governance-Formen siehe Benz/Dose 2004: 256ff.

4. Erklärungsansatz und theoretisches Analyseraster

Hinsichtlich der Nullhypothese muss aufgrund der Ergebnisse im vorangegangen Kapitel festgehalten werden, dass empirisch keine Konvergenz der nationalen Cyber-Policies festgestellt werden konnte. Dies kann aber dem Umstand geschuldet sein, dass das Problemfeld Cybersicherheit relativ junger Natur ist, und sich daher noch keine deutliche Konvergenz in Richtung hierarchischer Cyber-Policies herausbilden konnte. Um die Nullypothese zu widerlegen muss daher gezeigt werden, dass die Varianz der Cyber-Policies auf andere Ursachen zurückzuführen ist. Die theoretische Basis dafür soll in diesem Kapitel gelegt werden. Zur Erklärung der Varianz der Cyber-Policies wird das Vetospielertheorem heranzogen, welches auf die Vetospieler als zentralen Erklärungsfaktor fokussiert. Das Konzept der Pfadabhängigkeit ermöglicht es eine kausale Brücke zwischen der unabhängigen Variable der Vetospieler und der abhängigen Variable der Cyber-Policies zu schlagen.

4.1 Das Vetospielertheorem

Bei Betrachtung von Tabelle 1 fällt auf, dass zentralistisch-organisierte Länder wie Großbritannien und Frankreich sich für die Policy „Hierarchie“ entschieden haben. Die Cyber-Policy von föderalistischen Staaten wie Deutschland, Belgien und der Schweiz hat dagegen eher Netzwerk-Charakter. Diese Beobachtung lässt die Vermutung zu, dass es einen Zusammenhang zwischen Merkmalen des politischen Systems und der Ausprägung der Cyber-Policy gibt. Zur Typologie politischer Systeme gibt es verschiedene Ansätze, wie die Regierungssystemlehre (z.B. Steffani 1979; Shugart/Carey 1992) oder Demokratietypologien (Lijphart 1999). Diese Ansätze teilen die Annahme, dass die Präferenzen und das Handeln politischer Akteure nur im institutionellen Kontext verstanden werden können. Das Regierungssystem bzw. der Demokratietyp wird dabei als unabhängige Variable herangezogen um einen bestimmten politischen Outcome, die abhängige Variable, zu erklären (vgl. Croissant 2010: 117). Ein Nachteil dieser beiden Typologien ist, dass sie wenig über den Kausalzusammenhang zwischen Systemmerkmalen und Politikergebnissen verraten. Die jeweiligen Systemmerkmale, auf welche die Typologien fokussieren, sagen alleine wenig über das Handeln der beteiligten Akteure aus. Es bedarf eines Ansatzes, welcher stärker handlungstheoretische Aussagen trifft. Der Vetospieler-Ansatz von George Tsebelis (Tsebelis 2002) kann dies leisten, denn dieser fokussiert auf die Akteure, deren aktive Zustimmung im politischen Entscheidungsprozess notwendig ist. Durch die Anzahl der Akteure, ihre ideologische Distanz (Kongruenz) und ihr interner Zusammenhalt (Kohäsion) sollen Politikwandel und Politikkontinuität erklärt werden. Die Hypothese ist, dass je weniger

Vetospieler es in einem politischem System gibt, bzw. umso kongruenter und kohärenter diese sind, desto eher und schneller können Politikwechsel vollzogen werden. Steigt hingegen die Zahl von Vetospieler sowie deren ideologische Distanz und interne Heterogenität, dann gestalten sich Politikwechsel zunehmend schwieriger und der Status quo bleibt erhalten. Tsebelis unterscheidet zwischen institutionellen und parteipolitischen Vetospielern. Die Vetorechte der institutionellen Vetospieler sind im politischen System „verankert", d.h. in der Regel in der Verfassung festgeschrieben. Die Vetorechte der parteipolitischen Vetospieler ergeben sich aus dem verfassungsrechtlichen Rahmen und entstehen im politischen Prozess. Die Zahl der Vetospieler ergibt sich aus den Merkmalen des politischen Systems. Institutionelle Eigenschaften wie das Regierungssystem (präsidentiell oder parlamentarisch), der Parlamentstyp (Ein- oder Zweikammernsystem) oder das Organisationsprinzip (Zentralstaat oder Föderalstaat) bestimmen die Anzahl der institutionellen Vetospieler. Die Anzahl sowie die Kongruenz und Kohärenz der parteipolitischen Vetospieler kommt durch strukturelle Eigenschaften zustande wie der Regierungsform, dem Wahlsystem oder dem Gesetzgebungsprozess zustande sowie über gesellschaftliche *cleavage*-Strukturen (Croissant 2010: 133). Uwe Wagschal hat das Vetospielertheorem von Tsebelis an einigen Stellen erweitert (Wagschal 2005: 163ff.) So berücksichtigt er auch mögliche internationale Vetospieler wie den IWF oder die EU und deren Druckpotentiale. Auch Verfassungsgerichte, welche die Macht haben Entscheidungen im Nachhinein abzuändern und zu revidieren, werden als nachträgliche Vetospieler miteinbezogen. Wagschals erweiterte Definition beschreibt Vetospieler als „... ein individueller oder kollektiver Akteur, der eine Policy-Entscheidung verhindern, maßgeblich beeinflussen oder im Nachhinein ändern kann." (Wagschal 2005: 169). Eine Gegenüberstellung von Wagschals kompetitiven Vetospielerindex mit den Ausprägungen der nationalen Cyber-Policies der Fallauswahl zeigt eine Korrelation auf:

Tabelle 2: Gegenüberstellung des Vetospielerindexes mit Cyber-Policies

Land	Kompetitiver Vetospielerindex	Cyber-Policy
Schweiz	6	Netzwerk
USA	5	Netzwerk
Deutschland	5	Netzwerk
Belgien	3	Netzwerk
Österreich	3	Netzwerk
Australien	2,5	Hierarchie
Kanada	2	Hierarchie
Frankreich	2	Hierarchie
Niederlande	2	Netzwerk
Japan	1,5	Hierarchie
Norwegen	1	Netzwerk
Großbritannien	1	Hierarchie
Neuseeland	0	Hierarchie

Eigene Darstellung, Daten zum Vetospielerindex aus Wagschal (2005).

Wie anhand der Tabelle zu erkennen ist, weisen alle Länder mit einem Index von drei oder höher die Cyber-Policy „Netzwerk“ auf. Mit Ausnahme der Niederlande und Norwegen haben alle Länder mit einem Index von zweieinhalb oder kleiner eine Cyber-Policy mit hierarchischem Charakter aufgebaut. Die Ausreißer Niederlande und Norwegen erklären sich möglicherweise dadurch, dass der Vetospielerindex nur formelle Vetospieler berücksichtigt, jedoch keine informellen, situativen Vetospieler. Das „Skandinavische Modell“ zeichnet sich durch eine besondere Konsensorientierung und eine starke Einbindung von Interessensgruppen vor dem eigentlichen Entscheidungsprozess aus (Abromeit 2006: 127). Der Einfluss dieser situativen Vetospieler ist nachgewiesen (vgl. Lappalainen/Siisiäinen 2001: 116ff.). Vergleichbares gilt für die Niederlande, welche sich durch ein stark konsensorientiertes Konkordanzsystem zwischen den politischen Akteuren (von denen nicht alle Vetospieler sind) und neo-korporatistischen Arrangements auszeichnet. Die institutionalisierte Einbeziehung von Akteuren aus Wirtschaft und Gesellschaft kann die Anzahl der Vetospieler je nach Policybereich erhöhen. Dies geht in den Niederlanden soweit, dass im Rahmen sozio-ökonomischer Reformen der Sozial-Ökonomische Rat (SER) sogar die Funktion eines „Vorparlamentes“ einnahm (Abromeit/Stoiber 2006: 120, 121). Situative Vetospieler können jedoch aufgrund ihrer informellen Natur nicht vom Vetospielerindex erfasst werden, was einen bekannten Kritikpunkt darstellt (Croissant 2010: 135).

Basierend auf diesen empirischen Beobachtungen soll der Vetospieleransatz für die Erklärung des Untersuchungsgegenstandes fruchtbar gemacht werden: Die Cyber-Policies „Hierarchie“ oder „Netzwerk“ beschreiben eine Machtkonzentration bzw. Machtfragmentierung im Policybereich. Für die Ausgestaltung der Policy sind die jeweiligen Vetospieler des politischen Systems über die Agendasetzung und den Gesetzgebungsprozess verantwortlich. Es ist also plausibel anzunehmen, dass entweder die Interessen der Vetospieler oder die Interessen von Akteuren, welche Einfluss auf die Vetospieler nehmen, für die Ausgestaltung einer nationalen Cyber-Policy entscheidend sind. Zudem kann davon ausgegangen werden, dass in politischen Systemen mit einer hohen Anzahl von Vetospielern die Cyber-Policy einen Netzwerk-Ansatz folgen wird. Umgekehrt sollte in Systemen mit wenig Vetospielern die Cyber-Policy „Hierarchie“ zu beobachten sein. Folgende Hypothesen können formuliert werden: *Je weniger Vetospieler ein politisches System aufweist und umso kongruenter und kohäsiver diese sind, desto stärker weist die Cyber-Policy die Merkmale des „Hierarchie“-Ansatzes auf. Je mehr Vetospieler es gibt und umso ideologischer distanzierter und weniger kohäsiv diese sind, desto stärker weist die Cyber-Policy die Merkmale eines „Netzwerk“-Ansatzes auf.*

Bisher wurde auf die Vetospieler zur Erklärung der nationalen Cyber-Policies fokussiert. Andere Theorien bieten jedoch alternative Erklärungsansätze an, welche hier kurz diskutiert werden sollen. Es könnte erstens angenommen werden, dass die Struktur einer nationalen Cyber-Policy eine Folge der finanziellen Möglichkeiten des jeweiligen Landes ist. Die Umsetzung einer hierarchischen Cyber-Policy ist oftmals mit dem Aufbau neuer Behörden und Organisationen verbunden, welche mit ausreichend Ressourcen und Personal ausgestattet werden müssen. So hat z.B. Großbritannien 2012 rund 180 Millionen Euro für seine Cybersicherheits-Strategie zur Verfügung gestellt, wovon 56% der zentralen Behörden *Government Communications Headquarters* (GHCQ) zugeteilt wurden (Intelligence and Security Committee 2011: 54, 55; National Audit Office 2013: 4). In Ländern mit einer netzwerkartigen Cyber-Policy wurden hingegen überwiegend Kooperationszentren geschaffen. Die beteiligten Akteure agieren dabei größtenteils im Rahmen ihrer bereits zur Verfügung gestellten finanziellen Ressourcen. In Deutschland wurden z.B. keine gesonderten finanziellen Mittel für Cybersicherheit zur Verfügung gestellt. Dieses funktionale Argument lässt sich jedoch dadurch entkräften, dass Ausgaben von 180 Millionen Euro für Industriestaaten keine besonderen Größen darstellen. Dies kann verdeutlicht werden, indem man die Ausgaben im Cybersicherheitsbereich mit den Gesamtausgaben im Verteidigungssektor kontrastiert. So hat Großbritannien 2012 Verteidigungsausgaben von

63,6 Milliarden Euro ausgewiesen. Wären die Ausgaben für Cybersicherheit Teil dieses Haushaltes gewesen, hätten sie 0,0028 Prozent der Gesamtausgaben ausgemacht. Zum Vergleich: Deutschlands Verteidigungshaushalt betrug im selben Jahr 48,1 Milliarden Euro (NATO 2012: 4). Zudem sollte gemäß dieser Hypothese zu beobachten sein, dass Länder mit einem großen finanziellen Spielraum im militärischen Bereich eine hierarchische Cyber-Policy ausgebildet haben. Die USA, welche zweifelsohne die größten Verteidigungsausgaben tätigen, weisen jedoch die Cyber-Policy „Netzwerk" auf. Auch empirisch lässt sich die These daher nicht aufrechterhalten. Hierarchische Cyber-Policies mögen einen größeren finanziellen Aufwand als netzwerkartige Cyber-Policies erfordern, aber diese Ausgaben sind nicht Ursache für die Wahl der Cyber-Policy, sondern eine Konsequenz aus diesen.

Zweitens kann ein Zusammenhang zwischen dem Einfluss von Interessensgruppen und der Ausprägung der Cyber-Policy vermutet werden. So könnten Interessensgruppen aus dem militärischen, wirtschaftlichen oder gesellschaftlichen Sektor nach einer Beteiligung im Cybersicherheitsbereich streben um so Einfluss auf die Policy-Gestaltung zu nehmen und einen Zuwachs an Ressourcen, Informationen oder Kompetenzen zu erzielen. Ein Indikator für den Einfluss bzw. den Zugang von Interessensgruppen in einem politischen System ist das Maß an Korporatismus. Die Hypothese wäre demnach: Je mehr ein politischen System korporatistische Elemente aufweist, desto eher nimmt die Cyber-Policy einen Netzwerk-Charakter an. Diese Hypothese ist mit der Vetospieler-Hypothese vereinbar. Um ihre Beteiligung an der Cyber-Policy zu sichern, müssen Interessensgruppen Einfluss auf die kritischen Akteure im Gesetzgebungsprozess nehmen, welche durch die Vetospieler dargestellt werden. Möglich ist auch, dass die Interessensgruppen informelle Vetomacht haben, z.B. indem sie in konsensorientierten Gremien ihre Zustimmung verweigern. Dies soll bei der späteren Operationalisierung der Vetospieler berücksichtigt werden.

Drittens kann die Hypothese formuliert werden, dass die Nähe zu einer dominanten Sicherheitskultur zu einer Diffusion der Strukturen im Cybersicherheitsbereich in anderen Länder geführt hat. Da die USA zuerst mit der Entwicklung ihrer Cybersicherheits-Strategie begonnen haben, kann die Hypothese spezifiziert werden: Je mehr die Sicherheitskultur eines Landes, dem der USA ähnelt, desto stärker diffundieren die Strukturen der Cyber-Policy in diese Länder. Empirisch kann diese These jedoch widerlegt werden: Großbritannien, Australien und Neuseeland sind Staaten, welche eine lange Geschichte sicherheitspolitischer Kooperation mit den USA verbindet. Dennoch weisen alle drei Länder im Gegensatz zu den USA die Cyber-Policy „Hierarchie" auf.

4.2 Pfadabhängigkeit

Beim Konzept der Pfadabhängigkeit wird davon ausgegangen, dass historische Entwicklungen entlang bestimmter Kausalpfade verlaufen können und dass das Ergebnis einer Entwicklung mit Bezug auf den jeweiligen Pfad zu erklären ist. Entgegen der in Kapitel zwei erläuterten Konvergenzthese wird nicht davon ausgegangen, dass derselbe externe Druck bei verschiedenen Staaten zwangsläufig zu einer Annäherung der Politikergebnisse führt. Die Politikergebnisse sind stattdessen maßgeblich von den verschiedenen Rahmenbedingungen der jeweiligen Staaten beeinflusst. Die bedeutendsten dieser Rahmenbedingungen sind die formalen und informellen institutionellen Merkmale eines Staates, welche das Erbe vergangener Ereignisse sind. Institutionen werden als der zentrale Faktor zur Erklärung historischer Entwicklungen gesehen (Hall/Taylor 1996: 941). Pfadabhängigkeit bedeutet jedoch mehr, als dass vergangene Ereignisse einen Einfluss auf die Gegenwart haben. Zwei Definitionen können unterschieden werden: Bei der weiten Definition von Pfadabhängigkeit wird die kausale Verknüpfung zeitlich aufeinanderfolgender Entwicklungsschritte betont. Bei der engen Definition von Pfadabhängigkeit wird davon ausgegangen, dass bestimmte Ereignisse oder Entscheidungen zu frühen Zeitpunkten die weitere Richtung einer Entwicklung entscheidend determinieren. Je weiter die Entwicklung dem einmal eingeschlagenem Pfad folgt, desto zunehmend schwieriger wird ist es diesen wieder zu verlassen (Mahoney 2000: 507).

Die weite Definition von Pfadabhängigkeit wird auch als reaktive Sequenz (*reactive sequence*) bezeichnet. Eine solche Sequenz bezeichnet eine Kette von zeitlich aufeinander folgenden Ereignissen, welche jeweils in kausalem Zusammenhang zu dem vorangegangen Ereignis stehen. Das finale Ereignis stellt dabei das Ziel der Untersuchung dar, während die Kausalkette bzw. der Pfad die Erklärung für dieses Ergebnis darstellt. Dabei können frühe Ereignisse stärkere Wirkung entfalten als spätere, da sich ihr Effekt über die Kausalkette hinweg akkumulieren kann. In einer reaktiven Sequenz sollte idealerweise jedes Zwischenereignis einen kausalen Mechanismus darstellen, welche zusammen das Anfangsereignis mit dem letztendlichen Ergebnis verknüpfen (Mahoney 2000: 526-532).

Die enge Definition von Pfadabhängigkeit wird zuweilen als *self-reinforcing sequence* bezeichnet und stellt im Vergleich zu reaktiven Sequenzen ein engeres Konzept dar. Hierbei wird nicht nur davon ausgegangen, dass Ereignisse auf einen bestimmten Pfad zurückzuführen sind, sondern auch, dass sich die Richtung des Pfades mit zunehmender Dauer verfestigt und es immer schwieriger wird diesen zu verlassen. Zur Veranschaulichung werden *self-reinforcing sequences* auch mit den Ästen eines Baumes verglichen:

> „From the same trunk, there are many different branches and smaller branches. Although it is possible to turn around to clamber from one to the other – and essential if the chosen branch dies – the branch on which a climber begins is the one she tends to follow.“ (Levi 1997: 28, zitiert nach Pierson 2000: 252)

Anders als bei reaktiven Sequenzen kommt es bei *self-reinforcing sequences* zu einer Verfestigung früherer Ereignisse. Bei reaktiven Sequenzen hingegen können frühere Ereignisse transformiert, möglicherweise sogar rückgängig gemacht werden Die Stabilität eines bestimmten Pfades wird durch die Dynamik der *increasing returns*/*positive feedback* erklärt. Jeder Schritt entlang eines bestimmten Pfades erhöht die Wahrscheinlichkeit, dass die Richtung des Pfades beibehalten wird. Dies ist der Fall, weil sich der Nutzen bei Beibehaltung des Pfades im Vergleich mit anderen Optionen mit jeder Sequenz erhöht. Auch können mit zunehmender Dauer die Kosten beim Verlassen des Pfades immer weiter steigen – der sogenannte Lock-in-Effekt (Pierson 2000: 252). Die Logik von *increasing returns* wurde anhand einer Illustration aus der Mathematik, dem Polya-Urnen-Experiment, veranschaulicht. Dieses Experiment macht noch auf weitere Charakteristika von Pfadabhängigkeit aufmerksam. So gilt, dass das *Timing* von Ereignissen für den Verlauf des Pfades kritische Konsequenzen haben kann. Frühere Ereignisse können dabei stärkere Wirkung entfalten als spätere (Pierson 2000: 253). Zudem können sich langfristig produzierte Ergebnisse als ineffektiver erweisen, als die Ergebnisse alternativer Pfade.

Der Entstehungszeitpunkt von Institutionen wird als kritischer Zeitpunkt bezeichnet (*critical junctures*). Der Zeitpunkt hat kritische Qualität, weil die zu diesem Zeitpunkt getroffene Entscheidung nur schwer rückgängig gemacht und zu anderen Optionen zurückgekehrt werden kann (Collier/Collier 1991: 29). Nachdem Institutionen einmal geschaffen worden sind, können sie sich auch dann noch als stabil erweisen, wenn die ursprünglichen Kräfte, welche für ihre Entstehung verantwortlich waren, nicht mehr existieren. Die Prozesse, welche verantwortlich sind für die Entstehung einer Institution, sind von denen zu unterscheiden, welche ihre Stabilität begründen. Um die Stabilität und Reproduktion von institutionellen Mustern sowie deren möglichen Wandel zu erklären, werden je nach theoretischer Tradition unterschiedliche Mechanismen angeführt. Dabei kann zwischen machtpolitischen, utilitaristischen und legitimatorischen Erklärungsansätzen unterschieden werden.

Der machtpolitische Mechanismus ist dabei besonders geeignet um den Zusammenhang zwischen Vetospielern und der Art der Cyber-Policy aufzuzeigen. Bei dieser Perspektive wird von rationalen, nutzenmaximierenden Akteuren ausgegangen. Von zentraler Bedeutung ist, dass Institutionen eine unterschiedliche Verteilung von Nutzen und Vorteilen über die verschiedenen Akteure hinweg befördern können. Profitieren Akteure von institutionellen Strukturen, dann haben sie Interesse daran diese zu reproduzieren. Macht als Erklärungsfaktor für eine institutionelle Stabilität kommt dann ins Spiel, wenn ein Akteur oder eine Akteursgruppe über genügend Ressourcen verfügt, um eine Institution auch gegen den Widerstand anderer Akteure aufrechtzuerhalten. Zumeist handelt es sich dabei um eine Elite, welche von gegenwärtigen Institutionen profitiert und mit ausreichenden Machtressourcen für deren Stabilität sorgt. Sobald eine bestimmte Institution entstanden ist und Vorteile für eine bestimmte Akteursgruppe produziert, kann eine Machtdynamik ausgelöst werden, welche für die Reproduktion der Institution sorgt: Die profitierende Gruppe nutzt ihre zusätzliche Macht um die Institution auszuweiten und kann so zusätzliche Ressourcen ansammeln, welche wiederrum genutzt werden um die Institution zu reproduzieren. (Mahoney 2000: 523).

