‚Culture, Cooperation, Capabilities'. Internationale Geheimdienstkooperation und europäische Polizeikooperation im Spannungsfeld von Legitimität und Effektivität

Inauguraldissertation

zur

Erlangung des Doktorgrades der

Wirtschafts- und Sozialwissenschaftlichen Fakultät

der

Universität zu Köln

2019

vorgelegt

von

Dipl.Sc.pol.Univ. Verena Diersch

aus

Starnberg

Referent:

Prof. Dr. Thomas Jäger (Universität zu Köln)

Korreferent:

Prof. Dr. Wolfgang Leidhold (Universität zu Köln)

Tag der Promotion:

02.07.2019

Abkürzungsverzeichnis

ADEP	Automation of Data Exchange Processes
AP	Analysis Point, Analysepunkt
AWF	Analysis Work Files, Dateien zu Analysezwecken
BND	Bundesnachrichtendienst
BfV	Bundesamt für Verfassungsschutz
EDU	European Drug Unit
EIS	Europol Information System
EMPACT	European Multidisciplinary Platform
ESC	European Security Center
ESOC	European Security Operations Center
EU	Europäische Union
EURODAC	European Dactyloscopy, Europäische Fingerabdruckdatenbank
FTF	Foreign Terrorist Fighter
BND	Bundesnachrichtendienst
CNO	Cyber Network Operations
COSI	Standing Committee on Internal Security, Ständiger Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit
COSPOL	Comprehensive Operational Strategic Planning for the Police
CSEC	Communication Security Establishment Canada
DNE	Digital Network Exploitation
DNI	Digital Network Intelligence

DSD	Defense Signals Directorate
GCHQ	Government Communications Headquarters
GCSB	Government Communications Security Bureau
HENUS	Head of National Units
HLG	High Level Expert Group
HUMINT	Human Intelligence
IRU	Internet Referral Unit
JSA	Joint SIGINT Activity
MASP	Multi-Annual Strategic Action Plan
NCEUR	NSA/CSS Representative Europe
NEU	National Units
NSA	National Security Agency
OAPS	Operative Action Plans, Operative Aktionspläne
ODNI	Office of the Director of National Intelligence
OLAF	Europäisches Amt für Betrugsbekämpfung
OSINT	Open Source Intelligence
PCTF	Police Chief Task Force
SIENA	Secure Information Exchange Network Application
SIGINT	Signals Intelligence
SIS	Schengener Informationssystem
SOCTA	Serious and Organised Threat Assessment
SUSLAG	Special US Liaison Activity Germany
TECHINT	Technical Intelligence

TFTP	Terrorist Finance Tracking Program
TREVI	Terrorism, Radicalism, Extremism and Violence Internationally
UMF	Universal Messaging Format
USA	Vereinigte Staaten von Amerika
VIS	Visa-Informationssystem

Tabellenverzeichnis

Tabelle 1: Identifizierung wesentlicher Ergebnisse bisheriger Studien aus den Intelligence Studies und nachweisbare Forschungsbedarfe 39
Tabelle 2: Identifizierung wesentlicher Ergebnisse bisheriger Studien aus der Polizeiforschung und nachweisbare Forschungsbedarfe 44
Tabelle 3: Unabhängige und abhängige Variable vorliegender Arbeit in Abgrenzung zu anderen Forschungsdesigns 48
Tabelle 4: Kontrastierung von Neoliberalem Institutionalismus und Neuem Institutionalismus 53
Tabelle 5: Beeinflussende Kontexte für Organisationen und mögliche beobachtbare Formen der Anpassung in ihren Handlungen 62
Tabelle 6: Theoretische Annahmen über die Art der Kooperationsbeziehungen in der institutionellen und technischen Dimension 69
Tabelle 7: Operationalisierung der Prämissen der gesellschaftlichen Bindung und technischen Anpassung 73
Tabelle 8: Theoretische Annahmen über die Art der Kooperation und deren erwartete empirische Auswirkungen 78

Abbildungsverzeichnis

Abbildung 1: Der erweiterte Intelligence-Zyklus als Idealtypus der Intelligence-Arbeit 18
Abbildung 2: Das European Criminal Intelligence Modell (ECIM) als Ablauf der Koordinierung von Europol 30
Abbildung 3: Erklärung der interorganisationalen Kooperation 81
Abbildung 4: Erklärung der interorganisationalen Kooperation der Five Eyes 84
Abbildung 5: Erklärung der interorganisationalen Kooperation von NSA und GCHQ 101
Abbildung 6: Erklärung der interorganisationalen Kooperation von NSA und BND 115
Abbildung 7: Erklärung der interorganisationalen Kooperation bei Europol 132

Inhaltsverzeichnis

Abkürzungsverzeichnis

Tabellenverzeichnis

Abbildungsverzeichnis

1. Einleitung **9**

2. Arbeitsweise und Funktion von Nachrichtendiensten und Europol **16**

2.1 Arbeit und Funktion von Nachrichtendiensten 16

2.2 Die Arbeit und Funktion von Europol 29

2.3 Systematisierung des Forschungsstandes 37

3. Der Neue Institutionalismus als theoretischer Rahmen für die Kooperationsforschung **50**

3.1 Die kulturelle Beeinflussung von und durch Institutionen 51

3.2 Das internationale interorganisationale Kooperationsmodell als Weiterentwicklung des Neuen Institutionalismus 63

3.3 Vorgehensweise in der Anwendung des interorganisationalen Kooperationsmodells 70

4. Analyse der Kooperation bei Nachrichtendiensten und Polizei **82**

4.1 Die Kooperation der Five Eyes 83

4.1.1 Die Wirksamkeit der Kooperation: Gleichwertige Nutzung von Zugängen und Weiterleitungsstrukturen 84

4.1.2 Alles wird geteilt: Die internalisierte und demonstrierte Kontinuität der SIGINT-Aufklärung 87

4.1.3 Die Wirkung technischer Unsicherheit: Interpretation und technischer Vorteil 92

4.1.4 Präsenz und Absenz: Wie viele Daten werden gespeichert, wie viele genutzt? 98

4.2 Die Kooperation zwischen NSA und GCHQ 100

4.2.1 Automatisierte Netzwerkaufklärung mit De-Anonymisierungsfunktion 102

4.2.2 Kooperation auf Augenhöhe 108

4.2.3 Anpassung an Kommunikationsentwicklungen: Innovation oder Fortführung der kooperativen Kernkompetenz Kryptoanalyse? 110

4.2.4 Präsenz und Absenz: Der Ehrgeiz der Analysten und die Lücken im Material 114

4.3 Die Kooperation zwischen NSA und BND 115

4.3.1 EIKONAL als Projekt der Joint SIGINT Activity 116

4.3.2 Inkongruenz oder Abhängigkeit? 119

4.3.3 Die NSA als technischer Ausstatter des BNDs? 126

4.3.4 Präsenz und Absenz: Das Schlaglicht der Abhängigkeit? 130

4.4 Europäische Polizeikooperation: Europol 131

4.4.1 Entstehungs- und Vertiefungsgeschichte Europols 133

4.4.2 Die Wirksamkeit Europols als Informationsspeicher der Mitgliedsländer 137

4.4.3 Kooperation ohne Kooperationsbereitschaft? 142

4.4.4 Anpassung aus Effektivitätsgründen 147

4.4.5 Die Intentionalität der Berichterstattung Europols 150

5. Fazit und Ausblick 152

5.1 Das Spannungsfeld zwischen Legitimität und Effektivität aus empirischer Sicht 152

5.2 Grenzen der Betrachtung 159

5.3 Der allgemeine Einfluss technischer Entwicklungen 165

Literatur- und Quellenverzeichnis 169

1. Einleitung

„Datenschutz ist schön, aber in Krisenzeiten hat die Sicherheit Vorrang."
Thomas de Maizière

Sicherheitsbehörden sehen sich gegenwärtig zwei zentralen Entwicklungstendenzen ausgesetzt: Sowohl die Komplexität sicherheitspolitischer Bedrohungen und ihrer Bewältigung als auch das Ausmaß ihrer Rezeption in der Öffentlichkeit demokratischer Gesellschaften haben sich erhöht. Die Reaktion auf Phänomene, wie den islamistischen Terrorismus und Cyber-Angriffe, zeigt sich zum einen in neuen Potentialen und Strukturen der Organisationen (Krieger 2018). Die Globalität der Angriffsvektoren und Bedrohungen hat aber auch dazu geführt, dass Geheimdienste und Polizeibehörden sich im In- und Ausland immer stärker miteinander vernetzen. Denn durch die Terroranschläge des 11. September 2001 wurde vor allem eines offenbar: eine neue Vulnerabilität moderner Gesellschaften. Gerade die transnationale Dimension der Planung der Täter stellte dabei eine Zäsur dar, auf die Geheimdienste und Polizei nicht vorbereitet waren (Brimmer 2006; Segell 2004). Da die Terroristen ihren Anschlag in Europa planten und in den USA durchführten, ihre Interaktion und Kommunikation jedoch nicht vollumfänglich bekannt war und die Erkenntnisse hierzu nicht ausreichend weitergeleitet wurden, sorgte er dafür, dass in der Folge genau diese Strukturen des Datenaustauschs und des internationalen Warnens vor sogenannten Gefährdern geschaffen wurden und bis heute weiterentwickelt werden (Agrell/Treverton 2015a). Grund dafür war vorrangig, dass die Möglichkeit der Terroristen, den Anschlag ungestört vorbereiten sowie durchführen zu können und dabei das Gefühl der relativen Sicherheit derjenigen Menschen zu zerstören, die vor Ort oder medial von dieser Katastrophe betroffen waren, auf ein Versagen der Nachrichtendienste zurückgeführt wurde (Kean et al. 2004). Es begann daraufhin eine Internationalisierung der öffentlichen Sicherheit, die mit der Verschränkung, Verstärkung und Vernetzung geheimdienstlicher und polizeilicher Strukturen und Methoden einherging. Diese Tendenz wurde zusätzlich dadurch gestützt, dass die Erwartungen der Gesellschaften an Sicherheitsbehörden in Reaktion auf die Anschläge – und die darauffolgenden – gestiegen sind (Omand 2010: 9). Bei allen Anforderungen an ihr Handeln für die gesellschaftliche Sicherheit sind Nachrichtendienste und Polizeibehörden jedoch auch der paradoxen Situation ausgesetzt,

dass sie nicht nur Sicherheit garantieren, sondern dabei auch nach Legitimitätsvorstellungen, beispielsweise der Institution der Verhältnismäßigkeit, also nach einer angemessenen Balance zwischen Sicherheit und Freiheit, handeln sollen (DiFabio 2008). Der grundlegende Konflikt des Rechtstaates zwischen den Garantien der Freiheit des Individuums und öffentlicher Sicherheit flammt daher regelmäßig in der öffentlichen Debatte auf und kann nie langfristig zufriedenstellend gelöst werden, da aktuelle Sicherheitsrisiken und global verfügbare Bekämpfungsmethoden eine ständig neue institutionelle Abwägung erfordern (Krause 2018: 1563). Erschwert wird die Definition verhältnismäßiger Ziele und Mittel zusätzlich dadurch, dass die Trennung zwischen äußerer und innerer Sicherheit, die noch im Zeitalter des Kalten Krieges für eine klare Abgrenzung zwischen staatlicher Kontrolle durch Polizei und Inlandsnachrichtendienste, die auch die eigenen Bürger negativ betreffen kann, und auslandsnachrichtendienstlichen sowie militärischen Maßnahmen gegen einen äußeren Feind, obsolet geworden ist, da sowohl Gefährder als auch ihre Kommunikation nicht mehr durch Landesgrenzen einschränkbar sind (Wiefelspütz 2007: 9 f.). Daher lassen sich die meisten Gefährdungslagen nun der inneren Sicherheit zuordnen und verlangen eine gemeinsame Aktion von Inlands- und Auslandsgeheimdiensten sowie von Polizeien und ihren internationalen Kooperationspartnern. Unter deren zeitgemäße Definition fallen daher Maßnahmen zur Prävention und Bekämpfung von Kriminalität, Wahrung der öffentlichen Sicherheit und Ordnung, Schutz der demokratischen Verfassung, Schutz vor politisch oder religiös motivierter Gewalt und Sicherheit im Cyberspace (Krause 2018: 1560 ff.). Neben den traditionellen militärischen Aufgaben müssen Staaten also nun vor allem die Verhinderung schwerer, komplexer Gewalt und vernetzter Kriminalitätsstrukturen, deren Vorbereitung, Verabredung und Durchführung sich immer stärker in die globale Kommunikationsstruktur des Internets auslagern, in den Fokus nehmen (Jäger 2015; Sterbling 2009; Münkler 2002). Somit sind die Funktionen geheimdienstlicher und polizeilicher Akteure vielfältiger geworden, was sich auch in ihrer technischen Ausstattung und in der sich verstärkenden Interaktion mit internationalen Kooperationspartnern ausdrückt. Zur Verteidigung der öffentlichen Sicherheit und Ordnung werden so zahlreiche, auch internationale, polizeiliche und geheimdienstliche Maßnahmen erforderlich, die die Gesellschaft zur Wahrung ihres Wohlstandes, ihres Lebens und ihrer körperlichen Unversehrtheit fordert, unterstützt oder die sie zumindest nicht in der breiten Masse ablehnt. Diese Beobachtung steht damit in Zusammenhang, dass beispielsweise die Zahlen zur gefühlten Bedrohung der Deutschen seit Jahren ansteigen. Gleichzeitig ist der Ruf nach einem konsequenten Datenschutz und dem Schutz bürgerlicher Freiheiten hörbar. Dabei werden grundlegende gesellschaftliche Widersprüche offenbar: Wie eine Umfrage aus dem

Jahr 2016 zeigt, schätzen 77 Prozent die Gefahr eines Terroranschlages hoch ein. Gleichzeitig sind sie trotz der gefühlten Bedrohung nicht bereit, ihren physischen Bewegungsradius einzuschränken. Nur 28 Prozent der Befragten wollten ihr Verhalten, beispielsweise belebte Orte aufzusuchen, aufgrund dieser Bedrohung ändern (Köcher 2016). Die Widersprüchlichkeit gesellschaftlichen Verhaltens zeigt sich auch bei der Internetnutzung. Ebenfalls 2016 bezeichneten 83 Prozent der Befragten Datenschutz als sehr wichtiges Thema (Splendid Research 2016). Gleichzeitig werden Internet-Applikationen und -Services immer datenintensiver und die Datendiebstähle durch ausländische geheimdienstliche und nicht-staatliche Akteure häufen sich. Somit sind gesellschaftliche Erwartungen in drei Bereichen nachweisbar: Die Deutschen etwa wollen sich sicher, aber auch nicht in ihrer Freiheit eingeschränkt fühlen und ihre Daten frei von sicherheitsbehördlicher oder privater Ausspähung wissen. Abgeleitet von dieser konfligierenden öffentlichen Meinung entsteht eine verantwortungsvolle Rolle für Sicherheitsorganisationen, (neue) Sicherheitsrisiken und -bedarfe zu managen, ohne grundlegende Institutionen der Gesellschaft erodieren zu lassen. Diese Verankerung polizeilichen und geheimdienstlichen Handelns in der Sicherheitswahrnehmung ihrer Gesellschaften, mit allen damit in Zusammenhang stehenden Problemen und Inkongruenzen der Erwartungen zeigt aber auch, dass Nachrichtendienste keine allmächtigen Schattenapparate darstellen und unter Europol vernetzte Polizeibehörden nicht angetreten sind, um Sicherheitspolitik zu supranationalisieren und das Leben der Bürger gläsern werden zu lassen. Vielmehr versuchen sie, unter Rückgriff auf deren Erwartungen ihren Auftrag nach Sicherheit zu erfüllen. Anderslautende Auffassungen sind eher Bestandteil der Pop- und Medienkultur als der Realität moderner Geheimdienste (Jobs 2014). Diese Mythisierung, vor allem von Nachrichtendiensten, hängt aber auch damit zusammen, dass Nachrichtendienste durch die ihnen gesellschaftlich zugebilligte Klandestinität größtenteils in einer Sphäre der Intransparenz agieren. Sachlich betrachtet ist jedoch festzuhalten, dass Geheimhaltung integraler Bestandteil des nachrichtendienstlichen Ablaufs ist. Sicherheitsbehörden sind somit als gewöhnliche Organisationen, versehen mit einem spezifischen Handlungsrahmen, zu verstehen, die ihre Handlungen anhand unterschiedlicher Zielgrößen, die sie miteinander übereinbringen müssen, ausrichten (Harnisch 2008; Morisse-Schilbach/Peine 2008). So finden Sicherheitsbehörden Antworten auf Bedrohungen beispielsweise immer häufiger in der Kooperation, in der sie stabile Informationsweiterleitungsstrukturen und effektive Methoden erarbeiten. Doch auch hier müssen sie rechtfertigen, warum welche Strukturen und Techniken in ihrer Anwendung nötig sind und welche Grenzen des gemeinsamen Handelns zugunsten der Verhältnismäßigkeit gezogen werden müssen. Dabei sind sie, wie auch andere Organisationen,

ständig in der Sorge, sich durch zu rigide Vorschriften eingeschränkt zu sehen und so nicht die Leistung erbringen zu können, welche die Gesellschaft vor allem von ihnen erwartet: Alltagssicherheit zu gewährleisten (Daase 2010; 2009). Erschwert wird das Handeln der Sicherheitsbehörden dadurch, dass die divergente Erwartung der Gesellschaft hinsichtlich ihrer Sicherheit, aber auch ihrer Handlungsfreiheit keine eindimensionalen, generalisierbaren kongruenten Institutionen schafft, an denen sich die nachrichtendienstlichen und polizeilichen Organisationen in ihrer Reaktion auf technisch komplexe Aufgaben verlässlich ausrichten könnten (Senge/Hellmann 2006: 19). Verkompliziert wird diese Abschätzung und Abwägung gesellschaftlicher Zielgrößen zusätzlich, wenn sehr unterschiedliche Kooperationspartner zusammentreffen und kompatible technische Handlungsmodelle zur Kooperation diskutieren müssen, um eine gewisse Effektivität überhaupt gewährleisten zu können. Dann können die Entwicklungs- und Übertragungsmöglichkeiten von Methoden dort an ihre Grenzen stoßen, wo eine sehr divergente Auffassung der Verhältnismäßigkeit des (gemeinsamen) geheimdienstlichen oder polizeilichen Handelns vorliegt. Für eine dauerhaft stabile und zusätzlich gleichberechtigte Kooperation ist jedoch die Übertragung unterschiedlicher Definitionen verhältnismäßiger Mittel auf eine generalisierbare Lösung notwendig (Scott 2014: 126 f.). Dabei bestehen jedoch beispielsweise gerade zwischen dem europäischen Kontinent und den USA sowie deren anglophonen Partnern große Unterschiede. Somit ist die gesellschaftliche Bindung der Organisationen auch immer kulturell beeinflusst und stellt die internationale Kooperation vor große Hürden, da die Organisationen aufgrund unterschiedlicher historischer Erfahrungsmodelle methodisch unterschiedlich arbeiten und ihr Handeln unterschiedliche Reichweiten erfährt (Katzenstein 2008: 159). Aber auch innerhalb Europas gibt es Staaten, die sich der europäischen Integration der Polizeikooperation stärker zuwenden als andere sowie eine Angleichung von Methoden und Strukturen befürworten und diese mitgestalten, während andere sich nur mit Verzögerung Gemeinschaftsstrukturen anschließen, sodass der Erfahrungsraum tatsächlich gemeinschaftlicher europäischer Polizeikooperation gering ist, der Handlungsraum nur sehr divergent ausgeschöpft wird und die Gemeinschaftsstrukturen sich erst in den letzten Jahren immer mehr prozesshaft verstärken. Im Bereich der Sicherheitspolitik, die immer zuerst gesellschaftliche Eigeninteressen vor Gemeinschaftsinteressen berücksichtigt, sind alle Sicherheitsorganisationen – egal wie sehr sie nach Kooperation streben – also daran gebunden, maßvoll und hinsichtlich gesellschaftlicher und technischer Erfordernisse interpretativ zu agieren, um sowohl Legitimität als auch Effektivität ihrer Kooperationsbestrebungen zu wahren. Dennoch können Organisationen, die kulturell ähnlich sind, enger zusammenarbeiten als andere. Denn Organisationen müssen in der

Kooperation drei Erfordernisse beachten: Zum einen die gesellschaftliche Legitimität eines (engen) Kooperationsaustausches, deren Interpretation und Berücksichtigung zwischen Organisationen mit vergleichbaren Reichweiten und Einschränkungen leichter fällt. Zum anderen, die Notwendigkeit auf der interorganisationalen Ebene zu einer funktionierenden Kooperation auch effektive technische Modelle vorzuhalten oder zu übernehmen, wozu Organisationen mit ähnlichen gesellschaftlichen Bedingungslagen kompatiblere Fähigkeiten vorhalten, da sie sich auf eine kongruente Reichweite der Mittel einigen können. Zum Dritten muss diese Lösung den strukturellen Bedingungen der Gefahrenlage und den technischen Möglichkeiten, Wissen über sie zu erlangen, angepasst sein, wofür Organisationen aus strategisch starken gesellschaftlichen Kontexten sich überschneidende und weitreichendere Handlungsmodelle bereitstellen können, weil sie sich frühzeitiger auf technische Veränderungen methodisch einstellen können als Organisationen mit einer geringeren (strategischen) Reichweite. Weil diese Faktoren für die europäische und transatlantische Sicherheitskooperation so relevant sind, erlauben sie der politikwissenschaftlichen Disziplin der Internationalen Beziehungen (IB) zusätzliches Erklärungspotential für die Kooperation auf Akteursebene.

Trotz einer umfangreichen und ausdifferenzierten wissenschaftlichen Auseinandersetzung mit der nachrichtendienstlichen Arbeit, der ‚Intelligence‘,[1] konzentrieren sich bislang lediglich wenige Arbeiten darauf, wie gesellschaftliche Bindung und technische Erfordernisse in unterschiedlichen Partnerkonstellationen zu einem Zustand strukturell stabiler, weitreichender und kompatibler Kooperationen, sowohl im transatlantischen als auch im europäischen Verhältnis, führen. Die Sozialwissenschaften greifen diese Relevanz zwar teilweise auf, gerade die Disziplin der IB kann aber zu den, durchaus auch widersprüchlichen, gesellschaftlichen und interorganisationalen Wirkungen auf Kooperationsarrangements im Sicherheitsbereich und deren Folgen noch keine weitreichenden Erklärungen anbieten. Da beide Anspruchsgrößen, die der Legitimität und die der Effektivität sicherheitspolitischer Lösungen und Kooperationsarrangements, mit der intensiven öffentlichen Rezeption sicherheitspolitischer Herausforderungen und struktureller Vernetzung jedoch steigen, ist eine Auseinandersetzung mit der Fragestellung, auf welche Weise Sicherheitsbehörden beide Determinanten einbinden (können), dringend notwendig. Hier setzt die vorliegende Arbeit an. Um Erkenntnisse über den gegenwärtigen Zustand der Institutionalisierung geheimdienstlicher Kooperationsarrangements

[1] Intelligence ist eine angloamerikanische, jedoch auch in der deutschen Forschung gebräuchliche Definition für die Aktivität, die Organisation und das Wissen der Geheimdienste. In der vorliegenden Arbeit werden die Begriffe Geheimdienste, Nachrichtendienste und Intelligence-Organisationen synonym verwendet.

zu erhalten, wurden die ‚Snowden-Dokumente' untersucht. Diese Informationen, die durch den Whistleblower Edward Snowden an internationale Medien weitergegeben wurden und die durch die US-amerikanische Bürgerrechtsorganisation American Civil Liberties Union ACLU in zugänglicher Form online archiviert wurden (Dörr/Diersch 2017), stellen einen wichtigen Einblick in die Kooperationsarrangements der amerikanischen National Security Agency (NSA) mit internationalen Partnern dar und wurden in der Politikwissenschaft vorrangig auf ihre Wirkung und weniger auf ihre inhaltliche Dimension hin untersucht (Walsh/Miller 2016; Johnson et al. 2014). Sie bieten eine einzigartige Möglichkeit für die Wissenschaft, zeitaktuelle Prozesse und Strukturen, die vorher geheim waren, zu analysieren und so einen Einblick in generelle Mechanismen der geheimdienstlichen Arbeit zu erlangen. Um die Generalisierbarkeit der Wirkungen auch über den Kontext der Geheimdienste hinaus zu ergründen, wurde ebenfalls die europäische Polizeikooperation bei Europol in das Untersuchungsdesign mit einbezogen. Notwendig und berechtigt ist diese methodische Integration durch die Tatsache, dass sowohl Nachrichtendienste als auch Polizeien Aktivitäten durchführen, die mittlerweile vor allem auf die innere Sicherheit zielen (Krause 2018). Daher liegt es nahe, dass die IB beide Akteure sowohl komparativ als auch vervollständigend stärker in die Betrachtung nehmen muss.

Zunächst wird das zweite Kapitel weitere Kenntnisse über die Funktionsweise von Geheimdiensten, und insbesondere zur Kooperation, sowie über Europol und dessen Arbeitsweise vermitteln, die zum weiteren Verständnis der Untersuchung zentral sind. Gleichzeitig wird vor allem die Perspektive auf die gesellschaftliche Anbindung der geheimdienstlichen Arbeit und Kooperation sowie der Polizeikooperation bei Europol gestärkt, um die Relevanz der gewählten Untersuchungsperspektive für Sozialwissenschaft und Gesellschaft zu verdeutlichen.

Das dritte Kapitel stellt, diese Bedeutung aufgreifend, die theoretische Fundierung des Analyserahmens vor. Der verwendete Theorieansatz des Neuen Institutionalismus in seiner soziologischen Ausprägung kann sowohl die gesellschaftliche Beeinflussung von Kooperationsarrangements, als auch die sozialen und technischen Wirkmechanismen zwischen den Kooperationspartnern erklären. Dadurch wird ein dreifacher Nutzen erzeugt: Erstens kann die Theorie um empirisch messbare Zusammenhänge der internationalen sicherheitsbehördlichen Kooperation erweitert werden, auf die sie noch nicht strukturiert angewendet wurde. Zweitens führt auch die Erklärung der Empirie mithilfe dieser Theorie zu einer neuen Herangehensweise für die Intelligence-Forschung und die Untersuchung der

Polizeikooperation bei Europol. Drittens kann durch die Herausarbeitung des internationalen interorganisationalen Kooperationsmodells eine Erweiterung des Ansatzes erreicht werden.

Das vierte Kapitel beschäftigt sich mit der Analyse empirischer Daten spezifischer Kooperationsbeziehungen. Es werden die Kooperationen der angloamerikanischen Geheimdienste ‚Five Eyes', der amerikanischen NSA mit dem britischen Government Communications Headquarters (GCHQ), die als Einzelfallstudie aus dem oben genannten Gruppenverband herausgearbeitet wird, der NSA mit dem deutschen Bundesnachrichtendienst (BND) und die europäische Polizeikooperation (Europol) im Zeitraum 2002 bis 2017 untersucht.

Kapitel fünf führt die Ergebnisse der empirischen Untersuchung zusammen und erörtert die Erkenntnisse hinsichtlich der in der Darstellung der Arbeitsweise der Sicherheitsbehörden identifizierten Forschungsdesiderate. Gleichzeitig würdigt es den verwendeten Analyseansatz kritisch und versucht in einem Ausblick einzuordnen, ob die Ambiguität gesellschaftlicher Erwartungen an Sicherheitsorganisationen einen Wandel angesichts steigender technischer Komplexität darstellt.

2. Arbeitsweise und Funktion von Nachrichtendiensten und Europol

> „Es kommt darauf an, durch überzeugende Nachweise der Rechtstreue und der Leistungsfähigkeit Vertrauen zu erzeugen, was wiederum motivierend und unterstützend auf die Arbeit der Dienste zurückwirkt."
>
> *Wolbert K. Smidt*

Vorliegende Arbeit entwickelt eine dezidierte Perspektive auf die geheimdienstliche und polizeiliche Kooperation und Polizeikooperation. Sie berücksichtigt und erklärt die gesellschaftliche, kulturell beeinflusste, Bindung unterschiedlicher Organisationen, aber auch deren Versuch, durch kooperative Konstruktion eine effektive interorganisationale Reaktion auf sicherheitspolitische Herausforderungen zu gestalten. Daher versucht vorliegendes Kapitel eine Darstellung der Wechselwirkungen zwischen der gesellschaftlich geprägten Struktur und Praxis der Organisationen sowie der interorganisationalen Kooperationsebene einzuführen. Demnach müssen Organisationen einem Auftrag nach aktuell, langfristig und zukünftig benötigtem Wissen, deren Sammlung und Auswertung sie steuern sollen, ausführen, um Gefährdungen für das Staats- und Gemeinwohl zu verringern und nutzen hierzu auf Geheimdienstebene verstärkt Kooperation (Abschnitt 2.1) Auch auf polizeilicher Ebene sind Organisationen auf stabile, zeitaktuelle, aber auch zukünftige Wirksamkeit von legitim gestalteten Datenzentren und Datenweiterleitungsstrukturen zur Ermittlung von Erkenntnissen angewiesen (Abschnitt 2.2). Diese Feststellungen, die zum vertieften Verständnis der in dieser Untersuchung zentralen Zusammenhänge notwendigerweise vorgestellt werden müssen, werden aus Sekundärliteratur herausgearbeitet, deren Schlussfolgerungen gewürdigt und auf Möglichkeiten zu weiterer Forschung hin überprüft werden. Durch die Extraktion der Kernergebnisse über die Auftragserfüllung der Organisationen in Reaktion auf gesellschaftliche Bedarfe kann die Ansicht gestärkt werden, dass eine Perspektive, die den Analysefokus auf die Interpretation gesellschaftlicher Bindung und die Anpassung an methodische Erfordernisse legt, immer wichtiger wird (Abschnitt 2.3).

2.1 Arbeit und Funktion von Nachrichtendiensten

Eine hilfreiche Strukturierung, um die Bedingungen der Arbeit von Nachrichtendiensten darzulegen, bietet der sogenannte Intelligence-Zyklus. Da der Begriff Intelligence sowohl die Erkenntnisse als auch die Art der Organisation und die Funktion von Nachrichtendiensten

bezeichnet, ist der Zyklus als eine Darstellung des organisationalen Ablaufes der Wissensproduktion der Nachrichtendienste zu sehen, für dessen Produktion in vorliegender Arbeit vor allem technisch extrahierbare und auswertbare Daten als maßgeblich betrachtet werden. Anhand der im Zyklus angelegten Abfolge lässt sich zunächst betrachten, welche Kriterien die Arbeit von Nachrichtendiensten bestimmen. Daraus werden auch die Notwendigkeiten für die Kooperation ersichtlich.

Der Intelligence-Zyklus (Abbildung 1) stellt sowohl eine Veranschaulichung und Vereinfachung der realen Abläufe innerhalb einer Intelligence-Community – also der Gemeinschaft aller nachrichtendienstlichen Akteure eines Landes – als auch einen Idealtypus dar, der regelmäßig benutzt wird, um das geheimdienstliche Handeln zu erklären (Warner 2013; Gill/Phythian 2012). Damit ist der Intelligence-Zyklus tatsächlich kein rein wissenschaftliches Konstrukt, sondern ist eine illustrative Organisationsschablone, die auch von den Organisationen selbst genutzt wird.[2] Der Zyklus sieht sich aber der Kritik der Vereinfachung ausgesetzt (Omand 2014; Lowenthal 2017; Marrin 2011). So erfolgen Informationssammlung und Analyse in der Praxis beispielsweise meist parallel. Außerdem klammert der Kreislauf die Bereiche Gegenspionage und verdeckte Operationen aus.[3] Wie Lowenthal (2017) hervorhebt, zeigt der idealtypische Prozess zudem einen ständigen Fortschritt an, während in der Realität Rückschritte gemacht werden, wenn etwa die erzielten Ergebnisse nicht ausreichend sind oder in der Steuerung auf andere Informationsquellen gesetzt werden soll. Trotz dieser Kritik stellt der Zyklus die tatsächlichen Abläufe teilweise realistisch dar, wie Treverton (2001) aus seiner praktischen Erfahrung berichtet. Die gebräuchliche Variante des Zyklus wird nachfolgend für die Perspektive vorliegender Arbeit erweitert und betont dann, welche gesellschaftliche

[2] Der Intelligence-Zyklus wird beispielsweise in den Online-Auftritten des BND, der US-amerikanischen Central Intelligence Agency (CIA) und beim dänischen technischen Nachrichtendienst, dem Danish Defence Intelligence Service (DDIS), genutzt. Die Abgrenzung zwischen der Verwendung in der Intelligence-Arbeit und Intelligence-Forschung gestaltet sich aber zusätzlich dadurch diffizil, dass viele Intelligence-Forscher, darunter Herman, Treverton, Omand und Lowenthal, frühere und teilweise noch tätige Nachrichtendienstler sind (Fry/Hochstein 2008).