Utilitaristische und legitimatorische Pfadabhängigkeit können erklären, wieso sich Cyber-Policies nach ihrer Entstehung trotz veränderter machtpolitischer Verhältnisse als stabil erweisen. Utilitaristische Erklärungen fanden ursprünglich in der Wirtschaftsgeschichte Verwendung. Hier wird wie bei machtpolitischen Erklärungen von Individuen als rationale Akteure ausgegangen, welche die Kosten und Nutzen ihrer Entscheidungen strategisch abwägen. Akteure erhalten eine Institution aufrecht, wenn der potentielle Nutzen durch Wandel oder Abschaffung der Institution durch die zu erwartenden Kosten aufgehoben wird. Faktoren, welche die Höhe der Kosten beeinflussen können, sind z.B. Koordinierungseffekte, organisatorische Verflechtungen oder adaptive Erwartungen. Institutioneller Wandel tritt verallgemeinert formuliert dann auf, wenn die beteiligten Akteure kein Eigeninteresse mehr daran haben die Institution in ihrer jeweiligen Form aufrechtzuerhalten. Solch eine institutionelle Transformation kann durch Lerneffekte ausgelöst werden. Akteure können negative Konsequenzen in der Zukunft vorhersehen und daher bereit sein kurzfristige Kosten eines institutionellen Wandels in der Gegenwart auf sich zu nehmen. Es wird davon ausgegangen, dass Institutionen sich in der sozialen und politischen Welt stabiler als in einem wirtschaftlichen Kontext erweisen. Der Grund ist, dass es im politischen Kontext schwieriger ist konkrete Kosten-Nutzen-Abwägungen vorzunehmen und so die Risiken von

institutionellen Transformationen abzuschätzen. Diese Unsicherheit erschwert langfristige Entscheidungen und beförderte eine institutionelle Stabilität (Mahoney 2000: 519 ff.).

Legitimatorische Erklärungen führen die Reproduktion von Institutionen auf die Normvorstellungen und subjektiven Orientierungen von Akteuren zurück. Akteure setzten sich dann für die Reproduktion einer Institution ein, wenn sie diese als legitim, d.h. moralisch angemessen betrachten. Akteure können sich dabei aktiv für die Ausweitung der Institution einsetzen oder diese passive dulden. Pfadabhängigkeit tritt auf, nachdem eine Institution entstanden ist, und ein erstes Maß an Legitimität erreicht hat. Vergangene Erfahrungen über angemessenes Verhalten formen die Basis für zukünftiges Handeln. Die Institution wird zunehmend als legitim empfunden, internalisiert und dadurch verfestigt und ausgeweitet (Thelen 2003: 214 ff.). Diese drei Mechanismen der Pfadabhängigkeit können fruchtbar gemacht werden um den Zusammenhang zwischen den Vetospielern eines politisches Systems und der Art der Cyber-Policy sowie deren Stabilität aufzuzeigen. Dies soll bei der Operationalisierung im folgenden Kapitel geschehen.

5. Untersuchungsdesign

5.1 Fallauswahl

Da eine Korrelation zwischen der Anzahl der Vetospieler und der Ausprägung der Cyber-Policy aufgezeigt wurde, geht es nun darum die vermuteten kausalen Prozesse hinter dieser Korrelation aufzudecken. Dies soll durch eine vertiefte Analyse weniger Fälle erreicht werden. Der internen Validität wird hier der Vorzug gegenüber der externen Validität gegeben. Zu diesem Zwecke soll ein *Most Similar Cases Design* (MSCD) angewendet werden. MSCD werden angewandt, um den Einfluss von bestimmten unabhängigen Variablen auf das Explanandum zu untersuchen. Die Fallauswahl folgt der Differenzmethode nach John Stuart Mill. Ausgewählt werden Fälle, welche sich hinsichtlich der unabhängigen Variable unterscheiden, deren Rahmenbedingungen jedoch sehr ähnlich sind. Dadurch kann der Einfluss von möglichen Störvariablen auf die abhängige Variable minimiert bzw. über die Untersuchungsfälle hinweg konstant gehalten werden. Die unabhängige, erklärende Variable soll in den Untersuchungsfällen hingegen kontrolliert variieren. Bei der Fallauswahl werden also eine starke Varianz der unabhängigen Variablen und eine Ähnlichkeit bezüglich möglicher Drittvariablen angestrebt.

Als Untersuchungsfälle werden die Länder Großbritannien und Deutschland ausgewählt. Hinsichtlich der Vetospieler gibt es zwischen beiden Länder eine große Varianz.

Deutschland weist nach Wagschals Vetospielerindex fünf Vetospieler auf, Großbritannien dagegen nur einen. Dazu kommt, dass sich die beiden großen britischen Parteien *Labour* und *Conservatives* durch ein hohes Maß an Parteidisziplin auszeichnen, d.h. eine starke interne Kohärenz aufweisen. In Deutschland hingegen sind obgleich der viel beschworenen Fraktionsdisziplin interne Abweichler keine Seltenheit. Auch ist das Parteiensystem deutlich fragmentierter und zwischen den Parteien gibt es deutlichere ideologische Distanzen. Insgesamt zeichnen sich die Vetospieler in Deutschland daher durch eine schwächere interne Kohärenz und deutlich stärkere Kongruenz als in Großbritannien aus. Hinsichtlich der unabhängigen Variablen bilden die beiden Länder daher nahezu entgegengesetzte Extreme ab.

Der Einfluss von Drittvariablen kann in beiden Ländern konstant gehalten werden. Beide Länder sind entwickelte Industriestaaten und werden von der Weltbank in die höchste Kategorie „High-income OECD members“ eingestuft. Daraus kann geschlussfolgert werden, dass die Anfälligkeit für Cyberbedrohungen für beide Länder aufgrund ähnlicher struktureller Abhängigkeiten vom Cyberspace gleich groß ist (s. Seite 12). Als Indikator für den Grad der Vernetzung kann der Anteil von Internetnutzern an der Gesamtpopulation herangezogen werden. Dieser liegt bei Deutschland bei 82 Prozent und bei Großbritannien bei 83 Prozent, womit beide zu den am meisten vernetzten Ländern der Welt gehören (International Telecommunication Union 2011). Dass beide Länder auch eine ähnliche Bedrohungswahrnehmung haben, wird in den jeweiligen Strategiepapieren deutlich. Die britische Regierung bewertet Cybersicherheit als ein Risiko der höchsten Stufe 1. (HM Government 2010: 27). In Deutschland wird offiziell keine Priorisierung von internationalen Gefahren vorgenommen, aber Cybersicherheit wird als zentrale Herausforderung des 21. Jahrhunderts bezeichnet (BMI 2013). Zudem sind beide Länder demokratisch und weisen genügend Ressourcen für beide Arten von Cyber-Policy auf.

5.2 Empirisches Vorgehen

Zur Aufdeckung des Zusammenhanges zwischen den Vetospielern eines politischen Systems und der Art der Cyber-Policy soll auf die Methode der Prozessanalyse zurückgegriffen werden. Eine Prozessanalyse bietet sich an, wenn nach dem Befund einer Korrelation zwischen zwei Variablen die dahinter stehenden Kausalmechanismen aufgespürt werden sollen. Dabei wird auf den Prozess fokussiert und angestrebt die kausalen Mechanismen kleinschrittig empirisch zu belegen. Durch diese tiefergehende Analyse können die Probleme einer reinen Korrelationsanalyse, wie Schein-, Symptom- und umgekehrte Kausalität vermieden werden (Schimmelfennig 2006: 264).

Dazu wird der Prozess zunächst disaggregiert, d.h. in verschiedene Sequenzen unterteilt. Dabei muss nicht der gesamte Prozess oder alle Sequenzen im Detail nachgezeichnet werden. Es ist ausreichend die Sequenzen anhand zentraler Prozessstationen miteinander zu verbinden. Die Identifikation dieser Prozessstationen erfolgt theoriegeleitet. Zentrale Prozessstationen sind solche, welche kritisch für die Bestätigung oder Widerlegung eines kausalen Mechanismus sind. Diese Vorgehensweise unterscheidet eine Prozessanalyse von einer historischen, induktiven Studie. Eine Prozessanalyse ist dagegen geleitet von einer dahinterstehenden Theorie (Jahn 2006: 345ff.). Als zu untersuchende Prozessstationen werden die Entwicklungsprozesse der Strategiepapiere für Cybersicherheit und die zentralen Gesetzgebungsverfahren angesehen. In diesen Verfahren und Prozessen kommt der Einfluss der Vetospieler zum Tragen.

Bei der Prozessanalyse besteht die Gefahr, dass aus verschiedenen Beobachtungen eine plausible Erklärung „gestrickt" wird, welche mögliche Ursachen mit dem Ergebnis verbindet. Um dies zu vermeiden ist es notwendig vor der eigentlichen Analyse beobachtbare Implikationen für die vermuteten Kausalzusammenhänge herauszuarbeiten (Schimmelfennig 2006: 267). Dies soll bei der folgenden Operationalisierung geschehen. Eine Prozessanalyse ist prinzipiell mit unterschiedlichen Datentypen durchführbar; hier wird eine qualitative Dokumentenanalyse vorgenommen, welche auf Agenturmeldungen, Presseberichten und den Datenarchiven des Bundestages/Bundesrates und des britischen *House of Commons* basiert.

5.3 Operationalisierung

Beobachtbare Indikatoren für das Explanandum wurden bereits in Kapitel 3.2 herausgearbeitet. Auch auf die erklärende Variable der Vetospieler wurde eingegangen. Dabei wurde vor allem zwischen institutionellen und parteipolitischen Vetospielern unterschieden. Da diese Arbeit auf die Rolle der Vetospieler im politischen Entscheidungsprozess fokussiert, muss eine Ausdifferenzierung der unterschiedlichen Vetospieler vorgenommen werden. Dazu eignet sich die von Abromeit und Stoiber vorgenommene Gradualisierung von Vetospielern. So kann neben institutionellen und parteipolitischen Vetospielern, zwischen gestaltenden, bedingten, nachträglichen und situativen Vetospielern unterschieden werden, welche sich teilweise überschneiden. Gestaltende Vetospieler sind diejenigen Akteure, welche über Agendasetzungs-Kompetenz verfügen. Besitzt ein Vetospieler die alleinige Agendasetzungs-Kompetenz kann er großen Einfluss auf die Ausgestaltung eines Gesetzes oder einer Policy nehmen, da sich an seiner Idealposition die nachfolgenden Vetospieler orientieren müssen. Die Vetomacht von bedingten Vetospielern kann je nach Politikfeld variieren und zuweilen

auf eine reine Blockadefunktion beschränkt sein. Ein Beispiel dafür ist der Bundesrat, dessen Kompetenzen variieren. Nachträgliche Vetospieler hingegen besitzen keinerlei gestaltende Vetomacht, können die Entscheidungen anderer Vetospieler aber im Nachhinein revidieren. Ein typisches Beispiel dafür sind Verfassungsgerichte. Diese Unterscheidung macht auch auf die unterschiedlichen Machtpotentiale von Vetospielern aufmerksam. Um die tatsächlichen Vetospieler in einem Entscheidungsprozess zu identifizieren reicht es nicht die institutionellen Bedingungen zu berücksichtigen. Die relevanten Vetospieler müssen je nach Politikfeld und im Kontext des ablaufenden Parteienwettbewerbs ermittelt werden (vgl. Abromeit/Stoiber 2006: 71, 72). In diesem Zusammenhang ist die Absorptionsregel von Bedeutung, welche besagt, dass zwei Vetospieler, mit identischen Präferenzen, nur als ein Vetospieler gezählt werden. So wird z.B. das Verfassungsgericht nicht als Vetospieler berücksichtigt, wenn seine Präferenzen nicht von denen der anderen Akteure abweichen. Ebenso wird eine zweite legislative Kammer nicht als eigener Vetospieler gezählt, wenn die Mehrheitsverhältnisse in beiden Kammern ähnlich sind (Croissant 2010: 133). Als situative Vetospieler können Interessensverbände oder gesellschaftliche Gruppierungen auftreten. Diese Akteure besitzen keine formale Vetomacht im Gesetzgebungsprozess, werden aber in manchen Ländern über Gremien an der Ausgestaltung der Gesetze beteiligt. Entscheidungen in diesen Gremien werden zumeist nach dem Konsensprinzip gefällt, welches diesen Akteuren ein informelles Vetorecht zukommen lässt (Abromeit/Stoiber 2006: 70ff.).

Gemäß dem empirischen Vorgehen müssen beobachtbare Implikationen für die in Kapitel 4.2 beschriebenen kausalen Mechanismen herausgearbeitet werden. Beim machtpolitischen Mechanismus ist zunächst die Grundannahme, dass bestimmte Vetospieler ein Interesse daran haben können sich Einfluss in Form von Kontrolle oder Teilhabe auf die neu zu schaffenden Cybersicherheitsstrukturen zu sichern. Zudem werden Vetospieler grundsätzlich versuchen bereits vorhandenen Einfluss (formaler oder informeller Natur) zu verteidigen. Dazu können sie auf ihre Vetomacht zurückgreifen. Die Erfolgsaussichten der Vetospieler ihren bestehenden Einfluss zu verteidigen oder diesen auszudehnen hängt dabei von ihrer Machtstellung, festgelegt ab. Diese wird durch ihre formale oder informelle Rolle im politischen System bestimmt und dargestellt durch ihre jeweilige Form der Vetomacht. Bei starken Vetospielern, wie solchen mit Agenda-Setzer-Kompetenz oder Blockadefähigkeit, ist eher zu erwarten, dass sie ihre Forderungen gegenüber den anderen Vetospielern durchsetzen. Gibt es nur einen starken Vetospieler kann dieser die Entscheidungs- und Gesetzgebungsprozesse dominieren und sich so einen großen Einfluss auf die Cyber-Policy sichern. Diese nimmt dann hierarchischen Charakter an, an dessen Spitze eben jener

Vetospieler sitzt. Gibt es zwei ähnliche stark Vetospieler oder eine hohe Anzahl konkurrierender Vetospieler, dann kann keiner dieser Akteure den Gesetzgebungsprozess und damit die Ausgestaltung der Cyber-Policy dominieren. Aufgrund drohender Blockaden sind die Vetospieler zu einer Kompromisslösung gezwungen. Verschiedene Vetospieler machen dann ihren Einfluss auf die Ausgestaltung der Cyber-Policy geltend und diese nimmt einen Netzwerk-Charakter an.

Die interne Kohärenz und die Kongruenz zwischen den Vetospielern können als weitere Einflussfaktoren hinzukommen. Je mehr interne Kohärenz ein Vetospieler aufweist, desto stärker kann er nach außen agieren. Je weniger interne Kohärenz hingegen ein Vetospieler aufweist, desto schwächer kann er auftreten. Im Extremfall kann dies bei parteipolitischen Vetospielern sogar zum Verlust der effektiven Vetomacht führen, wenn zu viele Abgeordnete von der Parteilinie abweichen. Die allgemeine ideologische Distanz (Kongruenz), welche das Vetospielertheorem berücksichtigt, ist hier nicht so entscheidend. Wichtiger ist zu ermitteln wie stark das Interesse eines Vetospielers an einem Einfluss im Sicherheitsbereich und an den Cybersicherheitsstrukturen ist. Vor allem bei parteipolitischen Vetospielern sind dort starke Unterschiede zu erwarten. Aber auch bei institutionellen Vetospielern, wie Verfassungsgerichte, welche auf die Funktion als „Hüter der Verfassung“ beschränkt sind, ist nicht zu erwarten, dass sie ihre Vetomacht zur Einflussvergrößerung im Sicherheitsbereich einsetzen.

Die utilitaristische und die legitimatorische Pfadabhängigkeit sind geeignet um zu erklären, warum sich Cyber-Policies als stabil erweisen, obwohl sich die machtpolitischen Verhältnisse, welche für deren Entstehung verantwortlich waren, geändert haben. Ob ein Vetospieler sich dafür einsetzt eine hierarchische oder netzwerkartige Cyber-Policy aufrechtzuerhalten, hängt von strategischen Erwägungen ab. Bei einem utilitaristischen Mechanismus sollte zu beobachten sein, dass ein Vetospieler eine für ihn suboptimale Cyber-Policy dann toleriert, wenn die zu erwartenden Kosten einer Reform den potentiellen Nutzen übersteigen. Bei einem legitimatorischen Mechanismus hängt die Unterstützung eines Vetospielers hingegen davon ab, ob er die Art der Cyber-Policy als legitim erachtet. Vetospieler sollten Cyber-Policies unterstützen wenn diese im Einklang mit den von ihnen vertretenden Normen stehen. Dabei ist zu erwarten, dass konservativ eingestellte parteipolitische oder situative Vetospieler eher eine hierarchische Cyber-Policy unterstützen, während Vetospieler des linken politischen Spektrums eher zu einer netzwerkartigen Cyber-Policy tendieren.

Die Fallstudien sind folgendermaßen aufgebaut. Zunächst werden die relevanten Prozessstationen und die potentiellen Vetospieler im Sicherheitsbereich identifiziert. Für die jeweiligen Prozessstationen werden dann die tatsächlichen Vetospieler festgestellt und gegebenenfalls auf die interne Kohärenz und die externe Kongruenz eingegangen. Hiernach folgen die Prozessbeschreibungen und eine anschließende Bewertung ob die Beobachtungen mit den beschriebenen Pfadabhängigkeitsmechanismen in Einklang zu bringen sind. Zudem wird das Ergebnis der Prozesses, die Cyber-Policy beschrieben. Abschließend werden alternative Erklärungen für die Beobachtungen diskutiert.

6. Fallstudien

6.1 Deutschland

Im Zentrum der deutschen Cyber-Policy steht das 2011 eröffnete Nationale Cyber-Abwehrzentrum (NCAZ). Die Aushandlungsprozesse, welche die Struktur des NCAZ begründen, sowie die gesetzlichen Grundlagen wurde jedoch früher im Kontext der Gefahrenabwehr des Internationalen Terrorismus geschaffen. Um zu verstehen, warum das NCAZ und die dahinterstehende Cyber-Policy in seiner gegenwärtigen Form geschaffen worden ist, muss der Prozess von seinen Anfängen, den Reformen im Bereich der Inneren Sicherheit nach den Anschlägen am 11. September 2001, nachgezeichnet werden.

Die Prozessanalyse fokussiert auf drei Stationen. Diese sind jeweils die Gesetzgebungsverfahren und Verhandlungen zum Sicherheitspaket 1 und 2, dem gescheiterten Sicherheitspaket 3 und dem Strategiepapier für Cybersicherheit. Da es bei den Sicherheitspaketen 1 bis 3 unter anderem um eine Umverteilung der Kompetenzen von Sicherheitsbehörden der Länder hin zu jenen des Bundes ging, lassen sich anhand dieser Prozessstationen die machtpolitischen Implikationen testen. Als Folge des Scheiterns des Sicherheitspaketes 3, welches eine Zentralisierung in der Terrorismusabwehr verwirklichen sollte, setzt sich schließlich ein Netzwerk-Ansatz bei der Schaffung nachfolgender Sicherheitsstrukturen durch. So auch bei der letzten Prozessstation, der Entstehung des Strategiepapier für Cybersicherheit.

Im politischen System der Bundesrepublik Deutschland finden sich mit dem Bundeskanzler, dem Bundestag, dem Bundesrat und dem Bundesverfassungsgericht vier institutionelle Vetospieler. Der Bundeskanzler kann mit einer stabilen Regierungsmehrheit theoretisch starken Einfluss auf die Agendasetzung nehmen. Deutsche Regierungen werden jedoch seit den 1960er Jahren regelmäßig durch Koalitionen gebildet, was dem Kanzler

erschwert seine Mehrheit im Bundestag konstant zu disziplinieren. Zugeständnisse an die Koalitionspartner und Koalitionsverträge engen seine Richtlinienkompetenz ein. Dazu kann er durch ein Misstrauensvotum gestürzt werden. In der Praxis schränkt dies alles die Machtposition des Bundeskanzlers ein.