[3] Verdeckte Operationen (auch ‚Covert actions' genannt) bezeichnen durch die Regierung autorisierte Aktivitäten zur geheimdienstlichen Beeinflussung in anderen Ländern, ohne dass offenbar wird, dass die Aktivitäten direkt dem Auftrag der politischen Entscheidungsträger zugeordnet werden können (Morisse-Schilbach/Peine 2008: 27f.). Gegenspionage meint die geheimdienstliche Ausspähung fremder Nachrichtendienste zum Ziel der Aufdeckung von Methoden und Strukturen, welche die Geheimdienste nicht offen miteinander teilen würden. Oft wird unter die Gegenspionage auch die Spionageabwehr subsumiert, welche die Informationssicherheit und damit auch den Schutz vor der Anwerbung oder Erpressung fremder Agenten beinhaltet. Die Bereiche verdeckte Operationen und Gegenspionage spielen jedoch für vorliegende Arbeit nur eine untergeordnete Rolle, da vor allem geteilte informationelle Strukturen im Zentrum der Untersuchung stehen. Hervorzuheben bleibt jedoch, dass NSA und GHCQ digitale Techniken für verdeckte Operationen entwickelt haben, die in Abschnitt 4.2.1 behandelt werden.

Aufgabe mit der jeweiligen Phase verbunden ist und welche Chancen, Einschränkungen und Risiken sich für die Geheimdienste, ihre Kooperation und für die Gesellschaft ergeben.

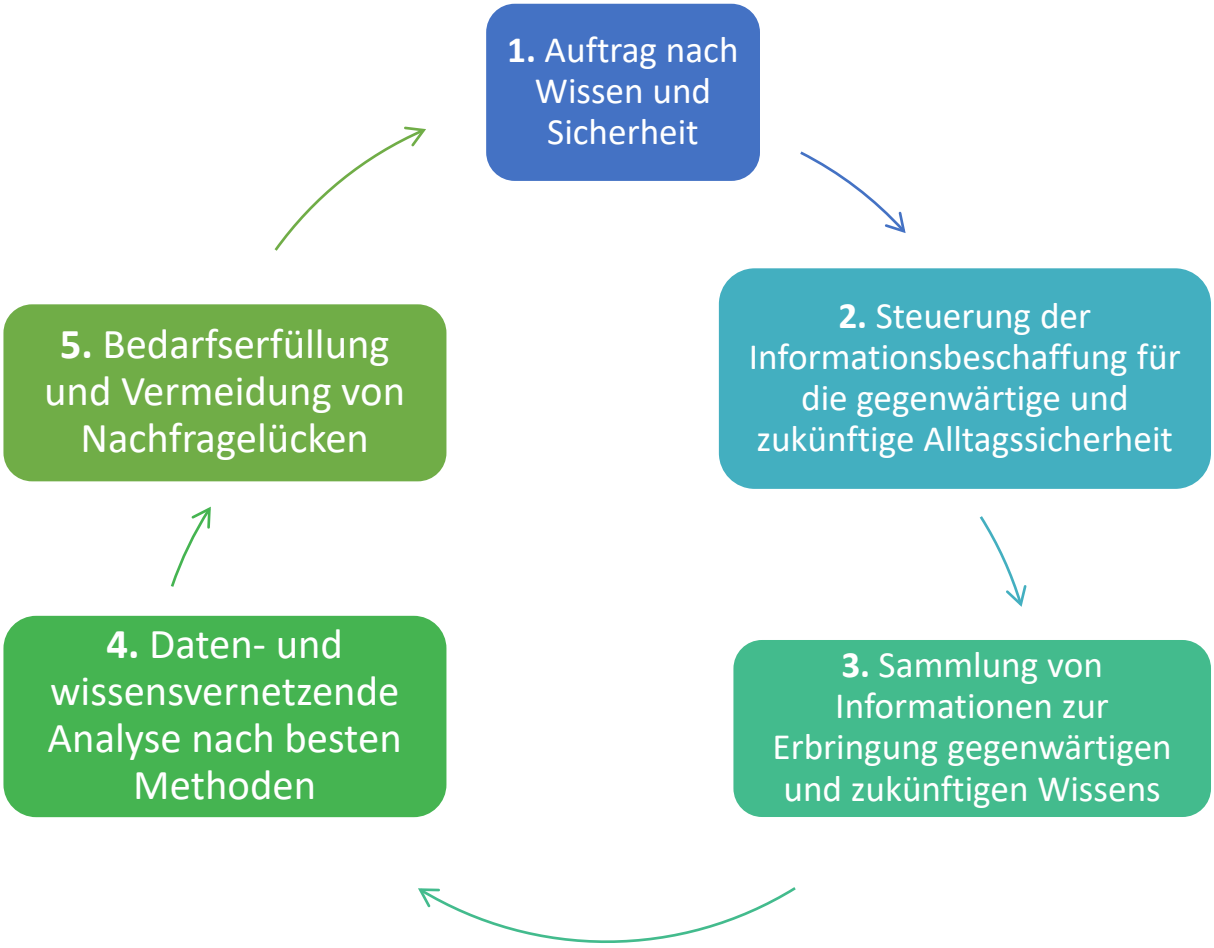


Abbildung 1: Der erweiterte Intelligence-Zyklus als Idealtypus der Intelligence-Arbeit.

Die Darstellung des erweiterten Intelligence-Zyklus ermöglicht es, die gesellschaftliche Bindung von Intelligence näher zu erläutern und dadurch den Fokus vorliegender Arbeit näher zu präzisieren. Dabei lässt sich diese Interdependenz von Nachrichtendiensten und Gesellschaft zu den strukturellen Bedingungen ihres technischen Arbeitsumfeldes kontrastieren. Denn Geheimdienste sollen vor allem Wissen, das von der Gesellschaft und – in deren Repräsentation – den politischen Entscheidungsträgern benötigt wird, erfassen und an sie weitergeben. Die Erfüllung dieser Aufgabe gelingt ihnen jedoch nur, wenn sie dieses in Form von Daten erschließen, verknüpfen und weiterleiten können. Bestehen Kooperationsstrukturen, können entweder Daten, Informationen oder aus ihnen gewonnenes Wissen auch internationalen Bedarfsträgern zur Verfügung gestellt werden. Dann erfüllen die Erkenntnisse, die Geheimdienste erbringen, nicht mehr einen rein außenpolitischen Zweck, sondern haben auch für die Untersuchung internationaler Politik und vor allem für die Prävention und Bekämpfung

von transnationalen Gefährdungen einen hohen Stellenwert (Behr/Ohlemacher 2009). Daher wird auch ein wesentlicher Teil der Erbringung dieses Wissens in Zeiten internationaler Bedrohungen in oder mithilfe von kooperativen Netzwerkstrukturen bewerkstelligt (Gill 2006). Die nachrichtendienstliche Kooperation ist gar in die Organisationsidentität westlicher Geheimdienste eingegangen. So weisen sowohl die NSA, der GCHQ, als auch der BND die Kooperation als wichtige Säule ihrer Arbeit aus.[4] Der gesellschaftliche Auftrag, Wissen zu erstellen und in der Kooperation auch an andere Partner weiterzugeben, drückt sich am deutlichsten in der ersten Zyklusphase, dem Auftrag nach Wissen und – daraus folgend – Sicherheit, aus. Intelligence-Organisationen sammeln spezielle Arten von Wissen. Das traditionelle Verständnis von Geheimdiensten, das aus Zeiten des Kalten Krieges stammt, geht vor allem von außenpolitisch nützlichen Informationen über die Lage in anderen Ländern aus. Diese Einschätzung ist insoweit weiterhin gültig, als die Aufklärung anderer Staaten tatsächlich immer noch einen Teil geheimdienstlichen Handelns ausmacht. Auch ist das Aufklärungsrepertoire der Nachrichtendienste vielschichtig: Sie beschaffen militärische, politische, ökonomische, soziale, ökologische und kulturelle Informationen, setzen diese in den jeweiligen Kontext und leiten hieraus analytisch Erkenntnisse ab (Lowenthal 2017: 7). Die US-amerikanische Intelligence Community überwacht beispielsweise militärische und politische Entwicklungen und Veränderungen in China, Russland, Iran, Nordkorea, dem Nahen Osten und Nordafrika (Diersch 2017: 76). Auch in Deutschland zählen die Aktivitäten anderer Staaten zum Aufklärungsprofil der Dienste. So stehen hier die Länder der ehemaligen Sowjetunion, die Türkei und der Balkan auf der Auftragsliste (Daun 2011b: 182). Auch Informationen über andere Nachrichtendienste und deren Aktivitäten zu beschaffen, gehört zum Auftragsprofil der Nachrichtendienste (Kent 1966[5]: 3 ff.).[6] Allerdings rückten im Untersuchungszeitraum 2002

[4] Diese Feststellung kann allein schon anhand des Aufrufs der Webseitenauftritte der Organisationen erfolgen. Während bnd.bund.de unter dem Reiter „Auftrag“ der Zusammenarbeit zu „Themen wie Internationaler Terrorismus, organisierte Kriminalität oder auch der nun abgeschlossene ISAF-Einsatz in Afghanistan (…) staatenübergreifende Bedeutung“ zuschreibt, spricht die NSA unter www.nsa.gov davon, dass „Knowing that the country, our friends and allies are relying on us, we are dedicated to fulfilling our commitment to serve and to excellence in the pursuit of our critical mission“. Der GCHQ hebt unter www.gchq.gov.uk in einer Beschreibung dessen „how we work“ von „international Partners“ und hebt hervor: „sharing knowledge and expertise with other countries helps us keep the UK safe“.

[5] Sherman Kents Definition der nachrichtendienstlichen Tätigkeit, Organisation und des geheimdienstlichen Wissens gilt bis heute als grundlegend für die wissenschaftliche Auseinandersetzung mit Nachrichtendiensten, die ‚Intelligence Studies‘ (Davis 2002).

[6] Geheimdienste zählen andere Nachrichtendienste zu potentiellen Sicherheitsrisiken hinzu. Bereits seit Entstehen moderner Geheimdienste zählt die Gegenspionage, also alle Tätigkeiten, die darauf abzielen, Kenntnisse über Struktur, Arbeitsweise und Absichten fremder Nachrichtendienste zu erhalten, zum Aufgabenbereich der Geheimdienste. Eine Erklärung hierfür ist, dass Spionageabwehr einen wesentlichen Aspekt geheimdienstlichen Handelns darstellt, weshalb es auch wichtig ist, zu ergründen, wie andere Nachrichtendienste arbeiten, und wo und wie sie potentiell die eigene Informationssammlung behindern, manipulieren oder auslesen können. Die Auffassung vorliegender Arbeit ist es, dass Gegenspionage und Spionageabwehr stabile, handlungsleitende

bis 2017 vor allem internationale Bedrohungen wie Terrorismus, digitale Angriffszenarien oder organisierte Kriminalität in den Fokus, weshalb die Komplexität der Arbeitserfüllung für Nachrichtendienste aufgrund der Notwendigkeit, sich sowohl auf traditionale Handlungsmuster als auch auf technische und kooperative Neuausrichtungen einzustellen, ständig steigt (Krause 2018; Fägersten 2010a; Aldrich 2009; Sterbling 2009; Daun 2005b; Johnson 2003; Huey 2002; Jäger 2002). Da terroristisch motivierte Gefährder sich vor allem der Internetkommunikation und -information bedienen, das Internet zur Rekrutierung und zur terroristischen Propaganda nutzen und auch andere Einzelpersonen und Gruppen die schwache staatliche Autorität im Internet zur Schädigung von Privatpersonen und Unternehmen in maliziöser Absicht nutzen, sind Sicherheitsorgane dazu angehalten, diese Kommunikationskanäle so zu überwachen, dass (potentiell) schädigendes Verhalten frühzeitig erkannt wird. Auch die Bezeichnung Gefährder selbst hat sich in Kongruenz zu den Anschlägen in New York erst entwickelt und löste den Begriff des ‚Schläfers' ab. Anders als diese als unauffällig begriffenen Personen, die jedoch durch äußere Aktivierung zu einem Anschlag motivierbar sind, zeichnet den Gefährder aus, dass er seine Absichten in geheimer Weise still vorbereitet, dann überraschend zuschlägt und daher immer ein schwelendes Aggressionspotential in sich trägt. Der Terminus des Gefährders ist daher nicht unumstritten, da er den nachrichtendienstlichen und polizeilichen Fokus von der Risikovermeidung hin zu einer ständigen Katastrophenannahme verschiebt (Kretschmann 2017; Schneckener 2013; Power 2004).[7] Gleichzeitig verleiht er dem Umstand Ausdruck, dass seit dem 11. September die Erwartung der Gesellschaft, in ihrem Alltagsleben durch den Staat geschützt zu werden, steigt:

> „Security has become itself a key objective of public policy: *national security today should be defined as a state of trust on the part of the citizen that the risks to everday life, whether from man-made threats or impersonal hazards, are being adequately managed to the extent that there is confidence that normal life can continue"* (Omand 2010: 9; Herv. i. O.).

Dadurch hat die Wichtigkeit der Sicherheitsbehörden, sowohl in der öffentlichen Wahrnehmung als auch in der Perzeption der Regierungen, zugenommen (Treverton 2014: 28). Diesen Akteuren obliegt dabei die Aufgabe, das Vertrauen in das soziale und politische System

Institutionen geheimdienstlichen Handelns sind und feste Größen des Handlungsrepertoires der Nachrichtendienste darstellen. Diese Handlungsformen stehen nicht in Widerspruch zu Kooperationsnormen, könnten diese jedoch belasten.

[7] Einige Autoren gehen gar davon aus, dass sich die moderne Sicherheitspolitik immer mehr in Richtung einer postmodernen Sicherheitsauffassung bewegt, in der Bedrohungsauffassungen und die Reaktion darauf sich immer stärker an der Wahrnehmung eines rasenden Wandels in allen Bedrohungsbereichen orientieren und daher immer weitreichendere Bekämpfungsstrukturen auslösen (Rathmell 2010; Dunn Cavelty/Mauer 2009).

und den Fortbestand des Wohlstands westlicher Kulturen zu sichern und zu bewahren und damit nicht nur faktisch Sicherheit zu schaffen, sondern auch die gefühlte Sicherheit zu gewährleisten:

> „People need to feel sufficiently safe domestically to justify investment, to be prepared to travel, indeed to leave the house in the morning to get on with ordinary life and to live it to the full even in the face of threats such as terrorism and hazards such as pandemics. Our adversaries – and the international markets – must know we have the confidence to defend ourselves against all possible vectors of attack" (Omand 2014: 20).

Erschwert wird die Arbeit von Nachrichtendiensten jedoch dadurch, dass diese nicht-staatlichen, gefährdenden Akteure sowie mögliche staatliche Aggressoren langfristig (strategisch), mittelfristig (taktisch) und kurzfristig (operativ) beobachtet werden müssen.[8] Daraus entsteht die Notwendigkeit, die Informationserbringung personell, technisch und – der Menge nach – umfassend zu organisieren. Diese Erfordernisse müssen in der Steuerung der Informationsbeschaffung für die gegenwärtige und zukünftige Alltagssicherheit (zweite Zyklusphase) berücksichtigt werden (Buuren 2014: 80; Kent 1966: 5). Diese Aufgabe bindet große technische und personelle Ressourcen. Da nicht nur die nationalen Fähigkeiten der Geheimdienste zur Überwachung globaler Gefährdungen nicht ausreichen, sondern auch stabile Strukturen zur Informationsübermittlung an andere Nachrichtendienste zur Abwehr transnationaler Bedrohungen vorhanden sein müssen, lässt sich eine Internationalisierung der nachrichtendienstlichen Tätigkeit beobachten. Buuren spricht gar von einer „globalization of intelligence" (Buuren 2014: 80) durch eine übergeordnete „idea of sharing" (Aldrich 2004: 739). Doch das Teilen relevanter Informationen alleine reicht nicht. Aufgrund von zeitlicher, räumlicher und informationaler[9] Komplexität ist zu jedem Zeitpunkt fraglich, welche Information *die entscheidende* Information sein wird, um Anschläge oder andere Sicherheitsgefahren zu verringern. Während Nachrichtendienste sich in der Phase des Auftrages noch die Verantwortung für die richtige Ausrichtung mit den politischen Entscheidungsträgern teilen, da sie gewissermaßen auf deren Weisung hin handeln, obliegt es in der Zyklusphase der Steuerung den Organisationen selbst, welche personellen und technischen Quellen, welche Kooperationsstrukturen und welche Methoden zur Erschließung von benötigten Erkenntnissen sie wählen. Sie versuchen dabei möglichst, Interpretationsfehler

[8] BKA-Präsident Holger Münch sprach in Interview vom 17. Januar 2018 von 730 Gefährdern, die unter Beobachtung der deutschen Sicherheitsbehörden stehen. Diese Zahl entspräche einer Verfünffachung in den letzten vier Jahren (Münch 2018).

[9] Personennetzwerke oder Einzelpersonen, die Cyber-Angriffe oder Terroranschläge planen, können sich in globalen Kommunikations- und Informationsnetzen – zum Beispiel durch Verschlüsselung ihrer Kommunikation – tarnen und haben somit immer einen Informationsvorsprung vor den Geheimdiensten und den Strafverfolgungsbehörden (Daun 2005b).

zu vermeiden, die gänzlich jedoch nie auszuschließen sind, was als Tragik der geheimdienstlichen Arbeit betrachtet werden kann:

„Since data about secrets are rarely complete and since humans are unable to predict the future (mysteries), intelligence analysts will fail from time to time in their efforts to anticipate and comprehend the meaning of world events“ (Johnson 2003: 10).

Da parallel die Erwartung der politischen Bedarfsträger nach einem „full reporting“ (Johnson 2003: 9) nach bestmöglichem Informationsstand besteht, kommt den Geheimdiensten eine starke Rolle im gesellschaftlichen System zu: es gilt, komplexe Phänomene bestmöglich vorherzusagen und zu beobachten, eine passende Methodik anzuwenden, die richtigen Schlüsse daraus zu ziehen und aus früheren Fehlern zu lernen. Als Zäsur in dieser Hinsicht, sowohl bezüglich der mangelhaften Informationsweiterleitung der Geheimdienste als auch – in der Folge retrospektiver Fehleranalysen – für das Auftragsprofil der Intelligence- und Polizeiarbeit identifizieren viele Wissenschaftler den 11. September 2001 (Johnson 2003; Daun 2009: 67 ff.). Seither haben sich Politik und Geheimdienste auf größtmöglichen Datenzugriff und teilautomatisierte Systeme zu deren Erfassung verständigt. Jedoch ist auch totale Sicherheit als Ziel aufgrund der daraus erwachsenden gesellschaftlichen Wirkungen – beispielsweise bezüglich der Einschränkung der Handlungsfreiheit des Einzelnen – nicht erwünscht (Omand 2014: 20; Treverton 2014: 32). Daher bewegt sich geheimdienstliches und polizeiliches Handeln immer im Spannungsfeld von Effektivität und Legitimität, vor allem deshalb, weil dieses schon auf gesellschaftlicher Ebene nicht zufriedenstellend aufzulösen ist und daher in einem permanenten Konfliktzustand schwelt. Dieser Zielkonflikt ist ständig in gesellschaftlicher Aushandlung befindlich und beschäftigt Sicherheitsbehörden daher in ihrem Alltag, da er maßgeblich bestimmt, auf welche Menge von Informationen und auf welche Weise sie auf Kommunikationsstrukturen zugreifen können und so die Steuerung der Informationsbeschaffung beeinflusst. Der Konflikt zeigt aber auch, dass sich Legitimität und Effektivität in der Arbeit der Sicherheitsbehörden nicht ausschließen. Beide Punkte gemeinsam bieten das Fundament, auf dem sie ihre Arbeit ausführen. Denn in der Phase der Steuerung müssen Intelligence-Organisationen festlegen, woher sie die Informationen beziehen, um den Auftrag, den ihnen die Regierung, oder andere, beispielsweise militärische, Bedarfsträger stellen, effektiv und angemessen erfüllen zu können (Wieck 2008: 58 f.). Dann entscheidet die Organisation, ob und welche Systeme der Kooperation sie nutzt. Dabei stellt sich die Frage, ob zu ihren Kooperationspartnern feste Strukturen bestehen. Welche formalen Beziehungen vorhanden sind, ließ sich aufgrund der Geheimhaltung vor der Veröffentlichung der Snowden-Dokumente schwer feststellen. Doch auch diese Enthüllungen bieten zwar einen vertieften

Einblick, decken jedoch noch lange nicht alle Kooperationen auf. Daun (2011b: 188) geht davon aus, dass beispielsweise Deutschland besonders enge und stabile Partnerschaften zu den USA, Frankreich, Großbritannien und Israel unterhält. Auch zu anderen Staaten des Nahen und mittleren Ostens bestehen nach ihrer Einschätzung Beziehungen, die jedoch nicht so stark institutionalisiert sind. In den bilateralen Beziehungen spielen indes nicht nur die Erfordernisse des Informationsbedarfs eine Rolle. Auch die kulturelle Verbundenheit der Kooperationspartner ermöglicht, erschwert oder erleichtert die Kooperation. Eine besonders stark formalisierte Geheimdienstkooperation besteht daher zwischen den britischen und den US-amerikanischen Geheimdiensten, von der jedoch auch die Dienste in Kanada, Australien und Neuseeland profitieren. An diese gewachsene Partnerschaft kulturell ähnlicher Organisationen reichen die Kooperationen zu Drittstaaten, zumindest aufgrund ihres geringeren Regelungsgrades, nicht heran (Westerfield 1996: 524; Herman 2003: 17). Gerade Großbritannien und die USA sind nachrichtendienstlich stark vernetzt: „Britain makes available to the USA a total of 15 bases thereby providing a crucial part of the global infrastructure that the USA relies on for power projection, signals intelligence intercept and analysis and missile defence“ (Jakobsen/Ringsmose 2015: 139). Allerdings betreiben auch die US-amerikanische NSA und der deutsche BND gemeinsame Infrastrukturen.[10] Westerfield (1996: 523) weist darauf hin, dass gerade die USA ein weitverzweigtes Netz der Kooperation, die er als Liaison[11] bezeichnet, vorhält. Er sieht diese Bemühungen vor allem darin begründet, den eigenen technischen Vorteil durch vielfältige Informationszuleitungen noch zu vergrößern. Auch Gill (2006) spricht von generellen Netzwerktendenzen in der Arbeit von Sicherheitsbehörden, da sowohl Bemühungen seitens der Politik als auch bei den Organisationen bestehen, viele und vielfältige Kooperationsbeziehungen aufzubauen und aufrechtzuerhalten, um dadurch eine größtmögliche Fülle an tatsächlicher oder möglicher Information zu erhalten. Vorliegende Arbeit sieht die Konstruktion unterschiedlicher Kooperationsarrangements vor allem als Reaktion auf die exogene Komplexität von Sicherheitsgefahren, aber auch die Interpretation gesellschaftlichen Erwartungen und daraus erwachsenden kooperativen Möglichkeiten. Dabei baut sie auf Einschätzungen auf, die internationale sicherheitspolitische Herausforderungen als Entwicklungskatalysator von Sicherheitskooperationen betrachten (Fägersten 2010a; 2010b; Daun 2005b; Bigo 2008; Gill 2006; Aldrich 2002). Allerdings geht die Argumentation insofern

[10] Zum Vergleich: in Deutschland befinden sich über 150 Punkte zur Kommunikationsüberwachung, einige davon könnten jedoch durch die NSA unilateral genutzt und dem BND unbekannt gewesen sein, wurden aber in der Auswertung der Snowden-Dokumente durch das Magazin „Der Spiegel“ aufgedeckt (Becker et al. 2014).

[11] Auch die NSA spricht von der Kooperation als Liaison. So wird beispielsweise die Kooperation mit Deutschland über das Zentrum Special US Liaison Activity Germany (SUSLAG) koordiniert (National Security Agency 2005b).

über diese Erkenntnisse hinaus, da sie den Grund für die Ausprägung unterschiedlicher Kooperationsarrangements auch und vor allem in der Interpretation des gesellschaftlichen Auftrags durch die Organisationen sowie der Berücksichtigung struktureller Unterschiede aufgrund kultureller Diversität sieht. Zwar entstehen aufgrund eines benötigten Informationspotentials „structures, that radiate trust, order and devotion to the public good" (Aldrich 2002: 50).[12] Um derartige Strukturen aufzubauen und zu pflegen, muss allerdings auch definiert werden, welche Mittel sie beinhalten sollen.

Denn zunächst müssen in der Kooperation unterschiedliche Informationsquellen ausgeschöpft und aus ihnen Daten gewonnen werden. Daher müssen zunächst unterschiedliche Kategorien der Information definiert werden, die für die Phase der Sammlung von Informationen zur Erbringung gegenwärtigen und zukünftigen Wissens (dritte Zyklusphase) je nach Auftrag und Möglichkeiten der Steuerung zentral sein können:

- TECHINT (technical intelligence): Überbegriff für technische Informationen aller Art.
- SIGINT (signals intelligence): Abfangen von Signalen, darunter Radio, Funk, Morse, Metadaten der Telefon-, Mobil- und Internetkommunikation.
- OSINT (open source intelligence): Informationen aus öffentlich zugänglichen Quellen.
- HUMINT (human intelligence): Überbegriff für Informationen aus menschlichen Quellen.

Die Intelligence-Fallstudien der vorliegenden Arbeit decken, in Reaktion auf die Darstellungen in den Snowden-Dokumenten, lediglich die technische Aufklärung ab. Somit werden SIGINT und die technischen Werte der OSINT in die Betrachtung genommen. Die Konzentration auf technische Daten alleine ist jedoch auch dadurch gerechtfertigt, dass sie mit dem größten Anteil in Analyseprodukte für die Regierung eingehen (Westerfield 1996: 524). Zusätzlich werden sie, gegenüber aus menschlichen Quellen gewonnenen Erkenntnissen, als besonders präzise und dadurch aussagekräftig bewertet (Johnson 2003: 6; Hulnick 2014: 48; Treverton 2014: 31).[13]

[12] Aldrich geht in seinen Ausführungen sogar davon aus, dass die Intelligence-Kooperation nach den Regeln des liberalen Institutionalismus und damit nach dem Streben nach einem höheren öffentlichen Gut – er hat dabei die größtmögliche Sicherheit für alle im Sinn – zu betrachten sei. Die Abgrenzung zwischen dem (neo)liberalen Institutionalismus und dem Analyseansatz vorliegender Arbeit wird in Abschnitt 3.1 erbracht.

[13] Technische Daten werden in der geheimdienstlichen Arbeit vor allem dadurch geschätzt, dass sie zukünftige Ereignisse abbilden können. Obwohl die meisten Produkte der Nachrichtendienste einen kurzen zeitlichen Fokus haben, sollen vor allem in den USA besonders tiefgehenden Analysen, ‚Estimates', angefertigt werden, die als Zukunftsprognosen verstanden werden können. Dafür müssen durch Auswertungsmethoden möglichst viele Informationen aus den vorhandenen Daten gewonnen werden. Hierfür muss jedoch gleichzeitig die Datenbasis besonders groß sein (Hulnick 2014: 48). Zusätzlich gibt das National Intelligence Council, eine Art Think Tank der US-amerikanischen Dienste, regelmäßig Papiere mit dem Titel „Global Trends" heraus. Aktuell wird der Zeitraum bis 2030 abgedeckt.

Ihre Auswertung verhinderte, vor und nach dem 11. September, beispielsweise bereits einige terroristische Anschläge (Richelson 2009: 162).[14] Die Sammlung und Auswertung technischer Daten lässt sich zudem besonders gut in internationalen Netzwerkstrukturen verfolgen, da sie auf relativ einfache Weise mit vielen Adressaten, die auf eine Informationssamlung auch dezentral zugreifen können, geteilt werden können. Außerdem können mit technischen Methoden sehr große Datensätze, teilweise automatisiert, miteinander verknüpft werden und so in der Auswertung persönliche Beziehungen zwischen Personen sichtbar gemacht werden. Diese ‚Metadatenanalyse' ist eine vergleichsweise neue Analysemethode. Sie ist unter anderem eine Konsequenz aus der Steigerung öffentlich verfügbarer Daten durch Soziale Netzwerke (Sims 2014: 71; Omand/Bartlett 2012). Diese Datentypen bieten außerdem ein großes Potential für Geheimdienste, da sie als Metadaten rechtlich nicht so stark geschützt sind wie Inhalte.[15] Die Auswertung von Metadaten – auch, aber nicht ausschließlich in Verknüpfung mit Inhaltsauswertungen – hat zudem den Vorteil, dass nicht nur die Handlungen von Personen ersichtlich werden, sondern sich sogar erst intendierte zukünftige Aktivitäten und Geschehnisse abbilden lassen (Dimitriu/Duyvesteyn 2014: 151f). Dies liegt daran, dass viele Geräte, die Menschen in ihrem Alltag nutzen, Daten erzeugen und eine steigende Anzahl von Vorgängen, die sie planen, sich beispielsweise durch Browserverläufe und Internetsuchen nachvollziehen lässt: „it is now a notable feature of our world that it is next to impossible to work, travel or communicate without leaving a digital exhaust behind us" (Omand 2014: 14). In der Wahrnehmung der Organisationen eignen Metadaten sich daher besonders für das Warnen von, durch nicht-staatliche Akteure hervorgebrachte, Bedrohungen, also das Hinweisen auf Geschehnisse, (lange) bevor diese überhaupt eintreten (Hulnick 2011: 240).[16] Dadurch entsteht die Maßgabe, möglichst jede zukünftige Bedrohung frühzeitig zu erkennen und zu vermeiden (Dunn Cavelty/Mauer 2009).[17] Aus dieser Fokussierung auf das Management möglicher

[14] Der bekannteste Fall in Deutschland ist die Aufdeckung der sogenannten Sauerlandgruppe im Jahr 2007, noch bevor diese einen Anschlag verüben konnte. Maßgeblich ermöglicht wurde dies durch eine gemeinsame Arbeitsgruppe der deutschen Sicherheitsbehörden und der CIA (Daun 2011a: 211 ff.).

[15] Für die Verknüpfung von Telefonmetadaten haben Wissenschaftler der Stanford Universität jedoch bereits herausgefunden, dass diese zunächst zufällig korrelierten Daten sehr viele Schlüsse zulassen, welche die Privatsphäre des Einzelnen erheblich verletzen, da Aufenthaltsort, Gesprächszeit, Gesprächsdauer und Häufigkeit der Anrufe auch etwaige sensible Themen sowie enge Beziehungen und Konflikte aufdecken können (Mayer et al. 2015).

[16] Dunn Cavelty und Mauer (2009) definieren ‚warning' „in a broad sense: as activities that provide vital support to national decisionmakers in their principal strategic missions – that is, understanding the complex geostrategic environment, facilitating a larger vision of objectives, assessing alternatives, determining strategy and protecting against consequential suprise" (Dunn Cavelty/Mauer 2009 unter Verweis auf Cooper 2005: 16). In der vorliegenden Arbeit wird Warnen vor allem als Vermeidung von Überraschungen verstanden und ist so auch auf den Polizeikontext anwendbar.

[17] Diese Tendenz lässt sich sowohl in der nachrichtendienstlichen, als auch in der Polizeiarbeit nachweisen (Abschnitt 2.2).