Das deutsche Parlament, der Bundestag, stellt das formale Entscheidungszentrum dar und wird von der Regierung als effektiver Vetospieler dominiert. Die Macht des Bundestages wird jedoch in manchen Gesetzesfragen durch den Bundesrat eingeschränkt. Der Bundesrat kann eine sehr starke Vetorolle einnehmen, wenn die Opposition die Mehrheit[3] in diesem stellt oder wenn länderübergreifende Interessen bedroht sind. Dabei muss aber bedacht werden, dass nur für 55 Prozent der Gesetze die Zustimmung des Bundesrates notwendig ist, was diesem im Umkehrschluss für 45 Prozent eine Vetomacht gibt. Zudem können Gesetzesvorlagen in zustimmungspflichtige und nicht-zustimmungspflichte Teile aufgeteilt, und so gegebenenfalls die Blockadefähigkeit des Bundesrates umgangen werden. Die Reformfähigkeit von Regierungen hängt also zuweilen von der Kreativität bei der Aufteilung von Gesetzen ab. In der Regel ist die Regierung in solchen Fällen jedoch zu Konsens-Verhandlungen gezwungen, welche in einem Vermittlungsausschuss zwischen dem Bundesrat und dem Bundestag stattfinden. Bei wichtigen Reformvorhaben werden jedoch oft im Vorfeld des Vermittlungsausschusses auf informellem Wege Einigungen erzielt (Abromeit 2006: 132). Der Bundespräsident soll nicht als Vetospieler berücksichtigt werden, da ihm im Gesetzgebungsprozess nur ein formales Prüfungsrecht zukommt.

Das Bundesverfassungsgericht (BVerfG) tritt nicht als Vetospieler im Gesetzgebungsprozess auf, sondern erst nachträglich um gegebenenfalls die Rechtmäßigkeit erlassener Gesetze zu prüfen. Das BVerfG wird auch nicht auf eigene Initiative hin tätig, sondern nur wenn Verfassungsbeschwerde eingereicht wird. Es kann als indirekter Vetospieler im Gesetzgebungsprozess Einfluss entfalten, wenn bereits absehbar ist, dass das Gericht Gesetze als verfassungswidrig zurückweisen würde. Insofern kann es die Rolle eines drohenden Vetospielers einnehmen. Die Position des BVerfG muss daher gegebenenfalls von den anderen Akteuren bei der Politikgestaltung berücksichtigt werden (Voigt 2006: 70). Das BVerfG ist kein politisches Organ, vertritt also keine politischen Interessen, sondern entscheidet am Maßstab des Grundgesetzes (Bundesverfassungsgericht 2013). Daher kann dem BVerfG, anders als parteipolitischen Vetospielern, nicht unterstellt werden, dass es seine

[3] Es ist anzumerken, dass eine Mehrheit im Bundesrat ist nicht gleichbedeutet mit einer Ländermehrheit ist, da diese nicht gleich vertreten, sondern unterschiedlich gewichtet sind (drei bis sechs Stimmen)

Vetomacht einsetzt um Einfluss oder Kontrolle im Sicherheitsbereich zu erlangen. Im Zuge der Reformen im Sicherheitsbereich wurde immer wieder kritisiert, dass die Vernetzung der Sicherheitsbehörden durch neue Strukturen wie der Antiterrordatei gegen das Trennungsgebot zwischen Nachrichtendiensten und Polizei verstoßen könnte. Verfassungsrechtliche Bedenken wurden von einzelnen politischen Verantwortlichen der FDP und der Grünen formuliert. Die Diskussion um das Trennungsgebot hatte aber keine so große Resonanz in den Medien erfahren, als dass das BVerfG als drohender Vetospieler Berücksichtigung gefunden hätte. Das BVerfG hat also auch keine indirekte Beeinflussung auf die Politikgestaltung genommen. Eine Verfassungsbeschwerde zum Trennungsgebot und der Antiterrordatei wurde erst im November 2012 eingereicht. Es sei hier vorweggenommen, dass die Richter in Karlsruhe im April 2013 die Antiterrordatei weitestgehend billigten (Spiegel Online 2013).

Die situativen Vetospieler, welche innerhalb der institutionellen Vetospieler agieren, sind die politischen Parteien. Die Koalitionspartner einer Regierung gelten dabei als Vetospieler. Gemäß Tsebelis und der Absorptionsregel fällt der Bundesrat effektiv als institutioneller Vetospieler weg, wenn die Regierungskoalition eine Mehrheit im Bundesrat hält. Hier muss jedoch ein Einwand formuliert werden. Die Absorptionsregel fußt auf der Annahme, dass der Bundesrat in allen Fällen nach den Präferenzen der jeweiligen parteipolitischen Mehrheit entscheidet. Dies ist häufig tatsächlich der Fall, da sich der Bundesrat bereits zu Zeiten der 1970er Jahre weg von seinem ursprünglichen Zweck als Ländervertretung hin zu einem parteipolitischen Instrument entwickelt hat. Es darf jedoch nicht vergessen werden, dass die Sitze von Vertretern der Landesregierungen besetzt werden, welche zuweilen eigene, spezifische Interessen haben. Das Abstimmungsverhalten orientiert sich daher nicht zwangsläufig an dem der Bundespartei, wie es von Tsebelis Absorptionsregel impliziert wird. Dies kommt insbesondere dann zum Tragen, wenn Gesetzesvorhaben des Bundes die Interessen mehrerer Länder oder die Interessen der Länder im Gesamten betreffen. Dann können über parteipolitische Grenzen hinweg Allianzen zwischen den Länderregierungen entstehen, welche eine Opposition gegenüber dem Bund bilden. Ein Beispiel dafür ist die Steuerreform im Jahr 2000 der SPD und der Grünen, welche auf breiten Widerstand im Bundesrat stieß. Darunter waren die mit SPD-Beteiligung regierten Länder Berlin, Brandenburg, Bremen und Mecklenburg-Vorpommern, welche allesamt finanzschwach waren und sich um ein Entgegenkommen des Bundes bemühten. Daraus lässt sich schlussfolgern, dass der Bundesrat nur dann gemäß der Absorptionsregel als Vetospieler wegfällt, wenn ausgeschlossen werden kann, dass keine föderalen oder länderübergreifenden Interessen bestehen.

Als informelle, indirekte Vetospieler traten in der Vergangenheit immer wieder Arbeitgeberverbände oder Gewerkschaften auf (z.B. durch die Hartz-Kommission bei der Arbeitsmarktreform unter der Regierung Schröder). Sie finden dann als Vetospieler Berücksichtigung, wenn sie über konsensorientierte, korporatistische Verhandlungsgremien Einfluss auf die Policygestaltung und/oder direkte Vetospieler nehmen können. Allerdings haben diese Vetospieler keinen Anspruch auf Mitentscheidung, sondern erfahren nur soviel Berücksichtigung, wie die politischen Akteure es zulassen (Abromeit 2006: 134). Im Politikfeld der Inneren Sicherheit müssen die Polizeigewerkschaften als informelle Vetospieler berücksichtigt werden. Diese können über korporatistische Aushandlungen zwischen ihnen und den Innenministerien der jeweiligen Länder Einfluss auf die Politikgestaltung nehmen. Polizeipolitik (Personalpolitik, Besoldung, Ausbildung, usw.) fällt in den Zuständigkeitsbereich der Länder. Daher sind die Innenministerien der Länder die zentralen Ansprechpartner für die Gewerkschaften um ihre Interessen bzw. die Interessen ihrer Mitglieder zu formulieren. Die ministeriellen Polizeiabteilungen haben wiederrum ein eigenes Interesse an einer Zusammenarbeit mit den Gewerkschaften. Die Polizeigewerkschaft kann als Vermittler zwischen den Innenministerien und den Beamten auftreten. Dabei trägt sie nicht nur die Forderungen seiner Mitglieder an die Länder weiter, sondern kann auch Reformvorstellungen der Ministerien an seine Mitglieder vermitteln (Lange 2000: 216, 216). Die Polizeigewerkschaften besitzen kein formales Vetorecht und sind auch nicht direkt am Gesetzgebungsprozess beteiligt. Sie formulieren ihre Interessen jedoch gegenüber den Länderministerien, wo diese berücksichtigt werden und die Präferenzen der Länder beeinflussen. Die Länder wiederrum nehmen über den Bundesrat und die Innenministerkonferenz direkten und indirekten Einfluss auf den Gesetzgebungsprozess. Außer den Polizeigewerkschaften besaßen keine anderen gesellschaftlichen Gruppen relevanten Einfluss auf die Politikgestaltung im Bereich der Inneren Sicherheit. Bürgerrechtsgruppen gehörten zwar mit den Medien zum politischen Umfeld, sind aber nicht über korporatistische Gremien wie die Gewerkschaften in die Policygestaltung eingebunden (Lange 2000: 218).

Das politische System in Deutschland zeichnet sich durch das Fehlen eines eindeutigen Machtzentrums aus. Die Machtfragmentierung ist das Resultat der institutionellen Rahmenbedingungen und des parteipolitischen Wettbewerbs (Abromeit 2006: 151). Je nach Mehrheitsverhältnissen kann die Machtfragmentierung schwanken. Hält die Opposition eine Mehrheit im Bundesrat, kann sie diesen institutionellen Vetospieler kontrollieren. Insgesamt kommt eine relative hohe Anzahl von Vetospieler mit zuweilen starken Positionen zustande,

welche schnelle Entscheidungen und Reformen behindern oder blockieren können. Die tatsächliche Anzahl der Vetospiele, bzw., deren Machtposition kann nach Politikfeld und Gesetzgebungsprozess schwanken. Diese muss also zeit- und kontextabhängig ermittelt werden.

Die Anschläge vom 11. September 2001 konfrontierten die westlichen Regierungen mit einem Problem, das zuvor eher als abstrakte Bedrohung wahrgenommen wurde: Dem globale Terrorismus. Die erfolgreich verübten Terroranschläge in New York und Washington D.C. hatten deutlich gemacht, dass die westlichen Sicherheitsarchitekturen auf diese neue Herausforderung nicht vorbereitet gewesen waren. Das Versagen der amerikanischen Geheimdienste und Polizeibehörden die geplanten Anschläge zu verhindern, beruhte maßgeblich auf der mangelnden Koordinierung der Sicherheitsbehörden und Informationszusammenführung. Diese Erkenntnis setzte die westlichen Regierungen unter einen starken Reformdruck. Um zukünftige Anschläge zu verhindern mussten die Kompetenzen der Behörden erweitert, die Informationssysteme relevanter Behörden verknüpft und die Handlungen zwischen diesen besser koordiniert werden. Die mediale Aufmerksamkeit der Anschläge, eine verunsicherte Bevölkerung sowie die Ungewissheit bezüglich möglicher Anschläge im eigenen Land setzten die Bundesregierung und den Bundesinnenminister in den Folgemonaten unter erheblichen Handlungsdruck. Einen Monat nach den Anschlägen vom 11. September wurde über das vom damaligen Bundesinnenministers Otto Schily (SPD) initiierte Sicherheitspaket 1 im Bundestag beraten. Zweieinhalb Monate später wurde bereits das weiterreichende Sicherheitspaket 2 geplant. Dieses umfasste vor allem Befugnis- und Kompetenzerweiterungen der relevanten Sicherheitsbehörden, wie dem Bundeskriminalamt (BKA), der Bundespolizei (BPol) oder dem Bundesamt für Verfassungsschutz (BfV) (FAZ 2001).

Seit 1998 wurde die Regierung im Bundestag durch eine Koalition aus SPD und Bündnis90/Die Grünen gebildet, welche mit 345 Sitzen die Mehrheit im Parlament stellten. Die beiden Koalitionspartner bildeten die zwei parteipolitischen Vetospieler. Im Bundesrat hingegen bestand die rot-grüne Mehrheit nur bis zum 7. April 1999. Der danach unionsdominierte Bundesrat hatte sich in der Vergangenheit bereits mehrmals gegen Gesetzesvorhaben der Regierung gewandt. Diese hatte versucht den Bundesrat durch Aufteilung der Gesetze in zustimmungspflichtige und nicht zustimmungspflichte Gesetze zu umgehen. Auch wurde versucht einzelne, von Großen Koalitionen regierte Länder durch Kompromisse aus der Unions-Blockade „herauszukaufen“. Diese Strategie war jedoch mit der Übernahme der absoluten Mehrheit durch schwarz-gelb im Bundesrat im Mai 2002 keine

Option mehr. Die Opposition konnte mit dem Bundesrat nun einen starken institutionellen Vetospieler kontrollieren. Die Koalition war zur Kompromisssuche mit der Opposition gezwungen, wenn es die Zustimmung des Bundesrates benötigte.

Die Sicherheitspakete 1 und 2 wurden jedoch grundsätzlich von der Opposition unterstützt. Die inhaltlich konservative Sicherheitspolitik der rot-grünen Koalition ähnelte dem, was die Union selbst gefordert hatte. Dementsprechend wurde von Seiten der Union überwiegend Lob für das Gesetzesvorhaben ausgesprochen. So äußerte sich Günther Beckstein (CDU), damaliger bayerischer Staatsminister des Innern: „Mit ihrem Sicherheitspaket II hat die Bundesregierung die richtige Richtung eingeschlagen." (Bundesrat 770 2001: 655). Die CDU/CSU war stärker von der Sorge getrieben, dass sich die SPD auf dem bei einer konservativen Wählerschaft bedeutenden Gebiet der Inneren Sicherheit profilieren könnte. Die Gesetzesvorschläge der SPD konnten nicht großflächig kritisiert werden, da diese bei eigener Regierungsverantwortung ähnlich gestaltet worden wären. Dies musste von der Union bedacht werden, da schon im nächsten Jahr die Bundestagswahl anstand (Meyer 2004). Deswegen forderten die Union und der unionsdominierte Bundesrat stattdessen noch eine Verschärfung der Gesetze. So setzten sich Beckstein und der Ministerpräsident von Baden-Württemberg Erwin Teufel (CDU) im Bundesrat unter anderem für die Ausweitung der Gesetze um Einbürgerungskontrollen und eine Erleichterung der Ausweisung gewaltbereiter Extremisten ein (Bundesrat 770 2001: 656). Dies ist aber eben eher auf die beschriebenen parteipolitischen Gründe, als auf starke inhaltliche Differenzen zurückzuführen. Die grundsätzliche inhaltliche Übereinstimmung wurde auch dadurch befördert, dass in der aufgeheizten Stimmung nach den Terroranschlägen in den USA gegenüber der Bevölkerung und damit den Wählern glaubwürdige Sicherheitsmaßnahmen präsentiert werden mussten, was eher eine konservative Sicherheitspolitik beförderte. Keine der Parteien wollte gegenüber der Öffentlichkeit dafür verantwortlich sein notwendige Gesetze zu blockieren (Preuß 2012: 204, 205). Dieser Effekt wurde zusätzlich dadurch verstärkt, dass die auf dem Feld der Inneren Sicherheit sich profilierende Schill-Partei zu dieser Zeit einige Popularität genoss und man diese durch zögerliches Handeln nicht begünstigen wollte (Spiegel Online 2001). Insgesamt führte dies zu einer eher konservativen Sicherheitspolitik der SPD, welche inhaltlich den Vorstellungen der CDU/CSU entsprach. Diese hatte aufgrund der anstehenden Wahlen und der Drucksituation kein Interesse an einer Blockade der Gesetzesvorschläge. Aufgrund dessen muss festgestellt werden, dass die inhaltliche Kongruenz zwischen der SPD und der CDU sehr hoch war.

Auch die Polizeigewerkschaften unterstützten die Anti-Terror-Pakete. Diese hatten seit den 1990er Jahren vor allem mit durch Strukturreformen bedingten Personalabbau zu kämpfen. Die Unterstützung der Gewerkschaft ist auf die Hoffnung zurückzuführen, dass eine Ausweitung der Kompetenzen von Sicherheitsbehörden zu einer Vergrößerung der Personalstellen führt. Die Gewerkschaften erhofften sich die Folgen der Strukturreformen und des Personalabbaus seit der 1990er Jahren abschwächen zu können (Preuß 2012: 204). In diesem Zusammenhang wurden Sparmaßnahmen kritisiert: „Polizei, Verfassungsschutz und Justiz sind in den letzten Jahren kaputt gespart worden." (Gewerkschaft der Polizei 2001).

Bei den Verhandlungen konnte sich die SPD in eine politische Vermittlerrolle zwischen den Grünen und der Union bringen. Die Grünen kritisierten die enthaltende Abschiebung auf Verdacht, während die Union an dieser festhalten wollte und eine Verschärfung der Maßnahmen forderte. Die SPD berücksichtigte die Kritik der Grünen und änderte die entsprechenden Passagen in der Gesetzesvorlage ab. Die Grünen zeigten sich grundsätzlich kompromissbereit und ließen andere Einwände fallen, nachdem die SPD zugesagt hatte, dass einige der Maßnahmen auf fünf Jahre befristet sind (FAZ 2001b).

Insgesamt gab lagen die Positionen bezüglich der Sicherheitsreformen der vier Vetospielern SPD, Grüne, Union (welche den Bundesrat kontrollierte) nicht zu weit auseinander. Die geplante Kompetenzerweiterung des BKA und des Verfassungsschutzes auf Bundesebene mobilisierte jedoch der Widerstand der Länder im Bundesrat. Beckstein dazu: „Wenn wir auf Grund der neuen Herausforderung schon die Kompetenzerweiterung des Bundes akzeptieren, muss den Ländern wenigstens die Möglichkeit gegeben werden, selbst dafür zu sorgen, dass sie die entsprechenden Auskünfte erhalten." (Bundesrat 770 2001: 655). Da Schily die Zustimmung des Bundesrates brauchte, war er gezwungen auf die Forderungen der Länder einzugehen und die ursprünglich nur für den Verfassungsschutz vorgesehen Kompetenzerweiterungen nun auch auf die jeweiligen Landesämter zu übertragen. Daraufhin signalisierten auch die Länder ihre Unterstützung (Spiegel Online 2001b). Sowohl das erste, als auch das zweite Sicherheitspaket wurden mit breiter Mehrheit, nur mit Widerspruch einzelner Abgeordneter von Bündnis 90/Grüne sowie der PDS, im Bundestag verabschiedet. Die Verabschiedung der Gesetze erfolgte außerordentlich schnell. Das umfangreiche Sicherheitspaket 2 wurde am 2. November als Entwurf vorgelegt und bereits am 14. Dezember vom Bundestag sowie am 20. Dezember vom Bundesrat verabschiedet (Meyer 2004).

Die Beobachtungen zur ersten Prozessstation decken sich mit den Erwartungen eines machtpolitischen Mechanismus. Die Motivation der SPD und CDU Sicherheitskompetenzen

stärker an den Bund zu koppeln, scheint zwar aus einem Aktionismus heraus motiviert, aber dies steht nicht im Widerspruch zu machtpolitischen Erwägungen. Die beiden Volksparteien hatten als aktuelle und potentielle Regierungsparteien ein grundsätzliches Interesse daran die Kompetenzen des Bundes gegenüber jenen der Länder auszuweiten, um die Machtstellung des Bundes zu stärken. Dies trifft auf die Grünen weniger zu, weil Sicherheit, anders als bei den beiden Volksparteien, nicht zu ihren Kernkompetenzen gehört und sie traditionell auch keinen Minister in diesem Ressort stellen. Eine Kompetenzausweitung der Sicherheitsbehörden des Bundes hätte jedoch einen Machtverlust für die Landesregierungen bedeutet. Um die Machtrelation im Sicherheitsbereich aufrechtzuerhalten und eine Tendenz zur Hierarchisierung zu verhindern, nutzten die Länder den Bundesrat als institutionellen Vetospieler. Der Bundesrat wird im Vetospielertheorem zumeist auf seine Rolle als parteipolitisches Instrument reduziert, mit welchen die Opposition, sofern sie eine Mehrheit im Bundesrat hält, Entscheidungen der Regierungen blockieren kann. Dabei wird übersehen, dass noch eine andere Frontlinie in Föderalen Systemen entstehen kann – nämlich jene zwischen Bund und Ländern. Aufgrund der drohenden Blockade musste die SPD einlenken und konnte ihren Einfluss im Bereich der Inneren Sicherheit nicht entscheidend vergrößern.

Während die ersten beiden Anti-Terror-Pakete eine Kompetenzausweitung der Sicherheitsbehörden realisierten, wurde damit noch nicht das Problem der Informationszusammenführung und der Koordinierung der verschiedenen Behörden angegangen. Zudem sollte Schily mit dem dritten Sicherheitspaket erneut versuchen die Kompetenzen des Bundes im Sicherheitsbereich gegenüber den Ländern zu stärken (FAZ 2001). Hierfür wurden im Vorfeld verschiedene Reformkonzepte gemacht. Eckart Werthebach (CDU), ehemaliger Berliner Innensenator und Präsident des BfV, formulierte 2002 den Vorschlag eine zentralisierte Bundesbehörde aufzubauen, welche die Kompetenzen des Verfassungsschutzes und des Bundeskriminalamtes vereinen sollte. Zudem sollte der Posten eines Sicherheitsberaters geschaffen werden, welcher für die Koordinierung der Aktivitäten der Sicherheitsbehörden verantwortlich sein würde (Spiegel Online 2002). Auch Prof. Eckard Jesse, Politologe an der TU Chemnitz, kritisiert die Koordinierungsmängel zwischen dem Bundesamt für Verfassungsschutz und den 16 Landesbehörden (Jesse 2003). Ein ähnliches Konzept zur Zentralisierung im Bereich der Inneren Sicherheit wurde 2004 in einem Gutachtenband von Werner Weidenfeld vorgeschlagen. Hier wurde dafür plädiert zu prüfen,

„...inwieweit BfV und BND eine gemeinsame Auswertung...institutionalisieren können..."
„...Die Angelegenheiten des Verfassungsschutzes in Deutschland sollten neu geordnet und am besten ausschliesslich auf Bundesebene angesiedelt werden. Zumindest ist zu fordern, dass die Zahl der 16 Landesverfassungschutzämter durch Zusammenlegung deutlich reduziert wird." (Weidenfeld 2004: 16).