Sicherheitsgefahren generiert sich auch für technisch sehr fähige Organisationen die Notwendigkeit, sicherzustellen, dass auch andere Organisationen effektiv arbeiten (Omand 2014: 17; Sims 2014: 58; Hulnick 2014: 56; Dunn Cavelty/Mauer 2009; Bigo 2008, Johnson 2003: 5 ff). Nur wenn sichergestellt ist, dass dem Partner keine notwendige Information entgangen ist, die er weiterleiten hätte müssen, kann auch eine selbst sehr kompetente Organisation sicher sein, dass keine entscheidende Entwicklung übersehen wurde. Daher ist nicht nur ein Konsens kulturell divergierender Organisationen zu anzustrebenden Zielen und Mitteln notwendig. Letztere müssen zwischen ihnen auch kompatibel einsetzbar sein. Daher kann es notwendig werden, Kooperationspartnern geeignete Technik zu übertragen, sodass sie selbst Daten im benötigten Umfang sammeln und nach Priorität filtern können.[18]

So wird die Analyse zwar, auch bei international verschränkten Infrastrukturen und Datenarchitekturen, im nachrichtendienstlichen Bereich weitestgehend einzelstaatlich bewältigt. Allerdings können große Datenmengen auch eine Analyseunterstützung durch Kooperationspartner erforderlich machen, da eine vernetzte Analyse nach besten Methoden (vierte Zyklusphase) für das Management von gegenwärtigen und zukünftigen Bedrohungen benötigt wird (Dunn Cavelty/Mauer 2009). So ist die US-amerikanische Intelligence Community durch die Menge an Daten, die durch den Internetverkehr generiert wird, auf Analysehilfe aus Großbritannien angewiesen (Jakobsen/Ringsmose 2015: 139). Auch im Rahmen der amerikanisch-deutschen Geheimdienstkooperation werden gemeinsame Analyseprojekte durchgeführt.[19] Denn eine gemeinsame Analysetätigkeit ist nicht nur Ausdruck von gegenseitigem Vertrauen, sondern auch der Tatsache geschuldet, dass zur Umwandlung technischer Daten in verwendbare Erkenntnisse Know-How gefragt ist (Clark

[18] Eine derart enge Kooperation stellt für Nachrichtendienste jedoch immer auch ein Risiko dar (Westerfield 1996: 539 ff.). So steigt etwa durch die Offenbarung zentraler (menschlicher und technischer) Quellen beim Datenaustausch die Gefahr der Gegenspionage, also die Ausspähung auch anderer informationeller oder technischer Details, die der jeweilige Nachrichtendienst geheim halten möchte, die Gefahr, dass menschliche Quellen von der Partnerseite ebenfalls angeworben werden und die Gefahr, dass andere Nachrichtendienste an derselben, dem Partner offenbarten Infrastruktur einen verdeckten Zugang anlegen. So können Nachrichtendienste beispielsweise gemeinsam einen Netzknotenpunkt wichtiger Glasfaserkabel aufklären. Theoretisch wäre es möglich, dass der Kooperationspartner dann an einer anderen Zugangsmöglichkeit unilateral ansetzt und den Kommunikationsfluss in seine eigene Überwachungsinfrastruktur splittet, in der er dann auch die inländische Kommunikation des anderen Geheimdienstes, die in der Kooperationspartnerschaft ausgeschlossen wurde, ausspioniert. Überraschenderweise führen selbst diese verdeckten Maßnahmen – wie die Vertiefung der Kooperation zwischen Amerikanern und Deutschen in der Abwehr von Cyber-Angriffen auch nach dem Skandal um das abgehörte Mobiltelefon der Bundeskanzlerin Angela Merkel gezeigt hat – nicht zu einer Verschlechterung oder gar dem Abbruch der Kooperationsbeziehungen (Aldrich 2002: 52) und nicht dazu, dass Geheimdienste Kooperationsarrangements generell scheuen (Clough 2004: 602 ff.).

[19] Durch diese Tendenz der der zumindest teilweisen Zentralisierung der Analyse auch im internationalen Bereich lässt sich womöglich eine generelle Entwicklung attestieren, die sich auch im Polizeibereich beobachten lässt und daher auch in diesem Kontext untersucht wird (Abschnitt 2.2; Abschnitt 4.4).

2013: 12 ff.).[20] Außerdem können sich in der Analyse, in der Praxis, auch Notwendigkeiten einer erneuten Steuerung oder Sammlung ergeben, die dann erweiterte technische Methoden benötigt. Denn in der Analyse, so ist der Anspruch an die Geheimdienste, sollten alle verfügbaren Informationen und möglichen Schlussfolgerungen abgedeckt sein: „[Analysis] almost always strives to enhance understanding of what is known, what remains unknown, what is happening, where events seem to be headed, what is driving them, and what might alter the trajectory of developments“ (Fingar 2011: 3). In dieser Bewältigung von Komplexität sind Organisationen dann nicht nur ihren gesellschaftlichen Auftraggebern verpflichtet, sondern auch ihren nachrichtendienstlichen Partnern, deren informationelle, technische oder methodische Unterstützung sie erhalten haben.

So sind Organisationen in der Bedarfserfüllung und Vermeidung von Nachfragelücken (fünfte Zyklusphase) zwar vor allem ihren politischen Entscheidungsträgern verpflichtet, denen sie die Analyseergebnisse in unterschiedlichen Formaten weitergeben. Entweder werden Briefings abgehalten oder die Informationen ergehen in Papierform. In den USA wird der Präsident beispielsweise täglich über die wichtigsten Erkenntnisse der Geheimdienste im President's Daily Brief informiert (Lowenthal 2017: 86). In Deutschland findet jeden Dienstag in der ‚großen Lage‘ eine umfassende Besprechung der Präsidenten der drei Dienste BND, Bundesamt für Verfassungsschutz (BfV) und Militärischer Abschirmdienst (MAD) und dem Leiter des Bundeskriminalamts (BKA) mit den zuständigen Staatssekretären des Auswärtigen Amtes, des Bundesministeriums des Inneren, des Bundesministeriums für Justiz, des Leiters der Stabsabteilung II des Führungsstabes der Streitkräfte im Bundesministerium für Verteidigung sowie, themenabhängig, mit dem Generalbundesanwalt und dem Vertreter aus der Abteilung 6 des Kanzleramts, der für die Koordinierung der deutschen Nachrichtendienste zuständig ist, statt (Daun 2011b: 177f.).[21] In der Unterrichtung zeigt sich, ob die Analyse die Bedarfe der Entscheidungsträger trifft und ob die Informationen so ausgestaltet sind, dass sie von ihnen verarbeitet werden können. So müssen alle Akteure, Entwicklungen und Trends, die relevant sind und wichtig werden können, abgedeckt sein, selbst wenn sogar der Auftraggeber diese Vorgänge aufgrund kognitiver Rigidität[22] nicht aktiv angefragt hatte. Dadurch ergibt sich ein Paradox, welches Geheimdienste oft in die Nähe des Verdachts autonomen Handelns

[20] Zusätzlich erschwert wird die Analyse durch die jeweiligen kognitiven Beschränkungen, die bei der Übertragung von technischen Daten in Erkenntnisse auftreten können. Dieses Fehlerpotential kann jedoch in diesem Kapitel aufgrund der geringen Relevanz für die vorliegende Untersuchung, die sich vor allem mit Regeln für und zu technischen Weiterleitungsstrukturen beschäftigt, nicht erörtert werden.

[21] Die Bundeskanzlerin ist nicht anwesend, wird aber entsprechend vom Bundeskanzleramt unterrichtet.

[22] Informationen, die vorgefertigte Schemata bestätigen, werden vorzugsweise berücksichtigt und stärker gewichtet als solche, die nicht ins gewohnte Bild passen (Jervis 1976).

drängt: denn obwohl die Geheimdienste auf den Auftrag ihrer Gesellschaft innerhalb definierter Grenzen ausgerichtet sind, haben sie doch die Aufgabe, die breite Sicherheitslage selbständig im Auge zu behalten. Zusätzlich haben sie aber auch Berichts- und Weiterleitungsverpflichtungen hinsichtlich Informationen und Daten ihren Kooperationspartnern gegenüber, die sie mit Informationen, Technik oder Methodik unterstützt haben (Daun 2011a; Clough 2004; Westerfield 1996). Aus den Maßgaben der zu erfüllenden gesellschaftlichen, aber auch der interorganisationalen Bedarfe, folgen beinahe zwangsläufig die Tendenz zur Ausdehnung geheimdienstlicher Aktivität zur Verhinderung von Nachfragelücken bei steigender Bedrohungsintensität, die dauerhafte Notwendigkeit und Institutionalisierung der Intelligence-Kooperation und die technische Aufrüstung gemäß von Gefährdern benutzter Kommunikationstechnik, um wirklich alle wichtigen Informationen erhalten zu können.

Aus dem Forschungsstand wird also deutlich, dass die vernetzte und vertiefte Zusammenarbeit von Geheimdiensten aufgrund der Notwendigkeit entsteht, dem gesellschaftlichen Auftrag nach Wissen unter den strukturellen Bedingungen seiner Erstellung gerecht zu werden. Dabei lässt sich im Vergleich zu den Zeiten des Kalten Krieges ein Wandel geheimdienstlicher Kooperation attestieren, als gegenseitige Zersetzung und der Einsatz von Agenten im Vordergrund stand und gemeinsame Aufklärungstätigkeiten sich in weniger institutionalisierten Strukturen abspielten als dies heute der Fall ist. Zwar gab es auch damals enge Kooperationspartnerschaften. Jedoch waren die Organisationen stärker als Instrumente ihrer Regierungen zur Manipulation der internationalen Beziehungen zu definieren, als dass sie dafür eingesetzt wurden, die gesellschaftliche Sicherheit vor Einzeltätern sowie radikalisierten und hochspezialisierten Gruppen zu garantieren (Aldrich 2001). Jedoch sollte sich die Wissenschaft auch vor einer zu unkritischen und schlaglichtartigen Perspektive hüten. Denn auch die Auswertung von Dokumenten schützt nicht vor Fehlurteilen, da relevante Informationen trotzdem fehlen (können) und ein allumfassendes Bild im hoch intransparenten Bereich der Intelligence zwangsläufig unmöglich zu erreichen ist (Scott/Jackson 2004; Rappert 2010: 579 ff.). Zusätzlich weist auch die jüngere Geheimdienstgeschichte einige Beispiele auf, in denen Geheimdienste – unter Autorisierung der Regierung – auch gesellschaftlich akzeptiertes Terrain verlassen haben. Jüngstes Beispiel ist der Skandal um das Internierungs- und Verhörprogramm der CIA (Nešković 2015). Auch wenn diese Aktivitäten einzelstaatlich bleiben, steht auch die Kooperation im Verdacht, zu wenig transparent zu sein und sich damit möglicherweise von einzelstaatlichen Rechtsgrundsätzen abzulösen. Auch ergibt sich ein Bruch zwischen dem Wissen, das die Gesellschaft über die Tätigkeit von Nachrichtendiensten

erlangen kann und der Tatsache, dass die Regierung diese Organisationen bewusst auf eine Weise nutzt, die die Reichweite und Art ihres Einsatzes möglichst gänzlich vor der Betrachtung durch die Bürger schützt. Denn was Geheimdienstkooperationen prägt, ist, dass die Information über eine Beteiligung der Kooperationspartner an gemeinsamen Projekten weder anderen Geheimdiensten noch der jeweiligen Regierung – aus Angst, dass der Kooperationspartner bei Veröffentlichung eigene negative gesellschaftliche Konsequenzen, die auch die Kooperation beeinträchtigen könnten, zu befürchten hätte – weitergegeben wird (Daun 2005b: 137). Ohne diese gegenseitige Versicherung der Klandestinität würde Geheimdienstkooperation, auch dem Sinne des Wortes nach, also nicht funktionieren. Boer et al. (2008) sprechen sich hinsichtlich der Autonomie und Zentralität der Geheimdienstkooperation für die Sicherheitspolitik moderner Gesellschaft daher für die Notwendigkeit aus, die Legitimität einzelner Austauschforen gezielt zu evaluieren. So beauftragt die Gesellschaft die Geheimdienste mit der Wahrung ihrer Sicherheit, kann ihnen letztlich jedoch nie ganz trauen, da ihr das Wissen über die konkrete Praxis fehlt. Anders als die nachrichtendienstliche Kooperation, so heißt es weiter, verfüge jedoch die Polizeikooperation, besonders bei Europol, zumindest über indirekte Legitimität, da die Strukturen und Methoden des Europäischen Polizeiamtes durch Beschlüsse der Regierungen der EU-Mitgliedsländer gedeckt seien (Boer et al. 2008: 102 f.).

2.2 Die Arbeit und Funktion von Europol

Wie die Nachrichtendienste verfolgt auch Europol, das Polizeiamt der Europäischen Union (EU), das Ziel der Steigerung von Erkenntnissen durch Datenweiterleitung und (zentralisierte) Datenauswertung (Ratcliffe 2008: 5). Denn die komplexen Anforderungen, die seit dem 11. September 2001 auch an Europol herangetragen werden, benötigen sowohl eine Datenweiterleitungsfunktion, eine Integration verschiedener (neuer) Sicherheitsthemen in die polizeiliche Kooperation, eine diesbezügliche Bündelung der analytischen Expertise und eine Auswertung zur Verfügung gestellter Daten, aus denen weitere Muster und Erkenntnisse gewonnen werden und die dann an die Mitgliedsländer weitergeleitet werden können. Auch die Arbeit bei Europol kann in einem Zyklus-Modell verdeutlicht werden. Der EU Policy Cycle, der auch als ‚European Criminal Intelligence Modell' (ECIM) bezeichnet wird, ist ein dem Intelligence-Zyklus ähnlicher, aber in seinen Schritten beinahe diametral entgegengesetzter Prozess (Europol 2011c; Europol 2009: 49). Denn am Anfang des ECIM steht beispielsweise bereits eine Analyse. Hierfür bezieht die Organisation zunächst Informationen aus dem eigenen Informationsspeicher, der durch übermittelte Erkenntnisse der Strafermittlungsbehörden der Mitgliedsländer gefüllt wird und leitet aus diesen vergleich- und strukturierbaren Informationen

eine Basis für die Notwendigkeit und die Ausgestaltung weiteren Handelns ab. Dieser Ablauf entspringt der Logik polizeilichen Handelns. Denn ein Lagebild stellt erst den Ausgangspunkt späterer Aktivitäten dar und ist nicht, wie bei der Intelligence, der Abschluss einer Informationserhebung. Polizeiarbeit ist dementsprechend „Lagebereinigung“ (Christe-Zeyse 2007: 186) und wird an den Maßgaben der zu bewältigenden Krisen angelegt (Europol 2016a; Europol 2015: 4). So startet das ECIM, wie Abbildung 2 zeigt, mit einer Priorisierung der Kriminalitätsbereiche, für die koordiniertes Handeln der Mitgliedsstaaten, und damit die informationelle Unterstützung durch Europol benötigt wird.

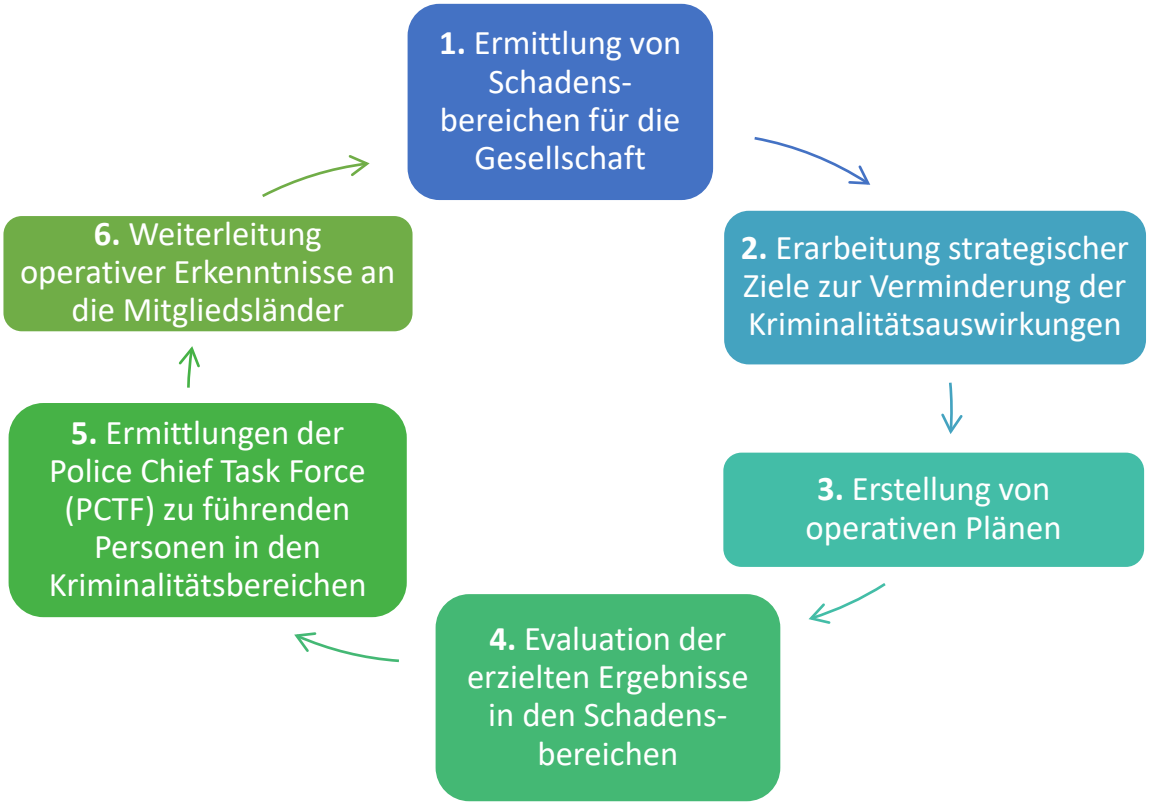


Abbildung 2: Das European Criminal Intelligence Modell (ECIM) als Ablauf der Koordinierung von Europol.

Der technische und personelle Ablauf des ECIM wird derzeit vor allem durch die Logik des ‚Intelligence led policing‘, auch als erkenntnisgestützte Strafverfolgung bezeichnet, getragen (Europol 2009: 49). Ratcliffe (2008: 6) versteht darunter eine Arbeitsweise sowie eine Management-Philosophie, in der die Datenanalyse und die Verknüpfung und Auswertung möglichst vieler Informationen rund um ein Verbrechen zu einer Reduktion und Prävention von Delikten führen sollen. Die erkenntnisgestützte Polizeiarbeit soll dabei sowohl lokale Alltagskriminalität als auch international organisierte Kriminalität verhindern sowie lokal und national Staatsschutz garantieren. Der Staatsschutz umfasst dabei alle Belange, die den materiellen und immateriellen Bestand des Staates gefährden. Dazu zählen Brand- und

Bombenanschläge, sowie die Verfolgung bestimmter Menschengruppen durch politisch motivierte Angreifer. Strafverfolgung, Gefahrenabwehr und Prävention werden so unter diesem Konzept zur zentralen Trias der Polizeiarbeit (Kühne 2012). Somit weist die erkenntnisgeleitete Polizeiarbeit Parallelen zur – eher kurzfristig angelegten – problemorientierten Polizeiarbeit der Strafverfolgung auf, soll aber nicht nur Erkenntnisse über begangene Straftaten, sondern alle relevanten Informationen, die mit deren Vorbereitung und Durchführung zusammenhängen und so auch Hinweise auf größere Strukturen und Informationsnetzwerke offenbaren, liefern (Maguire 2000: 315 ff.). Auch sollen – ähnlich wie in der nachrichtendienstlichen Erkenntnisarbeit – die Informationsbasis für Handlungen vergrößert sowie Ressourcen effektiver genutzt werden. Daher pflegt Europol mit den Analysedateien zu Arbeitszwecken (AWFs) eigene Datenbanken zu unterschiedlichen Kriminalitätsbereichen und koordiniert die Erkenntnisse und Bedarfe aus und von den Mitgliedsländern. Typisch für Europol ist zudem, dass die Kooperation themenspezifisch offen ist und sich nicht nur auf die gemeinsame Verfolgung bereits bekannter Deliktarten konzentriert, sondern auch versucht, die zukünftigen Entwicklungen in den Kriminalitätsbereichen zu prognostizieren (Boer/Bruggemann 2007: 82). Das ECIM unterstützt dieses Vorhaben seit 1998 in der Form eines Informationskreislaufes und zeigt die zentrale Rolle, die Europol bei der Erhebung und Auswertung von Informationen und die Unterstützung durch (weitere) Informationen einnimmt. Spätestens mit der britischen Ratspräsidentschaft in der zweiten Hälfte des Jahres 2005 wurde das ECIM mit dem Konzept der erkenntnisgestützten Polizeiarbeit direkt verknüpft. Seidem gilt das ECIM als zentrales ‚Geschäftsmodell' Europols (Europol 2009: 49).

Damit umfassende Erkenntnisse über die zu bewältigenden Kriminalitätsformen gewonnen werden können, steht am Anfang des sechsschrittigen Modells in der ersten Zyklusphase das Serious and Organised Threat Assessment (SOCTA) zur Festlegung von besonders schwerwiegenden Kriminalitätsbereichen, das derzeit auf vier Jahre angelegt ist. Hier erstellt Europol aus den Daten, welche durch die Mitgliedsstaaten an Europol übertragen wurden, eine strukturierte Auswertung. Durch sie sollen Zusammenhänge, die nicht aus den Einzeldaten, wohl aber aus ihrer Korrelation sichtbar werden, hervorgehoben werden. Bei der Erstellung des SOCTA arbeitet Europol auch mit Frontex, der europäischen Agentur für die Grenz- und Küstenwache, zusammen, nimmt also auch deren Informationen für die Ausrichtung gemeinsamer Aktionen oder benötigter Austauschstrukturen auf (Möllers 2012: 35). Es dient als Grundlage für die Priorisierung weiterer gebündelter Maßnahmen durch den Rat der Justiz- und Innenminister der EU, also die Festlegung der Kriminalitätsgebiete, auf welche die Ressourcen besonders konzentriert werden sollen. Das SOCTA erhob 2017 Cyberkriminalität,

Drogenproduktion, -schmuggel und -verbreitung, Menschenhandel und Schleuserkriminalität, organisierte Eigentumskriminalität, Finanzkriminalität, Dokumentenfälschung und illegalen Online-Handel zu Kernprioritäten, deren Bekämpfung durch Europol koordiniert werden und dadurch besser gelingen soll (Europol 2017a). Das wichtigste Kriterium für die Priorisierung im Rahmen des SOCTA besteht darin, welchen Schaden einzelne Kriminalitätsarten anrichten. Europol benutzt unterschiedliche Indikatoren, die messbar machen sollen, wie stark die EU-Gesellschaften von unterschiedlichen Formen der Kriminalität betroffen sind (Paoli 2014: 1 ff.). Aus der Priorisierung, die auf Grundlage des SOCTA entstanden ist, werden in der zweiten Zyklusphase mehrjährige Aktionspläne, die Multi-Annual Strategic Action Plans (MASP), erstellt. Sie halten konkrete strategische Ziele fest, die in jedem der priorisierten Bereiche erreicht werden sollen. Die Aktionspläne werden durch den Ständigen Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit (COSI) evaluiert (Piquet 2017: 1201). Sie werden seit 2010 unter der klaren Prämisse der notwendigen Kooperation zwischen den Ermittlungsbehörden der Mitgliedsstaaten, Europol, anderen EU-Agenturen und -Institutionen sowie relevanten Drittpartnern entwickelt. Aus den MASPs entstehen im Projekt European Multidisciplinary Platform, unter Einbezug der genannten Akteure, in der dritten Zyklusphase operative Aktionspläne (OAPs), welche zur Erfüllung der Ziele dienlich sein sollen. EMPACT hält generelle Zielsetzungen für einzelne Themenfelder fest, die jedoch alle mit der Disruption von Gruppen der organisierten Kriminalität und der Reduzierung ihrer Möglichkeiten zusammenhängen (Europol 2018a: 1). Beobachter weisen jedoch darauf hin, dass zwischen den Mitgliedsländern mitnichten immer eine Einstimmigkeit über die zu priorisierenden Bereiche sowie die zu entwickelnden Handlungen erreicht werden kann (Piquet 2017: 1201). Die Auswirkungen der OAPs in den priorisierten Bereichen werden anschließend evaluiert (vierte Zyklusphase).[23] Die Erreichung der Zielsetzung wird durch Europol selbst und nicht nur die Ermittlungsbehörden der Staaten durchgeführt. Sind die Ergebnisse nicht zufriedenstellend, werden neue OAPs erarbeitet. Europol hält also ein formales, koordiniertes System der informationellen Sicherheitskooperation bereit. Ein zentraler Punkt der (Weiter)entwicklung ist außerdem in der zunehmenden operativen Ausrichtung Europols zu sehen.[24] Das Polizeiamt kann kriminaltechnische und technische Unterstützung bieten, in der operativen Analyse helfen, finanzielle Unterstützung für operative Sitzungen oder

[23] Europol verwendet zwei Zyklus-Schablonen. Im EU Policy Cycle endet der Kreislauf mit der vierten Zyklusphase, der Evaluation der OAPs. Im ECIM wird der Zyklus auf sechs Schritte ausgedehnt. Vorliegende Arbeit verwendet das Sechserschema.

[24] Zentraler Kritikpunkt ist auch, dass Europolbedienstete bei der operativen Unterstützung – bei der sie jedoch keine Vollzugsgewalt haben und daher nur Bürotätigkeiten übernehmen können – Immunität genießen (Pechstein/Koenig 2000: 188)

Ermittlungen, beispielsweise in der Euro-Fälschung, anbieten, die Ausrichtung von Fallsitzungen informieren, operative Aktivitäten koordinieren und in einem mobilen Büro die Vor-Ort-Analyse unterstützen. Der Auftrag ergeht stets durch die Mitgliedsländer (Europol 2011d). Europol ist daher nicht nur als zentraler Daten-, Fähigkeits- und Erkenntnis-Speicher zu bewerten (Europol 2009: 49). Zwar stellt Europol Wissen zur Verfügung, das die Agentur aus Strukturen der durch die Mitgliedsländer gelieferten Daten gewinnen kann und kann darüber hinaus etwa durch "specialist threat assessments in priority areas" (ebd.), oder einer „list of top criminals and target profiles" (ebd.) zusätzlichen Mehrwert bieten. Zentrale Bedeutung für die Arbeit von Europol haben jedoch nicht nur Datenstrukturen und Technologien zum Herausarbeiten strukturierter Informationen aus den Daten der Mitgliedsländer. Auch die Erfahrung einzelner leitender Beamten und Spezialisten bildet einen wichtigen Faktor. Daher bindet Europol die ‚Police Chief Task Force (PCTF)', die sich aus Ermittlern der Mitgliedsländer, denen Europol-Personal zur Seite gestellt wird, zusammensetzt, in das ECIM ein (fünfte Zyklusphase).[25] Die PTCF hat keine formalen Verbindungen zu Europol. Allerdings stehen ihre Tätigkeiten in Zusammenhang mit den unter Europol verfolgten Kriminalitätsbekämpfungszielen und sie kann Europol-Datensammlungen für weitere, vertiefte Ermittlungen nutzen (Wahl 2010: 151; Ratzel 2008b: 114).[26] Aus der PCTF heraus können auch gemeinsame Ermittlungen über die Struktur Comprehensive Operational Strategic Planning for the Police (COSPOL) einzelne Projekte gezielt verfolgt[27] und so etwa nationale Ermittlerteams in der effektiven Nutzung der Europol-Datensammlung geschult[28] sowie Kriminelle, die eine zentrale Wirkung auf das Kriminalitätsfeld entfalten, verfolgt werden (Europol 2009: 49). Die PCTF ist in ihrer Form als Kompromiss zu sehen, da sich die Mitgliedsländer nicht darauf einigen konnten, ob das Gremium Strategien für Europol entwickeln oder eine rein operative Einheit bleiben sollte. Nach den Terroranschlägen in Madrid 2004 wurde die Einsetzung der PCTF dann von allen Organisationen befürwortet, ohne dass ihre endgültige Erscheinungsform geklärt gewesen wäre (House of Lords European Union Committee 2008: 81). Gemeinsame Ermittlungen in der Vergangenheit betrafen etwa die Operation Callidus und die Initiative gegen organisierte Kriminalität in Osteuropa. Callidus wurde von Schweden, letztere Operation von Polen geleitet. Die aus diesen kooperativen

[25] Parallel zur PCTF besteht auch das Gremium der ‚Heads of National Units' (HENUs) (Schuster 2000).
[26] Die PCTF kann beispielsweise auf AWFs zugreifen. Der Begriff AWF wird in Abschnitt 4.4.2 weiter erläutert.
[27] So wurde im Mai 2005 unter der Leitung von Schweden ein europaweit agierender Kinderpornographiering ausgehoben. Weiter an der Operation beteiligt waren Großbritannien, Dänemark, Frankreich, die Niederlande, Malta, Normwegen und Polen (Brady 2008: 105). Die gemeinsamen Operationen werden sowohl aus Ressourcen der Mitgliedsländer als auch aus EU-Mitteln finanziert.
[28] Seit 2006 hält die PCTF auch ein Handbuch mit Best practices für nationale Ermittlerteams bereit (Argomaniz 2001: 48).

Ermittlungen der PCTF entstandenen Informationen werden in einem weiteren Schritt wieder in das Europol-System, und dabei auch an die Mitgliedsländer, zurückgeleitet (sechste Zyklusphase). Die Rolle der PCTF soll langfristig gestärkt werden, um die Lücke zwischen dem reinen Wissensmanagement und operativen Tätigkeiten zu schließen (Bossong 2017; Kietz/Ondarza 2016; Bunyan 2006: 1). Obwohl Europol als Reaktion auf komplexe Sicherheitsbedrohungen – mit Unterstützung der europäischen Regierungen – ein sehr weitreichendes Instrumentarium entwickelt hat, steht die europäische Polizeikooperation auch in der öffentlichen Kritik. Gerade technische und konzeptionelle Weiterentwicklungen und die zentrale Speicherung von kriminalitäts- und personenbezogenen Daten wird nicht nur als notwendig betrachtet, sondern auch als Bedrohung informationeller Selbstbestimmung europäischer Bürger gesehen. Beobachter attestieren jedoch einen gewissen zeitabhängigen Gewöhnungseffekt, gar Konsens, bezüglich der Praktiken der Polizeiarbeit:

> „Die deutsche und die europäische Innenpolitik kennen viele erregende Diskussionen, obwohl nicht alle ihre erste scheinbare Bedeutung behalten: biometrische Merkmale, Rasterfahndung, Online-Durchsuchung, Terrorlisten. Einiges, was technisch neu daherkommt, verwirrt zuerst die Gemüter, stellt sich dann aber als unverzichtbar für moderne Polizeiarbeit heraus, wie der so genannte genetische Fingerabdruck“ (DiFabio 2008: 421).

In den Polizeibehörden selbst werden technische Neuerungen zur Unterstützung der Ermittlungen freilich von Anfang an positiv bewertet. Huey spricht gar vom „magic box view of the new technology“ (Huey 2002: 243), also einer möglicherweise übertriebenen Positivbewertung neuer technologischer Möglichkeiten durch deren Anwender. Wichtige Entwicklungen für die internationale Polizeiarbeit sind vor allem das DNA-Profiling, aber auch die Entwicklung von (gemeinsamen) Informationsräumen (Huey 2002; Sheptycki 1998). Zwar hat die technologische Weiterentwicklung die Polizeiarbeit einerseits schon immer beeinflusst. Andererseits muss gewährleistet bleiben, dass die Entwicklungen bei Europol in den legitimen Prozess einer Initiative der Mitgliedsstaaten eingebunden sind (Boer et al. 2008) und nicht einzig der supranationalen Eigeninitiative der Agentur unterliegen (Piquet 2017). Europol hat jedoch hohe Wichtigkeit für die europäische Sicherheitspolitik erreicht und kann ihr gegenüber teilweise selbst normativ konstitutiv agieren, also für neue (eigene) Handlungsformen plädieren. Zwar ist Europol alleine hinsichtlich der Weiterentwicklung von Strukturen nicht entscheidungsfähig. Doch in der EU-Kommission hat sie eine wichtige Unterstützerin, die den Rat der EU dazu aufrufen kann, die europäische Vernetzung in der Sicherheitspolitik weiter zu stärken. Zudem strebt Europol an, seine Services aktiver anzubieten und die strategischen Fähigkeiten weiter auszubauen: „providing a full intelligence picture (more strategic analysis) in priority crime areas“ (Europol 2015:2). Auch ist kritisch anzumerken, dass sich aus der

praktischen Arbeit der Polizei die Erprobung und Verwendung neuer technischer Möglichkeiten meist ergibt, bevor geeignete Regularien für deren Einsatz vom Gesetzgeber formuliert wurden (Sheptycki 1998: 62). Hier verdeutlicht sich erneut das Spannungsfeld zwischen Legitimität und Effektivität in der Bindung der Organisationen an die Gesellschaft. Denn ihrer effektiven Aufgabe, die Sicherheit der Gesellschaft zu wahren, müssen sie auch nachkommen, wenn für deren Erfüllung keine eindeutigen handlungsweisenden Institutionen zu einer geeigneten Vorgehensweise zur Verfügung stehen. Daher ist eine enge Abstimmung zwischen ausführenden Organisationen und beauftragenden oder verwaltenden Stellen notwendig, damit einer Regulierungslücke, aber auch einer möglichen Nachfragelücke nach Sicherheit(slösungen) vorgebeugt werden kann (Ratcliffe 2008: 16; Uhrlau 2009: 451). Es ist jedoch auch möglich, dass Regulierung nicht erfolgt oder verlangsamt wird, weil verwaltende und beauftragende Organe die tatsächlichen praktischen Abläufe nicht mehr nachvollziehen können (Sheptycki 1998: 68). Es entstehen also zwei Paradoxien: Erstens können kontrollierende und verwaltende Organe durch ihr Unwissen den Einsatz von Technologien in ihrer (sinnvollen) Nutzung verhindern, indem sie durch ihr Unverständnis versäumen, die notwendigen Räume und Regelungen für einige Organisationen zu schaffen (Ericson/Shearing 1986). Durch mangelnde Handlungsräume kann es dann geschehen, dass Kooperationswerkzeuge nicht effektiv genutzt werden können.[29] Zweitens kann das Unverständnis zu Untätigkeit in der (notwendigen) Regulierung führen und auch dadurch können unerwartete Folgen, beispielsweise für die Privatsphäre des Einzelnen oder die Freiheiten liberaler Gesellschaften, auftreten (Sheptycki 1998: 68). Politische Entscheidungsträger müssen daher über genügend Steuerungsinstrumente und Detailwissen verfügen, um das Handeln der Sicherheitsbehörden nachvollziehen, beurteilen und gegebenenfalls korrigieren zu können (Lange/Schenck 2004: 116). In diesem Zusammenhang kann auch die immer stärkere Verschränkung[30] zwischen nachrichtendienstlicher und polizeilicher Arbeit kritisch betrachtet werden (Daun 2011b: 187 ff.; Buuren 2014: 81). Wie die Geheimdienste gerät auch Europol in der Weiterentwicklung von Techniken und Strukturen an Grenzen, an denen die Gesellschaft ihre Aktivitäten als zu invasiv bewertet. In gemeinsamen Zentren, „fusion centres“ (Walsh/Miller 2016), wie dem Gemeinsamen Terrorismusabwehrzentrum (GTAZ) in Deutschland, können Strafverfolgungsbehörden auch

[29] Allerdings verweisen Studien (Deflem 2007a; Fägersten 2010b) auch darauf, dass unterschiedliche Organisationskulturen und interorganisationales Misstrauen dazu führen, dass Kooperationsforen nicht nach ihren eigentlichen Möglichkeiten genutzt werden.