Nach den Terroranschlägen in Madrid am 11. März 2004 wurde dieses Leitbild einer „Einheitlichen Megabehörde" (Norman 2006: 91) von einzelnen Politikern der CDU und der Grünen (Jürgen Rüttgers, Wolfgang Bosbach, beide CDU, und Volker Beck, Bündnis90/Die Grünen) aufgegriffen, welche forderten „...die Landesämter für Verfassungsschutz zugunsten eines zentralen Bundesamtes abzuschaffen" (Carstens 2004). Über dieses Zentralisierungskonzept entbrannte schnell eine heftige Diskussion. Die Fronten verliefen dabei vertikal, d.h. zum großen Teil zwischen befürwortenden Bundespolitikern und ablehnenden Landesvertretern. Dabei wurden auch immer wieder Sorgen bezüglich einer drohenden Aufhebung des Trennungsgebotes formuliert, welche Befürworter einer zentralen Behörde zu zerstreuen versuchten (Norman 2006: 103).

Im Juni 2004 schließlich brachte Schily eine Zentralisierung der Sicherheitsbehörden auf die politische Agenda. Die Verfassungsschutzbehörden der Länder sollten als Filialen dem Bundesamt für Verfassungsschutz unterstellt werden. Sollte dies nicht durchzusetzen sein, forderte der Minister für das BKA und das BfV zumindest „bestimmte Weisungsrechte oder mindestens Koordinierungsrechte" gegenüber den entsprechenden Landesämtern. Schily hielt „zentrales operatives Handeln für geboten" und forderte „stärkere präventive Kompetenzen für das BKA" bei der Bekämpfung von Terrorismus, aber auch der organisierten Kriminalität. Die Innenminister der unionsregierten Länder reagierten mit Ablehnung auf das Konzept einer zentralen „Mammutbehörde" und forderten stattdessen eine „Vernetzung in der Fläche". Zusammen mit dem BKA formulierten sie die alternative Idee eines gemeinsamen Analysezentrums in Berlin. Grundlage sollte eine gemeinsame Datei aller Sicherheitsbehörden sein (Käppner/Ramelsberger 2004). Im September 2004 kündigte Schily offiziell das dritte Sicherheitspaket an, welches die Rechte für präventive Maßnahmen des BKA und die Weisungsbefugnis der Bundesbehörden beinhaltete. Der Innenminister plante das Gesetzespaket noch im selben Jahr einbringen und schloss auch eine Änderung des Grundgesetzes nicht aus, falls die Konzepte mit dem Trennungsgebot kollidieren sollten (Spiegel Online 2004).

Die Reformvorschläge wurden von den Landesvertretern entschieden abgewiesen. Die Regierungen der Länder Nordrhein-Westfalen, Hessen, Rheinland-Pfalz, Hamburg und Sachsen lehnten Schilys Vorstoß ab. Innenminister Beckstein unterstützte zwar in Übereinstimmung mit allen anderen Innenministern eine verbesserte Zusammenarbeit zwischen den Sicherheitsbehörden, setzte sich jedoch weiterhin für die föderale Struktur des Verfassungsschutzes ein (Ramelsberger 2004; Carstens 2004b). Auf der Innenministerkonferenz kam es bezüglich der Kompetenzverteilung zwischen Bund und Ländern zwischen Schily und den Innenminister der Länder zu einer heftigen Auseinandersetzung, in Zuge dessen sich die Fronten verhärteten (Spiegel Online 2004b) Bremens Regierungschef Scherf (SPD) lehnte die Vorschläge seines Parteikollegen offen ab: „Die Innenminister der Länder sind allesamt über Kreuz mit Bundesinnenminister Otto Schily, der versucht das zentralistisch zu regeln.“. Kritik wurde jetzt auch von Seiten der nicht unions-regierten Länder verstärkt laut. Die sozialdemokratischen Innenminister von Schleswig-Holstein und Nordrhein-Westfalen lehnten die Eingliederung von Landesämtern in den BfV ab. Die Erweiterung der Befugnisse des BKAs um präventive Maßnahmen wurde hingegen begrüßt. Auch der BKA-Chef Ziercke äußerte sich positiv über die Befugniserweiterungen, lehnte eine zentrale Bundesbehörde jedoch ab (Pergande 2004; Schattauer/Vernier 2004). Auch die Polizeigewerkschaft sprach hinsichtlich dieser Pläne von einem „Ablenkungsmanöver“, um die technischen und personellen Defizite bei den bestehenden Behörden zu verschleiern (RP Online 2004).

Nachdem klar war, dass das geplante Sicherheitspaket 3 keine Zustimmung im Bundesrat erhalten würde, versuchte Schily sein Ziel über die laufende Föderalismuskommission zu erreichen. Diese war seit 2003 eingesetzt und sollte die Gesetzgebungszuständigkeiten und Mitwirkungsrechte zwischen Bund und Ländern reformieren. Die Kommission hatte 32 stimmberechtigte Mitglieder, jeweils 16 Mitglieder des Bundestags (8 SPD-Abgeordnete, 6 CDU, 1 Grüne, 1 FDP) und 16 Mitglieder des Bundesrats. Um das Reformvorhaben in die Kommission einzubringen, brauchte es jedoch die Zustimmung des Koalitionspartners. Mit den Grünen befand sich Schily jedoch seit Bekanntgabe des Reformvorhabens im offenen Streit über das Trennungsgebot. Grünen-Fraktionsvorsitzende Krista Sager, Parteichefin Claudia Roth und der Geschäftsführer der Grünen-Fraktion Volker Beck lehnten allesamt die geplanten Kompetenzerweiterungen des BKA ab und kritisierten Schilys Umgang mit dem Koalitionspartner. Grünen-Fraktionsvize Hans-Christian Ströbele unterstützte zudem die Position der Länder und betonte, dass eine Ausweitung der Befugnisse des BKA „eine der Säulen unserer föderalen Strukturen“ bedrohe

(SZ-Online 2004). Politiker der grünen Landesregierungen wie die schleswig-holsteinische Justizministerin Anne Lütkes oder der stellvertretende Ministerpräsident von Nordrhein-Westfalen Michael Vesper sprangen jetzt wiederrum ihren Parteikollegen auf Bundesebene zur Seite und lehnten eine Grundgesetzänderung ab (Handelsblatt 2004). Da keine Einigung mit den Grünen erzielt werden konnte, mussten die sozialdemokratischen Abgeordneten das Thema um eine Befugniserweiterung des BKA bei der Föderalismuskommission zurückziehen (Berliner Zeitung 2004). Schilys Pläne um eine Zentralisierung der Sicherheitsbehörden waren damit endgültig gescheitert.

Die machtpolitische Frontlinie zwischen Bundesregierung und Bundesländern tritt beim Sicherheitspaket 3 noch deutlicher zu Tage. Der Grund dafür ist, dass im Unterschied zu den ersten beiden Sicherheitspaketen nicht nur eine Kompetenzverschiebung hin zum Bund geplant war, sondern mit der angestrebten Zentralisierung die Länder einen Machtverlust hätten hinnehmen müssen. Dies erklärt die starke, parteiübergreifende Opposition der Länder. Das von diesen vorgeschlagene Alternativkonzept einer „Vernetzung in der Fläche“ hätte hingegen die Kompetenzen der Länder unberührt gelassen. Dass die Regierungspartei ihren Einfluss mittels einer hierarchischen Zentralisierung ausdehnen wollte, während die Länder als betroffene Vetospieler sich dagegen wehrten, entspricht der Erwartungen einer machtpolitischen Perspektive. Noch erfolgreicher als bei den ersten Sicherheitspaketen konnten die Länder den Bundesrat als starken institutionellen Vetospieler „übernehmen“ und mit einer drohenden Blockade das Reformvorhaben abwehren. Es ist anzunehmen, dass Schily aufgrund der Erfahrungen mit den ersten Sicherheitspaketen damit gerechnet hatte und bereits von Anfang an darauf abzielte, dass Vorhaben über die laufende Föderalismuskommission zu verwirklichen. Dies scheiterte jedoch wie beschrieben am Widerstand der Grünen. Dies ist nur schwer aus einer machtpolitischen Perspektive heraus zu begründen. Das Verhalten der Grünen scheint tatsächlich aus einem Legitimitätsglauben an das Trennungsgebot bestimmt zu sein. Aber selbst ohne den Widerstand der Grünen bleibt es höchst zweifelhaft, dass die Reform über die Föderalismuskommission hätte verwirklicht werden können. Diese bestand nämlich wie beschrieben zur Hälfte aus Vertretern der Bundesländer, welche das Vorhaben auch in der Kommission hätten blockieren können. Die Polizeigewerkschaft lehnte eine Zentralisierung ebenfalls ab, was darauf zurückzuführen ist, dass diese mit einem Stellenabbau in den Ländern verbunden gewesen wäre. Es ist aber nicht anzunehmen, dass die Haltung der Gewerkschaften ausschlaggebend für den Ausgang des Prozesses war. Die Bundesländer hätten aufgrund eines drohenden Kompetenzverlustes auch ohne Unterstützung der Polizeigewerkschaften gegen das Reformvorhaben votiert. Der

Ausgang des Prozesses hing also maßgeblich von der Vetomacht der stärksten Vetospieler ab. Entscheidend war dabei, dass der Regierung als starker Vetospieler mit dem Bundesrat ein ebenfalls starker Vetospieler entgegenstand. Die Regierung konnte den Prozess daher nicht dominieren und musste auf die Forderungen der Länder eingehen. Als Folge dieses Prozess fand eine Reproduktion der institutionellen Machtaufteilung zwischen Bund und Ländern in den Sicherheitsbereich statt. Da eine zentralisierte Bundesbehörde nicht durchsetzbar war, musste Schily alternative Strukturen unter Berücksichtigung der Interessen der Vetospieler schaffen. Mit der Blockade einer Zentralisierung im Sicherheitsbereich verhinderten die Länder also nicht nur einen Machtverlust, sondern es kam effektiv zu einer Machterweiterung, da die Länder für die Problembewältigung an der Schaffung neuer Sicherheitsbehörden beteiligt werden mussten. Die institutionelle Machtaufteilung zwischen Bund und Ländern spiegelt sich in den Strukturen des GTAZs wieder.

Im Dezember 2004 wurde in Berlin das Gemeinsame Terrorismus-Abwehrzentrum (GTAZ) eröffnet. Die Zusammenarbeit der involvierten Sicherheitsbehörden von Bund und Ländern entsprach dabei den Forderungen der Länder nach einer „Vernetzung in der Fläche“ (Käppner/Ramelsberger 2004). Die neue geschaffene Koordinierungsstelle sollte das Problem des mangelnden Informationsaustausches und Koordinierung der Sicherheitsbehörden bei der Terrorismusbekämpfung lösen. Zunächst waren nur rund 100 Mitarbeiter des BKA und 15 Mitarbeiter des BfV in den Zentrum untergebracht. Die Institution sollte jedoch schrittweise um weitere Sicherheitsbehörden und Mitarbeiter vergrößert werden. Bis Mitte 2005 war geplant die Zahl der Verfassungsschützer auf 50 Ermittler auszuweiten. Dazu sollten über Verbindungsbüros der BND, der Bundesgrenzschutz, das Zollkriminalamt, der Militärische Abschirmdient (MAD), die Bundespolizei, die Generalbundesanwaltschaft und die Kriminal- und Verfassungsschutzämter aus Bund und Ländern miteinbezogen werden. Das GTAZ stellt keine eigenständige Behörde dar, sondern eine Koordinierungsstelle, bei der die mitwirkenden Sicherheitsbehörden unter Wahrung ihrer gesetzlichen Aufgaben und Befugnisse zusammenarbeiten. Das Zentrum sollte den Austausch relevanter Informationen erleichtern und somit die Einleitung operativer Maßnahmen zügiger gestalten (BMI 2013b). Da es keine eigenständige Behörde darstellt, war ein Errichtungsgesetz als gesetzliche Grundlage nicht notwendig. Die Beteiligung der Landesbehörden unter vollständiger Wahrung ihrer Befugnisse entsprach den Forderungen der Bundesländer. Das GTAZ steht unter der Kontrolle des BMI. Wenn Gefahrenpotentiale erkannt werden, gehen die relevanten Informationen an die jeweilig zuständigen Behörden wie das BKA oder der BPol. Das GTAZ selber nimmt keine operativen Maßnahmen zur Gefahrenabwehr vor. Um den Forderungen

der Grünen nach einer Wahrung des Trennungsgebotes zwischen Geheimdiensten und Polizei gerecht zu werden, wurde das GTAZ in zwei getrennte Analysezentren unterteilt: Der Nachrichtendienstlichen Informations- und Analysestelle (NIAS) und der Polizeilichen Informations- und Analysestelle (PIAS), welche durch Koordinationsgremien miteinander verknüpft sind; die organisatorische Trennung wurde so gewahrt. Faktisch wurde das Trennungsgebot jedoch durch den Informationsaustausch zwischen beiden Zentren ausgehöhlt. Der organisatorische Aufbau wurde von Seiten der Union als „halbherzige Lösung„ kritisiert (Förster 2004). Bayerns Innenminister Beckstein (CSU) warf Schily vor, dass er die zu enge Auslegung der Grünen akzeptiert habe. Dadurch sei kein gemeinsames Sicherheitszentrum zwischen BKA und Verfassungsschutz entstanden, sondern zwei getrennte Zentren, was ein „Verwaltungsdickicht mit erheblichen Effizienz- und Reibungsverlusten“ mit sich brächte. Von Seiten der Grünen und der Polizeigewerkschaften sind keine Äußerungen oder Kritik am Aufbau des GTAZ zu finden. BKA-Präsident Ziercke und BND-Chef Hanning begrüßten die Einrichtung des GTAZ als wichtiges Forum des Informationssautausches: „Wir müssen dem Netzwerk des Terrors ein Netzwerk an Informationen gegenüberstellen.“ (RP Online 2004b).

Mit den zwei erfolgreichen und dem gescheitertem dritten Sicherheitspaket waren die wichtigsten Sicherheitsreformen abgeschlossen. Diese bildeten für die Zukunft die Grundlage für die Bildung von neuen Sicherheitsstrukturen bei neu aufkommenden Gefahren. Die Netzwerk-Struktur des GTAZ diente dabei als Blaupause für zukünftige Kooperationseinrichtungen. Auf das GTAZ folgte 2006 das Gemeinsame Analyse- und Strategiezentrum illegale Migration (GASIM), 2007 das Gemeinsame Internet-Zentrum (GIZ), und 2011 das Gemeinsame Abwehrzentrum gegen Rechtsextremismus (GAR), sowie das Nationale Cyber-Abwehrzentrum (NCAZ).

Im Vergleich mit den USA oder Großbritannien reagierte Deutschland etwas später auf die zunehmenden Cyberbedrohungen. Das BMI hatte 2009 ein Strategiepapier zum Schutz kritischer IT-Infrastrukturen veröffentlicht, in dem das Gefahrenpotential durch Terrorismus oder Kriminalität für Infrastruktureinrichtungen erkannt wurde (BMI 2009). Auf konkrete Bedrohungen im und aus dem Cyberspace wurde hier jedoch noch nicht eingegangen. Auf das gestiegene Gefahrenpotential durch Cyberbedrohungen machte erstmals der Bericht des Verfassungsschutzes von 2009 aufmerksam. Dieser hatte „auf breiter Basis durchgeführte zielgerichtete elektronische Angriffe auf Behörden und Wirtschaftsunternehmen in Deutschland“ Ursprungs (Bundesamt für Verfassungsschutz 2009: 354)seit 2005 festgestellt. Aufgrund der ausgewählten Ziele dieser Attacken wird von

ausländischen Spionagetätigkeiten ausgegangen. Ein Großteil dieser Angriffe war chinesischen Ursprungs (Bundesamt für Verfassungsschutz 2009: 355). Neben den Cyberbedrohungen durch staatliche Akteure nahmen auch die Gefahren durch Cyberkriminalität stetig zu. In dem Bundeslagebild zu Cyberkriminalität des BKA wurde von 2009 auf 2010 ein Anstieg der Cyberkriminalitätsrate von 19% angegeben. Der registrierte Schaden war sogar um mehr 66% gegenüber dem Vorjahr gestiegen (Bundeskriminalamt 2010: 6). Die Enthüllungen im April 2009 über GhostNet, ein Computer-Spionagenetzwerk, welches weltweit eingesetzt wurde um staatliche Behörden und internationale Organisationen auszuspähen, sowie im Juni 2009 über den Computerwurm Stuxnet brachten das Thema Cybersicherheit sehr schnell auf die politische Agenda. Insbesondere der Angriff durch Stuxnet und die erfolgreiche Störung des iranischen Atomprogrammes erhielten ein starkes mediales Echo und verdeutlichten das Gefahrenpotential durch elektronische Angriffe. Zugleich offenbarte es Abstimmungsprobleme zwischen den Betreibern kritischer Infrastrukturen und den Sicherheitsbehörden. Als die Bundesregierung eine Anfrage bezüglich des Gefahrenpotentials von Stuxnet und anderer Schadsoftware für deutsche Infrastrukturen stellte, dauerte es vier Tage bis Industrie und zuständige Behörden die nötigen Informationen bereitstellen konnten (Spiegel Online 2011). Diese Entwicklungen erhöhten den Druck auf die politischen Entscheidungsträger zur Entwicklung einer Cybersicherheitsstrategie.

Die am 23. Februar 2011 im Kabinett beschlossene "Cyber-Sicherheitsstrategie für Deutschland“ beinhaltete den Aufbau neuer Strukturen zur Herstellung von Cybersicherheit (BMI 2011). Im Zentrum standen dabei ein neues Nationales Cyber-Abwehrzentrum (NCAZ), sowie ein Nationaler Cyber-Sicherheitsrat. Ziel des NCAZ sollte der Schutz von Deutschlands Informationsinfrastrukturen vor Angriffen sein. Dazu sollten Angriffsformen analysiert sowie Informationen bezüglich Schwachstellen und Vorfällen ausgetauscht werden. Nicht nur die steigende Gefahr durch Cyberbedrohungen begründete die Notwendigkeit für ein solches Zentrum, sondern auch die Tatsache, dass die Art der Angriffe die Zuständigkeiten verschiedener Sicherheitsbehörden kreuzten (BT-Drucks. 17/5694 2011: 2). Das Kooperationszentrum hat am 1. April 2011 seine Arbeit mit Sitz in Bonn aufgenommen. Das NCAZ ist dem Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstellt. Es ist damit Teil des Bundesinnenministeriums und untersteht einer zivilen Kontrolle. Für die Struktur des NCAZ diente das GTAZ als Vorbild. Zu Beginn wurde das Zentrum von sechs Mitarbeitern des BSI, zwei Verfassungsschützern und zwei Mitarbeitern des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe besetzt. Neben diesen Kernbehörden wurden

später weitere assoziierte Sicherheitsbehörden außerhalb des BMI integriert, wie das BKA, die BPol, die Bundeswehr, der BND und das Zollkriminalamt. Diese werden regelmäßig und anlassbezogen über Verbindungsbeamte einbezogen. Die Zusammenarbeit mit der Wirtschaft erfolgt über bereits bestehende Kooperationen wie z.B. dem Umsetzungsplan KRITIS zwischen dem BSI und den Betreibern kritischer Infrastrukturen. Das neue Zentrum sollte die Kooperation der Behörden im Bereich Cybersicherheit auf eine institutionalisierte Basis stellen, was den Informations- und Erfahrungsaustausch zwischen diesen verbessern sollte. Wie beim GTAZ erfolgt die Zusammenarbeit dabei unter Beibehaltung der bisherigen gesetzlichen Befugnisse der einzelnen Behörden (BMI 2011). Die Analysen und erstellen Lagebilder sollen den beteiligten Sicherheitsbehörden, dem Cyber-Sicherheitsrat und der Bundesregierung zukommen. Das NCAZ grenzt sich in seinem Aufgabenbereich von bereits bestehenden IT-Sicherheitsstrukturen im BSI, wie dem IT-Lagezentrum (BSI-IT-LZ) oder dem CERT-Bund, ab. Diese sind für kleinere IT-Störfälle, wie z.B. Hacking oder Malware zuständig, während das NCAZ für größere Angriffe auf deutsche Rechnersysteme seitens Staaten oder Hackergruppierungen zuständig ist. In einem solchen Fall soll das Zentrum an einen Krisenstab des BMI Bericht erstatten. Unter Berücksichtigung des Trennungsgebotes findet im NCAZ keine operative Zusammenarbeit statt, weswegen aus Sicht der Bundesregierung keine verfassungsrechtlichen Bedenken bestehen. Auch verfügt die Einrichtung weder über Weisungsbefugnisse noch Mandate gegenüber den Herstellern von Informations- und Kommunikationstechniken, wie z.B. Internetprovidern (BT-Drucks. 17/5694 2011: 3, 4). Da das NCAZ, wie auch das GTAZ, keine eigenständige Behörde darstellt, war zu seiner Errichtung kein gesondertes Gesetz nötig. Die Zusammenarbeit der beteiligten Sicherheitsbehörden erfolgt auf Basis von Kooperationsvereinbarungen (BT-Drucks. 17/5694 2011: 2). Die gesetzliche Grundlage für den gemeinsamen Informationsaustausch war mit dem Gesetz zur Anti-Terror-Datei bereits gelegt.

Zusätzlich zum NCAZ wurde in der Cyber-Sicherheitsstrategie die Bildung eines Cyber-Sicherheitsrates beschlossen. Ziel des Rates ist in Zusammenarbeit zwischen Staat und Wirtschaft die Entwicklung von Strategien und Maßnahmen gegen Cyberangriffe auf Infrastrukturen und Kommunikationsnetzwerke. Auch über die Cyber-Außenpolitik wird in dem Gremium beraten. Der Sicherheitsrat setzt sich aus Vertretern des Kanzleramtes, des Auswärtigen Amtes und den Bundesministerien der Verteidigung, der Justiz, Forschung und Bildung, Finanzen, sowie Wirtschaft und Technologie zusammen. Die Bundesländer werden durch Vertreter der Länder Baden-Württemberg und Hessen im Rat repräsentiert. Zur Abstimmung der Länderinteressen haben die Länder eine Arbeitsgruppe auf

Staatssekretärsebene eingerichtet, welche im Vorfeld der Sitzungen des Cyber-Sicherheitsrates tagt. Als assoziierte Mitglieder sind Wirtschaftsvertreter des BDI, BITKOM, DIHK und des Übertragungsnetzbetreibers Amprion beteiligt. Nach Bedarf werden Wissenschaftsvertreter hinzugezogen (BMI 2013c). Die Mitglieder treffen sich dreimal jährlich sowie anlassbezogen. Zwischen dem NCAZ und Cyber-Sicherheitsrat besteht in keiner Richtung eine Weisungsbefugnis, welche auch aufgrund der fehlenden Behördenstruktur des NCAZ nicht möglich wäre (BT-Drucks. 17/5694 2011: 5).

Die Bundestagswahlen im September 2009 hatten mittlerweile zu einer Mehrheit der CDU/CSU und FDP im Bundestag geführt. Auch im Bundesrat hielt schwarz-gelb mit 37 Stimmen eine absolute Mehrheit. Dass die schwarz-gelbe Regierung einen Netzwerk-Ansatz für den Aufbau der Cybersicherheitsbehörden wählte, entspricht nicht den Erwartungen einer machtpolitischen Perspektive. Wie bei der SPD ist bei der CDU davon auszugehen, dass diese als Großpartei eine Hierarchisierung präferiert. Da diese, anders als die SPD, zudem eine starke Mehrheit im Bundesrat hielt, waren die Ausgangsbedingungen besser als bei Schilys Reformversuchen. Eine geplante Zentralisierung hätte zwar immer noch eine Kompetenzeinschränkung der Länder bedeutet, aber die Chance der Bundesregierung mit unions-regierten Länderregierungen Kompromisse auszuhandeln muss dennoch als größer eingeschätzt werden als dies bei der rot-grünen Regierung der Fall war. Dennoch lassen sich keinerlei Hinweise auf Planspiele einer Zentralisierung im Cybersicherheitsbereich bei der Union finden. Der Grund ist, dass die zu erwartenden politischen und finanziellen Kosten für eine Hierarchisierung-Reform mit jeder nach dem GTAZ geschaffenen Netzwerk-Behörde gestiegen waren. Hinter der Reproduktion der netzwerkartigen Sicherheitsstrukturen steckt also eine utilitaristische Pfadabhängigkeit.

Eine Zentralisierung im Cybersicherheitsbereich hatte praktisch bedeutet, dass man die relevanten Kernbehörden wie den BfV mit stärkeren Kompetenzen und Weisungsbefugnissen gegenüber den Äquivalenten auf Landesebene hätte ausstatten müssen. Eine Kompetenzaufwertung einer Sicherheitsbehörde in nur einem Sicherheitsbereich ist jedoch praktisch nicht umsetzbar. Wenn z.B. der BfV in einem Cybersicherheitsbereich Weisungsbefugnis gegenüber den Landesämtern hat, dann strahlen diese Befugnisse automatisch in andere Sicherheitsbereiche aus, weil diese nicht immer trennscharf zu unterscheiden sind oder sich überlappen. Starke Kompetenzstreitigkeiten sind vorprogrammiert. Das bedeutete in der Praxis, dass mit einer Zentralisierung im Cybersicherheitsbereich alle zuvor geschaffenen Netzwerk-Behörden in ihrer Struktur nicht länger funktioniert und neu strukturiert hätten werden müssen. Konkret hätten das GTAZ und

die später geschaffenen Behörden GASIM und GIZ sowie das geplante GAR abgeschafft und in hierarchisierter Form neu aufgebaut werden müssen. Mit jedem neu geschaffenen Kooperationszentrum waren die Kosten für eine Abschaffung der Netzwerk-Struktur und Einführung einer Zentralisierung angestiegen. Hinzu kommt, dass für die Sicherheitsbehörden, welche durch ihre Beteiligung an den Kooperationszentren an Einfluss gewonnen hatten, eine Abschaffung dieser Zentren einen Kompetenzverlust und Personalabbau bedeutet hätte. Mit jedem neuen Kooperationszentrum gewannen die Sicherheitsbehörden an Kompetenzen, was im Umkehrschluss bedeutete, dass die Sicherheitsbehörden immer mehr zu verlieren hatten, wenn diese wieder abgeschafft worden wären. Die Netzwerk-Struktur des NCAZ, wie auch bei den anderen nach dem GTAZ geschaffenen Kooperationszentren, ist das Resultat eines sich verstärkenden Lock-in-Effektes. Die politischen Kosten für eine Zentralisierung sind mit jedem hinzugekommen Kooperationszentrum bis zu dem Punkt gestiegen, an dem die potentiellen Vorteile einer Zentralisierung durch die Kosten negiert wurden. Das ist der Grund warum Pläne für eine Zentralisierung der Sicherheitsbehörden im Cybersicherheitsbereich mittlerweile keinerlei Rolle mehr spielen. Die institutionelle Machtverteilung zwischen Bund und Ländern, abgebildet durch die Netzwerk-Struktur der Kooperationszentren, hatte sich aufgrund der rationalen Kosten-Nutzen-Abwägungen der Entscheidungsträger reproduziert.

Dass die Netzwerk-Struktur des NCAZs als alternativlos gesehen wurde, spiegelte sich in einer verhaltenen Kritik wieder. Von Seiten des Koalitionspartners FDP war nur wenig Einwände zu hören. Kritisch äußerten sich nur einzelne Stimmen, wie der Netzpolitiker Manuel Höferlin oder Gisela Pitz, welche die Vermischung von polizeilichen und geheimdienstlichen Aufgaben kritisierten. Im Vorfeld konnte der Bundesinnenminister Thomas de Maizière jedoch die Unterstützung des Wirtschaftsministers Rainer Brüderle von der FDP für sein Vorhaben gewinnen (Spiegel Online 2011). Der Bund Deutscher Kriminalbeamter (BDK) und die Gewerkschaft der Polizei kritisieren erwartungsgemäß die geringe personelle Ausstattung des NCAZ und die unzureichende Beteiligung polizeilicher Behörden. BDK-Chef Klaus Jansen sieht eine effektive 24-Stunden Kontrolle des Internets nur durch „mindestens 100 Spezialisten“ gewährleistet (Heise 2011). Die Cyber-Sicherheitsstrategie und die dazugehörigen Sicherheitsinstitutionen stießen insgesamt auf sehr wenig Widerstand.

Anstatt einer machtpolitischen und utilitaristischen Pfadabhängigkeits-Erklärung könnte eingewandt werden, dass sich die Netzwerk-Struktur der nach dem 11. September geschaffenen Sicherheitszentren aus der Institution des Trennungsgebotes ergeben hat. Aus

der Perspektive einer solchen legitimatorischen Pfadabhängigkeit könnte argumentiert werden, dass eine Zentralisierung der Sicherheitsbehörden gescheitert ist, weil es von genügend Vetospielern als legitim und daher schützenswert erachtet wurde. Deswegen blockierten diese eine Hierarchisierung mit Hilfe ihrer Vetomacht. Das Trennungsgebot, konkret die operative Trennung von Polizei- und Geheimdiensten, reproduzierte sich als Folge in das neu geschaffene GTAZ. Nachdem das erste Kooperationszentrum nach diesem Prinzip etabliert war, verstärkte dies die Legitimität des Trennungsgebotes. Mit jedem neu geschaffenen Kooperationszentrum wurde es zunehmend schwieriger zukünftige Sicherheitsbehörden nicht unter der Beachtung der Norm des Trennungsgebotes zu schaffen. Zu dem Zeitpunkt an dem der Druck durch Cyberbedrohungen neue Sicherheitsbehörden in dem Bereich notwendig gemacht hatte, war das Trennungsgebot von den Vetospielern bereits so institutionalisiert, dass eine Zentralisierung im Cybersicherheitsbereich keine Alternative mehr darstellte. Gegen eine Erklärung, welche auf eine legitimatorische Pfadabhängigkeit zurückgreift, können drei Einwände gemacht werden.

Erstens decken sich die bei einer legitimatorischen Pfadabhängigkeit zu erwartenden Beobachtungen nicht mit den tatsächlichen Beobachtungen. Wäre das Trennungsgebot ausschlaggebend gewesen, dann hätten die entscheidenden Vetospieler bei ihrer Blockade des dritten Sicherheitspaketes auf das Trennungsgebot Bezug genommen. Die beiden Vetospieler, welche sich gegen das Sicherheitspaket 3 stellten, waren die Grünen und die Landesregierungen über den Bundesrat. Von diesen beiden begründeten jedoch nur die Grünen ihre Ablehnung mit dem Trennungsgebot. Die Grünen waren jedoch nicht der entscheidende Vetospieler. Deren Ablehnung war für die SPD zwar ein Problem, aber es war nicht unwahrscheinlich, dass das Sicherheitspaket 3 mit Stimmen aus den anderen politischen Lagern den Bundestag hätte passieren können. Die konservativen Reformvorhaben waren wie beschrieben von denen der Union nicht zu weit entfernt. Der entscheidende Vetospieler waren nicht die Grünen, sondern der Bundesrat, da dessen Ablehnung das Scheitern des Sicherheitspaktes 3 besiegelte. Die Landesregierungen formulierten jedoch keine Bedenken hinsichtlich des Trennungsgebotes. Deren Blockade gründete auf der Ablehnung einer Kompetenzabgabe an den Bund im Zuge einer Zentralisierung.

Zweitens verstoßen die geschaffen Kooperationszentren ebenfalls gegen das Trennungsgebot (wenn auch in einem geringeren Maße, als dies bei einer Hierarchisierung der Fall gewesen wäre) bzw. höhlen dieses aus. Das Trennungsgebot verbietet eine organisatorische Angliederung von Geheimdiensten und Polizeistellen. Zudem sollen den Geheimdiensten polizeiliche Befugnisse vorenthalten bleiben (das sogenannte Exekutivverbot

für Geheimdienste). Die Polizei soll wiederrum nicht auf Vorfelddaten der Geheimdienste zugreifen dürfen. Die Kooperationszentren höhlen diese Prinzipien des Trennungsgebotes jedoch faktisch aus. Mit den gemeinsamen Dateien werden die Arbeitsabläufe zwischen beiden Diensten miteinander verbunden. Die polizeilichen und geheimdienstlichen Sicherheitsbehörden können Zugriff auf Informationen nehmen, zu dessen Erhebung sie nach dem Trennungsgebot keine Befugnis gehabt hätten. Zwar hätte eine Zentralisierung hinsichtlich des Trennungsgebotes einen größeren Verstoß bedeutet, aber auch die Kooperationszentren waren diesbezüglich weit von einer Ideallösung entfernt. Nicht ohne Grund wurden auch diese immer wieder seitens der Grünen und FDP kritisch kommentiert. Wenn also die Kooperationszentren nicht dem Trennungsgebot entsprechen, dann ist fraglich, ob deren Entstehung mittels einer legitimatorischen Pfadabhängigkeit mit Rückgriff auf dieses Gebot erklärt werden kann.

Drittens ist es zu bezweifeln, ob beim Trennungsgebot wirklich von einer etablierten Norm gesprochen werden kann. Das Trennungsgebot ist nicht explizit im Grundgesetz verankert, sondern wird aus anderen Grundgesetzartikeln abgeleitet. Ohne auf einzelne Paragraphen einzugehen kann festgehalten werden, dass die Herleitung strittig ist. Zudem wir das Trennungsgebot auch in der Praxis unterschiedlich ausgelegt. So hat die CDU im Zuge der Auseinandersetzungen um das GTAZ den Grünen vorgeworfen, dass diese das Trennungsbot zu eng auslegen würden (Die Welt 2004). Bei der Auslegung des Trennungsgebotes scheint es also großen argumentativen Spielraum zu geben.

6.2 Großbritannien

Anders als in Deutschland zeichnet sich das politische System Großbritanniens durch ein hohes Maß an Machtkonzentration aus. Politische Reformen und Zentralisierungsbestrebungen sind daher deutlich einfacher umzusetzen als in der BRD. Sowohl die Sicherheitsstrukturen der Terrorismusabwehr, als auch die in jüngerer Zeit geschaffenen Sicherheitsstrukturen der Cyberabwehr zeichnen sich durch ein hohes Maß an Zentralisierung aus. Die Cyber-Policy ist in ihrer Entstehung anders als in Deutschland nicht maßgeblich durch die bereits existierenden Strukturen der Terrorismusabwehr beeinflusst worden. Der zentralisierte Aufbau in der Terrorismusabwehr als auch in der Cyberabwehr ist stattdessen auf die machtpolitischen Verhältnisse in Großbritannien zurückzuführen, welche der jeweiligen Regierung die Möglichkeit geben den Gesetzgebungsprozess zu dominieren.

Um den Entstehungsprozess nachzuzeichnen werden drei Prozessstationen untersucht: Die ersten beiden Stationen sind die zwei Cybersicherheits-Strategiepapiere von 2009 und

2011, in welchen die Organisationen und Strukturen der Cyber-Policy festgelegt werden. Die dritte Prozessstation ist die Polizeireform von 2013, welche die Zentralisierungstendenzen im Sicherheitsbereich vorantreibt und auch Auswirkungen auf den Cybersicherheitsbereich hat. Nur die Polizeireform musste dabei den formalen Gesetzgebungsprozess durchschreiten. Die beiden vorherigen Cybersicherheits-Strategiepapiere sollen jedoch untersucht werden, um festzustellen, ob die Zentralisierungsbestrebungen auf Widerstand innerhalb und außerhalb der jeweiligen Regierungspartei trafen.

Im Gegensatz zu Deutschland zeichnet sich das politische System Großbritanniens durch ein Höchstmaß an Machtkonzentration aus. Das britische Parlament, genauer das Unterhaus, befindet sich in einer sehr starken Machtposition. Diese leiten sich aus der Doktrin der „*parliamentary sovereignty*“ ab, welche neben dem Parlament keine anderen Mächte zulässt. Die Gesetzgebungsmacht liegt allein beim Parlament und muss mit keiner anderen Institution geteilt werden. In ihren Beschlüssen ist die Parlamentsmehrheit nicht an gesetztes Recht gebunden. Da es keine offizielle Verfassung gibt, sind alle Gesetze grundsätzlich gleichwertig, was dem Parlament das Recht gibt diese zu ändern oder abzuschaffen. Formal ist das Parlament nur an sich selbst gebunden. Das Parlament besteht aus zwei Kammern – dem Ober- und dem Unterhaus. Das Oberhaus hat aber im Laufe des 20. Jahrhunderts zunehmend an Einfluss verloren, weswegen es im Entscheidungsprozess keine bedeutende Rolle mehr spielt. Der Entscheidungsprozess wird von der Mehrheit im Unterhaus dominiert. Diese Mehrheit ist aufgrund des Zweiparteiensystems und der starken Kohärenz der Parteien in der Regel gleichzusetzen mit der eigentlichen Regierung. Der Regierung kommt wiederrum fast die alleinige Rolle des Agenda-Setzers zu. Der Premierminister wiederrum übt innerhalb der Regierung eine starke Dominanz aus: Über personalpolitische Instrumente sorgt er dafür, dass seine Parlamentarier auf der von ihm vorgegebenen Regierungslinie bleiben. Dazu hat er das Recht die Minister zu ernennen oder zu entlassen. Die formale „*parliamentary sovereignty*“ stattet also de facto den Premierminister mit einer starken Autonomie aus (Abromeit 2006: 81 ff.) Als einziger effektiver Vetospieler im politischen System Großbritanniens zählt daher der Premierminister. Für lange Zeit galt, dass das Unterhaus nur in Ausnahmefällen die Rolle eines situativen Vetospielers einnehmen kann, nämlich dann, wenn die Regierungsmehrheit zerstritten ist und der Premierminister seine Parlamentarier nicht mehr auf Parteilinie bringen kann. Da die beiden großen Parteien *Labour* und *Conservatives* jedoch eine starke interne Kohärenz aufweisen, kommt dies, anders als im 19. Jahrhundert., kaum noch vor. Seit 1974 wurde die Regierung immer durch eine der großen Parteien *Labour* oder *Conservatives* gebildet. Dies hat sich erstmals wieder mit den letzten

Unterhauswahlen 2010 geändert, wo keine der beiden großen Parteien eine absolute Mehrheit erreichen konnte. Die *Conservatives* gingen daraufhin mit den *Liberal Democrats* eine Koalition ein. Ob sich die *Liberals* langfristig als dritte Partei etablieren und so das Unterhaus zu einem echten Vetospieler transformieren können, bleibt abzuwarten. Insgesamt präsentiert sich die Unterhausmehrheit mit dem neuen Koalitionspartner als fragmentierter, aber ob sie als echter Gegenspieler auftritt, scheint im Moment noch stark von dem Politikfeld abzuhängen. Für die jeweilige Oppositionspartei gilt dennoch, dass diese aufgrund der beschriebenen Rahmenbedingungen keine Möglichkeit hat als Vetospieler aufzutreten.

Der Gesetzgebungsprozess in Großbritannien ist von der Exekutive und dem Premierminister dominiert. Über die von ihnen vorbereiteten Gesetzesvorlagen stimmt die disziplinierte Unterhausmehrheit ab. Das Oberhaus kann noch Korrekturen vorschlagen, aber abgesehen davon sind keine weiteren Akteure beteiligt. Unter den demokratischen Systemen ist Großbritannien eindeutig das Land mit der stärksten Machtkonzentration. Der britische Premierminister dominiert das Entscheidungssystem und ist kaum auf Kompromisse mit anderen Akteuren angewiesen. Wenn er seine Partei hinter sich versammeln kann, was aufgrund der starken internen Kohärenz in der Regel der Fall ist, dann ist sein Macht im Entscheidungssystem nahezu uneingeschränkt (Abromeit 2006: 84-87, 149).

Cyberbedrohungen wurden von der britischen Regierung früher als in Deutschland als ein sich ausweitendes Sicherheitsproblem erkannt. In dem jährlich erscheinenden allgemeinen Sicherheitsstrategiepapier Großbritanniens werden 2008 erstmals Cyberattacken als neue Bedrohung erwähnt (Cabinet Office 2008: 16). Dem vorausgegangen waren, wie in Deutschland, eine Reihe von Hackerangriffen aus dem Ausland. Im Dezember 2007 warnte der britische Geheimdienst MI5 die Führungsebenen von 300 britischen Firmen vor Cyberattacken ausgehend von chinesischen Staatsorganisationen. Die Angriffe sollen Schlüsselstellen der britischen Wirtschaft sowie den Computersystemen größerer Banken gegolten haben. Der Datendiebstahl beinhaltete technologisches Know-How, aber auch Informationen über die Angebote von britischen Unternehmen zum Erwerb von Gütern (The Times 2007: 2). Während in Deutschland die Enthüllung von Stuxnet der Entwicklung einer Cyber-Policy einen Schub verlieh, so waren es in Großbritannien die Cyberangriffe in Estland 2007. Die Angriffe selber richteten nur geringen Schaden an den Webseiten von Regierungseinrichtungen an, aber die Attacken wirkten dennoch wie ein Weckruf für einige NATO-Staaten (Downing 2011: 4). Konkrete Zahlen über den durch Cyberkriminalität entstandenen Schaden an der britischen Wirtschaft sind von der Regierung und den Geheimdiensten vor 2009 nicht offiziell veröffentlicht wurden. Spätere Schätzungen gehen

von rund 27 Millionen Pfund pro Jahr aus (Cabinet Office 2011b). Cyberattacken werden allgemein als Gefahr für die Ökonomie und dem öffentlichen Sektor angesehen, was auf der steigenden Abhängigkeit der Gesellschaft und der Wirtschaft vom Internet und modernen Kommunikationsmittel gründet (Cabinet Office 2011: 11 ff.).