[30] Diese Verschränkung ist keine direkte Folge des 11. Septembers 2001 sondern hatte sich bereits früher abgezeichnet. So kann der BND seit den 1990er Jahren Informationen zur organisierten Kriminalität erheben. Sie wird als politische Straftat betrachtet und ist damit verfassungsfeindlich (Daun 2011b: 185 f.).

an geheimdienstlich gewonnenen Informationen teilhaben. Auch auf Europol-Ebene entstehen immer mehr Zentren, an denen unterschiedliche Akteure beteiligt sind. Es entsteht gar der Eindruck eines vielschichtigen Netzes unterschiedlicher Koordinations- und Knotenpunkte. Europol hält beispielsweise Verbindungen zur Intelligence-Organisation der EU, dem INTCEN, sowie dem ‚Berner Club'.[31] Letzterer stellt ein Forum der Führungsebene der Nachrichtendienste Belgiens, Dänemarks, der USA, Luxemburgs, der Niederlande, Großbritanniens, der Schweiz und Deutschlands dar (Jäger/Daun 2005: 77 ff.). Europol ist zudem, was den Fokus der analysierten Informationen betrifft, nicht weit von einer geheimdienstlichen Behörde entfernt. Denn, anders als Interpol verarbeitet Europol auch Erkenntnisse, die nicht auf konkreten Sach- und Personensuchen im Rahmen von Fahndungsausschreibungen basieren, sondern auch ‚weiche' Daten, die komplexere Tat- und Täterzusammenhänge darstellen und Begleitumstände offenbaren sollen (Aden 1998: 99). Dieser Umstand, und auch die Vernetzung Europols mit unterschiedlichen Akteuren und eine daraus mögliche Beeinflussung der Methoden, sind bei gesellschaftlichen Akteuren nicht unumstritten. So ist Europol, gerade in der Kooperation mit dem Drittpartner USA, der Herausforderung ausgesetzt, die Eigenständigkeit und Organisationskultur als genuin europäische Behörde zu erhalten:

> „It is clear (…) that the United States would be very much interested in closer relationships in order to make sure that it would be the most important partner of Europol as and when it would become a fully developed ‚FBI-style' organization, as the United States has been expecting since the 1990s" (Kaunert 2010: 663).

Zwar kann Europol aufgrund seiner Gebundenheit an den europäischen Rechtskontext in seiner Struktur und Aktivität nicht die Form der US-amerikanischen Organisation annehmen (Ratzel 2008a: 28). Allerdings kann beobachtet werden, dass einige Konzepte aus dem angloamerikanischen Raum, wie zum Beispiel sowohl die erkenntnisgestützte Polizeiarbeit als auch das ‚Predictive policing' großen Einfluss auf die Tätigkeit von Europol hatten und haben (Ratcliffe 2010: 53). Letzteres methodisches Konstrukt zur Verhinderung von Straftaten befindet sich jedoch noch in der Erprobung. Es ist aber davon auszugehen, dass auch das Konzept der verhindernden Polizeiarbeit, ähnlich wie vorher die erkenntnisgestützte Polizeiarbeit, auch auf den europäischen Kontext übertragen wird (Europol 2014). Eine wichtige Brückenwirkung ist auch durch Großbritannien gegeben, welches als (Noch-

[31] Neben dem Berner Club soll auch noch die ‚Kilowatt Group' existieren, die 1977 in Reaktion auf die Terroranschläge auf die Olympischen Spiele in München im Jahr 1972 auf israelische Initiative hin gegründet worden sein soll und aus den EU-Mitgliedsstaaten, Kanada, Norwegen, Schweden, der Schweiz, den USA – hier sind vorrangig CIA und FBI beteiligt – dem israelischen Inlandsgeheimdienst Shin Beth und dem Auslandsgeheimdienst Mossad sowie Südafrika bestehen soll (Lefebvre 2003: 531).

)Mitgliedsstaat auf Europol zugreifen kann und somit, als gleichzeitig besonderer Partner der USA, entscheidende anglophone Initiativen eingeben kann.[32] Seit 2005 haben sich jedoch mit der schwedischen Initiative und dem – nach deutscher Idee entstandenen – ‚Prümer Vertrag' entscheidende Vertiefungen und Weiterentwicklungen für Europol ergeben. Auch wenn Europol nicht das einzige Forum europäischer Sicherheitskooperation darstellt, so ist es doch ein verlässlicher Kanal zur Verringerung der informationellen Komplexität, mit der sich nationale Ermittlungsbehörden tagtäglich konfrontiert sehen. So entsteht durch die Konstruktion gemeinsamer Strukturen und Methoden ein interorganisationaler Bereich der „good governance" (Boer/Bruggemann 2007) der polizeilichen Reaktion auf europäische und internationale Sicherheitsprobleme, das in seiner Form einzigartig ist, aber auch Parallelen zur interorganisationalen Kooperation der Geheimdienste aufweist.

2.3 Systematisierung des Forschungsstands

Die Darstellung der Arbeitsweise von Geheimdiensten und Europol hat bereits angedeutet, dass die Akteure ihre Zusammenarbeit und auch die Strukturierung ihrer Einzeltätigkeiten an gesellschaftlichen Institutionen durch deren Interpretation, ausrichten, und in der Kooperation vorrangig komplexitätsreduzierendes und effektives Handeln suchen. Dabei müssen sie Kompatibilität zu ihren Kooperationspartnern herstellen, gleichzeitig aber diesbezüglich die (retrospektiven) Bewertungen ihrer Gesellschaften antizipieren und reflektieren, ob ihre Reaktionen für die exogenen technischen Entwicklungen, die sie berücksichtigen müssen, ausreichend sind. Trotz eines umfangreichen Forschungsstandes ist eine Auseinandersetzung mit dieser Perspektive aber nur in geringem Maße vorhanden. So hebt er zwar hervor, dass gerade die Geheimdienstkooperation der Anglosphäre die Intention der Methodenkongruenz auf der Basis ähnlicher gesellschaftlicher Vorstellungen zur Reichweite von sicherheitsbehördlichem Handeln verfolgen kann. Auch gehen bisherige Arbeiten jedoch davon aus, dass sich die Geheimdienstkooperation mit anderen Partnern, wie dem deutschen BND, nicht so intensiv darstellt wie die Kooperationen der NSA mit den anglophonen Geheimdiensten. Allerdings wurde bislang nicht untersucht, wo auch die Grenzen der anglophonen Kongruenz liegen und warum zumindest eine teilweise Anpassung der Methodik

[32] Welche Folgen sich durch den möglichen Ausstieg Großbritanniens aus der EU ergeben, stand zur Beendigung dieser Arbeit noch nicht fest. Beobachter ordneten die möglichen Entwicklungen widersprüchlich ein: während einige von einer Chance für eine stärkere Integration europäischer Sicherheits- und Verteidigungspolitik ohne ein bremsendes Großbritannien sprechen (Friedrichs 2016), sprechen andere von der Schwächung eines europäischen Militärbündnisses, da mit Großbritannien ein starker Partner die gemeinsame Bühne verlasse (Ziedler 2016). Wissenschaftliche Beobachter haben den BREXIT einzig in seinen Folgen für Großbritannien bewertet. Inkster (2016) kommt zu dem Ergebnis, dass die Entwicklungen ohne Folgen für die britische Sicherheitspolitik bleiben werden, da diese sich ohnehin vor allem auf bilaterale Initiativen konzentriert.

auch zwischen NSA und BND erfolgt ist. Tabelle 1 strukturiert daher den Literaturstand nach den Zyklusphasen der Geheimdienste und wertet deren zentrale Erkenntnisse aus. Diese Einordnung ermöglicht es dann, weiteren Forschungsbedarf zu identifizieren, der durch die vorliegende Arbeit erfüllt werden soll.

Phase 1: Auftrag nach Wissen und Sicherheit	Bezugnehmende Studien	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
Regierungen demokratischer Gesellschaften vergeben – je nach gesellschaftlicher Bedrohungsauffassung – einen thematischen Auftrag an Geheimdienste. Sie sollen, ihrem gesetzlichen Auftrag und Rahmen entsprechend, Wissen produzieren, indem sie Daten erheben, auswerten und Informationen mit anderen Geheimdiensten austauschen.	Lowenthal 2017; Diersch 2017; Fägersten 2010; Omand 2010; Aldrich 2009; Sterbling 2009; Johnson 2004; Huey 2002; Kent 1966	Intelligence-Organisationen erstellen politisches, militärisches, soziales, ökologisches und ökonomisches Wissen. Seit dem 11. September konzentrieren sie sich vor allem auf transnationale Bedrohungen, wie den Terrorismus. Neue Bedrohungen ergeben sich aber auch durch Cyberkriminalität. Der Auftrag ist somit von einer zeitlichen Komponente beeinflusst, denn Wissen muss sowohl langfristig, als auch mittelfristig und zeitaktuell bereitgestellt werden und alle relevanten Themen und Trends abdecken, auch solche, die in der Realität der Auftraggeber noch keine Rolle spielen. Daher wird auch das Warnen vor zukünftigen Ereignissen immer wichtiger.	Welche Institutionen prägen die Intelligence-Kooperationen besonders und sind diese in unterschiedlichen Kooperationsarrangements divergent?

Phase 2: Steuerung der Informationsbeschaffung für die gegenwärtige und zukünftige Alltagssicherheit	Bezugnehmende Studien	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
In der Phase der Steuerung entscheiden Geheimdienste, welche menschlichen und technischen Quellen zur Erfüllung des gesellschaftlichen Auftrages dienlich sein könnten und kommen hier auch auf ihre Kooperationspartner zu.	Jakobsen/Ringsmose 2015; Buuren 2014; Daun 2011b; Daun 2005b; Aldrich 2004; Johnson 2003; Aldrich 2002	Unterschiedliche Partner decken, auch aufgrund technischen Zugangs, unterschiedliche Regionen ab. Auch sind einige Organisationspartnerschaften enger als andere und können möglicherweise stärker genutzt werden. Allerdings vernetzen sich Geheimdienste seit dem 11. September 2001 verstärkt mit Partnern überall auf der Welt.	Wann erreichen welche Partnerschaften stabile, also wiederholt ansteuerbare, Strukturen und wann verbleiben sie lediglich im Bereich der ad-hoc-Kooperation? Welche technischen Zugänge, Strukturen und Methoden sind zur Aufklärung aktueller und zukünftiger Bedrohungen notwendig?

Phase 3: Sammlung von Informationen zur Erbringung gegenwärtigen und zukünftigen Wissens	Bezugnehmende Studien	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
Bei der Sammlung von Informationen müssen die Geheimdienste möglichst viele relevante Daten zusammentragen.	Hulnick 2014; Omand 2014; Sims 2014; Dimitriu/Duyvesteyn 2014; Cavelty/Maurer 2009; Richelson 2009; Bigo 2008; Johnson 2003; Westerfield 1996;	Technische Daten erscheinen meist umfassender und glaubwürdiger als menschliche Informationen. Digitale Daten sind in großem Maße verfügbar und offenbaren Personennetzwerke sowie spezifische Zusammenhänge. Technische Daten eigenen sich daher besonders für das Warnen vor (intendierten) gefährdenden Handlungen nicht-staatlicher Akteure.	Konstruieren Geheimdienste die Ausspähung digitaler Daten nur nach technischer Machbarkeit oder auch nach Legitimität? Spielt beim Teilen großer digitaler Datenmengen eine starke Verbundenheit aufgrund kultureller Kongruenz zwischen den Partnern eine größere Rolle als die technische Fähigkeit oder Machbarkeit, dies zu tun?

Phase 4: Vernetzte Analyse nach besten Methoden	Bezugnehmende Studien	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
An der Analyse sind unterschiedliche Dienste beteiligt und es entsteht ein möglichst umfangreiches Wissensprodukt.	Jakobsen/Ringsmose 2015; Clark 2013; Fingar 2011	Durch die massive Verfügbarkeiten von Daten werden effektive, auch vernetzte, Analysemöglichkeiten benötigt. Damit die Analyse technisch auf dem höchsten Stand verläuft, ist außerdem die Notwendigkeit, geeignete gemeinsame und einzelne Techniken aufzubauen, gegeben.	Welche Analysen finden in Kooperation statt? Welche Faktoren entscheiden, wann technische Methoden zur bestmöglichen einzelnen oder gemeinsamen Analyse auch an Kooperationspartner übertragen werden?
Phase 5: Bedarfserfüllung und Vermeidung von Nachfragelücken	Bezugnehmende Studien	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
Die Weiterleitung des Wissensproduktes an den Auftraggeber findet im Rahmen eines Meetings oder als bloße Papiereingabe statt	Omand 2014; Scott/Jackson 2004	Die Unterrichtung findet in unterschiedlichen Formaten statt. Die Häufigkeit und das Publikum variieren je nach Dringlichkeit der Lage und nach Land.	Welcher Anteil der Informationen, die an die Entscheidungsträger weitergegeben werden, entsteht aus Kooperation beziehungsweise wie wichtig ist die Kooperation für die Verfügbarkeit und Validität der Informationen, die an die Entscheidungsträger weitergegeben werden (können)?

Tabelle 1: Identifizierung wesentlicher Ergebnisse bisheriger Studien aus den Intelligence Studies und nachweisbare weitere Forschungsbedarfe.

Bei der Forschung zu Europol ist augenfällig, dass sich die Autoren meist auf die Entstehungsgeschichte und Organisationsform konzentrieren. Was die Literatur bislang jedoch nicht ausreichend herausgearbeitet hat, ist, dass aufgrund der Notwendigkeit internationalisierten Handelns kompatible technische Kooperationslösungen für teilweise sehr divergente Kooperationspartner benötigt werden. Dies fordert einerseits die Ermittlungsbehörden der Mitgliedsländer heraus, die trotz Souveräntitätsvorbehalten eine gewisse Interaktion und Anpassung eingehen müssen, um Daten zu international agierenden Gefährdern austauschen zu können. Durch weitreichende Verbindungen diesbezüglich wird jedoch wiederum das gesellschaftliche Spannungsfeld zwischen Legitimität und Effektivität auch auf dem Gebiet der Strafverfolgung – das sich immer stärker in ein Feld der Strafverhinderung entwickelt – weiter verschärft.

Phase 1 des ECIM: Ermittlung von Schadensbereichen für die Gesellschaft	Bezugnehmende Studie	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
Das SOCTA legt als Analyse auf vier Jahre fest, welche Ziele priorisiert durch Europol verfolgt werden sollen	Möllers 2012	Der erste Schritt des European Criminal Intelligence Models (ECIM) ist bereits eine Analyse der Lage der internationalen Kriminalität und dient zur weiteren Planung des Handelns.	Welchen Einfluss haben Europol-Strukturen auf Planungen und Handlungen in den Mitgliedsstaaten?
Phase 2 des ECIM: Erarbeitung strategischer Ziele zur Verminderung der Kriminalitätsauswirkungen	Bezugnehmende Studie	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
Aus der Priorisierung, auf Grundlage des SOCTA, entstehen mehrjährige Aktionspläne, welche konkrete, strategische, Ziele festlegen, die in jedem der priorisierten Bereiche erreicht werden sollen.	Paoli 2014	Das SOCTA empfiehlt die Priorisierung bestimmter Kriminalitätsbereiche. Ausschlaggebend ist der Schaden, welcher durch die Kriminalitätsbereiche in den Mitgliedsstaaten entsteht.	Welche anderen Möglichkeiten neben dem SOCTA nutzt Europol, um sich für die Kriminalitätsbekämpfung in komplexen Bereichen aufzustellen?

Phase 3 des ECIM: Erstellung von operativen Plänen	Bezugnehmende Studie	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
Aus den MASPs entstehen operative Aktionspläne (OAPs), die zur Erfüllung der strategischen Ziele dienlich sein sollen	Piquet 2017	Die operativen Aktionspläne orientieren sich, wie das gesamte ECIM, an der Bedrohungs- und Erkenntnislage. Es ist eine Hinwendung zu einer warnenden und koordinierenden Polizeiarbeit erkennbar, die ihre Betätigungsfelder erweitern kann und möglichst viele Informationen zu Ermittlungen zusammenzieht.	Inwiefern wird die Tätigkeit von Europol durch lose Vernetzung mit anderen Sicherheitsforen ergänzt und ist der Interaktions- und Kompetenzbereich der Behörde fest strukturiert oder verläuft er fließend?
Phase 4 des ECIM: Evaluation der erzielten Ergebnisse in den Schadensbereichen	Bezugnehmende Studie	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
Die OAPs werden hinsichtlich ihrer Wirksamkeit auf die priorisierten Bereiche überprüft. Gleichzeitig werden auch die priorisierten Bereiche selbst hinsichtlich ihrer Relevanz in aktuellen Entwicklungen evaluiert.	Piquet 2017	Die operativen Aktionspläne werden hinsichtlich ihrer Wirksamkeit überprüft. Allerdings sind die Maßnahmen – wie auch die Ziele, für die sie ausgelegt sind – nicht immer einstimmig von allen Organisationen auf Mitgliedsländerebene unterstützt.	Wie sehr hemmt eine Uneinigkeit der Mitgliedsländer in der Ausrichtung von Europol dessen Wirksamkeit?

Phase 5 des ECIM: Ermittlungen der Police Chief Task Force (PCTF) zu führenden Personen in den Kriminalitätsbereichen	Bezugnehmende Studie	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
Viermal im Jahr trifft sich das informelle Gremium PCFT und plant gemeinsame Operationen.	Wahl 2010; Ratzel 2008b	Die PCTF ist ein lose an Europol gekoppeltes Gremium, das einen Kompromiss zwischen strategisch-planender Führungsriege der Ermittlungsbehörde auf Mitgliedsländerebene und operativer Einheit darstellt.	Ist die Einigung auf eine einheitliche, zentrale Struktur ein generelles Problem bei der Weiterentwicklung von Europol?
Phase 6 des ECIM: Informationen der PCTF werden in den ECIM-Zyklus zurückgegeben	Bezugnehmende Studie	Ergebnisse für die Zyklusphase	Weiterer Forschungsbedarf
Die durch weitere Ermittlungen der PCTF-Teams zutage geförderten Informationen werden in die Wissensmanagementsysteme von Europol eingegeben	Bunyan 2006	Durch das ‚Recycling' von – durch spezielle Ermittlungsteams erhobenen – Informationen soll ein System der Effektivität und ‚Good governance' des ECIM unterstrichen werden.	Welchen Grad der Nutzung erreichen die durch Europol bereitgestellten Informationen in den Mitgliedsländern?

Tabelle 2: Identifizierung wesentlicher Ergebnisse bisheriger Studien aus der Polizeiforschung und nachweisbare weitere Forschungsbedarfe.

Die Inhalte, welche die ausgewerteten Studien nicht bereitstellen, lassen sich darauf verdichten, dass die Internationalisierung und Vernetzung geheimdienstlicher und polizeilicher Strukturen Fragen hinsichtlich der Schaffung von technischer und methodischer Kompatibilität, deren Wirksamkeit von Kooperationsarrangements hinsichtlich sich exogen ständig weiterentwickelnder komplexer Kriminalitätsbereiche sowie hinsichtlich der tatsächlichen Fokussierung auf gesellschaftliche und (organisations)kulturelle Grenzen aufwirft. So ist nicht geklärt, welche Rolle kulturelle Kongruenz beziehungsweise Divergenz der Organisationen für den Zustand einer festen Institutionalisierung und die gleichwertige Nutzung von Strukturen zur Informationsweiterleitung hat. Dafür sollte untersucht werden, welche Rolle die gemeinsame Analyse und die hierzu benötigte internationale Datenweiterleitung, beziehungsweise die dazu benötigte Einigung auf Auswertungs- und Analysewerkzeuge für die nachrichtendienstliche, aber auch die polizeiliche Kooperation spielt. Zudem soll versucht werden, nachrichtendienstliche und polizeiliche Kooperation, trotz teilweise unterschiedlicher Abläufe, nicht als getrennte Phänomene aufzufassen, sondern deren empirischer Verschränkung auch die wissenschaftlich logische Konsequenz einer Untersuchung nach ähnlichen Mechanismen folgen zu lassen.

Die Aufdeckung der Forschungsdesiderate sowie der Notwendigkeit, (kulturelle) Heterogenität und die Auswirkungen auf gemeinsame Analysebestrebungen zu überprüfen, hat Folgen für die Wahl der Untersuchungsvariablen der vorliegenden Arbeit, da beide Hervorhebungen es erlauben, einen dezidierten methodischen Zuschnitt in Abgrenzung zu den dargestellten Untersuchungen einzunehmen. Zu der Schlussfolgerung, dass die sicherheitsbehördliche Kooperation nach unterschiedlichen Erklärungen zu untersuchen sei, hebt bereits Clough hervor, dass „number and choice of partners, the degree of mutuality between them, and the depth and breadth of intelligence shared“ (Clough 2004: 611 f.) nicht die einzigen relevanten Faktoren seien, die für die Tiefe der Zusammenarbeit eine Rolle spielen. Zwar verwendet vorliegende Arbeit die gleiche abhängige Variable wie Clough, indem sie die Tiefe der Kooperation als Ergebnis unterschiedlicher zusammenwirkender Einflussfaktoren betrachtet. Allerdings geht vorliegende Arbeit davon aus, dass, unabhängig von der Anzahl der Partner und der Wichtigkeit der geteilten Informationen, vor allem unterschiedliche Fähigkeitsvoraussetzungen durch divergierende kulturelle Denkmuster, bei gleichzeitig allseitiger Interpretation, das effektive gemeinsame Maßnahmen zur Datenweiterleitung und Analyse notwendig sind, erklärende Bedingungen darstellen. Die Hervorhebung der gesellschaftlichen Bindung und diesbezüglicher Wirkungen, und ihr Spannungsfeld zur Effektivität, stellen eine neue Ausrichtung in der Analyse dar. Dadurch kann vorliegende Arbeit

in Abgrenzung zu anderen Forschungsdesigns durch die Wahl ihrer erklärenden Variablen einen Mehrwert zur Intelligence-Forschung, aber auch zur Untersuchung der Polizeikooperation bei Europol leisten, wie Tabelle 3 verdeutlicht.

Studie	Unabhängige (erklärende) Variable(n)	Abhängige (zu erklärende) Variable
Clough 2004	Anzahl der Partner, Einigkeit, Wichtigkeit der geteilten Informationen	Art und Tiefe der Kooperation
Westerfield 1996	Interdependenz der Interessen in Korrelation zum Risiko der Gegenspionage und Manipulation	Art und Tiefe der Kooperation
Lander 2009	Vertrauen und Notwendigkeitserwägungen durch externe Bedrohungen	Art und Tiefe der Kooperation
Boer et al. 2008	Informalität der Kooperationsbeziehungen	Effektivität der Sicherheitskooperation
Vorliegende Arbeit	Kulturell beeinflusste gesellschaftliche Bindung und kooperative Konstruktion einer effektiven Anpassung	Zustand der Institutionalisierung der Kooperation

Tabelle 3: Unabhängige und abhängige Variable vorliegender Arbeit in Abgrenzung zu anderen Forschungsdesigns.

Gleichzeitig nimmt die vorliegende Untersuchung durch die Wahl eines soziologischen Konzeptes eine ontologisch divergente Perspektive zu den dargestellten Forschungsarbeiten ein. So steht weniger im Vordergrund, ob die Organisationen Kooperationen eingehen, um sich im Gegenzug technischen Zugang zu sichern (Westerfield 1996). Zusätzlich liegt es weniger im Fokus, welche Machtstrukturen und Interessenlagen eine Rolle für Intelligence-Kooperation spielen. Auch werden Institutionen weniger als Anreizstrukturen zur (kostengünstigen) Kooperation bei sich überschneidender Interessenlage betrachtet oder gar als Mittel um eigenen Einfluss auszudehnen (Daun 2011a). Institutionen, verstanden als soziale Regeln, stellen vielmehr den einzig verfügbaren Rahmen zur Verringerung der Komplexität interorganisationaler Beziehungen für Organisationen dar und sorgen so für die Stabilität der Kooperation. Gleichzeitig sind dynamischere Institutionen, beispielsweise methodische Verfahrensmodelle, auch übertragbar und können so Handlungsmuster auch über relativ stabile kulturelle Handlungs- und Erfahrungsgrenzen hinweg schaffen. Vorliegende Arbeit kann daher einen Mehrwert zur Intelligence- und Polizeiforschung leisten, indem sie eine spezifische theoretische Ausgangslage wählt, die nachfolgend erklärt, erweitert und auf die nachrichtendienstliche Kooperation und die Polizeikooperation angewendet werden soll.

3. Der Neue Institutionalismus als theoretischer Rahmen für die Kooperationsforschung

> „We recognise space as always under construction. Precisely because space (…) is a product of relations-between, relations which are necessarily embedded material practices which have to be carried out, it is always in the process of being made. It is never finished; never closed. Perhaps we could imagine space as a simultaneity of stories-so-far."
>
> *Doreen Massey*

> "Just as the locations where sea water meets fresh water are particular supportive of varied forms of marine life, so the areas of overlap and confluence between institutional spheres generate rich possibilities for new forms."
>
> *W. Richard Scott*

Aus der Analyse des Literaturstandes zur Zusammenarbeit von Sicherheitsbehörden lässt sich ableiten, dass die Konzentration auf nutzenorientierte Interessenlagen alleine technisch und strukturell weitreichende Kooperationsarrangements im transatlantischen und europäischen Bereich nicht ausreichend erklären kann. Zwar können exogene Bedingungen zur Kooperation führen. Deren Ausgestaltung ist jedoch nur anhand einer diesbezüglichen Fokussierung nicht vollumfänglich nachzuvollziehen. Wie bereits Ulbert (1997: 10) feststellt, können Interessen zudem nur dann maßgebliche Erklärungen liefern, wenn spezifiziert wird, durch welche Ideen sie informiert sind beziehungsweise innerhalb welcher gesellschaftlicher Referenzsysteme sie zur Umsetzung kommen können. Zur Weiterentwicklung wissenschaftlicher Erkenntnisse wird daher eine Perspektive vorgeschlagen, die den Fokus stärker auf die organisationale Interpretation[33] gesellschaftlicher Erwartungen und technischer Umweltbedingungen in der

[33] Der Begriff der Interpretation unterscheidet sich vom Terminus der Wahrnehmung insofern, als dass Organisationen wahrgenommene Sachverhalte in Abgleich mit ihren Erfahrungen und ihrem Wissen über sinnvolles Handeln bringen und daraus mögliche Handlungen und deren Grenzen ableiten. Wahrnehmung kommt im Verständnis dieser Arbeit ohne den Abgleich mit diesen Organisationserfahrungen und ihrer Reichweite aus. Interpretation geht somit einen Schritt weiter als bloße Wahrnehmung, weil sie mit einer Handlungsableitung direkt verknüpft ist und diese Ableitung auch Ziel der Interpretation, nicht nur bloße Folge ist.

Planung, Ausführung und Begründung kooperativen Handelns legt. Durch diese Festlegung lässt sich das Organisationshandeln als Intention der kulturellen und gesellschaftlichen Erwartungsverwirklichung beziehungsweise als Reaktion auf diese Erwartungserwartung verstehen (Senge/Hellmann 2006). Kultur definiert damit das Handlungsrepertoire von Organisationen, während Institutionen ihren kognitiv wahrnehmbaren konkreteren formalen und informellen Handlungsrahmen bilden. Dann sind Organisationen nicht nur eigenorientiert, sondern beziehen auch ihre gesellschaftliche, und damit kulturelle Umwelt mit ein. Diese Erwartungserfüllung ist jedoch wiederum durch Komplexität gekennzeichnet und diese Wirkungen und ihre Wechselwirkungen müssen in der Kooperationsforschung der IB stärker betrachtet werden. Besonders geeignet für eine Untersuchung nach genau diesen Prämissen erscheint die soziologische Organisationstheorie des Neuen Institutionalismus, die sich mit der Ausrichtung von auf das eingangs diskutierte Spannungsfeld zwischen Legitimität und Effektivität beschäftigt und in der kulturell-institutionellen Faktoren eine entscheidende Bedeutung zukommt (Abschnitt 3.1). Um für das Anwendungsgebiet der Kooperationsforschung operationalisiert werden zu können, muss der Analyseansatz jedoch ausreichend präzisieren, welche komplexen Wirkungen sich auf und in der Akteursebene ergeben. Aus dieser theoretischen Auseinandersetzung entsteht mit dem internationalen interorganisationalen Kooperationsmodell eine Weiterentwicklung des Neuen Institutionalismus (Abschnitt 3.2). Diese daraus erwachsende Möglichkeit der Einbettung des Ansatzes in die sozialkonstruktivistische Kooperationsforschung der IB erleichtert dann eine Darlegung des methodischen Vorgehens der vorliegenden Untersuchung (Abschnitt 3.3).

3.1 Die kulturelle Beeinflussung von und durch Institutionen

Zur Einordnung und Nutzbarmachung des Neuen Institutionalismus[34] ist eine Spezifikation der Akteursperspektive, also eine Erläuterung der Variablen und ihrer Dimensionen, durch welche Akteure in ihrem Handeln beeinflusst werden, notwendig. Auf Grundlage dieser Festlegungen kann dann das Kooperationskonzept des Neuen Institutionalismus entwickelt werden, wofür einige Präzisierungen und Erweiterungen nötig sind. Die Kooperation von Sicherheitsbehörden mit dieser kulturell-institutionellen Perspektive zu erklären, erscheint aber gerade deshalb wertvoll, weil sie nicht nur die Interessen der Akteure in den Fokus nimmt, sondern die Blickrichtung weitet, indem sie die Organisationen in einen gesellschaftlichen Kontext eingebunden sieht, an dem sich die Akteure in der Definition ihrer Interessen orientieren

[34] Für eine konzise Abgrenzung von Neuem zu ‚altem' Institutionalismus, siehe DiMaggio/Powell 1991: 13 f. und Senge/Hellmann 2006 13 ff..

müssen (Katzenstein 1996). Für die internationale Kooperation bedeutet dies vor allem, dass unterschiedliche Akteure mit heterogenen kulturellen Determinanten, und damit divergenten geronnenen Ideen und Praktiken konfrontiert sind, welche die Ergebnisse ihres Zusammenwirkens verkomplizieren, aber dadurch erst vollständig erklärbar machen (Ulbert 1997: 16). Dieser wissenschaftliche Perspektivenwechsel entsteht maßgeblich dadurch, dass der Neue Institutionalismus sowohl für das Akteurshandeln, als auch für den Akteur selbst, andere Prämissen anlegt, als dies Ansätze mit positivistischem Blick auf die Aktivitäten von Individuen und Gruppen tun.[35]

Der Neue Institutionalismus hat sich wesentlich aus der Kritik an der rationalistischen Perspektive in den Sozialwissenschaften entwickelt (Senge 2011). Dabei wird vor allem das behavoristisch geprägte Institutionenverständnis bemängelt, welches in ähnlicher Weise auch in der Ökonomik zu finden ist (Ebers/Gotsch 2006). Diese Kritik lässt sich jedoch auch auf die IB und auch auf die Forschung zu Geheimdiensten übertragen. In der Disziplin ist vor allem der Institutionenbegriff von Keohane (1989: 3) gängig, der Institutionen als zusammenhängende, formale und informelle Regeln, die den Akteuren Rollenverhalten vorschreiben und ihre Handlungsspielräume definieren sowie ihre Erwartungen formen, versteht. Hierbei spielen als legitim begriffene Strukturen und Regeln zwar eine entscheidende Rolle für das Verhalten der Akteure. Diese Vorstellungen sind ihnen jedoch nicht vorgelagert – und damit nicht regulativ, normativ oder habituell zwingend –, sondern entsprechen lediglich Anreizen, nach denen sie ihre eigene Interessensformulierung ausrichten können. Tabelle 4 verdeutlicht, wie in einem positivistischen Modell interessengeleitete Akteure und deren Wirkung auf internationale Strukturen in den Vordergrund rücken. Angesichts der durch Regeln eingeschränkten Handlungsoptionen wählen die Organisationen aus Sicht des Neoliberalen Institutionalismus dasjenige Verhalten, das ihren Interessen am meisten entspricht. Der Neue Institutionalismus hebt in der Abgrenzung dazu hervor, dass Individuen nicht als Maximierer ihres individuellen Nutzens handeln *können*, da sie vielmehr in einen intersubjektiven (gesellschaftlichen) Kontext eingebunden sind, der ihre Verhaltensweisen maßgeblich bestimmt, dessen Regeln sie nicht hinterfragen, und den sie lediglich zum Teil beeinflussen können (Giddens 1984). Außerdem hebt der Ansatz hervor, dass regulative und normative Strukturbedingungen vor allem durch ihre kognitive Verankerung und ihre bewusste

[35] In den Sozialwissenschaften werden positivistische und post-positivistische Analyseansätze unterschieden, deren Paradigmen sich wesentlich darin widersprechen, dass positivistische Ansätze von objektiv festzulegenden Kausalwirkungen ausgehen, während post-positivistische Analysemethoden, unter die strukturalistische Methoden wie die vorliegende zu fassen sind, davon ausgehen, dass Einflussfaktoren auf Akteurshandeln immer kontextbezogen und daher nicht objektiv festlegbar und verallgemeinerbar sind (Stetter 2017: 261).

oder unbewusste Reflexion Wirksamkeit entfalten und nicht durch externe Anreizsetzung und Strafen (Senge 2006: 41; Klatetzki 2006: 53).

Theorie	Definition von Institution	Annahmen über die Handlungsfähigkeit des Akteurs (Agency)	Nutzen von Kooperation
Neoliberaler Institutionalismus	Institutionen sind Beschränkungen und Anreize für das Verhalten rationaler Akteure, die sich diese Regeln selbst geben	Akteure sind befähigt, sich eigene Regeln für ihr Zusammenwirken zu geben	Gemeinsame Interessensdurch-setzung
Neuer Institutionalismus	Akteure sind durch Regeln und Normen beschränkt und befähigt, die sie von der Umwelt auferlegt bekommen und die sie lediglich – in geringem Maße – mitgestalten können	Akteure sind in der Regelung von Inter-Akteursbeziehungen von der Einhaltung bestimmter Legitimitätsregeln der Umwelt abhängig	Gemeinsame Interessensdurch-setzung abhängig von gesellschaft-lichen Regeln und Normen und ihrer kognitiven Nachvollziehbarkeit

Tabelle 4: Kontrastierung von Neoliberalem Institutionalismus und Neuem Institutionalismus.

Die Entscheidungen der Organisationen und ihrer Mitglieder werden dann nicht aufgrund persönlicher oder akteursspezifischer Nutzenerwägung, sondern aus der Auffassung heraus, etwas Sinnvolles und Richtiges zu tun und weil andere angemessene Alternativen nicht denkbar sind, da die institutionalisierten Verhaltensmuster habitualisiert sind, getroffen (Finnemore/Sikkink 1998: 911; Zucker 1983). Anstelle des Akteurs tritt die Struktur in den Vordergrund der Betrachtung und der Akteur ist in der Abwägung zur Wahl seiner Mittel in ständiger Außenorientierung insofern begriffen, als dass er sie nur in Auseinandersetzung mit den Zielen und denkbaren Möglichkeiten seiner Umwelt – der kulturell beeinflussten Gesellschaft sowie den kognitiven kooperativen Handlungsräumen seines Kooperationspartners – wählen kann (Stetter 2017: 262; Friedland/Alford 1991).

Diese Perspektive auf den Akteur und seine Handlungsfähigkeit ist also eine andere als im Ansatz des Neoliberalen Institutionalismus. Akteure bilden die Regeln, nach denen sie handeln, nicht selbst aus, sondern diese werden maßgeblich durch diejenigen Erwartungen geprägt, welche die Umwelt an das Verhalten der Organisationen hat.[36] Diese Erwartungen können als Institutionen bezeichnet werden, die aus kulturellen Vorstellungen entstehen, in formelle und informelle Handlungsmuster ‚gerinnen' und in konkreten Handlungsstrukturen ihren Ausdruck finden, die im geronnenen Zustand nicht mehr hinterfragt werden (Senge 2006: 39 ff.; Ulbert 1997: 15 f.). Institutionen sind im Sinne des Neuen Institutionalismus „soziale Regeln (…), die organisationale Prozesse in zeitlicher Perspektive *dauerhaft* (für die Dauer der Beobachtung), in sozialer Hinsicht *verbindlich* (Akteure halten sich daran) und in sachlicher Hinsicht *maßgeblich* (sie sind für ein Phänomen bedeutsam) beeinflussen" (Senge/Hellmann 2006: 35; Herv. i. O.). Sie bieten eine Verhaltens- und Sinnorientierung für Organisationen (Göhler 1990: 10). Somit wählen die Organisationen die beste Handlungsoption nur begrenzt strategisch, denn sie bewegen sich vielmehr innerhalb der Handlungsmuster, die ihnen rational erscheinen, da sie von außen erwartet werden, demnach kulturell als angemessen definiert sind und, abgeleitet aus der kulturellen Bedeutung, kognitiv verankert sind, egal ob sie regulativ vorgeschrieben sind oder nicht. Erst in der Auseinandersetzung mit diesen Institutionen wird Organisationshandeln ermöglicht und praktiziert. Auch die Organisation selbst ist damit in gewisser Weise eine strukturierte Form von Institutionen. Dadurch ist sie immer zugleich fixiert – da ihre jetzige Form Ergebnis vorangegangener, im Sinne des Institutionenbegriffs dauerhafter Erwartung ist – und gesellschaftlichem Wandel unterworfen, dem sie sich anpassen muss (Senge/Hellmann 2006: 19 ff.; Siedschlag 2000: 18; Türk 1999: 44 ff.). Damit weisen Institutionen unterschiedliche Zustände auf. In ihrer dauerhaftesten Form sind sie habitualisierte Normen, die befolgt werden, ohne dass dies demonstriert, spezifiziert oder diskutiert werden muss.[37] Gerade in den, dieser Stufe vorangehenden Zuständen der Entstehung und der Verbreitung, sind Diskussion und Demonstration jedoch häufig zu beobachtende Normzustände. Finnemore und Sikkink (1998: 894) sprechen daher vom ‚Lebenszyklus der Norm' mit unterschiedlichen Stufen der Normentwicklung, die empirisch betrachtet werden können. Wenn also in vorliegender Arbeit von Institutionen gesprochen wird, dann sind sowohl deren Entstehung, Verbreitung und Internalisierung mögliche Formen der Institutionalisierung, die beobachtet

[36] Allerdings hebt DiMaggio hervor, dass Akteure in ihrer Rückwirkung auf die Struktur durchaus Interessen entwickeln und durchsetzen können, etwa indem sie als ‚Norm entrepreneur' auf die Um- und Durchsetzung legitimer Verfahrensweisen pochen (DiMaggio 1988).

[37] Die dadurch angenommene fehlende ‚Sichtbarkeit' ist freilich für die empirische Forschung zur Wirkung kultureller Determinanten ein Hindernis.

werden können. Dabei kann nicht nur der Grad einer gesellschaftlichen Norm, ob diese beispielsweise internalisiert, also ‚geronnen' ist, betrachtet werden, sondern auch der Grad der allseitigen Internalisierung einer durch Kooperation ‚importierten' Norm und die Begründung dieses Prozesses der Anpassung oder Nicht-Anpassung. Dabei ist es wichtig, hervorzuheben, dass die empirische Forschung mit dem Neuen Institutionalismus nicht die Analyse der modernen Gesellschaft in den Fokus nimmt, sondern die Eigenschaften und Handlungen der Organisationen in einer gesellschaftlichen und organisationalen Organisationsgesellschaft betrachtet. Die Gesellschaft ist also nicht Fokus der Untersuchung, sondern lediglich Kontext der Untersuchungsobjekte (Senge/Hellmann 2006: 23). Daher ist die Untersuchung der Möglichkeiten der Interpretation von und Anpassung an gesellschaftliche Erwartungen und deren Übereinbringung mit interorganisationalen Gesichtspunkten in der Kooperation an die Grundausrichtung neo-institutionalistischer Forschung anschlussfähig. Zusätzlich wird die Erweiterung des Ansatzes auf das internationale interorganisationale Kooperationsmodell zeigen, dass die gesellschaftliche Bindung der Organisationen in ihrem Handeln keine rein binäre Größe ausmacht, in dem Sinne, dass sie entweder berücksichtigt oder ignoriert wird. Vielmehr müssen die Erwartungen der Gesellschaft durch die Organisationen stets interpretiert werden, sind jedoch nicht immer konkret abzuschätzen. Dies resultiert daraus, dass der Neue Institutionalismus nicht nur ein genuines Akteursverständnis, sondern auch ein solches Umweltverständnis verwendet. So ist die Umwelt durch die Variable der Unsicherheit geprägt. Die Rationalisierung von Organisationsentscheidungen findet durch die Akteure unter der Prämisse statt, dass ihre Festlegung in rückwärtiger Betrachtung durch die Gesellschaft als fehlerhaft, ungenügend, gewissermaßen als der Situation und Zeit nicht angemessen, bewertet werden kann. Entscheidungsfindung in Sicherheitsbehörden wäre dann der wirtschaftlichen Investition ähnlich, bei der Investoren zum Zeitpunkt ihres Mitteleinsatzes eine Risikoeinschätzung vornehmen und nur basierend auf ihrem zum Investitionszeitpunkt bestehenden Wissens handeln können. Unsicherheit kann demnach als Grundkonzept der Organisationssoziologie verstanden werden (Brosziewski 2015). Wenn die Interpretation von Erwartungen jedoch nicht als hundertprozentig verlässliche Handlungsgrundlage bietet, ist die Bindung an die Gesellschaft zwar vorhanden, ist dann aber eher als beschränkend denn als befähigend aufzufassen.[38] ‚Gelöst' wird dieses Problem durch das bewusste oder unbewusste

[38] Dann müssen die Organisationen eine Entscheidung in Ermangelung einer „vollen Kenntnis" (Brosziewski 2015: 25) treffen. Diese Form der Präferenzbildung durch die bewusste Abwägung und Demonstration von Narrativen kann im vorliegenden empirischen Material beobachtet werden. Der Hinweis darauf erfolgt jedoch in erster Linie, um Möglichkeiten zu weiterer Forschung aufzuzeigen und ist kein weiterführender Bestandteil der Argumentation vorliegender Arbeit. Es kann beispielsweise anhand vorhandenem Textmaterial nicht vollumfänglich untersucht werden, in welchen Situationen Organisationen besonders zur Abwägung von

Einwirken kognitiver Institutionen, oder – bei schwächeren Zuständen der Institutionalisierung, die noch nicht zur Internalisierung geführt haben – durch Demonstration oder Diskussion von Normen, die sich aus dem Erfahrungsraum der Organisationen ergeben, beispielsweise des Vorrangs der Sicherheit und der Notwendigkeit der technischen Weiterentwicklung. Ebenfalls hinzukommen können spezifische Referenzen. Wenn beispielsweise Hellmann die „Eigendynamik der Einsatzrealität“ (Hellmann 2015: 203) als wichtige zu berücksichtigende Institution der Bundeswehr beschreibt, dann könnten in dieser Weise wirkende spezielle Institutionen auch in der Kooperation von Auslandsgeheimdiensten oder in der Polizeikooperation vorhanden sein. Zusätzlich möglich ist, dass die Organisationen durch die Wahrnehmung von Unsicherheit in der Entscheidungsfindung ihre Abstimmung unter narrativem Hinweis auf einige gesellschaftliche Bedarfe, und die Problematisierung anderer, bestreiten und somit als ‚Norm entrepreneur‘ kommunikativ-strategisch auftreten (DiMaggio 1988). Auch dann handeln sie jedoch nicht einzig aufgrund von Eigeninteressen, sondern werden vorrangig durch die Notwendigkeit, technischer Unsicherheit zu begegnen und dabei auch die Erwartungen der Organisationspartner nach einer gemeinsamen technischen Basis zu berücksichtigen, motiviert. Gerade in kulturell divergenten Kooperationsstrukturen können durch die Wirkung spezifischer, aber auch kulturell beeinflusster, Institutionen jedoch Konflikte entstehen, etwa, wenn sich (die einen) Organisationen aufgrund eines mangelnden Handlungsraums beschränken müssen, die Organisationen sich aber trotzdem – um Kompatibilität und Koordination zu und mit ihrem Kooperationspartner herzustellen – in gewisser Weise anpassen (müssen). Schwierig gestaltet sich dies insbesondere dann – und hier gelingt die Verbindung zwischen gesellschaftlichen Erwartungen und Unsicherheit – wenn die Organisationen geeignete Handlungsschablonen nicht abrufen können, da die gesellschaftlichen Erwartungen zur angemessenen Reaktion auf Strukturen oder andere Akteure divergent und damit nicht eindeutig regulativ, normativ oder habituell vorhanden sind und (auch in der Vergangenheit) nicht zu Organisationsfähigkeiten führen konnten, die (nun) – rein technisch betrachtet – für effektives und kompatibles Kooperationshandeln notwendig wären.

Den Neue Institutionalismus zeichnet also vor allem durch ein anderes Akteursverständnis und, in Koexistenz dazu, auch durch ein genuines Umweltverständnis aus. Anders als im Neoliberalen Institutionalismus verfügen die Akteure im Neuen Institutionalismus damit nicht

Narrativen neigen und wann nicht. Es wird vielmehr betont, dass Organisationspräferenzen aus mangelnder Kenntnis entstehen und dies in der Tendenz zu interorganisationaler Anpassung führt.

über freie Handlungskompetenz, die ‚Agency', sondern sind einem Prozess der exogen beeinflussten (Weiter-)Entwicklung von, als angemessen betrachteten, Handlungen und Strukturen ausgesetzt, nach denen sie sich ausrichten müssen. Nur in Auseinandersetzung mit diesen unterschiedlich wirkenden kulturellen Vorstellungen, die sich in diversen formalen und informellen institutionellen Handlungsrahmen und organisationalen Praktiken ausdrücken, können sie wissen, welche Maßnahmen für die Institutionalisierung ihrer Kooperation ergriffen werden können und müssen.[39] Die Institutionen, nach denen sich Organisationen richten, entstehen also auf der Ebene der Gesellschaft, haben jedoch auch Auswirkungen auf die Kooperation auf Organisationsebene, denn sie eröffnen organisationale Handlungsmuster und damit auch den Boden für interorganisationale Zusammenarbeit. Denn Gesellschaften sind unterschiedlichen historischen und gegenwärtigen Kontexten ausgesetzt, die maßgeblich ihren Erfahrungsraum prägen (Katzenstein 2008: 158 f.). Gesellschaftliche Erwartungen und damit organisationale Handlungskontexte bilden sich demnach erst in der Interpretation dieses kulturellen Raumes, der damit national-historisch entwickelt und daher materiell und immateriell nie völlig deckungsgleich zu dem anderer Gesellschaften ist.[40] Nicht nur Organisationen, sondern auch Gesellschaften besitzen demnach eine ‚Embedded agency', eine Handlungsfähigkeit, die sich nur in Auseinandersetzung mit kulturellen Regeln und Vorstellungen angemessenen Handelns verstehen lässt.[41] Diese Maßgabe gilt auch für die Kooperation, die damit auf einer Mesoebene stattfindet, einer Ebene, die sowohl von den Erwartungen der nationalen Gesellschaften, als auch vom Grad der Kongruenz und Inkongruenz dieser kulturellen Handlungsrahmen in der bi- und multilateralen Kooperationskonstellation, beeinflusst ist. Dabei sind Organisationen jedoch oft dem Dilemma ausgesetzt, dass sie sich – aufgrund unterschiedlicher gesellschaftlich Kontexte – den aus den kulturellen Kontexten ihrer Kooperationspartner entstehenden Kooperationserwartungen dieser Partner nicht (immer) beugen können, jedoch aus rein technischen Gründen zumindest marginal anpassen müssen, um eine in gewissem Rahmen noch legitime, aber gleichzeitig effektive

[39] Diese Annahme fußt auf der Wissenssoziologie von Berger und Luckmann (1977), auf die sich die Vertreter des Neuen Institutionalismus wesentlich beziehen (Walgenbach 2006: 355). Die Hauptaussage der Wissenssoziologie ist, dass Denken und Wissen sozial geprägt sind und somit von Gruppe zu Gruppe verschieden sein können.

[40] Organisationale Handlungsmuster haben also immer zugleich eine immaterielle und eine materielle Komponente. In der vorliegenden Arbeit, in der es um digitale, technische Lösungen von Sicherheitsbehörden geht, erhält dies gleich zweifach Bedeutung. Erstens sind Organisationen aufgrund ihrer kulturellen Herkunftskontexte mit unterschiedlichen kognitiven Handlungsprozessen ausgestattet, die Hofstede (1991) als ‚Software of the Mind' bezeichnet. Gleichzeitig verwenden sie auch in ihrer Handlungspraxis tatsächlich unterschiedliche Software in der Auswertung von Informationen.

[41] Dies schränkt die Handlungsfähigkeit von Organisationen jedoch nicht notwendigerweise nur ein. Denn erscheinen Organisationen in der Wahrnehmung ihrer gesellschaftlichen und organisationalen Umwelt legitim und erfolgreich, so können sie ihr Umfeld in gewissem Maße auch selbst mitgestalten und bemühen sich auch deshalb um Regeleinhaltung (Battilana 2006).

Kooperation zu gewährleisten. Aus den technischen Gegebenheiten der Kooperation ergeben sich damit gewissermaßen ebenfalls Erwartungen und somit eine zweite, von den Organisationen zu beachtende, Ebene der notwendigen Anpassung, bei der interpretiert werden muss, ob sie gesellschaftlich legitim wäre. Es findet in der internationalen interorganisationalen Kooperation also eine gleichzeitige Anpassung an nationale gesellschaftliche Legitimitätserwartungen und interorganisationale Effektivitätserwartungen statt.[42] Bildlich gesprochen ‚ziehen' beide Kontextebenen, die gesellschaftliche und die interorganisational-technische, an den sich in Kooperation befindlichen Akteuren und sie müssen beiden Ebenen zu einem gewissen Maße nachgeben. Die kulturelle Prägung der Organisationen führt somit gleichzeitig zu jeweils eigenen Technologien und Methoden, die in vorliegender Arbeit auch als ‚Organisationsdesigns' bezeichnet werden. Diese sind immer sowohl technisch als auch kulturell gestaltet und weisen materielle und immaterielle Bestandteile auf. Im Neuen Institutionalismus sind Kooperationen jedoch nie nur Formen unilateraler Organisation, sondern beinhalten eine soziale Konstruktionsleistung gemeinsamer Strukturen oder Praktiken und die potentielle Anpassung kulturell nur relativ stabiler Designs unter Abwägung dessen, welche kooperative Kompatibilität, hinsichtlich möglicherweise sehr unterschiedlicher Kontexte und Handlungsprogramme, denkbar ist.[43] Organisationen sind damit in der internationalen interorganisationalen Kooperation nicht (nur) als nationale, stabile Gebilde zu verstehen, sondern als Einheiten von Strukturen und Sub-Strukturen, die sich auch interorganisational (weiter)entwickeln. Bildlich gesprochen handelt es sich bei einer Organisation in der interorganisationalen Kooperation also um einen internationalen Organismus mit nationaler Nabelschnur, von der sie versorgt werden muss.

Zusammenfassend lässt sich also festhalten, dass erstens Akteure in einen Kontext eingebunden sind, der ihre Handlungen beeinflusst und somit einer eingebetteten Handlungsfähigkeit unterliegen. Dieser Kontext lässt sich als Kultur bezeichnen, die Auswirkungen auf die Reichweite des (möglichen) Organisationshandelns und den Erfahrungsraum der Organisation festlegt. Internationale Kooperation ist somit aufgrund potentiell divergierender kultureller

[42] Effektiv ist ein Verhalten dann, wenn es als Mittel zu einem gesellschaftlich definierten Ziel führt und dessen ausgelobtes Ausmaß und erwartete Qualität erreicht. Die Wirtschaftlichkeit fällt, anders als beim Terminus der Effizienz, höchstens nachrangig ins Gewicht.

[43] Diese Feststellung ermöglicht es, den Neuen Institutionalismus als theoretische Perspektive von der strategischen Kulturforschung abzugrenzen. Letztgenannte Methodik betrachtet Kultur als relativ stabil und sieht Veränderungen nur durch einen Bewusstseinswandel der Eliten möglich (Siedschlag 2006: 21). Der Neue Institutionalismus sieht dieses Veränderungspotential jedoch auch in der internationalen interorganisationalen Zusammenarbeit und, präzisiert in der vorliegenden Arbeit, auch durch die Wirkungen von Kongruenz und Inkongruenz institutioneller und technischer Erwartungen gegeben, die durch technische Unsicherheit verstärkt wird.

Hintergründe immer ein Kontext, in dem ein gewisser institutioneller und technischer Konsens erzielt werden muss. Die Umweltbedingung Unsicherheit wirkt dabei als allgemeine Bedingung des Organisationshandelns und wirkt sich auf die aktuelle Planbarkeit und die Zukunftsplanung von legitimem und effektivem Organisationshandelns aus. Akteurshandeln ist im Neuen Institutionalismus daher vom Organisationsverhalten der Interpretation und Reflexion der eigenen Reichweite sowie der Reichweite des anderen sowie den Möglichkeiten des eigenen und fremden Erfahrungsraums geprägt und geht mit habituellen Verhaltensmustern, aber auch mit der Demonstration und Diskussion geeigneter Maßnahmen mit anderen Akteuren auf unterschiedlichen Ebenen einher, wobei in vorliegender Arbeit vor allem die Ebene der Kooperation betrachtet wird. Daher lautet die untersuchungsleitende Annahme, dass die Kongruenz kulturell sehr ähnlicher Partner zu einer leichteren und tieferen Anpassung aneinander und daher auch zu ‚festeren' und damit weitreichenderen und habituellen Strukturen führt, als dies bei kulturell unähnlichen Organisationen möglich ist, dass aber auch ‚Inkongruenz als Motor für interorganisationale Anpassung' ein gewisses kooperatives Ergebnis erzielt, da diese mit einem praktischen und möglicherweise auch strukturellen Wandel in der als inkongruent dargestellten Organisation einhergehen kann.

Im Neuen Institutionalismus fehlt jedoch zunächst ein explizites Konzept für die internationale Kooperation. Zwar legt die Theorie durch die Kategorie der eingebetteten Handlungsfähigkeit fest, wie sich die Organisationen zueinander verhalten können. Sie können demnach nur in Auseinandersetzung mit ihrem kulturellen Kontext miteinander agieren. Es wird jedoch nicht ausgeführt, wie sich kulturell kongruente und divergente Akteure strukturell und praktisch miteinander organisieren können und ob dies zu Unterschieden in ihren Kooperationsstrukturen führt. Auch wird der Neue Institutionalismus meist so verwendet, dass mit ihm lediglich Organisationen innerhalb eines Staates – und wie sie sich zueinander verhalten – betrachtet werden können. Die Strukturen, in denen dann Kooperation entstehen, und in denen wiederum Kooperationsstrukturen gebildet werden, werden als ‚organisationales Feld' bezeichnet. So sind die Organisationen in einem organisationalen Feld der Organisation Krankenhaus beispielsweise das Krankenhaus selbst, die Krankenhausbetreibergesellschaft, die Krankenkassen, die Apotheken und Pharmakonzerne, gemeinnützige oder betriebliche Strukturen für Krankentransporte, aber auch das Parlament und die Regierung als wesentliche verwaltende und regulierende Einheiten des Krankenhausmarktes. Dies bilden sie jedoch nur, wenn sich eine gesteigerte Interaktion zwischen den Organisationen in der Form ausbildet, dass sich die einzelnen Einheiten strukturell aneinander anpassen und sich dem Feld zu einem gewissen Grad zugehörig fühlen. Das würde bedeuten, dass das Krankenhaus die

institutionellen Vorgaben der Betreibergesellschaft, dem Parlament und der Regierung, aber auch die Erwartungen der betrieblichen oder gemeinnützigen Krankentransportgesellschaften und der Medizinzulieferer insofern berücksichtigt, als dass sie, beispielsweise, passende Anfahrten und, dem medizinischen Material entsprechende, Lagerhaltungsmöglichkeiten und Personal bereit stellt, weil sie um deren Erwartungen weiß und sie als legitim betrachtet. Diese Anpassung an die Erwartungen alleine können jedoch nur dann zu einer steigenden Interaktion führen, wenn diese Art der Koordinierung nicht nur legitim ist, weil sie den jeweiligen Erwartungen entspricht, sondern, wenn sie auch in gewissem Maße technisch erfolgreich ist, wenn etwa durch dieses Zusammenwirken Produkte oder Dienstleistungen unterschiedlicher Art entstehen. Im gewählten Beispiel wäre dies die Verbesserung des Gesundheitszustandes der Patienten, ohne den das organisationale Feld Krankenhaus ein wesentliches Ziel verfehlt hätte und eine Anpassung der unterschiedlichen Akteure in einer abgestimmten ‚Produktionskette der Gesundheit' ineffektiv, und damit aus der Perspektive der Gesellschaft sinnlos verlaufen wäre.[44] Diese Unterscheidung einer legitimen Erwartungserfüllung auf der einen Seite und einer technischen Bedarfserfüllung auf der anderen Seite, in der die Erfüllung eines der Bereiche jedoch nie gänzlich ohne die Verwirklichung des anderen auskommt, wird im Neuen Institutionalismus auch in der Dichotomie der ‚institutionellen und technischen Felder' hervorgehoben. Ursprünglich sah die Theorie eine Trennung beider Kategorien als divergente Kontexte mit heterogenen Wirkungen vor. Während in technischen Feldern vor allem Marktbeziehungen bestehen und möglichst viele Produkte entstehen sollen, die an Bedarfsträger weitergegeben werden können, müssen sich Organisationen nach Meinung der frühen Neo-Institutionalisten in institutionellen Feldern vor allem nach Regelerfüllung richten (Scott/Meyer 1983: 149). Scott (1991: 167 f.) schlägt jedoch vor, institutionelle und technische Kategorien als Dimensionen der generellen Anpassung an Umwelten zu betrachten, zwischen denen immer eine gewisse Balance erreicht werden muss. Beide Bereiche stehen aber auch in komplexer Wechselwirkung, da eine Einführung eines Modells aus Effektivitätserwägungen im organisationalen Feld durch die breite Gefolgschaft vieler Organisationen oder besonders erfolgreicher Organisationen an Legitimität gewinnen kann (Becker-Ritterspach/Becker-Ritterspach 2006: 109). Somit ist die Anpassung von Organisationen im organisationalen Feld verwandt mit der Sozialisation im Sozialkonstruktivismus, in der Demonstration und

[44] Letztendlich zeigt sich auch in diesem Beispiel, dass nicht nur im Bereich der Sicherheitspolitik ein Spannungsfeld zwischen dem legitimen Ziel – in diesem Fall Gesundheit – und den Mitteln einer effektiven Bereitstellung desjenigen nachzuweisen ist. Denn auch Krankenhausbetreibergesellschaften und Pharmakonzerne sind nicht frei von gesellschaftlicher Kritik dahingehend, ob sie Gesundheit und effizientes ökonomisches Konzernhandeln verhältnismäßig in Balance bringen. Trotz dieser Kritik sind sie maßgebliche und unverrückbare Pfeiler einer gesamtgesellschaftlichen Gesundheitsversorgung.

Diskussion von als legitim betrachteten Praktiken zur Internalisierung von Verhalten führen (Brummer/Oppermann 2014: 59 f.). Daher muss berücksichtigt werden, dass Legitimität nicht nur durch die Gesellschaft ausgesprochen werden kann, sondern sich auch Akteure in der interorganisationalen Kooperation auf den Standpunkt stellen, Legitimität durch Demonstration und Diskussion verleihen zu können. Damit ist einerseits eine Anschlussfähigkeit des Neuen Institutionalismus an die sozialkonstruktivistische Theorieströmung der IB gewonnen. Andererseits kann der Ansatz dadurch erweitert werden, dass hervorgehoben wird, dass die Anpassung an die technische Umwelt aus Effektivitätsgründen durch Unterstützung weiterer Organisationen nicht nur den Status der Effektivität, sondern der Legitimität verliehen bekommt.

Aus den ausgeführten Gründen kann die Annahme, dass auch im Verhalten von Sicherheitsbehörden eine Ausrichtung an sowohl legitimen als auch technischen Dimensionen relevant ist, zur empirischen Untersuchung vorgeschlagen werden. Zur Prüfung dieser Auffassung ist es hilfreich, Organisationen als an drei Kontexte berücksichtigend zu begreifen, an die sie sich nachweisbar anpassen. Tabelle 5 verdeutlicht, dass Organisationen sich in der Konstruktion ihrer Wirklichkeit und damit ihrer Kooperationshandlungen und -strukturen mit ihrem internalisierten, selbstverständlichen Wissen, also geronnen, internalisierten Ideen und Praktiken, ihrer gesellschaftlichen und ihrer technischen Umwelt auseinandersetzen und dabei auf Anpassung an die von diesen inneren und äußeren Kontexten ausgehenden Erwartungen, insofern sie diese konkret interpretieren können, ausgerichtet sind (Klatetzki 2006; Becker-Ritterspach/Becker-Ritterspach 2006: 108 f.). Der Prozess der Institutionalisierung gerät in dieser Betrachtung zu einem Ablauf der Vertiefung und/oder Nicht-Vertiefung. Diese eben genannten Pole sind oder werden dadurch erreicht, dass eine Übereinstimmung in ‚Bündeln von interpretierten Erwartungen', die sowohl aktuell interpretiert werden als auch erfahrungsgeschichtlich verankert sind, entweder fehlt, durch technische Anpassung teilweise erreicht wird oder (bereits) vorhanden ist. Während die Anpassung an geronnene, internalisierte Praktiken habitualisiert ist, wird die Anpassung an die gesellschaftliche und technische Umwelt durch Demonstration und Diskussion von Normen begleitet.

Kontexte zur inneren und ggf. extern beobachtbaren Interpretation im organisationalen Feld	Begründung dieser kontextuellen Auseinandersetzung	Form der Anpassung aufgrund dieser kontextuellen Auseinandersetzung
Internalisierte Ideen und Praktiken	Erfahrungsraum	Umgang der Selbstverständlichkeit bezüglich Durchführung, Weiterführung und Weiterentwicklung der organisationalen Arbeit und Kooperation
Gesellschaftliche Umwelt	Handlungsraum	Interpretation der gesellschaftlichen Erwartungen bezüglich Verhältnismäßigkeit, vor allem bei neuen technischen Entwicklungen und weitreichenden Kooperationen, soweit dies möglich ist
Technische Umwelt	Entwicklungs- und Anpassungsraum	Interpretation der Notwendigkeit der sicherheitstechnischen Anpassung an allgemeine technische Entwicklungen, auch in Kooperationen

Tabelle 5: Beeinflussende Kontexte für Organisationen und mögliche beobachtbare Formen der Anpassung in ihren Handlungen.

Diese Präzisierungen ermöglichen es, die Dimensionen gesellschaftlicher und technischer Erwartungen als Ausprägung des bereits aufgezeigten Spannungsfeldes zwischen Legitimität und Effektivität zu betrachten und die damit verbundenen Auswirkungen auch in internationalen Umwelten, in einem interorganisationalen Feld der Kooperation, zu betrachten. Dadurch informieren die Annahmen über eine Anpassung von Organisationen an kulturell legitime und technisch effektive Erwartungen das Kooperationskonzept vorliegender Arbeit. Das aus der Auseinandersetzung mit diesen Kategorien und ihren speziellen Wirkungen entstehende internationale interorganisationale Kooperationsmodell kann als Erweiterung des Neuen Institutionalismus betrachtet werden und soll nachfolgend weiter konkretisiert werden.