Das erste Strategiepapier zu Cybersicherheit wurde in der Regierungszeit von Premierminister Gordon Brown von der *Labour Party* initiiert. Nachdem Tony Blair (ebenfalls *Labour*) 2007 zurückgetreten war, wurde das Kabinett unter der Führung von Brown neu zusammengestellt. Schon vor Blairs Rücktritt hatte sich Brown für dessen Nachfolge in politische Stellung gebracht. Dabei machte er sich für eine Neuausrichtung der nationalen Sicherheitsagenda an die neuen globalen Herausforderungen stark. Dazu sollten die Polizei- und Geheimdienste mit mehr Personal, mehr Kompetenzen und zusätzlichen finanziellen Mitteln ausgestattet werden. Weiterhin setzte er sich für den Aufbau einer Datei mit biometrischen Daten für die Sicherheitsbehörden ein (The Guardian 2006). Kurz nach Browns Amtsantritt wurde zudem die Grenzkontrolle zentralisiert, indem die Grenz- und Immigrationsbehörde mit UKvisas und Teile der Zollbehörden fusioniert wurde (The Guardian 2007). Obwohl sich keine expliziten Aussagen bezüglich Cybersicherheit von Brown finden lassen, scheint seine Agenda im Sicherheitsbereich davon bestimmt zu sein, bestehende Sicherheitsbehörden zu stärken und gegebenenfalls zu zentralisieren.

Die im Juni 2009 veröffentlichte *Cyber Security Strategy of The United Kingdom: Safety, Security and Resilience in Cyberspace* überträgt diese Bestrebungen auf den Bereich der Cybersicherheit. Das Papier sollte die Rahmenbedingungen für eine ganzheitliche Cybersicherheitsstrategie in Großbritannien legen und kündigte den Aufbau von zwei neuen Institutionen an: Dem *Office of Cyber Security* und dem *Cyber Security Operations Centre* (CSOC) (Cabinet Office 2009: 17). Das *Office of Cyber Security* wurde 2009 eröffnet und wurde 2010 zum *Office of Cyber Security and Information Assurance* (OSCIA) umbenannt. OSCIA untersteht dem *Cabinet Office* und unterstützt den Sicherheitsminister sowie den britischen Nationalen Sicherheitsrat in Fragen bezüglich Cyberspace und Cybersicherheit. Darüber hinaus gibt die Behörde die strategische Ausrichtung vor und koordiniert das nationale Cybersicherheits-Programm inklusive der Mittelverteilung. Die Behörde arbeitet zu diesem Zweck mit einer Reihe von Einrichtungen zusammen, wie dem Verteidigungsministerium, dem *Government Communications Headquarters* (GCHQ), dem *Communications Electronics Security Department* (CESG), dem *Centre for the Protection of National Infrastructure* (CPNI), dem *Foreign & Commonwealth Office* (FCO) und dem *Department for Business, Innovation & Skills* (BIS) (Gov.uk 2013; ENISA 2011). Das *Cyber*

Security Operations Centre (CSOC) wurde 2009 eröffnet und ist Teil des GCHQ, untersteht aber ebenfalls der Kontrolle durch das *Cabinet Office*. Das GCHQ ist neben dem Inlandsnachrichtendienst MI5 und dem Auslandsnachrichtendienst MI6 der dritte Geheimdienst und ist auf Kryptographie und Datenübertragung spezialisiert. Das CSOC hat die Aufgabe Bedrohungen aus dem Cyberspace für die britische Infrastruktur durch Überwachung frühzeitig zu erkennen und gegebenenfalls Gegenmaßnahmen einzuleiten (Infosecurity 2010). Obwohl die Abteilung primär für defensive Aufgaben geschaffen worden ist, wurde bestätigt, dass sie auch über offensive Fähigkeiten verfügt (ZDNet.com 2009). Das CSOC umfasst um die 20 Mitarbeiter (Stand 2010). Neben Experten aus verschiedenen Ministerien wurde auch außerhalb von Regierungsbehörden rekrutiert. Der „Juniorminister" für Sicherheit und Terrorismusbekämpfung des Innenministeriums Alan West bestätigte, dass auch ehemalige Hacker für das CSOC angeheuert wurden (BBC News UK 2009). Eine gesonderte Gesetzgebung war für die Errichtung der beiden Ämter nicht notwendig, da diese innerhalb bestehender Behörden geschaffen wurden.

Infolge der Unterhauswahlen 2010 wurde die *Labour Party* durch eine Koalition aus der *Conservative Party* und den *Liberal Democrats* abgelöst, welche den neuen Premierminister David Cameron stellten. Die neue Regierung ordnete im Mai 2010 eine Überprüfung der Verteidigungs- und Sicherheitspolitik an. Das *Strategic Defence and Security Review* wurde im Oktober desselben Jahres veröffentlicht und nimmt unter anderem eine Neubewertung von Cybersicherheit vor. Cybersicherheit wird jetzt als Risiko der höchsten Stufe bewertet und befindet sich damit in derselben Priorisierung wie Terrorismusabwehr (HM Government 2010: 10). Risiken der Stufe 1 genießen höchste Priorität, was ausschlagend für die Allokation nationaler Ressourcen und Kapazitäten ist (HM Government 2010b: 27). Bei der Vorstellung des *Strategic Defence and Security Review* vor dem Parlament unterstrich Cameron die Neuausrichtung der Verteidigungsstrategie hinsichtlich neuer unkonventioneller Bedrohungen wie Cyberattacken. Zu diesem Zweck kündigte er Investitionen von 650 Millionen Pfund für die nächsten vier Jahre an, welche in ein nationales Cybersicherheits-Programm fließen sollen (House of Commons 2010: Column 798, 804). In der eigenen Regierung trafen die Pläne auf keinen Widerstand. Schatzkanzler George Osborne stellte die geforderten Mittel bereit und unterstrich die Notwendigkeit der Ausgaben mit der Aussage, dass das HM Treasury, das Finanz- und Wirtschaftsministerium, eines der von Cyberangriffen am meisten betroffenen Ministerien sei (Daily Mail 2011). Osborne gehört den *Conservatives* an und hatte den Wahlkampf Camerons für das Amt des Parteivorsitzenden geleitet, wofür er zum Schatzkanzler erst im Schattenkabinett und später in

der Regierung ernannt wurde. Auch der Koalitionspartner äußerte keine Kritik. In ihren Kernbereichen wie Wirtschaft, Steuern und Arbeitsplätze hatten die *Liberal Democrats* bereits Einfluss auf die Vorhaben der *Conservatives* genommen. Die Sicherheitspolitik und insbesondere Cybersicherheit gehören jedoch nicht zu den Kernkompetenzen der Partei. Weder in einer Erklärung vom Parteivorsitzenden Nick Clegg bezüglich der Sicherheitspolitik seiner Partei, noch im offiziellen Parteiprogramm der *Liberal Democrats* finden sich Hinweise auf eine Cyber-Policy (RUSI 2010; Liberal Democrats 2012).

Im November 2011 wurde das zweite Strategiepapier *The United Kingdom Cyber Security Strategy: Protecting and Promoting the UK in a Digital World* veröffentlicht. Die britische Cybersicherheits-Strategie konzentriert sich nun vor allem auf die übergeordnete Aufgabe, Großbritannien zu einem der wichtigsten Märkte im Bereich der Informations- und Kommunikationstechnologie aufzubauen und das allgemeine Wirtschaftswachstum zu fördern. Cyberbedrohungen werden mit dem Ziel bekämpft, den Cyberspace sicherer für Bürger und Unternehmen zu machen. Damit sollen Innovationen und Investitionen gefördert und das volle Potential des Cyberspace ausgeschöpft werden (ENISA 2012: 6). Das Strategiepapier bestätigt zudem die zentrale Rolle der Geheimdienste in der britischen Cyber-Policy. 59 Prozent der angekündigten Investitionen sollten dem GCHQ zukommen (Cabinet Office 2011: 25).

Mit dem *Crime and Courts Act 2013* wurde die Zentralisierung und Hierarchisierung im Sicherheitsbereich vorangetrieben. Während die CSOC für die Abwehr größerer Cyberangriffe und Angriffe fremder Staaten geschaffen wurden, lag die Zuständigkeit für Cyberkriminalität bisher bei der *Police Central e-Crime Unit* und der *Serious Organised Crime Agency* (SOCA). Mit dem *Crime and Courts Act 2013* sollte eine zentrale Strafverfolgungsbehörde, die *National Crime Agency* (NCA), geschaffen werden, welche dem Innenministerium unterstellt werden sollte. Bisher bestehende, spezialisierte zivile Sicherheitsbehörden sollten als Unterabteilungen in die NCA integriert werden. Die *Police Central e-Crime Unit* und SOCA fusionierten und formten innerhalb der NCA die *National Cyber Crime Unit* (Gov.uk 2013b). Die *National Cyber Crime Unit* wurde bereits im Juni 2011 von der Innenministerin Theresa May angekündigt (BBC News UK 2011). Nachdem das Gesetz eingebracht wurde, wurde es nach der zweiten Lesung im Unterhaus in einem Ständigen Ausschuss überführt (*Public bill committee*), worauf die *Labour Party* bestanden hatte. In diesen Ausschüssen werden Gesetze Klausel für Klausel bearbeitet und eventuelle Änderungsvorschläge diskutiert. Da sich die Zusammensetzung der Ausschüsse jedoch an den Mehrheitsverhältnissen im Unterhaus orientiert, werden kaum noch Änderungen an den

Gesetzen vorgenommen. Die Debatte im Ausschuss fand erwartungsgemäß hauptsächlich zwischen der *Conservative* und der *Labour Party* statt.

Obwohl die *Labour Party* keinen Vetospieler darstellte, soll hier nicht unerwähnt bleiben, dass Kritik von Seiten der Opposition an der NCA auf dessen Finanzierung abzielte. Abgeordnete der *Labour Party* wie Keith Vaz oder die Schatten-Innenminister Yvette Cooper kritisierten, dass die neue Behörde mehr Aufgaben bei deutlich verringertem Budget übernehmen sollte (House of Commons 2013: Column 634, 644, 645). Die Zentralisierung hingegen wurde nicht kritisiert. Cooper machte sich sogar für eine zusätzliche Stärkung der Behörde stark: „...given the changing patterns of national and international crime, it should have more powers and scope." (House of Commons 2013: Column 646). Substantielle Änderungen erfuhr das Gesetz jedoch nicht mehr, sodass es am 25. April offiziell erlassen wurde.

Diese Beobachtungen decken sich mit den Erwartungen einer machtpolitischen Erklärung. Die *Labour Party* saß zwar in der Opposition, stellt jedoch eine potentielle Regierungspartei dar, welche erwarten kann bei der nächsten Regierungsübernahme erneut das Innenministerium zu besetzen. Dementsprechend liegt es ebenfalls in ihrem Interesse, dass die Kompetenzen hierarchisiert werden, da dies eine stärkere Kontrolle auf Ministerebene bedeutet hätte. Vergleichbares konnte in Deutschland beim Sicherheitspaket 1 beobachtet werden, wo die CDU als Oppositions-, aber potentielle Regierungspartei, die geplante Hierarchisierung unterstützte. Die *Liberal Democracts* unterstützten das Gesetzesvorhaben der *Conservatives* mit der Ausnahme des *Communications Data*-Klausel. Dieses sollte unter anderem GCHQ die Echtzeit-Überwachung von Kommunikationsverbindungen und der Zugriff auf Daten von Telekommunikationsanbietern erlauben. Das Gesetz wurde heftig von Seiten der *Liberal Democrats* und vom Verfassungsausschuss des Oberhauses kritisiert. Die Klausel wurde schließlich als eigenständiges Gesetz aus dem *Crime and Courts Act 2013* ausgesondert und separat verhandelt (The Guardian 2013). Die Ablehnung der Klausel durch die *Liberal Democrats* gründet auf Bedenken hinsichtlich der Bürgerrechte, welcher sie sich als liberale Partei verpflichtet sieht, nicht jedoch auf einer grundsätzlichen Ablehnung der Cyber-Policy ihres Koalitionspartners.

Wie die Untersuchung der drei Prozessstationen zeigt, konnte die zentralisierte Cyber-Policy der jeweiligen Regierung ohne große Widerstände umgesetzt werden. Sowohl die *Labour Party* als auch die *Conservatives* strebten nachweislich eine Zentralisierung im Sicherheitsbereich an und konnten ihre Agenden auch im Cybersicherheitsbereich umsetzen.

Neben den Premierministern und seiner Regierungspartei trat mit den *Liberal Democrats* ab 2010 ein einziger zusätzlicher situativer Vetospieler hinzu. Diese machten jedoch nicht von ihrer Vetomacht Gebrauch, um die Reformvorhaben zu blockieren. Der Grund ist, dass das Sicherheitsressort nicht zu den Kernkompetenzen der *Liberal Democrats* gehört, was an dem fehlenden Parteiprogramm gezeigt werden konnte. Bedenken der Partei an den Sicherheitsreformen betrafen lediglich den Datenschutz nicht jedoch die geplante Struktur. Dafür spricht, dass von Seiten der *Liberal Democrats* keinerlei kritische Stimmen gegen Zentralisierungsbestrebungen im Sicherheitsbereich im Vorfeld der Gesetzesvorhaben zu finden sind.

Die Hierarchisierung und Zentralisierung des Sicherheitsbereiches einschließlich der Cybersicherheitsbehörden in Großbritannien sind die Folgen einer machtpolitischen Pfadabhängigkeit. Das politische System Großbritanniens stattet die Regierung mit einer starken Machtstellung gegenüber anderen politischen und gesellschaftlichen Akteuren aus, welche es ihr erlaubt ihre Reformvorhaben nahezu ungehindert umzusetzen. Über ihre starke Agendasetzungs-Kompetenz und die Dominanz im Gesetzgebungsprozess konnte eine Hierarchisierung im Sicherheitsbereich umgesetzt werden und so die eigene Machtposition auf neue und schon bestehende Sicherheitsstrukturen übertragen werden. Es fand also eine Reproduktion der machtpolitischen Verhältnisse statt. Daher ist auch nicht nur eine Zentralisierung zu beobachten, sondern auch, dass die neu geschaffenen Strukturen im Cybersicherheitsbereich stark an das Machtzentrum im politischen System Großbritanniens gebunden sind. Die neu geschaffenen Behörden OSCIA und CSOC sind nicht dem Innenministerium, sondern dem *Cabinet Office* unterstellt worden. Das *Cabinet Office* ist primär dem Premierminister und dann erst seinen Ministern unterstellt. Dadurch fällt der Intermediär eines Ministers weg, was die Behörden der Cybersicherheit einer engeren Kontrolle durch den Premierminister unterstellen. Auch dies bestätigt eine machtpolitische Pfadabhängigkeit. Die Hierarchisierung und stärkere Bindung an den Premierminister gelingt in diesem neuen Problembereich eher, als in alten Sicherheitsbereichen, in welchen bereits Strukturen existieren und parteiinterne Akteure, sprich Minister, entmachtet werden müssten. Für die machtpolitische Pfadabhängigkeit spricht auch, dass die Hierarchisierung offensichtlich kein spezielles Programm einer Partei war, sondern von beiden großen Parteien angestrebt wurde. Dies stärkt die Annahme, dass jene Vetospieler, welche potentiell die Regierung stellen und das Sicherheitsministerium besetzen, ein grundsätzliches Interesse daran haben den Einfluss im Sicherheitsbereich auszudehnen. Die empirischen Befunde bestätigen, dass für die beiden großen Parteien eine zentralisierte Sicherheitspolitik die erste

Wahl war. Anders als in Deutschland gab es zudem keine Vetospieler, für die eine zentralisierte Cyber-Policy einen Machtverlust bedeutet hätte. Insgesamt lief die politische und öffentliche Diskussion in Hinblick auf die Sicherheitsreformen daher deutlich weniger kontroverser in Großbritannien als in Deutschland ab.

6.3 Auswertung

In beiden Fallstudien war die institutionalisierte Machtverteilung zwischen den Akteuren im politischen System die Ursache für die jeweilige Ausprägung der Cyber-Policy. Über eine machtpolitische und utilitaristische Pfadabhängigkeit reproduzierten sich die Machtstrukturen in den Sicherheitsbereich und den Bereich der Cybersicherheit und sorgten so für eine hierarchische oder netzwerkartige Ausprägung der Cyber-Policy.

In Deutschland ist vor allem das Bundesstaatsprinzip entscheidend, welches eine föderale Rechte- und Kompetenzverteilung zwischen Bund und Ländern vorschreibt und damit für eine Machtfragmentierung im politischen System sorgt. Über den institutionellen Vetospieler des Bundesrates haben die Länder die Möglichkeit ihre Kompetenzen gegenüber dem Bund zu verteidigen, da ihre Zustimmung benötigt wird, um diese zu ändern. Durch die Androhung oder Ausführung ihrer Blockademacht können die Länder jedoch nicht nur ihre Kompetenzen bewahren, sondern sorgen gleichzeitig dafür, dass der Bund beim Aufbau neuer Strukturen sie gemäß ihrer festgeschriebenen Kompetenzen beteiligen muss. In der Konsequenz führte dies zu einer Reproduktion der institutionalisierten Machtteilung zwischen Bund und Ländern in den Sicherheitsbereich, welche sich zuerst in der kooperativen Netzwerk-Struktur des GTAZ manifestierte. Eine utilitaristische Pfadabhängigkeit sorgte dann für eine Reproduktion dieser Struktur in andere Sicherheitsbereiche. Mit dem Aufbau des GTAZs und weiterer Kooperationszentren stiegen die finanziellen und politischen Kosten für eine nachträgliche Abschaffung der Behörden und der Umsetzung einer hierarchischen Struktur weiter an. Zu dem Zeitpunkt, an dem ein Handlungsdruck durch steigende Cyberbedrohungen entstanden war, hätten die Kosten für hierarchische Sicherheitsstrukturen die potentiellen Vorteile überstiegen. Dieser Lock-in-Effekt sorgte für eine Reproduktion der Netzwerk-Struktur in den Bereich der Cybersicherheit, welche sich vor allem in der Kooperations-Struktur des NCAZs wiederspiegelt.

In Großbritannien sorgt das Prinzip der „*parliamentary sovereignty*“ für eine starke Machtkonzentration im politischen System, in dessen Zentrum die jeweilige gewählte Regierung steht. Da es keine anderen Vetospieler gibt, kann die Regierung ungehindert ihre Vorstellungen beim Aufbau neuer Cybersicherheitsstrukturen umsetzen. Dabei werden

hierarchische Strukturen präferiert, da die Regierung naturgemäß an der Spitze dieser Hierarchie steht. Die institutionalisierte Machtkonzentration des politischen Systems reproduziert sich dadurch in den Cybersicherheitsbereich, dargestellt durch die Führungsrolle von OSCIA im *Cabinet Office* und dessen Weisungsbefugnisse an die zentralen Exekutivbehörden CSOC und *National Cyber Crime Unit*. Da die neue Regierung die Sicherheitsbehörden dem *Cabinet Office* unterstellte, konnte es diese enger an sich binden, als die Behörden anderer Sicherheitsbereiche.

Die institutionalisierte Machtverteilung in den politischen Systemen ist sehr stabil. Das Bundesstaatsprinzip ist im deutschen Grundgesetz für unabänderlich erklärt. Versuche die Aufgabenverteilung zwischen Bund und Ländern zu reformieren, haben sich ebenfalls als schwierig erwiesen. Föderalismuskommissionen, wie jene die in der Fallstudie beschrieben ist, setzen sich zur Hälfte aus Vertretern des Bundes und aus Vertretern der Länder zusammen, was letzteren die Möglichkeit gibt eine für sie ungünstige Machtumverteilung zu blockieren. Die Kommission selbst spiegelt die Machtverteilung im politischen System wieder. Analog dazu ist es unwahrscheinlich, dass die britische Regierung freiwillig ihre Machtstellung beschneidet. Eine institutionalisierte Machtverteilung ist aus den politischen Systemen selbst heraus also schwer zu ändern, da dies eine freiwillige Machtabgabe der Akteure verlangen würde.