3.2 Das internationale interorganisationale Kooperationsmodell als Weiterentwicklung des Neuen Institutionalismus

Das dominante positivistische Kooperationsverständnis in den IB ist wesentlich von der Vorstellung geprägt, dass die Akteure in ihrer Kooperation gemeinsame Interessen verwirklichen wollen und dabei einen gewissen Grad an Koordinierung erreichen (Keohane 1984: 51f.). Für den Neuen Institutionalismus, verstanden als konstruktivistische Kritik an dieser rationalistischen Position, folgt daraus eine Konzentration darauf, dass Organisationen in ihrer internationalen Zusammenarbeit diejenigen Ziele verfolgen, die sie aus der Interpretation der kulturell-institutionellen, aber auch der technischen Erwartungen ihrer Gesellschaften als ihre Interessen definiert haben und deren Umsetzung sie im Rahmen ihrer gesellschaftlich gewährten Reichweite und ihres technischen Erfahrungsraums in der Kooperation zu erreichen suchen, wobei sie stets sowohl eigene organisationale als auch gemeinsame interorganisationale Ziele verfolgen, die zu einem gewissen Maße sowohl deckungsgleich, als auch deckungsfremd sind.[45] Somit können sich Kooperation nur auf diejenigen Ziele erstrecken, die für die Gesellschaften der zusammenarbeitenden Organisationen überschneidend sind. Weit wesentlicher ist jedoch, dass sie sich in einer Koordinations- und Konstruktionsleistung auf gemeinsame Mittel einigen müssen, die von allen Gesellschaften akzeptiert werden können. Dadurch müsste die Kooperation für diverse Kooperationspartner unterschiedlich (eng) ausfallen, da nicht alle Ziel-Mittel-Kombinationen aufgrund unterschiedlicher kultureller Erfahrungsräume – und damit gesellschaftlicher Vorstellungen – gleich sind, selbst wenn die Organisationen vom gleichen technischen Umfeld und seinen Notwendigkeiten betroffen sind. Daher wird angenommen, dass dieser Inkongruenz durch unterschiedlich starke Teilhabe an (Gemeinschafts-)strukturen Rechnung getragen wird. Als Unterscheidungswert für enge – also weitreichender formal und informell institutionalisierte, aber vor allem habitualisierte – und weniger enge Kooperationsarrangements – die sich in einem Status der Diskussion und Demonstration legitimer Mittel befinden – wird somit der Zustand der Institutionalisierung festgelegt, wodurch vor allem die gleichwertige, Nutzung kompatibler Mittel Variabilität aufweist, da die Nutzung

[45] Im Neuen Institutionalismus generiert sich diese Überschneidung beziehungsweise Unterscheidung vor allem aus den nebeneinander bestehenden Konzepten des organisationalen Feldes (DiMaggio/Powell 1983), das von einer gewissen Schnittmenge und Interdependenz ausgeht und der gleichzeitig vorhandenen Annahme der ‚World polity', die die Anpassung an global gültige Normen, beispielsweise Management-Konzepte, auf der Makroebene untersucht (Krücken 2006). Durch die Mesoebene des organisationalen Feldes ist die Wirkung der Makroebene immer zu einem gewissen Teil mitberücksichtigt und muss thematisiert werden. Dies erfolgt in vorliegender Arbeit beispielsweise durch technische Erwartungen, da diese auch und vor allem auf die globale Struktur Internet und ihre Funktionslogiken rekurrieren. Näher betrachtet wird dieser globale Einfluss beispielsweise in Kapitel 5.3.

in einigen Fällen bereits internalisiert ist und in anderen nicht. Damit trägt die Untersuchung der angenommenen empirischen Realität Rechnung, wonach die Ziele von zeitgeschichtlicher Kooperation zwar vorrangig auf exogene Bedrohungslagen rekurrieren, die Definition geeigneter gemeinsamer Mittel – auch hinsichtlich der Notwendigkeit der Anpassung[46] an soziale, aber auch an technische Bedingungen – für Kooperationspartner aber aufgrund möglicherweise kulturell inkongruenter Herkunftskontexte der Organisationen eine Herausforderung darstellt.

Ein Kooperationsmodell nach dem Neuen Institutionalismus muss jedoch noch zwei weitere Bedingungen berücksichtigen. Zum einen müssen in der Zusammenarbeit mit anderen Organisationen auch diese als Umwelt behandelt und somit auch deren Erwartungen in gewissem Maße berücksichtigt werden. Hierauf wird gleich noch eingegangen werden. Zum anderen handelt es sich bei dem organisationalen Verhalten der Anpassung an gesellschaftliche Erwartungen nach Meinung der Neo-Institutionalisten immer um eine Tätigkeit, die nicht durch direkte spezifische Beauftragung abgewickelt wird, sondern durch Interpretation und Anpassung vonstattengeht (Becker-Ritterspach/Becker-Ritterspach 2006: 120; DiMaggio/Powell 1983: 141 f.). Daher gehen Organisationen einem eher allgemein gehaltenen gesellschaftlichen Auftrag, ausgedrückt durch die vertikale Anbindung an beauftragende und regulierende Organisationen, nach, der erst durch den Gesetzgeber und die Exekutive weiter spezifiziert wird, wobei auch diese beauftragenden Einheiten meist erst mit Verzögerung auf neue, vor allem auch technische, Erfordernisse reagieren (können), da das Wissen darüber ihrer Gruppe möglicherweise nicht zur Verfügung steht (Dreher 2016; Berger/Luckmann 1977). Für das organisationale Feld halten die Autoren der Theorieschule des Neuen Institutionalismus deshalb fest, dass nicht zu jeder Zeit erstens eindeutig bestimmbar ist, welche Erwartungen die Gesellschaft aufweist und zweitens, dass nicht zu jedem Zeitpunkt bereits fest habitualisierte geeignete methodische Modelle und strukturierte Verfahrensweisen für die Bearbeitung dieser Anforderungen vorhanden sind. Diese beiden Bedingungen können als Ausprägungen technischer Unsicherheit bezeichnet werden und sind von jeder Organisation zu bewältigen (DiMaggio/Powell 1983: 151 f.). Dafür sind Organisationen jedoch erneut an den Erfahrungsraum ihrer jeweiligen Gesellschaft gebunden. Treffen die Akteure hier auf einen Mangel an verfügbaren, institutionell vorgeprägten Handlungsmustern, so wird angenommen, dass sie versuchen, möglichst viele Hinweise auf erwünschtes und effektives Verhalten aus

[46] Die organisationale Anpassung an ihre technische und soziale Umwelt wird im Neuen Institutionalismus auch als Isomorphie bezeichnet (Becker/Ritterspach/Becker-Ritterspach 2006). Dieser Terminus wird in vorliegender Arbeit jedoch nicht verwendet, um die Begrifflichkeiten nicht weiter zu abstrahieren.

ihren eigenen Erfahrungen oder denjenigen des Kooperationspartners zu extrahieren. Die Unsicherheit ist demnach ein Phänomen, das Organisationen sowohl in ihrer vertikalen Auseinandersetzung mit ihren Gesellschaften, als auch in ihren horizontalen Beziehungen zu anderen Organisationen betrifft, die ihren Ausdruck in unpräzisen Legitimitätsbewertungen durch die Gesellschaft und damit erschwerten Interpretationsmöglichkeiten durch die Organisationen, sowie möglicherweise mangelnder organisationaler Erfahrung hinsichtlich effektiver Reaktion auf externe technische Bedingungen findet, und die deshalb einen allgemeinen Einflussfaktor auf Kooperationen jeder Art darstellt.

Technische Unsicherheit als Umweltbedingung stellt damit eine allgemeine, äußere Beeinflussung des Kooperationshandelns dar, mit der die Organisation in einer einseitigen Reaktionsbeziehung steht, in dem Sinne, dass sie die externen Faktoren nicht beeinflussen, sondern lediglich auf sie reagieren kann (Klatetzki 2006: 54). Besonders deutliche Auswirkungen hat sie auf die Möglichkeiten der Anpassung von Organisationen an ihre gesellschaftliche und ihre technische Umwelt, wie die beiden unteren Zeilen der Tabelle 5 bereits verdeutlichten. Demnach kann sie eine gegendynamische Wirkung auf die Anpassung von Organisationen an gesellschaftliche Erwartungen haben, da sie ebenfalls einen gewissen Zwang zur Anpassung an diese externalisierten Bedingungen fordert. Technische Unsicherheit hat damit das Potential, in inkongruenten Kooperationskonstellationen als ‚Anpassungskatalysator' zu wirken, da sie Kompatibilität als wichtigstes Ziel auslobt und daher kompatible Mittel, zumindest zu einem gewissen Maße, entwickelt werden müssen. Es lässt sich jedoch vermuten, dass sie graduell unterschiedliche Auswirkung je nach Konstellation der kooperierenden Akteure haben kann. Es wird nämlich davon ausgegangen, dass die Anpassung an technische Erfordernisse bei sehr ähnlichen Kooperationspartnern zu Tendenzen der Vereinheitlichung führt, da bereits ein sich überschneidender genereller gesellschaftlicher Konsens zu möglichen Handlungen besteht und damit ein fester Zustand der Institutionalisierung erreicht werden kann, der den beteiligten Kooperationspartnern einen gesellschaftlich legitimen und gleichwertig technisch effektiven Handlungsraum ermöglicht. In kulturell inkongruenten Partnerschaften ist jedoch weder dieser Konsens vorhanden, noch sind gleiche technische Handlungsmöglichkeiten zu erwarten. Daher ist anzunehmen, dass Akteure mit einem kulturell weniger großen Handlungsrahmen auch schlechter auf externe technische Erfordernisse reagieren können. Treffen sie nun auf einen Kooperationspartner mit einem, kulturell bedingt, größeren Handlungsraum, werden sie motiviert, beziehungsweise durch die organisationalen Erwartungen ihres Kooperationspartners zur Herstellung eines kompatiblen Handlungsraums zur Reaktion auf externe technische Bedingungen gewissermaßen gezwungen

sein, sich organisational in ihrer Handlungsfähigkeit in eine zum Kooperationspartner anschlussfähige Richtung in der Wahl ihrer Mittel entwickeln zu müssen. Dann werden Wandlungsprozesse dadurch angestoßen, dass die Erfahrungen der Partner zu divergent sind und bei dem Kooperationspartner mit dem geringeren Erfahrungsschatz eine Tendenz zur Anpassung an den erfahrenen Partner erfolgt.[47]

Diese unterschiedlichen Verläufe der Kooperation lassen sich erneut unter Rückgriff auf die Ausführungen von DiMaggio und Powell (1983: 148) zum organisationalen Feld schärfen. Die Autoren unterscheiden gewissermaßen zwei ‚Tiefengrade' der Kooperation, wobei sie organisationales Zusammenwirken hier als einen Prozess der Angleichung, vor allem an gesellschaftliche Erwartungen und an die technischen Erwartungen des Kooperationspartners, verstehen. Dabei unterscheiden sie, genau betrachtet, zwei Zustände der Institutionalisierung. Auf der einen Seite eine starke kognitive Verbundenheit von Akteuren, die ein gemeinsames Bewusstsein ihrer tiefen, bereits internalisierten, und wo dies nicht geschehen ist, erfahrungsgeschichtlich demonstrierten Verbindung aufweisen. Auf der anderen Seite ist der Zustand einer Akteursbeziehung vorhanden, die sich vor allem technisch durch eine gesteigerte Interaktion der Akteure auszeichnet. Letztere Kooperationsform lässt sich so interpretieren, dass die Organisationen keine gemeinsamen kognitiven, internalisierten Referenzsysteme vorweisen können, in Reaktion darauf aber einen technischen Kooperationsmodus konstruieren, mit dem die Organisationen versuchen, ihre Inkompatibilität hinsichtlich ihrer Mittel durch den Import von Mitteln oder die Entwicklung gemeinsamer Mittel auszugleichen und möglicherweise sogar durch strukturelle Wandlungsprozesse in ihren Organisationen zu verringern. Grundsätzlich ist dabei die Kooperation inkongruenter Organisationen nicht einzig eine Anpassung an die Erwartungen des Kooperationspartners, sondern gleichzeitig Ausdruck der Erwartung ihrer Gesellschaften, die die Erwartung an ihre Organisationen stellen, dass diese gemäß den externen technischen Entwicklungen effektiv handeln. Anpassung ist somit ein gleichermaßen vertikaler, wie auch horizontaler Prozess. Da die Gesellschaft ihre Organisationen (auch) damit beauftragt, aktuelle und zukünftige externe Entwicklungen in ihrem Organisationshandeln mit zu berücksichtigen und möglichst vielfältige und daher gesellschaftlich sinnvolle Kooperations- und Koordinationsstrukturen vorzuhalten, kann davon

[47] Scott (2014: 126 f.) spricht in diesem Zusammenhang von ‚Marginal Players' und meint damit Akteure in organisationalen Feldern, die sich, ausgelöst durch die Zurschaustellung neuer Methoden durch erfolgreichere Kooperationspartner, nun auch neue organisationale Formen und Handlungen vorstellen können. Hier kommt es also zu einem Bewusstseinswandel der ‚Eliten', wie ihn auch die strategische Kulturforschung als zentralen Schritt für Wandel auslobt. Allerdings ist der Prozess ein anderer, da der Bewusstseinswandel nicht innerhalb der Exekutive oder Legislative eines Staates durch eigene Reflexion heraus geschieht, sondern innerhalb einer ausführenden Organisation durch das Erfahren und Erlernen externer Modelle.

gesprochen werden, dass die Organisationen gegenüber ihren Gesellschaften zu Spezialisierung und technischer Weiterentwicklung aufgerufen sind. Wie bereits erwähnt, geraten diese Vorstellungen je nach kultureller Ausprägung, und hier vor allem je nach Handlungs- und Erfahrungsraum der Organisationen, zu unterschiedlichen Ausprägungen in den Methoden der Organisationen (Davies 2002; Gray 1988). Denn Organisationen mit gleichermaßen kulturell verankerter (großer) institutioneller Reichweite können zur Erfüllung dieser Erwartungen (bereits) fest institutionalisierte technische Strukturen oder Handlungsmodelle vorweisen, die Organisationen mit einem beschränkteren Kontext ohne Kooperation mit reichweitenstärkeren Organisationen nicht zugänglich waren oder sind. Einerseits können Akteure, deren Gesellschaften eine größere Erwartung an möglichst weitreichende technische Informationsverarbeitungsmodelle aufweisen, diese Modelle vorweisen, während andere Akteure Innovationen in diesem Bereich möglicherweise nicht bieten können.[48] Andererseits kann eine ‚lang gespürte Verbundenheit' zu einer bereits früh sehr weitreichenden gemeinsamen Modellierung von Organisationspraktiken geführt haben, die das kooperative Organisationshandeln zum Beobachtungszeitpunkt bereits sehr weitreichend macht. Daher lässt sich hier auch von einer kulturellen Pfadabhängigkeit sprechen, durch die Nachteile von, zum Beispiel durch fehlende Ressourcen beschränkten Organisationen, die aber gesellschaftlich betrachtet eine höhere Reichweite erreichen dürfen, durch Anpassung frühzeitig verschwanden oder schrittweise überwunden werden. Wenn sich Akteure also in einem bilateralen oder multilateralen Kooperationsverhältnis gegenüberstehen, muss in der empirischen Betrachtung zweierlei berücksichtigt werden, um den Grad der Institutionalisierung ihrer Kooperation ausreichend untersuchen zu können: die kulturelle Kongruenz oder Inkongruenz, die kulturellen Grenzen einer Anpassung an technische Erfordernisse und technische Unsicherheit.

Da sich vorliegende Arbeit darauf konzentriert, legitimes und effektives Handeln von Organisationen als Spannungsfeld sowohl für Organisationen, aber durch deren Wechselseitigkeit auch für die Gesellschaft betrachtet, muss durch einen Exkurs hervorgehoben werden, dass der Grad der Institutionalisierung der Kooperation strukturelle und praktische Folgen für Gesellschaften haben kann. Wenn beispielsweise eine Organisation aufgrund mangelnder Erfahrung und in der Kooperation zu einem kulturell inkongruenten Partner auf die Übertragung entsprechender Techniken und Methoden durch den Kooperationspartner angewiesen ist, kann sie, erstens, in eine Situation der Abhängigkeit und der Verpflichtung

[48] Zilber (2006) arbeitete beispielsweise heraus, dass die gesellschaftliche Wahrnehmung von digitaler Technologie die Möglichkeit der in Israel ansässigen Unternehmen, effektive Businesslösungen in diesem Bereich anzubieten, deutlich erhöhte. Ähnliche Beobachtungen ließen sich auch auf den Sicherheitsbereich übertragen.

geraten. Daher ist bei der Prüfung des Grades der Institutionalisierung auch darauf zu achten, ob das Kooperationsverhältnis eine Form von Gleichwertigkeit der Partner oder Abhängigkeit aufweist. Zweitens kann die Bewältigung technischer Unsicherheit für Organisationen mit einer weniger großen kulturellen Reichweite auch als dynamisierendes Element verstanden werden. Denn da Kultur sich in Festlegungen darüber ausdrückt, welche materiellen Artefakte und immateriellen Sachverhalte in einer Gesellschaft Bedeutung erhalten und welche Handlungen daraus abgeleitet werden können (Klatetzki 2006; Zucker 1983: 2), erweitert die Auseinandersetzung mit (neuen) Technologien und damit verbundenen Ansätzen das kulturell Denkbare – durch Austausch mit inkongruenten Kulturen mit größerem Erfahrungsschatz – und kann dadurch neue Handlungen ermöglichen. Somit unterliegen stabile kulturelle Hintergründe in der Kooperation durch die Interaktion mit kulturell divergenten Akteuren immer auch dem Potential des Wandels. Die nationale Sicherheitskultur erhält damit eine dynamische, durch internationale Kooperation beeinflusste, Determinante, die kulturell verankerte methodische und immaterielle Wissensbestände möglicherweise verändern kann. Daher wird die kulturelle Kongruenz oder Inkongruenz in dieser Arbeit als Start- und relative Vertiefungsbedingung der Kooperation aufgefasst, die die Möglichkeiten einer institutionalisierten Vertiefung der Kooperation zwar bereits in gewisser Weise festlegt, in deren Umsetzung der Überwindung technischer Unsicherheit jedoch auch dynamisierendes Potential für die Kooperation und für die beteiligten Organisationen vorhanden ist. Aus den bisherigen Ausführungen können in Tabelle 6 die Bedingungen des internationalen interorganisationalen Kooperationsmodells für kulturell kongruente und kulturell inkongruente Konstellationen in Bezug auf die unterschiedlichen Dimensionen institutioneller und technischer Umwelten dargelegt werden.

Art der Kooperations-beziehung	Theoretische Annahmen des internalisierten Grades der Kooperation in der institutionellen Dimension unter Berücksichtigung der Umweltbedingung technischer Unsicherheit	Theoretische Annahmen des internalisierten Grades der Kooperation in der technischen Dimension unter Berücksichtigung der Umweltbedingung technischer Unsicherheit
Kongruenz	Bündelung (gemeinsamer) – auf Erfahrung und Handlungsraum basierender – methodischer und technischer Reichweite und kognitiver, daher auch sozialer, Verbundenheit. Durch gesellschaftlich gestützte große Reichweite, gleichwertige Möglichkeit der Entwicklung von Handlungsmodellen zur gegenwärtigen und zukünftigen Bedarfserfüllung.	Weitreichende Modelle zur Beherrschung externer technischer Faktoren sind vorhanden, daher hohe gesellschaftliche Bedarfserbringung. Technische Unsicherheit wird als gleichberechtigt zu bewältigende Herausforderung interpretiert, die unter Rückgriff auf die technisch erfolgreichsten Modelle erfolgt.
Inkongruenz	Beschränkung eines Partners durch kulturell bedingte mangelnde Erfahrung und geringe Reichweite. Einschränkende Bindung an gesellschaftliche Erwartungen und/oder oder das Fehlen von Handlungsmodellen führt zur Anpassung an das Modell des modellübertragenden Partners.	Da nicht beliebig viele Methoden zur Verfügung stehen, passt sich der ‚gesellschaftlich und technisch beschränktere' Kooperationspartner an die Organisation(en) mit der größeren Reichweite und den dadurch erfolgreicheren technischen Handlungsmodellen an, die die jeweilige Organisation als effektiv demonstriert.

Tabelle 6: Theoretische Annahmen über die Art der Kooperationsbeziehungen in der institutionellen und technischen Dimension.

Kooperation wird dieser Beschreibung folgend in vorliegender Arbeit als internationales interorganisationales Handeln begriffen. Diese Perspektive erweitert die in der Disziplin der IB

gängige Betrachtung der Makroebene der Kooperation. Nach deren Annahme arbeiten Staaten in einem spezifischen Themengebiet (‚Issue area') durch multilaterale Vereinbarungen zusammen und bilden hierfür internationale Organisationen (DiMaggio/Powell 1991: 3ff.). Die Regimetheorie geht zwar von gemeinsamen Grundannahmen, Verhaltensstandards, spezifischen Verhaltensvorschriften und verabredeten Prozeduren aus (Hasenclever et al. 1997: 9; Krasner 1983), allerdings beziehen sich diese auf Regelungskonflikte zwischen Staaten[49], wohingegen der Neue Institutionalismus davon ausgeht, dass die internationale Kooperation eine interorganisationale Zusammenarbeit von Organisationen und damit eine logische Konsequenz der menschlichen Grundeigenschaft des Organisierens ist (Gukenbiel 1995). Dadurch wird analytisch eine Mesoebene dargestellt, die Organisationen als in Makrosysteme, aber auch in Beziehungen zu horizontalen organisationalen Subsystemen, wie beispielsweise organisationale Felder mit anderen Organisationen, eingebettet und mit ihnen in Austausch befindlich, sieht. Die in Tabelle 6 dargestellten Arten der Kooperationsbeziehung und ihre empirisch beobachtbaren Auswirkungen zeigen bereits, dass eine Untersuchung interorganisationaler Kooperation erstens wissenschaftlich notwendig und zweitens empirisch möglich ist. Dabei ist es besonders wichtig festzuhalten und herauszuarbeiten, dass Kongruenz und Inkongruenz durch interorganisationale Anpassungsprozesse eine dynamische und damit nur relativ stabile Beziehung aufweisen. Gleichzeitig müssen sowohl die Folgen dieser Anpassung als auch die unterschiedlichen Wirkungen vorhandener Kongruenzen und Inkongruenzen so dargestellt werden, dass Prozesse und ihre Ergebnisse, aber auch eindeutige Zustände und Unterschiede aufgezeigt werden können, um überhaupt reliabel und valide auf maßgebliche Faktoren schließen zu können. Daher soll im Folgenden das Forschungsdesign vorliegender Arbeit dezidiert ausgeführt und diskutiert werden.

3.3 Vorgehensweise in der Anwendung des internationalen interorganisationalen Kooperationsmodells

Um möglichst aussagekräftige Ergebnisse hinsichtlich der Kooperation von Sicherheitsbehörden und der Ausrichtung der Zusammenarbeit an der Interpretation gesellschaftlicher Erwartungen, technischer Erfordernisse und, damit verbunden, technischer Unsicherheit zu erzielen, wurde die vorliegende Arbeit methodisch als ein ‚Most different systems design' (MDSD) angelegt. Diese Methodik ermöglicht die Einbindung und Gegenüberstellung divergierender systemischer Bezugsysteme, beispielsweise

[49] Daun (2011: 174) hält zudem fest, dass gerade die Intelligence durch das Fehlen von internationalen Regimen gekennzeichnet ist. Auch gemessen an dieser Aussage erscheint das Vorhaben, die Kooperation von Sicherheitsorganen nicht auf der Makro-, sondern auf der Mesoebene zu untersuchen, sinnvoll.

Regierungssysteme, unter Annahme der Gültigkeit gleicher oder ähnlicher beeinflussender Faktoren (Anckar 2008). Mittels der Auswahl nach MDSD wurden Fälle mit unterschiedlichen Voraussetzungen einander gegenübergestellt, wobei als Unterscheidungsmerkmale divergierende Akteurskonstellationen sowie Problembereiche angewendet wurden. Als Fall wird hierbei eine Untersuchungseinheit bezeichnet, die eine bi- oder multilaterale Sicherheitskooperation auf Organisationsebene abbildet. Die divergierenden Bezugsysteme der einzelnen Fallstudien ergeben sich zum einen aus der Berücksichtigung verschiedener Organisationsformen – Nachrichtendienste und die Plattform der europäischen Polizeikooperation Europol – und zum anderen aus den unterschiedlichen Werten – also, Erscheinungsformen – der kulturellen Inkongruenz der beteiligten Organisationen. So wird zunächst, im ersten Fall, die multilaterale Kooperation zwischen der US-amerikanischen NSA und den Auslandsnachrichtendiensten Großbritanniens, Kanadas, Neuseelands und Australiens untersucht, deren Kultur homogen ist, da sich die Staaten alle dem Kulturraum Anglo-Amerika zurechnen, die Sicherheitskulturen der Länder ihren Nachrichtendiensten eine große Reichweite der Organisationsaktivitäten und eine große technische Erfahrung zugestehen und daher ihre Kooperation mit kompatiblen Techniken und eine Vertiefung der Kooperationsstrukturen einher gehen müsste. Da gerade die Kooperation der NSA und des britischen GCHQs in der Forschung jedoch als besonders habitualisiert und reichweitenstark eingeschätzt wird (Westerfield 1996; Richelson/Ball 1985), soll diese Annahmen durch eine dezidierte Hervorhebung dieser bilateralen Akteurskonstellation in einer vergleichenden Einzelfallstudie, einer ‚Within case analysis'[50], noch einmal überprüft werden, um testen zu können, ob in dieser, sehr fest institutionalisierten Kooperation gleichwertiger Partner keine Faktoren wirken, die von den dargelegten Prämissen abweichen und über diese hinausreichen, sowie um nachvollziehen zu können, ob die theoretisch abgeleiteten Annahmen anhand dieses Falls weiter empirisch konkretisiert werden können. Gleichzeitig dient die Einzelfallstudie als Test dafür, ob hinreichend davon auszugehen ist, dass die identifizierten Erklärungsfaktoren relevant sind. Denn da beide Partner effektive Handlungsmodelle entwickelt haben, ist es nötig zu überprüfen, ob dies auch mit einer kognitiven Verbundenheit und einer Gleichwertigkeit zusammenhängt, da ansonsten die aufgebaute Argumentation nicht haltbar wäre. In der dritten Fallstudie zur Kooperation der NSA mit dem deutschen BND und in der vierten Fallstudie zur Kooperation der Ermittlungsbehörden der EU-Mitgliedsstaaten mit der europäischen Polizeiagentur Europol kann dann die Auswirkung der Divergenz der kulturellen Hintergründe

[50] Within cases sind eine nützliche Methode, um Zusammenhänge zwischen abhängiger und unabhängiger Variable noch kleinteiliger zu erforschen (Evera 1997: 51 f.).

näher betrachtet werden. Es muss außerdem hervorgehoben werden, dass in den untersuchten bi- und multilateralen Organisationskooperationen methodisch jeweils eine Fokalorganisation gewählt wurde. Deren Dominanz rekurriert zum einen auf die zur Verfügung stehenden Dokumente, sodass in den Kooperationsfällen, welche die NSA beinhalten, zu dieser Organisation und ihren Interpretationen die meisten Informationen vorliegen. In dem Untersuchungsfall Europol wurde diese Organisation als Fokuspunkt gewählt, da eine Konzentration auf alle mit ihr in Verbindung stehenden Organisationen kein einheitliches Bild ermöglicht hätte. Zum anderen resultiert die Position der Fokalorganisation aber auch aus der Rolle, die diese Organisation in den Kooperationen einnimmt. So stellt die NSA sich selbst in allen ihren Kooperationspartnerschaften als zentrale Organisation dar, während dies bei Europol ebenfalls der Fall ist. Diesem Umstand muss aufgrund der Gefahr von Verzerrungen Rechnung getragen werden.[51] In jeder Falluntersuchung werden dann unterschiedliche Kooperationsstrukturen dargelegt und die aus der Theorie extrahierten Erklärungsfaktoren der kulturell beeinflussten gesellschaftlichen Bindung von Organisationen und ihrer Kongruenz oder Inkongruenz in der Kooperationskonstellation (als erste unabhängige Variable) und der Wirkung der Umweltbedingung der technischen Unsicherheit (als zweite unabhängige Variable) sowie deren Zusammenwirken als Erklärung für die jeweils empirisch vorhandenen Strukturen eingeführt und hinsichtlich ihrer Aussagekraft und Schlüssigkeit diskutiert. Während King, Keohane und Verba (1994: 117) vorschlagen, einen beobachtbaren Faktor in seiner Wirkung auf ein Ergebnis zu testen, wird in vorliegender Arbeit so verfahren, dass zwei Erklärungsfaktoren aus dem Neuen Institutionalismus extrahiert werden, wobei ein Faktor ein eher stabileres Element – die Kultur – aufweist und ein Einflussfaktor hinsichtlich einer möglicherweise dynamisierenden Wirkung durch Anpassung aufgrund der Notwendigkeit der kooperativen Anpassung an externe technische Bedingungen, wo das aus Gründen kooperativer Effektivität nötig ist, geprüft werden soll. Für die Erörterung, welche Auswirkungen kulturelle Kontexte nach den Annahmen des Neuen Institutionalismus auf die Kooperation haben können, erweist sich, wie bereits eingangs erwähnt, die Unterscheidung der institutionellen und technischen Dimension der Erwartungserfüllung als hilfreich, die in der internationalen Kooperation nicht nur für die Gesellschaft, sondern auch für die Kooperationsumwelt – also andere Organisationen – und hier vor allem technisch, erbracht werden muss. Dieses Ziel der Erwartungserfüllung, das sich in der Interpretation, textlichen Reflexion und Diskussion der institutionellen und technischen Erwartungen ausdrückt, ist – so die Annahme – im

[51] Gliederungspunkt 5.2 nimmt darauf noch einmal ausführlich Bezug.

ausgewerteten Material nachweisbar. Es wird erwartet, dass die Organisationen – wie in Tabelle 7 dargelegt – ihre Anpassung an Erwartungen und technische Notwendigkeiten explizit diskutieren und ihre Handlungen und Strukturen damit begründen oder, dass sie diesen Erwartungen implizit folgen und sich das Streben nach Erwartungserfüllung und strukturellen Anpassung in der habituellen Ausrichtung der Organisation ausdrückt. Für das Vorhaben vorliegender Arbeit ist es daher notwendig zu prüfen, ob für alle oder einige dieser Annahmen konkrete empirische Ergebnisse festzustellen sind und ob diese als maßgeblich für die beobachtbaren Kooperationskonstellationen angenommen werden können. Während der Diskurs[52] zur Anpassung – in vorliegender Arbeit auch als soziale Konstruktion der Kooperation bezeichnet – explizit festgestellt werden kann, müssen für die habituelle Erwartungserfüllung Rückschlüsse darüber gezogen werden, ob die Handlungen als Ausdruck von Erwartungen gelten können. Eine Ausrichtung an der technischen Dimension lässt sich durch eine explizite Diskussion nötiger organisationaler Mittel für die Bewältigung einer solchen Anforderung, über deren Legitimität, oder eine implizite Anpassung der Organisationshandlungen an ein externes technisches Umfeld herausarbeiten.

Theoretische Kategorie	Empirisch beobachtbarer Vorgang
Institutionelle Dimension	Explizite Diskussion oder implizite Befolgung gesellschaftlicher Erwartungen.
Technische Dimension	Explizite Diskussion nötiger organisationaler Mittel zur Bewältigung technischer Anforderungen oder implizite Anpassung der Handlungen an ein externes technisches Umfeld.

Tabelle 7: Operationalisierung der Prämissen der gesellschaftlichen Bindung und technischen Anpassung.