Die machtpolitischen und utilitaristischen Pfadabhängigkeitsmechanismen haben sich als geeignet erwiesen um die Ausprägung der Cyber-Policy zu erklären. Die Ergebnisse der Fallstudien machen jedoch eine Spezifizierung der Hypothese in Bezug auf die unabhängige Variable nötig. Die Anzahl der Vetospieler im politischen System sowie ihre interne Kohärenz und externe Kongruenz sind nicht maßgeblich für die Ausprägung der Cyber-Policy. Entscheidend sind die Interessen der relevanten Vetospieler im Politikfeld Cybersicherheit sowie deren unterschiedliche Formen der Vetomacht. Diese Spezifizierung basiert auf drei Erkenntnissen. Erstens haben Akteure unterschiedlich starkes Interesse Einfluss im Cybersicherheitsbereich zu nehmen. So war es für die dominanten Regierungsparteien, welche das Innenministerium besetzen, deutlich wichtiger Einfluss auf den Bereich der Inneren Sicherheit zu nehmen als für die kleineren Regierungsparteien, welche andere Kernthemen haben und andere Ressorts kontrollieren. Auch haben Verfassungsgerichte zwar ein nachträgliches Vetorecht, aber als unpolitische Organe kein Interesse und keine Möglichkeit an einer Einflussnahme in Behörden, sondern folgen im Regelfall ihrer Aufgabe als Hüter der Verfassung. Zweitens weisen die relevanten Vetospieler unterschiedliche Formen der Vetomacht auf. Eine Differenzierung wurde bereits bei der

Operationalisierung vorgenommen und dies hat sich in den Fallstudien als sinnvoll erwiesen. Die dominierende Regierungspartei konnte mit ihrer Agendasetzungs-Kompetenz die Richtung der Cyber-Policy vorgeben. An ihren Gesetzesvorschlägen mussten sich gegebenenfalls die nachfolgenden Vetospieler abarbeiten. Der bedingte Vetospieler Bundesrat konnte die Regierung über seine Blockademacht zu Kompromissen zwingen, aber selber nur eingeschränkt gestaltend wirken. Nachträgliche Vetospieler wie die Verfassungsgerichte nahmen hingegen so gut wie keinen Einfluss auf die Policy-Gestaltung. Der Einfluss informeller Vetospieler, der Polizeigewerkschaften, hat sich als nicht entscheidend erwiesen. Gibt es neben der Regierungspartei keinen zweiten Vetospieler, wie in Großbritannien, dann ist die Regierung zu keinen Kompromissen gezwungen.

Die Hypothese lässt sich also in spezifizierter Form neu formulieren: *Je größer die Machtkonzentration in einem politischen System, desto stärker weist die Cyber-Policy die Merkmale des „Hierarchie"-Ansatzes auf. Je geringer die Machtkonzentration in einem politischen System (Machtfragmentierung), desto stärker weist die Cyber-Policy die Merkmale eines „Netzwerk"-Ansatzes auf.* Bei dieser neuen Hypothese dienen die Vetospieler als Indikatoren um die Machtkonzentration bzw. Machtfragmentierung eines politischen Systems festzustellen.

7. „Architecture is Politics"

In dieser Arbeit sollte untersucht werden, warum trotz vorhandener Bedingungen keine Konvergenz nationaler Cyber-Policies festgestellt werden kann und wie die unterschiedlichen Ausprägungen erklärt werden können. Die zu diesem Zwecke aufgestellte Nullhypothese einer Konvergenz nationaler Cyber-Policies muss aufgrund der Ergebnisse verworfen werden. Erstens konnte keine Konvergenz in Richtung hierarchischer Cyber-Strukturen festgestellt werden. In Tabelle 2 weist insgesamt nur ein Staat mehr die Cyber-Policy „Hierachie" als die Cyber-Policy „Netzwerk" auf. Dies reicht nicht aus um einen Trend in Richtung hierarchischer Strukturen auszumachen. Aus demselben Grund kann zweitens auch keine allgemeine Konvergenz ausgemacht werden, da die beiden Ausprägungen der Cyber-Policy über die Fallauswahl hinweg in etwa gleich verteilt sind. Drittens konnte nicht bestätigt werden, dass ein gemeinsamer Problemdruck durch Cyberbedrohungen und ähnliche Abhängigkeiten vom Cyberspace die bestimmenden Faktoren zur Erklärung der nationalen Cyber-Policies sind. Stattdessen konnte gezeigt werden, dass die Ausgestaltung der Cyber-Policy auf die Machtverteilung der Akteure im jeweiligen politischen System zurückgeführt

werden kann. Daher wird die Nullhypothese zugunsten der modifizierten Alternativhypothese verworfen.

Dass Polity und Politics starken Einfluss auf Policy nehmen, ist bekannt. Die Herausforderung dieser Arbeit war es die dahinter stehenden Kausalmechanismen anhand des Politikfeldes Cybersicherheit aufzuzeigen. Zudem konnte gezeigt werden, dass selbst bei starkem externem Problemdruck die nationalen Strukturen zur Erklärung von Policy-Outcomes nicht zu vernachlässigen sind. Gerade die nationalen Strukturen wirken als wichtigster Konverter zwischen dem externen globalen Druck und der internen nationalstaatlichen Lösung. Globalisierungseffekte und auch externe Schocks sind jedoch wichtig um zu erklären, warum es überhaupt zu einer Ausbildung von Strukturen in einem Politikfeld kommt. Externe Schocks wie Sputnik, 9/11 oder Stuxnet erzeugen einen Handlungsdruck bei den politischen Verantwortungsträgern. Dies legitimiert die Mobilisierung von zusätzlichen Ressourcen und Kapazitäten gegenüber den Bürgern eines Staates. Sodann beginnt die Auseinandersetzung der Akteure im politischen System über die Kontrolle dieser neuen Kapazitäten.

Da durch die Fallauswahl und das Aufzeigen der Kausalprozesse Alternativerklärungen für die Ausprägung der Cyber-Policy ausgeschlossen werden können, ist die interne Validität gegeben. Durch das gewählte Untersuchungsdesign wurde in dieser Arbeit der internen Validität der Vorzug gegenüber der externen Validität gegeben. Aufgrund dessen können die hier gewonnen Erkenntnisse nicht valide auf andere Fälle übertragen werden. Die in Tabelle 2 festgestellte Korrelation zwischen der Anzahl der Vetospieler, welche als Indikator für Machtfragmentierung dienen kann, und der Ausprägung der Cyber-Policy scheint die aufgestellte Hypothese zu unterstützen. Jedoch ist die Anzahl der Fälle für ein robustes Ergebnis zu klein. Dies ist vor allem dem Umstand geschuldet, dass Cybersicherheit ein relativ neues Problemfeld ist, auf welches noch nicht alle Staaten umfassend reagiert haben. Viele Länder sind noch im Prozess ihre Strategiepapiere zu entwickeln oder bei der Umsetzung ihrer Cyber-Policies und konnten deswegen nicht in die Fallauswahl aufgenommen werden. Die Entwicklungsrichtungen der Cyber-Policies dieser Länder scheinen die modifizierte Hypothese jedoch zu bestätigen. Schweden und Finnland entwickeln einen ähnlichen Netzwerk-Ansatz wie Norwegen und verteilen die Kontrolle und Verantwortung über die Cyber-Policy auf verschiedene Ministerien (Robinson et al. 2013: 15; Swedish Civil Contingencies Agency 2012: 29). Italien baut zurzeit ein Behörde zur Abstimmung der relevanten Akteure im Problemfeld auf an der verschiedene Ministerien, die Geheimdienste und das Militär beteiligt werden sollen (Ascoli/Scamoni 2013). Diese Trends

passen zu den Untersuchungen von Abromeit, welcher relativ fragmentierte Machtverhältnisse in den politischen Systemen Schwedens, Finnlands und Italiens ausmacht[4] (Abromeit 2006: 150). Für Großbritannien konnte zudem beobachtet werden, dass der dominante Vetospieler, die Regierung, die Kontrolle über die Sicherheitsstrukturen nicht über die Ministerien ausübt, sondern diese über das *Cabinet Office* enger an sich gebunden hat. Ein Blick auf Tabelle 1 bestätigt dies auch für andere Länder mit einer hierarchischen Cyber-Policy: Österreich übt die Kontrolle über das Bundeskanzleramt, Neuseeland und Japan über die jeweiligen Cabinet Offices, Australien über das Attorney-General's Department und Frankreich über das SGDN, welches dem Premierminister untersteht, aus. Alle diese Einrichtungen dienen der Koordination der anderen nationalen Ministerien und/oder sind strukturell enger mit der Regierung und dem Regierungsoberhaupt verbunden als andere Ministerien. Die einzige Ausnahme ist Kanada, wo die Verantwortung für Cybersicherheit dem Ministerium Public Safety Canada obliegt. Diese Beobachtungen stützen die Vermutung, dass es den dominanten Vetospielern im Cybersicherheitsbereich aufgrund geringer problemfeldinterner Pfadabhängigkeit und *vested interests* gelingt engere Kontrollstrukturen aufzubauen. Aber auch hier gilt, dass die Anzahl der Untersuchungsfälle für eine valide Generalisierbarkeit vergrößert werden muss. In den nächsten Jahren werden weitere Staaten Cybersicherheitsstrategiepapiere veröffentlichen und ihre Policy-Strukturen ausbauen. Mit der steigenden Anzahl von Untersuchungsfällen kann dann nach robusteren Korrelationen gesucht werden.

Die Erkenntnisse hinsichtlich des Nutzens einer differenzierteren, qualitativen Anwendung des Vetospielertheorems im Politikfeld Cybersicherheit, können auf die Untersuchung anderer Politikfelder übertragen werden. Erstens müssen die tatsächlichen Vetospieler je nach Politikfeld gesondert ermittelt werden. So besitzt z.B. der Bund in bestimmten Politikfeldern die ausschließliche Gesetzgebungskompetenz, wodurch der Bundesrat als Vetospieler wegfällt. Dies verändert die Dynamik im Gesetzgebungsverfahren und kann zu einer unterschiedlichen Reproduktion der Machtverteilung je nach Politikfeld führen. Zweitens geben uns die Interessen der Vetospieler Aufschluss darüber, ob und wofür diese ihre Vetomacht einsetzen. Wie die Fallstudien gezeigt haben, müssen Akteure mit Vetomacht diese nicht zwangsläufig zu jeder Zeit ausreizen. Ob ein Akteur tatsächlich seine Stellung einsetzt um eine rigorose Blockade umzusetzen, hängt auch von parteipolitischen

[4] Abromeit untersucht die Machtkonzentration und Machtfragmentierung von neun Ländern und berücksichtigt dazu nicht nur die institutionelle Vetospieler, sondern auch die Mechanismen des Parteienwettbewerbs und nationale Eigenheiten. Dadurch entsteht ein differenzierteres Bild der Machtverhältnisse, als dies mit einer reinen Fokussierung auf die institutionellen Vetospieler möglich ist.

Erwägungen ab und ob dies als legitim erachtet wird. Vetomacht ist daher nicht immer mit Vetorecht gleichzusetzen. Drittens konnte der Nutzen der von Abromeit und Stoiber vorgenommenen Gradualisierung von Vetospielern anhand der Untersuchungen aufgezeigt werden. Gerade für eine machtpolitische Erklärung ist eine Differenzierung der Vetorechte von entscheidender Bedeutung.

Regierungen haben erst seit kurzem mit dem Aufbau von Regulierungs- und Sicherheitsstrukturen im Politikfeld Cybersicherheit begonnen. Ein Merkmal dieser Strukturen ist das hohe Maß an Kooperation mit dem wirtschaftlichen und zivilgesellschaftlichen Sektor, z.B. über Public-Private-Partnerships. Wirtschaftliche und gesellschaftliche Kräfte sind immer noch maßgeblich für die Weiterentwicklung des Internets und des Cyberspace verantwortlich und es bleibt abzuwarten ob und inwiefern diese ihren Einfluss bei der zunehmenden Regulierung geltend machen. Aufgrund des Zusammenspieles von Staat, Wirtschaft und Gesellschaft bei der Gestaltung des Cyberspace bleibt Cybersicherheit ein spannendes Politikfeld für die Zukunft. Das für dieses Schlusskapitel gewählte Zitat von Mitch Kapor, Mitbegründer der *Electronic Frontier Foundation*, fasst die Ergebnisse dieser Arbeit zusammen: „Architecture is Politics“ (Kapor 2006). Die Regulierungs- und Sicherheitsstrukturen zur Herstellung von Cybersicherheit sind das Resultat politischer Prozesse. Bislang sind an der Gestaltung dieser Strukturen vor allem staatliche Akteure beteiligt. Es bleibt abzuwarten, ob sich Kapors Hoffnung einer dezentralen Architektur unter stärkerer Beteiligung zivilgesellschaftlicher Akteure in Zukunft erfüllt.

8. Literaturverzeichnis

Abbott, Kenneth W./Keohane, Robert O./Moravcsik, Andrew-Slaughter, Anne-Marie/Snidal, Duncan, 2000: The Concept of Legalization, in: International Organization 54 (3), S. 401-419.

Abromeit, Heidrun/Stoiber, Michael, 2006: Demokratien im Vergleich. Einführung in die vergleichende Analyse politischer Systeme. Wiesbaden: VS Verlag für Sozialwissenschaften.

Benz, Arthur/Dose, Nicolai, 2004:Von der Governance-Analyse zur Policytheorie, in: Benz, Arthur/Dose, Nicolai (Hrsg.), Governance. Regieren in komplexen Regelsystemen. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 251-274.

Betz, David J., 2011: Cyberspace and the State. Toward a Strategy for Cyber-Power. New York, NY: Routledge.

Carstens, Peter, 2004: Zusammenfassung von Sicherheitsbehörden gefordert, in: Frankfurter Allgemeine Zeitung 2004 (65), S. 2.

Carstens, Peter, 2004b: Schily will Sicherheitskompetenzen bei sich bündeln, in: Frankfurter Allgemeine Zeitung 2004 (140), S. 1.

Collier, Ruth B./Collier David, 1991: Shaping the Political Arena: Critical Junctures, the Labor Movement, and Regime Dynamics in Latin America. Princeton, NJ: Princeton University Press.

Cooper, Richard N., 1968: The Economics of Interdependence: Economic Policy in the Atlantic Community. New York: McGraw Hill.

Croissant, Aurel, 2010: Regierungssysteme und Demokratietypen, in: Lauth, Hans-Joachim (Hrsg.), Vergleichende Regierungslehre. Eine Einführung. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 117-139.

DiMaggio, Paul/Powell, Walter W., 1991: Introduction, in: DiMaggio, Paul/Powell, Walter W. (Hrsg.), The new institutionalism in organizational analysis. Chicago, IL: University of Chicago Press, S. 1-38.

Evans, Peter B./Rueschemeyer, Dietrich/Skocpol, Theda, 1985: Bringing the State Back In. Cambridge: Cambridge University Press.

Gibbons, Llewellyn J., 1997: No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting For Governance in Cyberspace, in: 6 Cornell J.L. & Pub. Pol'y 475.

Gourevitch, Peter A., 1978: The Second Image Reversed: The International Sources of Domestic Politics, in: International Organization 32 (4), S. 881-912.

Hall, Peter A./Taylor, Rosemary C. R., 1996: Political Science and the Three New Institutionalisms, in: Political Studies 44 (5), S. 936-957.

Hall, Peter/Soskice, David, 2001: Varieties of Capitalism. The Institutional Foundations of Comparative Advantage. Oxford: Oxford University Press.

Holzinger, Katharina/Jörgens, Helge/Knill, Christoph, 2007: Transfer, Diffusion und Konvergenz: Konzepte und Kausalmechanismen, in: Holzinger, Katharina/Jörgens, Helge/Knill, Christoph (Hrsg.), Transfer, Diffusion und Konvergenz von Politiken. Wiesbaden: Verl. für Sozialwissenschaften, S. 11-35.

Jahn, Detlef, 2006: Einführung in die vergleichende Politikwissenschaft. Wiesbaden: VS Verlag für Sozialwissenschaften.

Johnson, David R./Post, David, 1996: Law and Borders: The Rise of Law in Cyberspace, in: 48 Stan. L. Rev. 1367.

Käppner/Ramelsberger, 2004: Netzwerk der Informationen gegen Netzwerk des Terrors, in: Süddeutsche Zeitung 2004 (151), S. 10.

Krugman, Paul R., 1995: Growing World Trade. Causes and Consequences, in: Brookings Papers on Economic Activity 1, S. 327-362.

Kuehl, Daniel T., 2009: From Cyberspace to Cyberpower: Defining the Problem, in: Kramer, Franklin D. (Hrsg.), Cyberpower and National Security. Dulles, VA: Potomac Books, S. 24-42.

Lange, Hans-Jürgen, 2000: Innere Sicherheit, in: Schiller, Theo (Hrsg.), Perspektiven der politischen Soziologie im Wandel von Gesellschaft und Staatlichkeit. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 203-220.

Lappalainen, Pertti/Siisiäinen, Martti, 2009: Finnland. Freiwillige Vereinigungen in der Gesellschaft und Gewerkschaften im politischen System, in: Reutter, Werner/Rütters, Peter (Hrsg.), Verbände und Verbandssysteme in Westeuropa. Stuttgart: Opladen, S. 103-124.

Levi, Margaret, 1997: A Model, a Method, and a Map: Rational Choice in Comparative and Historical Analysis, in: Lichbach, Mark I./Zuckerman, Alan S. (Hrsg.), Comparative Politics: Rationality, Culture, and Structure. Cambridge: Cambridge University Press, S. 19-41.

Lewis, James A., 2009: Innovation and Cybersecurity Regulation. Center for Strategic and International Studies.

Lewis, James A., 2010: The Cyber War Has Not Begun. Center for Strategic and International Studies.

Libicki, Martin C., 2007: Conquest in Cyberspace. National Security and Information Warfare. New York, NY: Cambridge University Press.

Lijphart, Arend, 1999: Patterns of Democracy. Government Forms and Performance in Thirty-Six Countries. New Haven/London: Yale University Press.

List, Martin/Zangl, Bernhard, 2003: Verrechtlichung internationaler Politik, in: Hellmann, Gunther/Wolf, Klaus-Dieter/Zürn, Michael (Hrsg.), Die neuen Internationalen Beziehungen. Forschungsstand und Perspektiven in Deutschland. Baden-Baden: Nomos, S. 361-400.

Mahoney, James, 2000: Path Dependence in Historical Sociology, in: Theory and Society 29 (4), S. 507-548.

Netanel, Neil Weinstock, 2000: Cyberspace Self-Governance: A Skeptical View form Liberal Democratic Theory, in: California Law Review 88 (2), S. 395-498.

Norman, Lars, 2006: Deutsche Sicherheitsstrukturen im 21. Jahrhundert. Streitbare Demokratie und ihre institutionelle Umsetzung durch den Verfassungsschutz. München/Ravensburg: GRIN Verlag.

Ohmae, Kenichi, 1995: The End of the Nation-State: The Rise of Regional Economies. New York: Simon and Schuster Inc.

Pergande, Frank, 2004: Kieler Innenminister für Stärkung des BKA, in: Frankfurter Allgemeine Zeitung 2004 (253), S. 2.

Pierson, Paul, 2000: Increasing Returns, Path Dependence, and the Study of Politics, in: The American Political Science Review 94 (2), S. 251-267.

Ramelsberger, Annette, 2004: Schily will Kampf gegen den Terror an sich ziehen, in: Süddeutsche Zeitung 2004 (138), S. 1.

Rid, Thomas, 2011: Cyber War will not take place, in: Journal of Strategic Studies 35 (1), S. 5-32.

Rodrik, Dani, 1997: Has Globalization Gone too Far? Washington, D.C.: Institute for International Economics.

Rose, Richard, 1991: What is Lesson-Drawing?, in: Journal of Public Policy 11, S. 3-30.

Schattauer, Gören/Vernier, Robert, 2004: Unsere Chancen steigen, in: Focus 2004 (45), S. 44ff.

Schimmelfennig, Frank, 2006: Prozessanalyse, in: Behnke, Joachim (Hrsg.), Methoden der Politikwissenschaft. Neuere qualitative und quantitative Analyseverfahren. Baden-Baden: Nomos.

Schimmelfennig, Frank/Engert, Stefan/Knobel, Heiko, 2003: Costs, Commitment and Compliance: The Impact of EU Democratic Conditionality on Latvia, Slovakia and Turkey, in: Journal of Common Market Studies 41 (3), S. 495-518.

Shugart, Matthew S./Carey, John M., 1992: Presidents and Assemblies. Constitutional Design and Electoral Dynamics. Cambridge: Cambridge University Press.

Steffani, Winfried, 1979: Parlamentarische und präsidentielle Demokratie. Strukturelle Aspekte westlicher Demokratien. Opladen: Westdeutscher Verlag.

Stone, Diane, 2000: Non-Governmental Policy Transfer: The Strategies of Independent Policy Institutes, in: Governance 13 (1), S. 45-70.

Strange, Susan, 1996: The Retreat of the State. The Diffusion of Power in the World Economy. Cambridge: Cambridge University Press.

Thelen, Kathleen, 2003: How Institutions Evolve, Insights from Comparative Historical Analysis, in: Mahoney, James/Rueschemeyer, Dietrich (Hrsg.), Comparative Historical Analysis in the Social Sciences. Cambridge: Cambridge University Press, S. 208-240.

Tsebelis, George, 2002: Veto Players. How Political Institutions work. New York: Russell Sage Foundation.

Voigt, Rüdiger, 2006: Das Bundesverfassungsgericht in rechtspolitologischer Sicht, in: van Ooyen, Robert Christian/ Möllers, Martin H.W. (Hrsg.), Das Bundesverfassungsgericht im politischen System. Wiesbaden: VS Verlag für Sozialwissenschaften, S.65-85.

Wagschal, Uwe, 2005: Steuerpolitik und Steuerreformen im internationalen Vergleich. Eine Analyse der Ursachen und Blockaden. Münster: LIT Verlag.

Weidenfeld, Werner, 2004: Für ein System kooperativer Sicherheit, in: Weidenfeld, Werner (Hrsg.), Herausforderung Terrorismus. Die Zukunft der Sicherheit. Wiesbaden: VS Verlag für Sozialwissenschaften, S. 11-29.