Hierbei wird angenommen, dass die kulturelle Inkongruenz die größte Schwierigkeit in dieser Kooperation ausdrückt, wie die Annahmen in Tabelle 6 bereits hervorheben, die Anpassung aufgrund technischer Unsicherheit die Konstruktion der Kooperation jedoch ebenfalls maßgeblich beeinflusst und somit in einigen Untersuchungsfällen ebenfalls dynamische Anpassungsprozesse erwartet werden. Es wird davon ausgegangen, dass der Grad der

[52] Der Begriff des Diskurses wird hier nicht im Sinne der Diskursanalyse verwendet, die von einer maßgeblichen Einflusswirkung der Narrative bestimmter Gruppen und der darin zum Ausdruck kommenden Begrifflichkeiten ausgeht (Alvesson/Karreman 2000). Vielmehr wird in vorliegender Arbeit unter dieser Bezeichnung eine sprachliche Auseinandersetzung der Organisationen miteinander über angemessene Mittel der Kooperation verstanden.

kulturellen Kongruenz und die damit verbundenen Möglichkeiten der kognitiv und technisch kompatiblen Kooperationsausführung Auswirkungen darauf haben, wie stark sich die Organisationen aneinander anpassen können beziehungsweise angepasst haben und damit auf ihre gesellschaftlichen und gegenseitigen interorganisationalen Erwartungen, die letztlich wiederum die Interpretation von gesellschaftlichen Bedingungen darstellen, reagieren können. Es wird angenommen, dass es inkongruenten Akteuren schwerer fällt, sich auf eine habituell deckungsgleiche Struktur zu einigen – da keine diesbezügliche kognitive Grundlage vorhanden ist – und eine gleichwertige Teilhabe an Strukturen zu gestalten sowie durchzusetzen, da die jeweiligen Vorstellungen zu diesen Strukturen zu divergierend sind, beziehungsweise die gesellschaftlich bedingten Möglichkeiten der Nutzung inkongruent ausfallen. Zurückkommend auf den in Gliederungspunkt 3.1 eingeführten Lebenszyklus der Norm verfügen kongruente Akteure dann über geronnene, also internalisierte, gemeinsame Institutionen, während inkongruente Kooperationspartner Normen diskutieren, demonstrieren und gegebenenfalls importieren müssen. Daher können sich kulturell kongruente Akteure leichter auf einige reichweitenstarke sowie gleichzeitig legitime und effektive Strukturen einigen, also beispielsweise auf gemeinsame Datenbanken, Datenweiterleitungssysteme und Aufklärungsprojekte, in denen die Rollen der partizipierenden Organisationen gleichwertig und habitualisiert sind, da eine kognitive Selbstverständlichkeit der Gleichheit und dadurch Verbundenheit besteht. Demnach ist nicht entscheidend, ob die gesellschaftlichen Erwartungen an die bi- oder multilateralen Kooperationspartner gleich sind. Grundlegend ist, dass die gesellschaftlichen Erwartungen sich an einem ähnlichen oder gleichen gesellschaftlichen Selbstbild orientieren und so Reichweite und Erfahrungsraum der Organisationen (mit)bestimmen. Ausgedrückt in der sozialkonstruktivistischen Terminologie konstruieren kulturell kongruente Partner eine intersubjektive Einigung, dass sie sich in Bezug auf die Unterscheidung zwischen ‚dem Selbst' und ‚dem Anderen' eher als Teil eines ‚kollektiven Selbst' begreifen (Wendt 1992: 399) und dadurch der Möglichkeitsraum, eine selbstverständliche, internalisierte Verbundenheit zu haben und dieser durch Kooperationspraxis Ausdruck zu geben größer ist als dies bei inkongruenten Partnern der Fall wäre. Die Wirkung der generellen Umweltbedingung für sowohl kongruente als auch inkongruente Kooperationskonstellationen, die technische Unsicherheit, stellt jedoch auch in dieser Konstellation eine grundsätzliche Herausforderung für Organisationen dar und ist damit ein dynamisierendes Element für jede Kooperationsbeziehung. Allerdings wird angenommen, dass kulturell kongruente Organisationen in ihrer Kooperation eine höhere Wahrscheinlichkeit aufweisen, Erfahrungs- und Handlungsmodelle für komplexe technische Bedarfe vorzuhalten,

wobei zugegeben werden muss, dass in vorliegender Arbeit eine kulturell kongruente Gruppe analysiert wurde, die mit einer großen Reichweite ihrer Organisationshandlungen planen kann. Theoretisch wäre es aber genauso möglich, dass eine kongruente Gruppe mit kongruenten gesellschaftlichen Erwartungen hinsichtlich einer organisationalen Selbstbeschränkung auftritt, für die dementsprechend begrenztere Strukturen angenommen werden könnten, wobei auch hier davon auszugehen wäre, dass die Form der Kooperation internalisierte Institutionen aufweist und dadurch einen tiefen Grad der Institutionalisierung aufweist. In vorliegendem Forschungsdesign werden sowohl stabile als auch dynamisierende Faktoren jedoch nicht als Kausalfaktoren für Kooperationsstrukturen oder strukturelle Organisationsanpassung begriffen, sondern werden im Sinne sozialkonstruktivistischer Forschung lediglich als maßgebliche Einflüsse identifiziert, deren angenommene Wirkungen auf Strukturen durch dichte Beschreibung dargelegt werden müssen. Geleitet wird die Untersuchung von der Frage: *„Warum sind einige Kooperationen weitreichender institutionalisiert und weisen eine gleichwertigere Teilhabe der Kooperationspartner an Kooperationsstrukturen auf als andere?“*. Hierbei wird angenommen, dass Kooperation unterschiedliche Grade der Institutionalisierung aufweisen kann. Sie kann entweder sehr eng sein und eine kognitive Verbundenheit symbolisieren, sie kann aber auch eine Interaktion darstellen, bei der nur geringer, nicht gleichwertiger, Austausch vorhanden ist und der auch von Nicht-Kooperation in anderen organisationalen Teilbereichen begleitet werden kann.

Zusätzlich muss hervorgehoben werden, dass aufgrund der konstruktivistischen Grundannahmen keine trennscharfe Abgrenzung zwischen den gewählten unabhängigen Variablen – der kulturellen Kongruenz und Inkongruenz und der Bewältigung technischer Unsicherheit – und den unterschiedlichen Werten der abhängigen Variablen – den jeweiligen Strukturen der Kooperation und, damit einhergehend, den divergierenden Zuständen zwischen Interaktion und Verbundenheit – vorgenommen werden kann, da sich sowohl unterschiedliche Strukturen, als auch Akteure und Strukturen wechselseitig bedingen. Zudem kann auch die Festlegung auf den Zustand der Institutionalisierung der Kooperation nie objektiv eindeutig erfolgen, da gesellschaftliche Organisationsformen und Gesellschaft immer einem dynamischen Wandel ausgesetzt sind (Seidel 2015; Mense-Petermann 2005; Giddens 1984).[53]

[53] Vorliegende Arbeit konnte aufgrund einer abweichenden Fokussetzung auf die Wirkungen von Kongruenz und Inkongruenz – und nicht vordergründig auf den Wandel – die Formen und Hinweise eines möglichen organisationalen Wandels in einigen Fällen nicht näher untersuchen. Vorstellbar wäre jedoch, dass Veränderungen hinsichtlich der Kongruenz oder Inkongruenz durch Typologisierungen der Strukturen und Aktivitäten der Organisationen zu einem gewissen Zeitpunkt und durch die Varianz des Zeitrahmens näher ergründet werden könnten (Collier/Seawright 2008; Elman 2005; Mahoney/Thelen 2002). Erschwert wird eine solche Untersuchung aber sicherlich dadurch, dass nicht eindeutig feststellbar ist, ob Wandel alleine auf nationaler Ebene oder durch

Ebenfalls hervorgehoben werden muss, dass durch die sozialkonstruktivistische Annahme der Wechselseitigkeit zwischen Akteur und Struktur unabhängige Wirkfaktoren zugleich Bestandteil des Ergebnisses ihres Wirkens sind.[54] So lässt sich die kognitive Verbundenheit aufgrund kultureller Kongruenz gleichzeitig als Typologisierung des Untersuchungsfalls und damit als Startbedingung der Untersuchung, als unabhängige Variable und als Kooperationsergebnis fassen, denn die Anfangsverbundenheit und die Wirkung der Verbundenheit führen im Ergebnis zu mehr Verbundenheit. Die Argumentation scheint sich somit im Kreis zu drehen und in der empirischen Beobachtung keine neuen Ergebnisse zu liefern. Zentral ist sie jedoch dann, wenn hervorgehoben werden soll, dass Akteure nicht interessengeleitet, sondern stabil ‚eingebettet' handeln. Dies ist erstens eine wertvolle Erkenntnis für die Prognose, wie sich Akteure angesichts neuer Herausforderungen verhalten werden und welche Auswirkungen das, zweitens, vor allem für Akteure hat, die nicht Teil dieser kognitiv verbundenen Organisationsgruppe sind, aber vielleicht passiv von ihren Handlungen betroffen sind. Drittens ist zentral, das technische Unsicherheit – und hier vor allem die Notwendigkeit der Reaktion auf externe technische Bedarfe, aber auch auf die konfligierenden, und damit nicht eindeutigen Gesellschaftserwartungen – eine variable Schnittmenge zwischen kongruenten und inkongruenten Akteuren erlaubt, verbunden mit der Gefahr oder Chance, dass hier eine Anpassung der Organisationsstrukturen, und damit möglicherweise auch ein Wandel im Gesellschaftsgefüge, entstehen kann. Viertens wird durch die Wahl einer recht komplexen zweiten unabhängigen Variable dem Umstand Schuldigkeit getan, dass Organisationen von einer multikontextuellen Umwelt betroffen sind und somit auch die Einflussfaktoren nicht zu eindimensional gewählt werden dürfen (Senge/Hellmann 2006: 19). Daher ist die technische Unsicherheit als eine Variable gewählt worden, die die empirische Wechselwirkung zwischen technischer organisationaler Reaktion und der gesellschaftlichen Bindung berücksichtigt. Denn Technik ist immer in eine Gesellschaft eingebunden, da sie aus ihr hervorgeht.

Vorliegende Arbeit konzentriert sich damit auf sehr spezifische Zusammenhänge und Wirkungen des Organisationshandelns. Deren Annahmen wurden jedoch aus einem größeren Theoriegebäude entlehnt. Daher folgt die Vorgehensweise der zugrundeliegenden Untersuchung weitestgehend einer Struktur der deduktiven Erklärung, deren Prämissen sich aus dem Neuen Institutionalismus ableiten (Tönnesmann/Alemann 1995: 40). Es soll jedoch darauf

Effekte der Globalisierung hervorgerufen wird. Denn so bestehen zwar in unterschiedlichen Ländern Divergenzen ihrer organisationalen Ausprägung, aber auch gewisse Gemeinsamkeiten, hervorgerufen durch international gültige Normen (Katzenstein 2012b).

[54] Für die Darstellung des Untersuchungsprozesses dieser Arbeit wurden die unabhängigen und abhängigen Variablen also (künstlich) getrennt.

hingewiesen werden, dass die deduktive Anwendung einer Theorie die Gefahr birgt, weitere maßgebliche Faktoren, die nicht durch das Theoriesystem abgebildet werden, zu vernachlässigen. Daher ist die vorliegende Arbeit als Perspektive auf die organisationale Kooperation in der Sicherheitspolitik und nicht als alleinige Erklärung für Organisationshandeln zu verstehen, da sie weder eine holistische, noch eine generalisierbare Erklärung liefern kann und dies auch nicht angestrebt wird. Vielmehr wird durch die Vorgehensweise eine kritische Prüfung und gegebenenfalls Erweiterung und Präzisierung der Theorie durch den Test der Erklärungen, ihre Präzisierung und die Beschreibung der jeweiligen empirischen Ausprägung angestrebt. Tabelle 8 fasst die in dieser Arbeit betrachteten Untersuchungseinheiten, Arten der Kooperationsbeziehung, untersuchte empirische Kooperationsstrukturen und die erwarteten Ergebnisse unter Berücksichtigung der theoretischen Annahmen zur Art der Kooperationsbeziehungen noch einmal zusammen.

Untersuchungseinheit	Art der Kooperationsbeziehung	Untersuchte Kooperationsstrukturen	Erwartetes Ergebnis unter Berücksichtigung der theoretischen Annahmen zur Art der Kooperationsstrukturen aus Tabelle 6
Erster Fall (4.1) NSA und ‚Five Eyes'	Kongruent	WINDSTOP ICREACH TICKETWINDOW	Enge kognitive Verbundenheit, daher gleichwertige Möglichkeiten, weitreichende, effektive Modelle zu entwickeln oder an ihnen teilzuhaben.
Zweiter Fall (4.2) NSA und GCHQ	Kongruent	QUANTUMTHEORY REMNATION II GVE-Aufklärung	Effektive Handlungsmodelle, da kognitive Verbundenheit und gleichwertige Teilhabe an Strukturen.
Dritter Fall (4.3) NSA und BND	Inkongruent	Joint SIGINT Activity (JSA) EIKONAL XKEYSCORE	Kompatibilitätsprobleme aufgrund unterschiedlicher gesellschaftlicher Kontexte und mangelnden Erfahrungsraums des BND. Der ‚eingeschränktere' Partner BND passt sich an die erfolgreichere NSA an.
Vierter Fall (4.4) Europol	Inkongruent	EIS AWF SIENA	Keine kognitive Verbundenheit, daher keine gleichwertigen Möglichkeiten, weitreichende, effektive Modelle zu entwickeln und eine inkongruente Teilhabe an Strukturen. ‚Stärkere' Ermittlungsbehörden und Europol als Akteur nutzen die Europol-Struktur als Übermittlerin von Methoden.

Tabelle 8: Theoretische Annahmen über die Art der Kooperationsbeziehungen und deren erwartete empirische Auswirkungen.

Aufgrund der Konzentration auf kulturelle Faktoren und ihre Auswirkungen in der Kooperation von Sicherheitsorganisationen lässt sich vorliegende Arbeit in das Forschungsprogramm der Sicherheitskulturforschung eingliedern. Ihm liegt die Fokussierung auf die gesellschaftliche Bedeutung von Sicherheit zugrunde, die explizit auch die Beobachtung eines Wandels in dieser Beziehung berücksichtigt. Daher strebt der Forschungsansatz an, Kultur nicht nur als stabiles Konstrukt – resultierend aus historischen Erfahrungen – zu betrachten, sondern auch das Wandlungspotential durch Dynamiken der Kooperation und externer technischer Entwicklungen zu berücksichtigen (Daase 2012). Diese Zielsetzung übernimmt die vorliegende Arbeit, indem sie die kulturelle Kongruenz oder Inkongruenz im Sinne einer relativ stabilen kulturellen Pfadabhängigkeit begreift, welche den Zustand der Institutionalisierung zunächst entweder vertiefend unterstützt oder – bei Inkongruenz – beschränkt. Die konkrete Umsetzung der Kooperation wird jedoch nicht nur von diesen beeinflussenden Bedingungen geprägt, sondern richtet sich ganz wesentlich auf das Ziel einer dynamischen Reaktion auf aktuelle und zukünftige technische Bedingungen aus, die – unter Reflektion der kulturellen Bedingungen – technisch prozesshaft bewältigt und begleitet werden müssen. Vorliegende Arbeit kann der Forschungsrichtung der Sicherheitskulturforschung durch den Fokus auf die Prämissen des Neuen Institutionalismus zudem die Perspektive hinzufügen, dass Sicherheitspolitik im 21. Jahrhundert wesentlich durch die gesellschaftliche Eigenschaft des Organisierens geprägt ist und damit darauf hinweisen, dass zeitgeschichtliche politische Entwicklungen zunehmend durch die gesellschaftliche Tendenz geprägt sind, technische Lösungen für Probleme zu finden und dabei Gefahr läuft, auszublenden, dass Technik eigene Herausforderungen, Probleme und drängende gesellschaftliche Fragestellungen entstehen lassen kann (Maschewski/Nosthoff 2018). Die Angliederung an die Sicherheitskulturforschung ermöglicht darüber hinaus eine Einbettung der Arbeit in das methodische und terminologische Bezugsystem des Sozialkonstruktivismus. Das Vorgehen entspricht einer qualitativen Analyse, die die „Organisation von Wirklichkeit“ (Daase 2012: 35) als Prozess der Wechselseitigkeit von Akteur und Struktur betrachtet, der unterschiedliche Ausprägungen der Institutionalisierung aufweist und die durch die Organisationen in Dokumentenmaterial textlich ausgedrückt wird. Somit findet die Methodik Anschluss an die sozialkonstruktivistische Schule der IB insofern, als sie sich mit der intersubjektiven Konstruktion sozialer Realität auseinandersetzt (Brummer/Oppermann 2014: 51 f.; Boekle et al. 1999). Nach dieser Auffassung können die Akteure ihre Kooperation nur in der interpretativen Auseinandersetzung mit den immateriellen Strukturen, in die sie und andere eingebunden sind, sowie der komplexen materiellen Struktur, die sie zur Erfüllung ihrer gesellschaftlichen Aufgabe beherrschen müssen, gestalten und

müssen zur funktionierenden und legitimen Kooperation eine gewisse formale und informelle Übereinkunft, aber auch ein bewusstes Verständnis mit dem und für den Kooperationspartner, erzielen. „What matters (…) is the competence of actors to interpret themselves and the world and to share these interpretations with others“ (Katzenstein 2008: 159). Daher ist die Interpretation immaterieller und materieller Bedingungen sowie die Wahrnehmung und Umsetzung geronnener Ideen und Praktiken im Sinne des Neuen Institutionalismus eine zentrale Akteursmotivation und ein maßgebliches Akteurshandeln, dessen Ergebnis eine gleichzeitig relativ stabile, aber gleichzeitig auch relativ dynamische Kompatibilität und Inkompatibilität mit national-organisationalen und interorganisationalen Anpassungstendenzen ist. Diese Feststellung erscheint zunächst paradox, ist aber nicht nur theoretisch entwickelt, sondern zuletzt den Beobachtungen der empirischen Realität geschuldet sowie der politikwissenschaftlichen Notwendigkeit, internationalen Veränderungspotentialen den Raum einzugestehen, die sie in einem Zeitalter schneller und komplexer technischer und gesellschaftlicher (Weiter-)Entwicklung verdienen. Zusammengefasst destilliert sich aus den dargelegten Zusammenhängen von kulturell-gesellschaftlichen Bindungen und technischen Erfordernissen, die kognitiv gespeichert sind oder aktiv interpretiert werden müssen und nach denen gehandelt wird oder werden muss, ein allgemeines Vorgehen, das in Abbildung 3 noch einmal verdeutlicht wird. Dieses Schema wird in allen Fallstudien wiederholt, um das Vorgehen zu gliedern und die Ergebnisse der Einzelstudien vergleichbar zu gestalten. Zusätzlich werden die Validität und Reliabilität der aus dieser Untersuchung extrahierten Erklärungen in jeder Fallstudie zusätzlich durch eine Dokumentenkritik auf mögliche Verzerrungen hin geprüft, da die Akteursmotivation, das Akteurshandeln sowie deren Auswirkung auf (institutionalisierte) Strukturen nur anhand begrenzt vorhandenem Textmaterial ergründet und ausgewertet werden kann. Hierbei wird kritisch dazu Stellung genommen, welcher Grad an Objektivität und Vollständigkeit der dargestellten Vorgänge im zitierten Textmaterial angenommen werden kann (Rappert 2015; 2014; 2010; George/Bennett 2005: 99 f.). Dadurch wird dem Umstand Rechnung getragen, dass die Studie Quellen nutzt, deren Herausgabe nicht unumstritten ist und deren Texte Lücken aufweisen können.[55]

[55] Für eine umfassende Auseinandersetzung mit dem Gehalt, den Auswirkungen und der Reaktion auf die ‚Leaks‘ von Edward Snowden vergleiche Dörr/Diersch 2017, Walsh/Miller 2016 und Johnson et al. 2014.

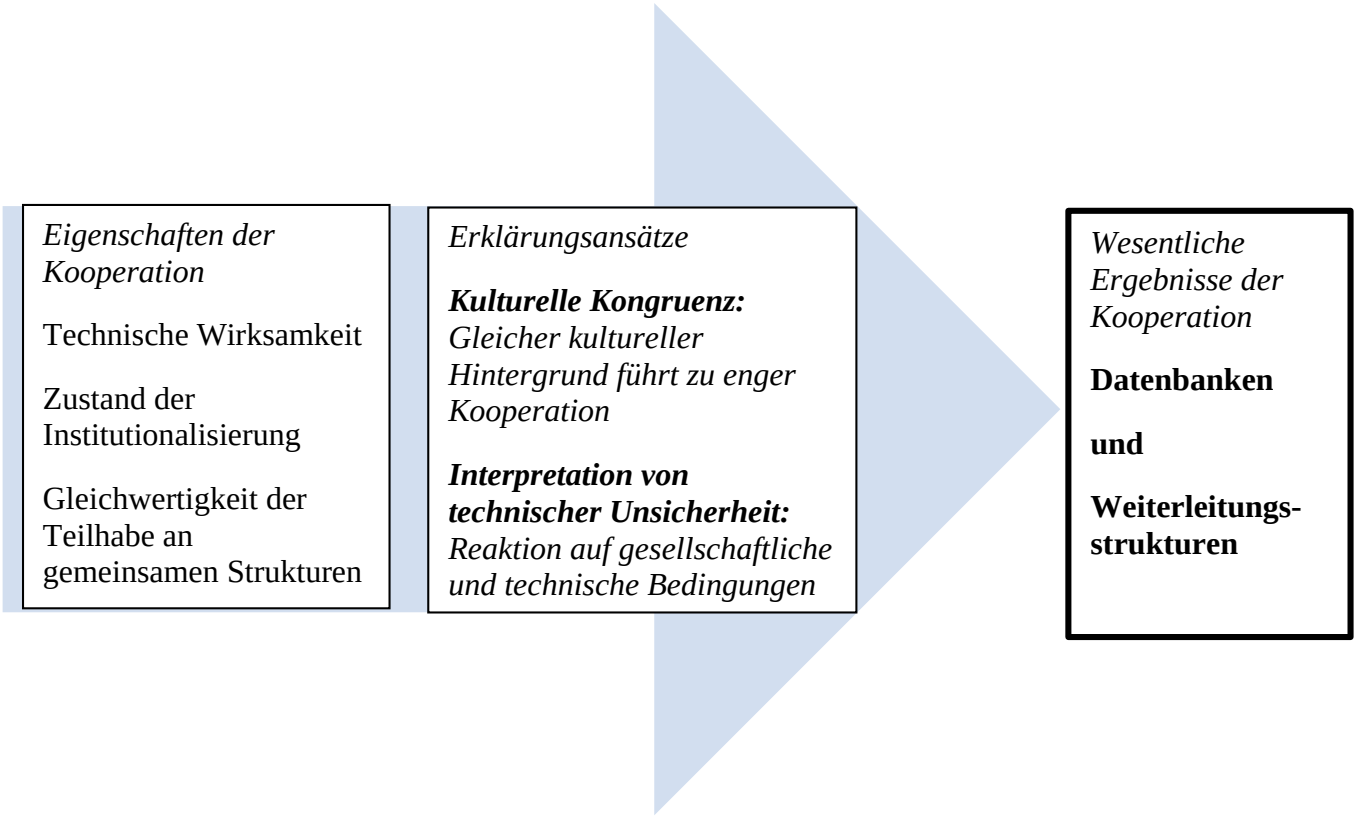


Abbildung 3: Erklärung der interorganisationalen Kooperation.

4. Analyse der Kooperation bei Nachrichtendiensten und Polizei

> "[XKEYSCORE] has become so important because with it, analysts can downsize their gigantic shrimping nets to tiny, handheld goldfish-sized nets and merely dip them into the oceans of data, working smarter and scooping out exactly what they want."
>
> *Anonym*

Die Ausrichtung an gesellschaftlichen Erwartungen unter der Prämisse der gleichzeitigen Berücksichtigung technischer Erfordernisse spielt eine entscheidende Rolle für den Zustand der Institutionalisierung der Kooperation und die gleichwertige Teilhabe an nachrichtendienstlichen und polizeilichen Kooperationsstrukturen. Weitgehende Untersuchungen mit institutionalistischen Forschungsansätzen, die dieser Auffassung gerecht werden, sind jedoch bislang unterblieben. Offenbar wird die Notwendigkeit einer Analyse aber bereits durch die empirische Betrachtung der Reichweite der Strukturen zur Verknüpfung und Weiterleitung vielfältiger Datentypen. Gleichzeitig wird jedoch deutlich, dass internationale Datenstrukturen in Zeiten transnational digital vernetzter Akteure auch eine gewisse technische Notwendigkeit ausdrücken. Vorliegende Arbeit beleuchtet deshalb den Fall der Geheimdienstgruppe Five Eyes – die Kooperation zwischen National Security Agency (NSA) der USA, dem britischen Government Communications Headquarters (GCHQ), dem Communication Security Establishment Canada (CSEC), dem australischen Defense Signals Directorate (DSD) und dem neuseeländischen Government Communications Security Bureau (GCSB) (Abschnitt 4.1). Anschließend wird, aufgrund einer vorhandenen Binnenstruktur innerhalb dieser multilateralen Struktur, der vergleichende Einzelfall der Zusammenarbeit zwischen NSA und GCHQ näher erklärt (Abschnitt 4.2). Darauffolgend verändert sich in der Betrachtung der Kooperation der NSA mit einem Drittpartner, dem deutschen Bundesnachrichtendienst (BND), die unabhängige Variable der kulturellen Ähnlichkeit, da die Kooperationspartner – anders als bei den Five-Eyes-Partnern – stark inkongruent sind (Abschnitt 4.3). Sicherheitskooperation findet jedoch nicht nur zwischen Geheimdiensten statt und weist eine immer stärkere Verschränkung auch zu Polizeien auf. Daher werden die Ergebnisse der transatlantischen Geheimdienstkooperation mit der europäischen Polizeikooperation im Rahmen von Europol kontrastiert, um die Zentralität der Konstruktion

der Kooperation auch in der Polizeizusammenarbeit sowie deren kulturell und technisch bedingte Varianzen in diesem Kontext zu untersuchen (Abschnitt 4.4).

4.1 Die Kooperation der Five Eyes

Die Kooperation der NSA mit ihren anglophonen Partnerdiensten ist auf historisch gewachsene und gefestigte Beziehungen zurückzuführen. Die Entwicklung der Five Eyes begann bereits 1943 mit dem ‚BRUSA Agreement', welches zwischen dem US-amerikanischen Verteidigungsministerium und der British Government Code and Cypher School[56] geschlossen wurde.[57] Es stellte vorrangig eine Kooperation auf dem Gebiet der technischen Aufklärung dar. Fortgeführt wurde diese Vereinbarung 1946 durch das ‚UKUSA Agreement', das die gemeinschaftliche SIGINT-Aufklärung der USA und Großbritanniens weiter institutionalisierte, später ergänzt durch die SIGINT-Dienste Kanadas, Australiens und Neuseelands. Seit 1998 treten die genannten Dienste als gemeinsame Gruppe – als Five Eyes – auf: „Although NSA has had bilateral relationships with individual Second Party countries going back to the 1940's and 1950's, we did not have any group (5-EYES) partnership until 1993" (National Security Agency 2003d).[58] Aufgrund dieser Bedeutung gilt es im Folgenden, die technischen Strukturen der Kooperation zu spezifizieren, die als deren zentrale Ergebnisse aufgefasst werden. Im Rückgriff auf das Analyseschema der vorliegenden Arbeit lässt sich die Erklärung dieser institutionalisierten Zustände der Kooperation innerhalb der Five Eyes synoptisch darstellen, indem die wesentlichen ‚Outcomes' der Kooperation, WINDSTOP, ICREACH und TICKETWINDOW, durch das Zusammenwirken von kultureller Kongruenz und der Interpretation von technischer Unsicherheit erklärt werden (Abbildung 4).

[56] Diese im Ersten Weltkrieg gegründete Organisation ist der Vorläufer des heutigen GCHQs.
[57] Die diesbezüglichen Dokumente sind inzwischen der Öffentlichkeit freigegeben. Sie können über die offizielle Webseite der NSA abgerufen werden: https://www.nsa.gov/news-features/declassified-documents/ukusa/
[58] Dokumente, die Kooperationsinhalte betreffen oder Informationen über Einzelprojekte enthalten, wobei Informationen hierzu jedoch mit den Partnern geteilt werden sollen, werden mit der Bezeichnung FVEY versehen. Welche formalen Schritte die Five Eyes 1993 und 1998 konkret vollzogen haben, ist nicht bekannt.

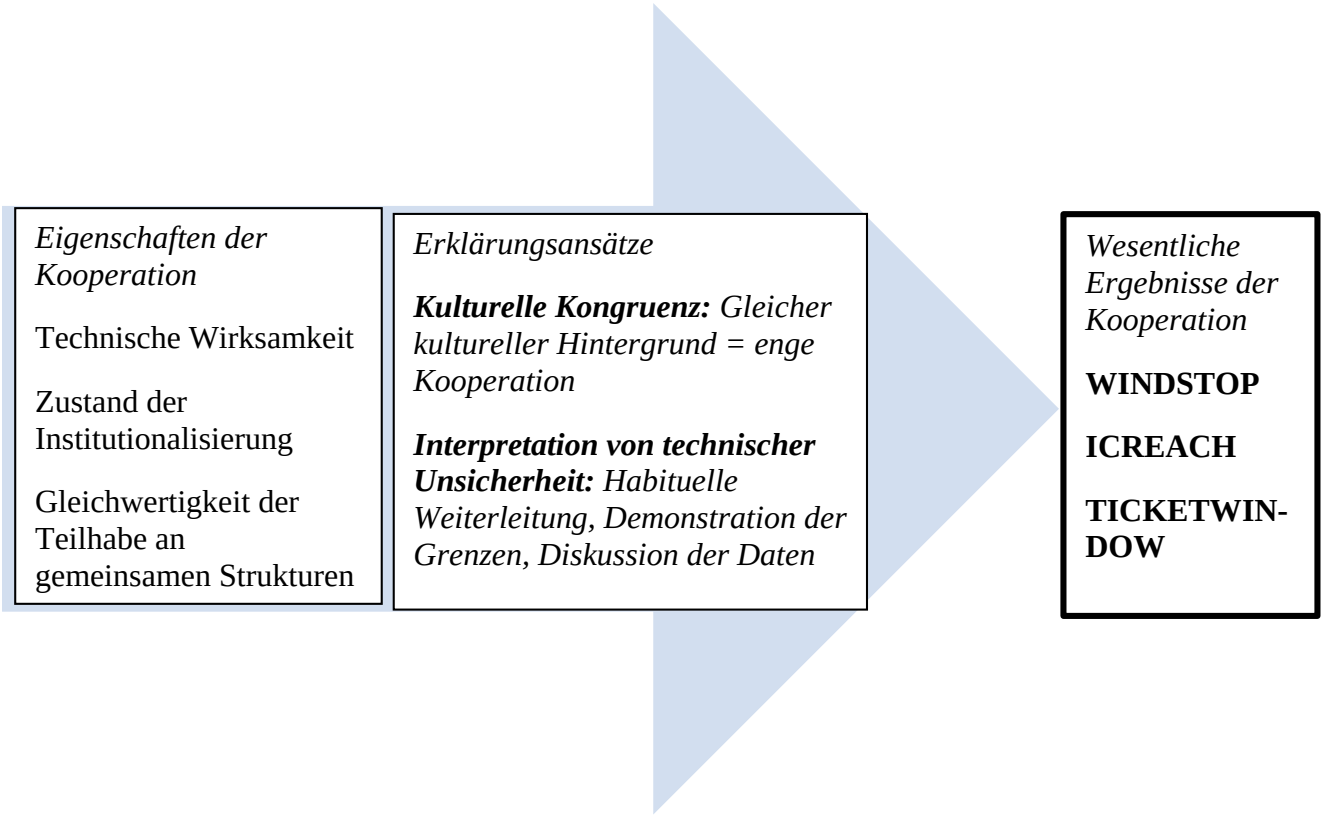


Abbildung 4: Erklärung der interorganisationalen Kooperation der Five Eyes.

Zum Verständnis der Inhalte und Strukturen von WINDSTOP, ICREACH und TICKETWINDOW ist zunächst eine Darstellung ihrer Funktionsweise notwendig. Es zeigt sich, dass die Strukturen einen großen Umfang an Daten verfügbar und besonders sensible Informationen besser vernetzbar machen (Abschnitt 4.1.1). Dadurch entsteht eine wirksame und enge Kooperation, die vor allem durch die kulturelle Ähnlichkeit der Akteure und eine sich darin ausdrückende kognitive Verbundenheit erklärbar ist (Abschnitt 4.1.2). Die Schaffung gemeinsamer Regeln sowie die Gestaltung der Programme sind jedoch maßgeblich auch auf die Interpretation gesellschaftlicher Erwartungen sowie deren Übereinbringung mit organisationalen Reaktionsmöglichkeiten auf technische Bedingungen zurückzuführen (Abschnitt 4.1.3). Letztlich lassen sich aus den Snowden-Dokumenten wesentliche Erkenntnisse über die Routinen der Five Eyes, deren Institutionalisierung und die Wirkung kultureller Prägungen erschließen. Die Schlussfolgerungen aus dem fragmentierten Material sollen jedoch noch einmal kritisch bewertet werden (Abschnitt 4.1.4).