Zürn, Michael, 2013: Globalization and Global Governance, in: Carlsnaes, Walter/Risse, Thomas/Simmons, Beth A. (Hrsg.), Handbook of International Relations. Los Angeles, CA: SAGE Publications, S. 401-425.

Webseiten und Internetquellen

ANSSI, 2010: Common Criteria Certification. Online unter http://www.ssi.gouv.fr/en/certification/common-criteria-certification/presentation-198.html [Letzter Zugriff: 05.06.13].

ANSSI, 2011: Information systems defence and security France's strategy. Online unter http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf [Stand: 02.11; letzter Zugriff: 08.07.13].

Ascoli, Adonnino/Scamoni, Cavasola, 2013: The Cybersecurity Decree now published in the Italian Official Gazette – new notification requirements for private operators? Online unter http://www.lexology.com/library/detail.aspx?g=f1ba2cb1-a1ab-49ee-895f-2984c8990360 [Stand: 04.13; letzter Zugriff: 15.07.13].

Attorney-General's Department, 2009: Cyber Security Strategy. Online unter http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf [Letzter Zugriff: 08.07.13].

B-ccentre, 2013: About. Online unter http://www.b-ccentre.be/?page_id=2 [Letzter Zugriff: 05.06.13].

BBC News UK, 2009: UK 'has cyber attack capability'. Online unter http://news.bbc.co.uk/2/hi/uk_politics/8118729.stm [Stand: 25.06.09; letzter Zugriff: 04.07.13].

BBC News UK, 2011: National Crime Agency details outlined by Theresa May. Online unter http://www.bbc.co.uk/news/uk-13678653 [Stand: 08.06.11; letzter Zugriff: 07.07.13].

Bcg.perspectives, 2012: The Internet Economy in the G-20. Online unter https://www.bcgperspectives.com/content/articles/media_entertainment_strategic_planning_4_2_trillion_opportunity_internet_economy_g20/ [Stand: 19.03.12; letzter Zugriff: 14.05.13].

Berliner Zeitung, 2004: Schilys BKA-Pläne gescheitert. Online unter http://www.berliner-zeitung.de/archiv/widerstand-der-gruenen-und-in-den-laendern-schilys-bka-plaene-gescheitert,10810590,10228382.html [Stand: 04.11.2004; letzter Zugriff: 26.06.13].

BMI, 2009: Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie). Online unter http://www.bmi.bund.de/cae/servlet/contentblob/544770/publicationFile/27031/kritis.pdf [Stand: 06.2009; letzter Zugriff: 25.06.13].

BMI, 2011: Cyber-Sicherheitsstrategie für Deutschland. Online unter http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf?__blob=publicationFile [Letzter Zugriff: 08.07.13].

BMI, 2011b: Bundesinnenminister Dr. Hans-Peter Friedrich eröffnet das Nationale Cyber-Abwehrzentrum. Online unter

http://www.bmi.bund.de/SharedDocs/Pressemitteilungen/DE/2011/mitMarginalspalte/06/cyber.html [Stand: 16.06.2011; letzter Zugriff: 26.06.13].

BMI, 2013: IT und Cybersicherheit. Online unter http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/it-cybersicherheit_node.html [Letzter Zugriff: 16.06.13].

BMI, 2013b: Zusammenarbeit der Sicherheitsbehörden. Online unter http://www.bmi.bund.de/DE/Themen/Sicherheit/Terrorismusbekaempfung/Sicherheitsbehoerden/sicherheitsbehoerden_node.html [Letzter Zugriff: 22.06.13].

BMI, 2013c: Cyber-Sicherheitsrat. Online unter http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/IT-Cybersicherheit/Cybersicherheitsstrategie/Cybersicherheitsrat/cybersicherheitsrat_node.html [Letzter Zugriff: 27.06.13].

BT-Drucks. 17/5694, 2011: Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Petra Pau, Jan Korte, Dr. Petra Sitte, weiterer Abgeordneter und der Fraktion DIE LINKE. Online unter http://dip21.bundestag.de/dip21/btd/17/056/1705694.pdf [Stand: 02.05.2011; letzter Zugriff: 26.06.13].

Bundesamt für Verfassungsschutz, 2009: Verfassungsschutzbericht 2009. Online unter http://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/verfassungsschutzberichte [Stand: 21.06.2010; letzter Zugriff: 26.06.13].

Bundeskanzleramt, 2013: Österreichische Strategie für Cyber Sicherheit. Online unter http://www.bka.gv.at/DocView.axd?CobId=50748 [Letzter Zugriff: 08.07.13].

Bundeskriminalamt, 2010: Cybercrime. Bundeslagebild 2010. Online unter http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true [Letzter Zugriff: 26.06.13].

Bundeskriminalamt, 2011: Cybercrime. Bundeslagebild 2011. Online unter http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html?__nnn=true [Letzter Zugriff: 16.06.13].

Bundesverfassungsgericht, 2013: Aufgabe des Bundesverfassungsgerichts. Online unter http://www.bundesverfassungsgericht.de/organisation/aufgaben.html [Letzter Zugriff: 22.06.13].

Cabinet Office, 2008: The National Security Strategy of the United Kingdom. Security in an interdependent world. Online unter http://www.official-documents.gov.uk/document/cm72/7291/7291.pdf [Letzter Zugriff: 02.07.13].

Cabinet Office, 2009: Cyber Security Strategy of the United Kingdom. Online unter http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf [Stand: 06.09; letzter Zugriff: 04.07.13].

Cabinet Office, 2011: The UK Cyber Security Strategy. Protecting and Promoting the UK in a Digital World. Online unter https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [Stand: 25.11.2011; letzter Zugriff: 03.07.13].

Cabinet Office, 2011b: The Cost of Cyber Crime. Online unter https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60942/THE-COST-OF-CYBER-CRIME-SUMMARY-FINAL.pdf [Stand: 17.02.2011; letzter Zugriff: 03.07.13].

ComputerWeekly.com, 2009: A history of cloud computing. Online unter http://www.computerweekly.com/feature/A-history-of-cloud-computing [Stand: 04.09; letzter Zugriff: 14.05.13].

Daily Mail, 2011: Security alert as Osborne admits hackers attempt to breach Treasury computers every day. Online unter http://www.dailymail.co.uk/sciencetech/article-1387589/George-Osborne-admits-hackers-attack-Treasury-computers-EVERY-DAY.html [Stand: 16.05.11; letzter Zugriff: 04.07.13].

Die Welt, 2004: Polizei läuft Sturm gegen Schilys Anti-Terror-Konzept. Online unter http://www.welt.de/print-welt/article358447/Polizei-laeuft-Sturm-gegen-Schilys-Anti-Terror-Konzept.html [Stand: 14.12.2004; letzter Zugriff: 01.07.13].

Downing, Emma, 2011: Cyber Security – A new national Programme. Online unter http://www.parliament.uk/briefing-papers/SN05832 [Stand: 23.06.2011; letzter Zugriff: 03.07.13].

Eidgenössisches Departement VBS, 2012: Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken. Online unter http://www.isb.admin.ch/themen/strategien/01583/index.html?lang=de [Stand: 14.05.13; letzter Zugriff: 08.07.13].

EMarketer, 2013: Ecommerce Sales Topped $1 Trillion for First Time in 2012. Online unter http://www.emarketer.com/Article/Ecommerce-Sales-Topped-1-Trillion-First-Time-2012/1009649 [Stand: 05.02.13; letzter Zugriff: 14.05.13].

ENISA, 2011: Belgium Country Report. Online unter http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Belgium.pdf [Stand: 05.11; letzter Zugriff: 08.07.13].

ENISA, 2011b: Norway Country Report. Online unter http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/Norway.pdf [Letzter Zugriff: 06.06.13].

ENISA, 2011c: United Kingdom Country Report. Online unter http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/UK.pdf [Stand: 05.11; letzter Zugriff: 04.07.13].

ENISA, 2012: National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace. Online unter http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper [Letzter Zugriff: 04.03.13].

FAZ, 2001: Kernpunkte des Sicherheitskompromisses. Online unter http://www.faz.net/aktuell/politik/das-sicherheitspaket-ii-kernpunkte-des-sicherheitskompromisses-139781.html [Stand: 28.10.2001; letzter Zugriff: 22.06.13].

FAZ, 2001b: Schily will auf Länder-Wünsche eingehen. Online unter http://www.faz.net/aktuell/politik/sicherheitspaket-ii-schily-will-auf-laender-wuensche-eingehen-139279.html [Stand: 09.12.2001; letzter Zugriff: 22.06.13].

Förster, Andreas, 2004: Getrennt ermitteln, gemeinsam auswerten. Online unter http://www.berliner-zeitung.de/archiv/polizei-und-geheimdienste-analysieren-in-einem-terrorismusabwehrzentrum-gemeinsam-die-lage-getrennt-ermitteln--gemeinsam-auswerten,10810590,10240350.html [Stand: 15.12.2004; letzter Zugriff: 25.06.13].

Gewerkschaft der Polizei, 2001: Sicherheitspakete brauchen auch gesellschaftliche Akzeptanz. Online unter http://www.gdp.de/gdp/gdp.nsf/id/8944947CA321B235C1256D0200436864 [Stand: 24.10.2001; letzter Zugriff: 22.06.13].

Gov.uk, 2013: Office of Cyber Security and Information Assurance. Online unter https://www.gov.uk/government/policy-teams/128 - aims-and-objectives [Letzter Zugriff: 04.07.13].

Gov.uk, 2013b: Keeping the UK safe in cyber space. Online unter https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace/supporting-pages/setting-up-a-national-cyber-crime-unit [Stand: 20.02.13; letzter Zugriff: 07.07.13].

Handelsblatt, 2004: Rot-grüner Streit um Bundeskriminalamt verschärft. Online unter http://www.handelsblatt.com/archiv/rot-gruener-streit-um-bundeskriminalamt-verschaerft/2453886.html [Stand: 15.12.2004; letzter Zugriff: 25.06.13].

Heise, 2011: Kritik am geplanten Cyber-Abwehrzentrum. Online unter http://www.heise.de/newsticker/meldung/Kritik-am-geplanten-Cyber-Abwehrzentrum-1196787.html [Stand: 24.02.2011; letzter Zugriff: 26.06.13].

HM Government, 2010: Securing Britain in a Age of Uncertainty. The Strategic Defence and Security Review. Online unter http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf [Stand: 09.10; letzter Zugriff: 04.07.13].

HM Government, 2010b: A Strong Britain in an Age of Uncertainty: The National Security Strategy. Online unter https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61936/national-security-strategy.pdf [Letzter Zugriff: 16.06.13].

Homeland Security, 2003: National Strategy to Secure Cyberspace. Online unter http://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf [Letzter Zugriff: 23.05.2013].

House of Commons, 2010: Strategic Defence and Security Review. Online unter http://www.publications.parliament.uk/pa/cm201011/cmhansrd/cm101019/debtext/101019-0001.htm#10101928000003 [Stand: 19.10.10; letzter Zugriff: 04.07.13].

House of Commons, 2013: Crime and Courts Act 2013. 2nd reading. Online unter http://www.publications.parliament.uk/pa/cm201213/cmhansrd/cm130114/debtext/130114-0002.htm#13011420000001 [Stand: 14.01.13; letzter Zugriff: 07.07.13].

Infosecurity, 2010: UK government Cyber Security Operations Centre going live soon. Online unter http://www.infosecurity-magazine.com/view/8020/uk-government-cyber-security-operations-centre-going-live-soon/ [Stand: 12.03.10; letzter Zugriff: 04.07.13].

Intelligence and Security Committee, 2011: Intelligence and Security Committee Annual Report 2010–2011. Online unter http://www.official-documents.gov.uk/document/cm84/8403/8403.pdf [Letzter Zugriff: 17.06.13].

International Telecommunications Union, 2011: Statistics. Percentage of individuals using the Internet. Online unter http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx [Letzter Zugriff: 16.06.13].

International Telecommunications Union, 2013: The World in 2013: ICT Facts and Figures. Online unter http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf [Stand: 02.12; letzter Zugriff: 14.05.13].

Internet Society, 2012: Brief History of the Internet. Online unter http://www.internetsociety.org/brief-history-internet [Stand: 15.10.12; letzter Zugriff: 14.05.13].

Jesse, Eckhard, 2003: Streitbare Demokratie. Online unter http://www.welt.de/print-welt/article496136/Streitbare-Demokratie.html [Stand: 19.03.2003; letzter Zugriff: 22.06.13].

Kapor, Mitch, 2006: Architecture is Politics (and Politics is Architecture). Online unter http://blog.kapor.com/index9cd7.html?p=29 [Stand: 23.04.06; letzter Zugriff: 20.07.13].

Liberal Democrats, 2012: Our policy on...Defence. Online unter http://www.libdems.org.uk/siteFiles/resources/docs/policy/International/Defence.pdf#search=%22cyber%22 [Stand: 04.12; letzter Zugriff: 07.07.13].

Meyer, Berthold, 2004: Die innere Gefährdung des demokratischen Friedens. Staatliche Terrorismusabwehr als Balanceakt zwischen Sicherheit und Freiheit. Online unter http://www.ag-friedensforschung.de/themen/Innere-Sicherheit/meyer.html [Stand: 16.05.2004; letzter Zugriff: 22.06.13].

Ministry for Communications and Information Technology, 2011: New Zealand's Cyber Security Strategy. Online unter http://www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf [Stand: 06.11; letzter Zugriff: 08.07.13].

Ministry of Security and Justice, 2011: The National Cyber Security Strategy (NCSS). Online unter https://www.ncsc.nl/english/organisation/about-the-ncsc/background.html [Stand: 06.11; letzter Zugriff: 08.07.13].

National Audit Office, 2013: The UK cyber security strategy: Landscape review. Online unter http://www.nao.org.uk/publications/1213/cyber_security.aspx [Letzter Zugriff: 17.06.13].

NATO, 2012: Financial and Economic Data Relating to NATO Defence. Online unter http://www.nato.int/cps/en/natolive/news_85966.htm?mode=pressrelease [Stand: 13.04.12; letzter Zugriff: 17.06.13].

Norwegian Ministries, 2012: Cyber Security Strategy for Norway. Online unter http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Cyber_Security_Strategy_Norway.pdf [Stand: 12.12; letzter Zugriff: 08.07.13].

Preuß, Torsten, 2012: Terrorismus und Innere Sicherheit. Eine Untersuchung der politischen Reaktionen in Deutschland auf die Anschläge des 11. September 2001. Online unter http://www.qucosa.de/fileadmin/data/qucosa/documents/8861/20120602_Torsten_Preu%C3%9F_Terrorismus_und_Innere_Sicherheit.pdf [letzter Zugriff: 20.06.13].

Public Safety Canada, 2010: Canada's Cyber Security Strategy. Online unter http://www.securitepublique.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-eng.pdf [Letzter Zugriff: 10.07.13].

Robinson, Neil/Gribbon, Luke/Horvarth, Veronika/Robertson, Kate, 2013: Cyber-security threat characterisation. A rapid comparative analysis. Online unter http://www.rand.org/pubs/research_reports/RR235.html [Letzter Zugriff: 15.07.13].

RP Online, 2004: Schily will BKA und Verfassungsschutz zentralisieren. Online unter http://www.rp-online.de/politik/deutschland/schily-will-bka-und-verfassungsschutz-zentralisieren-1.1618330 [Stand: 26.09.2004; letzter Zugriff: 22.06.13].

RP Online, 2004b: Neues Terror-Abwehrzentrum sorgt für Streit. Online unter http://www.rp-online.de/politik/deutschland/neues-terror-abwehrzentrum-sorgt-fuer-streit-1.1611784 [Stand: 14.12.2004; letzter Zugriff: 23.06.13].

RUSI, 2010: The Liberal Democrats View of Defence and Security Policy. Online unter http://www.rusi.org/analysis/commentary/ref:C4BCEC769462C7/ [Stand: 21.04.10; letzter Zugriff: 07.07.13].

Spiegel Online, 2001: Sicherheitspaket II. Eile mit Keile. Online unter http://www.spiegel.de/politik/deutschland/sicherheitspaket-ii-eile-mit-keile-a-172408.html [Stand: 12.12.01; letzter Zugriff: 20.06.13].

Spiegel Online, 2001b: Anti-Terror-Paket. Noch mehr Macht für Geheimdienste. Online unter http://www.spiegel.de/politik/deutschland/anti-terror-paket-noch-mehr-macht-fuer-geheimdienste-a-171918.html [Stand: 09.12.01; letzter Zugriff: 20.06.13].

Spiegel Online, 2002: Sicherheitsbehörden: Terror-Experte Werthebach fordert radikale Reformen. Online unter http://www.spiegel.de/politik/deutschland/sicherheitsbehoerden-terror-experte-werthebach-fordert-radikale-reformen-a-204192.html [Stand: 06.07.02; letzter Zugriff: 20.06.13].

Spiegel Online, 2004: Terrorismus. Schily kündigt Sicherheitspaket III an. Online unter http://www.spiegel.de/politik/deutschland/terrorismus-schily-kuendigt-sicherheitspaket-iii-an-a-319893.html [Stand: 25.09.04; letzter Zugriff: 20.06.13].

Spiegel Online, 2004b: Schily provoziert Krach mit Landesinnenministern. Online unter http://www.spiegel.de/spiegel/vorab/a-328772.html [Stand: 20.02.2004; letzter Zugriff: 26.06.13].

Spiegel Online, 2011: Nationales Cyber-Abwehrzentrum. Bundesregierung will "Cyber-Raum" besser schützen. Online unter http://www.spiegel.de/netzwelt/netzpolitik/nationales-cyber-abwehrzentrum-bundesregierung-will-cyber-raum-besser-schuetzen-a-747140.html [Stand: 22.02.2011; letzter Zugriff: 26.06.13].

Spiegel Online, 2013: Bundesverfassungsgericht. Gesetzgeber muss Anti-Terror-Datei nachbessern. Online unter http://www.spiegel.de/politik/deutschland/bundesverfassungsgericht-richter-billigen-anti-terror-datei-a-896175.html [Stand: 24.04.13; letzter Zugriff: 20.06.13].

Süddeutsche, 2013: USA am Pranger im Cyber-War. Online unter http://www.sueddeutsche.de/politik/neue-enthuellungen-durch-whistleblower-snowden-usa-am-pranger-im-cyber-war-1.1703971 [Stand: 24.06.13; letzter Zugriff: 10.07.13].

Swedish Civil Contingencies Agency, 2012: Sweden's Information Security National Action Plan 2012. Online unter https://www.msb.se/RibData/Filer/pdf/26419.pdf [Letzter Zugriff: 15.07.13].

SZ-Online, 2004: Schily provoziert die Grünen. Online unter http://www.sz-online.de/nachrichten/schily-provoziert-die-gruenen-622122.html [Stand: 15.12.2004; letzter Zugriff: 25.06.13].

The Guardian, 2006: Leader-in-waiting sets out his National Security Agenda. Online unter http://www.guardian.co.uk/politics/2006/feb/14/terrorism.immigrationpolicy [Stand: 14.02.2006; letzter Zugriff: 04.07.13].

The Guardian, 2007: Brown sets out sweeping but risky terror and security reforms. Online unter http://www.guardian.co.uk/politics/2007/jul/26/uk.humanrights1 [Stand: 26.07.2007; letzter Zugriff: 04.07.13].

The Guardian, 2013: Lib Dem opposition to communications data bill 'putting country at risk'. Online unter http://www.guardian.co.uk/uk/2013/may/23/woolwich-nick-clegg-communications-bill-risk [Stand: 23.05.13; letzter Zugriff: 07.07.13].

The Times, 2007: Spy chiefs fear Chinese cyber attack. Online unter http://www.timesonline.co.uk/tol/news/uk/article5993156.ece [Stand: 29.03.2009; letzter Zugriff: 01.07.13].

Tromparent, Patrice, 2012: French Cyberdefence Policy. Online unter http://www.ccdcoe.org/publications/2012proceedings/2_2_Tromparent_FrenchCyberdefensePolicy.pdf [Letzter Zugriff: 05.06.13].

White House, 2009: Cyberspace Policy Review. Online unter http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf [Letzter Zugriff: 10.07.13].

World Bank, 2013: High-income OECD members. Online unter http://data.worldbank.org/about/country-classifications/country-and-lending-groups#OECD_members [Letzter Zugriff: 10.07.13].

Yamada, Yasuhide/Yamagishi, Atsuhiro/Katsumi, Ben T., 2010: A Comparative Study of the Information Security Policies of Japan and the United States. Online unter http://infosecmgmt.pro/sites/default/files/us-japan_information_security_comparison_4_yamada.pdf [Stand: 29.09.10; letzter Zugriff: 08.07.13].

ZDNet.com, 2009: UK Cybersecurity Centre starting Operations in March. Online unter http://www.zdnet.com/uk-cybersecurity-centre-starting-operations-in-march-3039877965/ [Stand: 13.11.09; letzter Zugriff: 04.07.13].

Eigenständigkeitserklärung:

Hiermit erkläre ich, dass ich die Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel angefertigt habe.

Unterschrift München, der 22.07.2013