4.1.1 Die Wirksamkeit der Kooperation: Gleichwertige Nutzung von Zugängen und Weiterleitungsstrukturen

Organisationen gehen nach den Annahmen des Neuen Institutionalismus dann eine Zusammenarbeit ein, wenn sie eine gewisse Wirksamkeit gegenüber einzelstaatlichen

Lösungen verspricht und eine institutionalisierte Form aufweist, die den gesellschaftlichen Erwartungen entspricht. Daher bleibt zunächst zu prüfen, ob die gemeinsamen Datenbanken und Datenweiterleitungssysteme wirksam sind, bevor in einem zweiten Schritt geprüft werden kann, ob sie für alle Partner übereinstimmend mit kulturellen Vorstellungen sind, sie dementsprechend gleichwertig an ihnen teilhaben, ob diese Teilhabe internalisierten Abläufen folgt und ob die Organisationen dabei effektiv auf externe technische Bedingungen reagieren können, ohne zu fürchten, gegenüber ihrer Gesellschaft illegitim zu handeln. Um einen sowohl gesellschaftlichen als auch technisch sinnvollen Mehrwert erzielen zu können, müssen technische kooperative Strukturen somit zunächst Daten erschließen, Daten verknüpfen oder Daten weiterleiten. Dies dient dem Zweck, durch Kooperation ein möglichst weitreichendes (durch viele Daten), ein möglich verständliches (durch Verknüpfung unterschiedlicher Datentypen, die dann zu Erkenntnissen führen können) und ein möglichst vernetztes (wenn andere Akteure Daten erhalten, können sie entweder ihr eigenes Erkenntnisbild schärfen, oder dem weiterleitenden Akteur zusätzliche Informationen zukommen lassen, um dessen Wissen zu vergrößern) Maß zu erreichen. Anhand dieser Punkte lässt sich also der effektive Erfolg der Kooperation für die beteiligten Organisationen messen. Die, in den Snowden-Dokumenten behandelten Kooperationsstrukturen der Five Eyes, müssen also zunächst hinsichtlich dieser Determinanten untersucht werden.

Die Erschließung von Daten gelingt dadurch, dass Zugänge an Internetkommunikationsinfrastrukturen – vor allem Glasfaserkabeln – genutzt werden. Dies kann grundsätzlich mit oder ohne Zustimmung des jeweiligen Kooperationspartners geschehen. Die NSA beispielsweise behält sich ausdrücklich vor, auch eigenmächtige Zugänge zu Glasfaserkabeln zu erschließen. Zu diesem Zweck hält die NSA eine Auflistung der ihr bekannten Kabel weltweit vor. Eine verdeckte Operation ist jedoch nicht immer notwendig. Denn auch Kooperationspartner ermöglichen die Infiltration der Datenarchitekturen auf ihrem Territorium. Daher wird angenommen, dass gerade bei einer größeren Anzahl von Zugangspunkten die Kooperation vor einer groß angelegten verdeckten Aktion bevorzugt wird, wenn sie technisch sinnvoll und gesellschaftlich legitim ist. In das Netz der Partnerzugänge WINDSTOP sind alle Five-Eyes-Partner und, durch eine hohe Anzahl von bereitgestellten Zugängen, besonders Großbritannien fest eingebunden. WINDSTOP ermöglicht das Abfangen von Kommunikation aus Europa und dem Mittleren Osten (National Security Agency 2014d). Zusätzlich zu der geographischen Reichweite steigt die technische Wirksamkeit dadurch, dass WINDSTOP erstens mehrere Zugänge umfasst und, zweitens, unterschiedliche Datenformate durch das Netz an Zugangspunkten zugänglich gemacht werden können. Darunter fallen

beispielsweise E-Mail-Verkehr, Informationen zu Internetverhalten, Chatprotokolle und Voice-over-IP-Gespräche und ihre Metadaten. Die durch WINDSTOP erbrachten Daten müssen dann in Datenbankstrukturen und Datenweiterleitungssysteme eingebracht werden, um die Erkenntnisse der Kooperationspartner gegenüber einer einzelstaatlichen Aufklärung gleichwertig zu erhöhen. Wie viele Daten in das System durch welchen Partner eingebracht werden, ist jedoch im Zeitraum 2005 bis 2010 durchaus unterschiedlich (National Security Agency 2007c; National Security Agency 2007d). Deshalb muss – obwohl die Wirksamkeit der Struktur grundsätzlich aufgrund des Mehrwerts in den eingangs definierten Bereichen der Erschließung, Verknüpfung und Weiterleitung bestätigt werden kann – die Tiefe der Kooperation hinsichtlich einer gleichwertigen Nutzung weiter überprüft werden. Zusätzlich muss untersucht werden, ob eine solche Zugänglichkeit auch für TICKETWINDOW besteht. Die Struktur besteht seit 1999 und wird durch die NSA als Steigerung zuvor bestehender Austauschprozesse betrachtet:

> „Simply put, TICKETWINDOW is the sharing of sensitive-source collection with Partners; the exchange of sensitive source data that had not been shared with Partners under normal circumstances. This project has made excellent SIGINT available to the International Intelligence Community[59], enabling many product reports to be written that would not have been otherwise available" (National Security Agency 2003g).

Über TICKETWINDOW werden für die Five-Eyes-Partner Informationen über die afghanische Armee, den Mittleren Osten, Teile des afrikanischen Kontinents und europäische Kommunikationen verfügbar, die die NSA durch die Zusammenarbeit mit der polnischen Regierung unter der US-Coverbezeichnung[60] ORANGECRUSH gewinnen konnte (National Security Agency 2014l). Doch nicht nur die Daten aus der Auslandsaufklärung der Five Eyes fließen in TICKETWINDOW ein. Auch aus den jeweiligen bilateralen Kooperationspartnerschaften mit Drittpartnern können Informationen in die Struktur eingebracht werden. Die NSA bezeichnet TICKETWINDOW daher als „truly (…) international effort!" (National Security Agency 2003g). Auch die Struktur ICREACH hat einen besonderen Wert für die NSA. Über sie können die Daten aus der Kooperation mit den Five-Eyes-Partnern auch an über 100 Analysten der anderen 23 US-amerikanischen Geheimdienste weitergeleitet werden (National Security Agency 2010b; 2007c; 2007d).[61] Ob diese Weiterleitung auch den

[59] Es wird vermutet, dass sich der Begriff International Intelligence Community auf unterschiedliche US-Einrichtungen in Partnerstaaten, die entweder unilateral oder bilateral betrieben werden, bezieht.
[60] Der polnische Name für das Programm ist BUFFALOGREEN (National Security Agency 2014l).
[61] Nach gängiger Zählung besteht die amerikanische Intelligence Community aus 16 Diensten, wobei das übergeordnete ‚Office of the Director of National Intelligence (ODNI)' häufig als 17. Organisation bezeichnet wird (Diersch 2017: 67). Zu der aus den Snowden-Dokumenten zitierten Anzahl müssen demzufolge entweder Geheimdienste mitgezählt werden, die der Forschung nicht bekannt sind, oder auch Ober- und Untereinheiten hinzugenommen werden.

anderen Organisationen möglich ist, ist nicht bekannt. Ersichtlich ist jedoch, dass die Struktur als Weiterleitungsplattform der durch die Five-Eyes-Auslandsnachrichtendienste an die NSA weitergereichten Daten dient (National Security Agency 2007d). Zusammenfassend kann jedoch festgestellt werden, dass die dargestellten Datensammel- und Speicherungssysteme hinsichtlich der Maßgabe einer gewissen Datenmenge, Datenweiterleitung und Datenvernetzung technisch wirksam sind und durch Narrative der erfahrungsgeschichtlichen Wirksamkeit – etwa durch den Hinweis auf erzielte Datenmengen und die potentielle Reichweite dieser Daten – getragen werden. Da die Kriterien der Kooperation nicht nur Wirksamkeit, sondern auch Übereinstimmung mit dem (gemeinsamen) gesellschaftlich-kulturellen Kontext und mit der Notwendigkeit, sich an technische Bedingungen anzupassen beziehungsweise eine Interpretation der gesellschaftlichen Grenzen dieser Anpassung vorzunehmen, voraussetzt, muss geprüft werden, ob auch diese Bedingungen in der Kooperation empirisch erfüllt sind und ob sie als maßgebliche Erklärungen für die eingangs beschriebenen Strukturen dienen können.

4.1.2 Alles wird geteilt: Die internalisierte und demonstrierte Kontinuität der SIGINT-Aufklärung

Der Neue Institutionalismus geht davon aus, dass kulturell kongruente Organisationen, aufgrund einer ähnlichen kognitiven Wirklichkeitskonstruktion, in Form von Erfahrungsraum, Handlungsraum und Entwicklungs- und Anpassungsraum, eine gleichberechtigte und eine sowohl technisch, als auch gesellschaftlich Mehrwert schaffende, Kooperation aufbauen können und dabei nicht nur eine starke Interaktion, sondern auch eine soziale Verbundenheit erreichen können. Eine solche Zusammenarbeit würde dann in gleichwertigem Zugang zu Datenbanken, einer gewissen Institutionalisierung und einer großen Reichweite kooperativer Lösungen kulminieren. Daher muss nachfolgend zunächst geprüft werden, ob eine kulturelle Ähnlichkeit und eine daraus bereits resultierende Startbedingung der kognitiven Verbundenheit zwischen den Five-Eyes-Staaten überhaupt gegeben ist, hinsichtlich der auch eine strukturelle Form anzunehmen ist.

Die USA, Großbritannien und Kanada spannen gemeinsam den kulturellen Raum Anglo-Amerika auf (Bell 2012; Katzenstein 2012a). Auch Neuseeland und Australien rechnen sich der Anglosphäre zu (MacDonald/O'Connor 2012: 200; Pauly/Reus-Smit 2012). Diese Behauptung einer kulturellen Verbindung muss jedoch zusätzlich durch spezifische kulturelle Gemeinsamkeiten konkretisiert werden (Hofstede 2001: 25 f.) Es kann zunächst davon ausgegangen werden, dass sowohl die gesellschaftliche Akzeptanz einer großen Reichweite

nachrichtendienstlicher Tätigkeiten eine Relevanz für die nachrichtendienstliche Arbeit, und daher auch für den Grad der Ähnlichkeit oder Unähnlichkeit von Kooperationspartnern hat. Hinsichtlich der Legitimität expansiver Strategien und Aktivitäten der Geheimdienste lassen sich daher zumindest für Großbritannien und die USA Gemeinsamkeiten feststellen (Klavehn/Müller 2008; Peine/Sturm 2008). Jedoch lassen sich auch diese Befunde weiter zuspitzen, denn der Handlungsraum beeinflusst die Modelle der jeweiligen Mitarbeiter in ihrer konkreten Arbeit und so können kulturelle Merkmale letztendlich auf eine – hier so bezeichnete – gemeinsame SIGINT-Kultur verdichtet werden (Baitsch/Nagel 2014). Die kulturelle Ähnlichkeit kann empirisch hinsichtlich der drei Punkte Automatisierung von SIGINT-Aufklärung, Grad der eigenen Fähigkeiten zur Erschließung der Internetkommunikation sowie Innovation und Forschung und der Ähnlichkeit der Partner in diesen Belangen weiter typologisiert und dadurch besser nachvollziehbar dargestellt werden. Es wird angenommen, dass diese Merkmale einerseits die kulturell erwünsche Reichweite, als auch die notwendigen technischen Bedingungen berücksichtigen und abbildbar machen. Es kann festgestellt werden, dass die USA, Großbritannien und Kanada den höchsten Grad zur Erschließung von Internetkommunikation aufweisen und auch der Grad der Automatisierung in den Systemen der drei Auslandsnachrichtendienste hoch ist (National Security Agency 2012e; National Security Agency 2012f; National Security Agency 2008b). Für Neuseeland und Australien kann nachgewiesen werden, dass die Fähigkeiten der Erschließung und Automatisierung sich im Aufbau befinden, aber vor allem durch die Ausstattung und das Training durch NSA-Personal gestützt sind (National Security Agency 2003i). So lässt sich für die Five Eyes festhalten, dass die kulturelle Kongruenz allen Organisationen einen großen Handlungsraum bietet, weswegen kompatible Fähigkeiten vorhanden sind und das technische Niveau sowohl in der Automatisierung als auch in den generellen Fähigkeiten gleich hoch ist. Allerdings muss berücksichtigt werden, dass sich bereits eine starke institutionalisierte Beeinflussung durch die NSA in den Organisationsstrukturen der Organisationen CSEC, GCSB und DSD feststellen lässt, da sie technisches Equipment der NSA beziehen (National Security Agency 2013h; National Security Agency 2003i). Der kanadische CSE wird zusätzlich durch die Zuteilung von Forschungsgeldern unterstützt (National Security Agency 2013h).[62] Die gegenseitige Hilfe, um einen gleichwertigen Grad der Automatisierung, der Innovation und der generellen

[62] Diese Investition in den CSEC scheint sich auszuzahlen. Der kanadische Dienst war maßgeblich an der Ausspähung der brasilianischen Regierung beteiligt (National Security Agency 2012f). Im Rahmen der durch die Veröffentlichung der Snowden-Dokumente ausgelösten ‚NSA-Affäre' schlug diese Regierungsspionage – neben der Ausspähung des Mobiltelefons der deutschen Kanzlerin Angela Merkel – hohe Wellen. Die NSA und der CSEC betreiben außerdem den bilateralen Glasfaserzugang CATAPULT (National Security Agency 2003m).

Fähigkeiten zu erreichen, kann dabei zusätzlich als Hinweis für eine kognitive Verbundenheit der Kooperationspartner gelten.

Um zu überprüfen, ob die Auslandsnachrichtendienste einen Umgang der Selbstverständlichkeit bezüglich Durchführung, Weiterführung und Weiterentwicklung der organisationalen Arbeit und Kooperation – und damit den tiefsten Grad der Kooperation, den der Verbundenheit – aufweisen, oder ob sich ihre Strukturen und Regeln in der Diskussion oder Demonstration befinden, sollen der Umgang mit Kooperationsstrukturen und etwaige Diskussionen hinsichtlich einer gesellschaftlichen Verhältnismäßigkeit des kooperativen Handlungsraums näher betrachtet werden. Da die kulturelle Kongruenz und eine damit verbundenes Streben nach einem gemeinsamen hohen Grad der Automatisierung, Fähigkeiten und Innovation nachgewiesen wurde, soll zunächst geprüft werden, ob die Kooperationsstrukturen einer geronnenen Praktik entsprechen und somit die Institutionalisierung der Kooperation einer Selbstverständlichkeit folgt. Zunächst ist festzustellen, dass eine gewisse Reziprozität des Datenaustauschs für die Five Eyes als selbstverständlich angesehen wird. Dies lässt sich nicht durch die Diskussion über, sondern durch den Umgang mit Kooperationsstrukturen nachweisen. So ist beispielsweise bei TICKETWINDOW eine Gleichwertigkeit des Datenaustauschs gegeben, denn der Austausch verläuft so, dass alle Partner einen Zugang aufweisen und die Struktur zu Empfang und Übermittlung von Informationen nutzen können, ohne durch diese Weiterleitung Quellen oder Methoden zu offenbaren (National Security Agency 2003g). Gleichzeitig wird diese Praktik der Reziprozität dadurch begleitet, dass diskutiert wird, welche institutionellen Grenzen zu beachten sind. Diese Diskussion wird jedoch einen Narrativ der erfahrungsgeschichtlichen Wirksamkeit begleitet. Der Mehrwert der Struktur ist, in der Darstellung der NSA, für alle Partner gleich oder ähnlich hoch:

> „New sources from our Partners have helped NSA be more productive, while DSD reports that more than 40% of their product reporting is now from TICKETWINDOW collection, particularly from NSA collection. Both GCHQ and CSE have doubled their output of TICKETWINDOW-based reports in the last year" (National Security Agency 2003g).

Gleichzeitig kann die Datenübertragung sogar Informationen über die Inländer der jeweiligen Partnerstaaten beinhalten, wenn die Daten von Hinweisen zu Selektoren, die die Inländer des weitergebenden Staates betreffen und diese theoretisch zur Ausspähung durch ‚ihren' Auslandsdienst ausliefern könnten, bereinigt wurden (National Security Agency 2007c). Dieser tiefe Datenaustausch wird durch gemeinsame Regelungen der Five Eyes möglich, die ihre Grundlage in der UKUSA-Vereinbarung vom 5. März 1946 finden und die auch im

Untersuchungszeitraum noch als wichtigste institutionelle Grundlage der Kooperation und als bewusste Regel der Kooperation dient:

> „Under the British-U.S. Communications Intelligence Agreement of 5 March 1946 (commonly known as the United Kingdom/United States of Amerika (UKUSA) Agreement), both governments agreed to exchange communications intelligence products, methods and techniques as applicable as long as it was not prejudicial to national interests. This agreement has evolved to include a common understanding that both governments will not target each other's citizens/persons. However, when it is in the best interest of each nation, each reserved the right to conduct unilateral COMINT action against each other's citizens/persons. Therefore, under certain circumstances, it may be advisable and allowable to target Second Party persons and second party communications systems unilaterally when it is in the best interests of the U.S. and necessary for U.S. national security" (National Security Agency 2007f).

Die Vereinbarung kann so betrachtet werden, dass sie aus internalisierten Bestandteilen besteht, denn es wird hier auf ein Einverständnis hingewiesen, das besteht und nicht diskutiert werden muss. Diskutiert werden muss jedoch die Anwendbarkeit hinsichtlich bestimmter Umstände. Diese Gegebenheiten treten beispielsweise auf, wenn die Bürger eines anderen Five-Eyes-Staates von den Abhörmaßnahmen betroffen sind. Wie, zumindest die NSA, hier jedoch festhält, sind diese besonderen Bedingungen nur zu einem gewissen Maße diskussionswürdig. Denn der internalisierten Idee der Verbundenheit aufgrund bereits feststehendem Einverständnis steht gewissermaßen die Verbundenheit mit der eigenen Gesellschaft gegenüber. Doch auch diese wirkt nicht automatisch, denn die beiden ‚Verbundenheiten' müssen gegeneinander abgewogen werden, wofür die NSA beispielsweise eine eigene Organisationsroutine vorhält:

> „When sharing the planned [Second Party persons'] targeting information with a Second Party would be contrary to U.S. interests, or when the Second Party declines a collaboration proposal, the proposed targeting must be presented to Signals Intelligence Director for approval with justification for the criticality of the proposed collection. If approved, any collection, processing and dissemination of the Second Party information must be maintained in NOFORN channels" (ebd.).

Demnach dürfen alle Bürger der Kooperationspartner bei begründetem Verdacht und erwiesener Notwendigkeit überwacht werden. Dieses Verhalten der NSA, das potentiell auch für die anderen Five-Eyes-Organisationen gilt, zeigt zunächst eine große habituelle Reichweite an genereller Informationssammlung und -auswertung. Gleichzeitig wird jedoch auch deutlich, dass jede Verbundenheit Grenzen dort erfährt, wo die Bindung zur eigenen Gesellschaft in Gefahr gerät. Dabei ist jedoch ebenfalls nachweisbar, dass die Diskussion geeigneter Regelungen sich immer zugleich an den technischen Bedingungen, neue Datentypen auswerten zu können und hierfür auch die Möglichkeiten innerhalb des kulturellen Kontexts einerseits und des verbindenden Kontexts andererseits, fortwährend prozesshaft zu ergründen. So erarbeiteten

beispielsweise NSA und das UK Liaison[63] Office bei NSAW, dem Standort der NSA in der Umgebung von Washington (D.C.), 2007 eine neue formale Verfahrensweise, die es der NSA erlaubt, alle britischen Metadaten zur verdachtsabhängigen Analyse zuzulassen. Die ältere Regelung von 2004 sah dies nur mit Telefondaten vor (National Security Agency 2007a). Diese Informationen können die NSA entweder unilateral verwerten oder die Briten über ihre Informationen unterrichten. Jedoch zeigt sich, dass dieses Vorgehen keineswegs uneingeschränkt funktioniert. Der „unmask[ed] UK contact identifier" (ebd.) darf nicht „primary subject" (ebd.). der Aufklärung sein und seine personenbezogenen Daten – nicht aber die dadurch erbrachten Hinweise – werden in der Analyse wieder hinausgelöscht. Außerdem bezieht sich die Sammlung britischer Daten zu diesem Zweck nicht auf „deliberately" (ebd.)., also spezifisch ausgewählte, Metadaten – es werden Handy-, Fax-Nummern, E-Mail und IP-Adressen erfasst –, sondern auf solche, die zufällig, also „incidentally" (ebd.). erfasst wurden. Glenn Greenwald, der die Snowden-Dokumente als erster systematisch auswertete, gibt zudem an, dass seit 2011 eine ähnliche Praxis auch mit dem australischen Dienst DSD bestünde (Greenwald 2014: 203 f.).[64] Aussagen in den Snowden-Dokumenten deuten außerdem darauf hin, dass die australische Regierung sich von der NSA Hinweise auf Australier verspricht, die an international vernetzten extremistischen Aktionen teilnehmen (National Security Agency 2014o). Es lässt sich jedoch nicht spezifizieren, welcher der Partner wie viele Daten über die Inländer der Kooperationspartner speichert und ob er diese weiterverarbeitet oder weiterleitet.

Somit lässt sich feststellen, dass selbst in dieser engen Kooperation sowohl internalisierte, als auch diskutierte Normen bestehen. Letztere drücken sich darin aus, dass immer übereingebracht werden muss, welche Grenzen hinsichtlich des Invasivitätsgrades der gemeinsamen Aufklärung gezogen werden müssen. Internalisiert ist aber vor allem die Besonderheit der Five-Eyes-Beziehungen gegenüber Beziehungen zu Drittpartnern. So unterscheidet sich das Kooperationsarrangement der Five Eyes zu Kooperationen mit Drittpartnern nachweisbar vor allem durch ein – zumindest allgemein höheres – Datenvolumen: „Our Third Party relationships are different from our Second Party ties in that we do not share information across the board with the nations involved" (National Security Agency 2003j).[65] Die Verbundenheit der Five

[63] Liaison ist der in der geheimdienstlichen Praxis gebräuchliche Begriff für Kooperation (Sims 2006; Aldrich 2002; Westerfield 1996).

[64] Informationen dazu liegen in den bis zum Bearbeitungsende der vorliegenden Arbeit am 1. Februar 2019 veröffentlichten Snowden-Dokumenten nicht vor.

[65] Es lassen sich jedoch auch Regeln feststellen, die für Five-Eyes-Partner und Drittpartner gleich sind: so existiert eine ‚Third party rule', die besagt, dass die Geheimhaltung von Operationen oder Einrichtungen ein legitimes Verhalten auch enger Kooperationspartner sei – denn schließlich beschäftigt diese Wahrung eines gewissen Informationsvorsprungs vor anderen Gesellschaften gegenüber der eigenen Gesellschaft jede Organisation gleichermaßen (National Security Agency 2012c). Es wird vermutet, dass dies die NSA jedoch nicht davon abhält,

Eyes untereinander zeigt sich also vor allem darin, dass die Organisationen bestrebt sind gemeinsam möglichst viele Daten mit einander und für einander produzieren. Dass dieses gemeinsame Handeln ständig fokussiert wird, spricht für eine Verbundenheit, die über eine bloße Interaktion nicht nur mengenmäßig, sondern vor allem verfahrensmäßig, hinausgeht. Auch in Bezug auf vertiefende Praktiken ist die Kooperation als enger zu werten als die zu Drittpartnern. So sichern sich die Dienste die Kontinuität, und sogar die Weiterentwiclung, ihrer Beziehungen langfristig durch eine ‚Business vision' zu. Ihr oberstes Ziel ist „maintaining business continuity" (National Security Agency 2003d). Briefings, die mit der Business vision in Zusammenhang stehen, behandelten „specific targets of interest, such as the Global War on Terrorism, proliferation, North Korea, and ways to maximize our collection strategies" (National Security Agency 2003d). Die Dokumente rund um diese gemeinsame strategische Ausrichtung zeigen jedoch außerdem, dass diese vor allem von NSA und GCHQ, in enger Absprache, strukturiert werden. So trafen sich 2003 Vertreter der NSA, des DSD und des GCSB um ein Briefing unter Leitung des NSA SIGINT Directorates zur Business vision abzuhalten (National Security Agency 2003h).[66] Diese Zusammenstellung legt nahe, dass diese nur von der NSA oder zumindest im Zusammenschnitt NSA und GCHQ maßgeblich entwickelt und in den Ergebnissen lediglich an die anderen Partner weitergegeben wurden. Da der Partner GCHQ am Verhandlungstisch fehlte, liegt es nahe zu vermuten, dass die Inhalte des Briefings zuvor von ihm abgesegnet wurden. Auch in Bezug auf TICKETWINDOW bekräftigten GCHQ und NSA ihr Vorhaben, eine "united front in its dealings with the other foreign partners" (National Security Agency 2003g) einnehmen zu wollen. Diese Binnenstruktur innerhalb der Five Eyes lässt sich mit der Annahme der Wirkungen der kulturellen Ähnlichkeit alleine nicht erklären.

4.1.3 Die Wirkung technischer Unsicherheit: Interpretation und technischer Vorteil

Da festgestellt wurde, dass die Eigenschaften der Kooperation sich – ermöglicht durch eine kognitiv vorhandene und praktisch realisierte Verbundenheit – auf Gleichwertigkeit der Kooperationspartner und das Bestehen gemeinsamer oder ähnlicher geronnener Praktiken und eines tiefen gemeinschaftlichen Handlungsraums beziehungsweise eines vorhandenen

sich für die unilateralen Einrichtungen ihrer Kooperationspartner zu interessieren, denn auch hier ist die Bindung an die eigene Gesellschaft stärker, als an die zum Organisationspartner. Dass die Third party rule Kooperationspartnern ausdrücklich erlaubt, Geheimnisse zu haben, war vor der Veröffentlichung der Snowden-Dokumente nicht in der Form bekannt. Zuvor ging man davon aus, dass diese Regel vor allem die Verschleierung der Teilnahme von Kooperationspartnern an verdeckten Handlungen beinhalte (Daun 2005b).

[66] Zwischen den Five Eyes finden nicht nur persönliche, sondern auch virtuelle Meetings statt (National Security Agency 2003b). 2003 konnte der GCHQ jedoch nicht teilnehmen - wegen eines Computerproblems (National Security Agency 2003a).

ähnlichen Handlungsraums verdichten lassen, ergibt sich zunächst das Rätsel, dass allein eine kulturelle Ähnlichkeit dieses Ergebnis nicht vollumfänglich zu erklären scheint, denn es besteht eine hohe Wirksamkeit aufgrund weitereichender Strukturen und institutioneller Vertiefung, die auch und vor allem durch technische Innovation gelungen ist und deren Einbringung in die Gruppenkonstellation vorrangig durch GCHQ und NSA durchgeführt wurde. Die Partner CSEC, DSD und GCSB können zwar an allen Strukturen teilhaben und werden bei dem Ziel, eine Kontinuität der gemeinsamen Aktivitäten zu wahren, berücksichtigt. Allerdings werden der Aufbau der dafür benötigten Strukturen und die, in diesen angewandten, Handlungsmodelle, vorrangig zwischen NSA und GCHQ vollzogen. Daher soll nun geprüft werden, ob diese Binnenstruktur durch die weitere Annahme des Neuen Institutionalismus, wonach Organisationen auf die technische Unsicherheit und die Interpretation ihrer eigenen legitimen und effektiven Reaktionsmöglichkeiten hin handeln, überprüft werden. Der Neue Institutionalismus hält zur Erklärung des eben skizzierten Rätsels zwei Annahmen über die Unsicherheit bereit. Diesen zufolge sind die Entscheidungen der Organisationen in hohem Maße durch deren Interpretation mehrerer Kontexte beeinflusst. Die Unsicherheit entsteht aus einer Wechselwirkung zwischen gesellschaftlicher und organisationaler Ebene und exogenen technischen Bedingungen. Dabei rekurriert die Unsicherheit nicht auf eine zeitgebundene Bedrohungswahrnehmung oder technische Realität, sondern ist eher ein immanenter Bestandteil gesellschaftlicher und organisationaler Wirklichkeit, da gegenwärtiges Handeln immer zu einem gewissen Grad mit Nicht-Wissen darüber, wie legitim oder effektiv die Aktivitäten retrospektiv bewertet werden können, verknüpft ist (March/Olsen 1976). Diese Wirkung auf Organisationen ist also generell vorhanden, egal ob es sich um gemeinsame Handlungen kulturell kongruenter oder divergenter Akteure handelt und kann sowohl beschränkende, als auch befähigende Wirkungen haben. Es ist jedoch davon auszugehen, dass auch dieser Einfluss sich in einer Tendenz zur Anpassung der Kooperationspartner aneinander ausdrückt.

Die Bewertungen hinsichtlich der gesellschaftlichen Ebene und der Anpassung an die strukturellen Bedingungen können zunächst für die NSA wiedergegeben werden. Hier ist durch das Textmaterial nachweisbar, dass sie die Erwartungen der Gesellschaft über die Metadatenaufklärung nicht adäquat einschätzen kann, da keine übergeordneten Regelungen und auch keine geeigneten Präzedenzfälle als Organisationsschablonen verfügbar sind. Es herrschen somit weder geronnene Praktiken zum Umgang mit einigen Datentypen noch spezifische gesellschaftliche Vorgaben. Besonders relevant ist dies in Bezug auf ‚Converged Data' (National Security Agency 2014g; 2010c). Diese Datentypen entstehen beispielsweise

bei der Telefonie und Internet-Nutzung mit Smartphones, da hier Standortdaten mit Webtraffic, Chatprotokollen und anderen Daten gebündelt werden können (National Security Agency 2010c). Die Five Eyes thematisierten auf der ‚Metadata Policy Conference' 2007, dass für den Umgang mit diesen Daten keine gesellschaftlichen Institutionen zur Orientierung bereitstünden:

> „Given the nascent state of many of these data types then no, or limited, precedents have been set with respect to proportionality or propriety, or whether different legal considerations applies to the 'ownership' of this data compared with the communications data that we were more accustomed to handle" (National Security Agency 2007c).

Diese Feststellung stellt in der Interpretation der Organisationen zunächst also eine Beschränkung dar, da sie betonen, dass sie in Bezug auf diese Datentypen keine ausreichende Erfahrung für legitimes Verhalten besitzt. Augenfällig ist zweierlei: Die Organisationen heben hervor, dass ihnen die legitime Grundlage fehlt, eine eindeutige Entscheidung hinsichtlich eines sinnvollen Verhaltens fehlt. Sie legen den Fokus also darauf, die Komplexität der Gemengelage des notwendigen Umgangs mit diesen Daten – da die Daten vorhanden sind – und einer gleichzeitig fehlenden Grundlage – da keine gesellschaftliche Entscheidung aufgrund einer mangelnden Einschätzung zu Verhältnismäßigkeit – darzustellen. In der Problematisierung dieser Unsicherheiten konzentrierten sich die Organisationen daher besonders auf einen erfahrungsgeschichtlichen Narrativ, nämlich darauf, dass der bekannte Umgang ihrer Kooperation der der Informationsweiterleitung ist:

> „An increasing amount of new data types are available to SIGINT agencies, some proving difficult to categorise as either content or communications data. The conference agreed to step back from trying to categorise the data and simply to focus on what is shareable in bulk" (National Security Agency 2007c).

Zunächst wird also das Problem der mangelnden Möglichkeiten des Abgleichs technisch notwendiger, oder doch zumindest möglicher, Praktiken mit gesellschaftlichen Erwartungen zur Verhältnismäßigkeit diskutiert. Anstatt auf eine gesellschaftlich-legitime Grundlage zur Organisationsentscheidung verweisen zu können, wird dann eine Entscheidung unter Einbezug des Selbstverständnisses der Kooperation, des bereits zitierten Teilens „across the board" (National Security Agency 2003j) mit den Five-Eyes-Partnern, also damit die Kooperationsverbundenheit, getroffen. Dadurch wird die Anpassung der Organisationen in Ermangelung einer eindeutigen Interpretation gesellschaftlicher Erwartungen hinsichtlich geronnener Ideen und ‚altem, bewährten Handlungsraum' getroffen. Hier entsteht der Verdacht, dass diese Uneindeutigkeit nicht notwendigerweise eine Beschränkung für Organisationen darstellt. Sie könnte auch eine Befähigung für die Kooperation und die beteiligten

Organisationen darstellen. Denn eine fehlende Regulierung bedeutet erst einmal auch keine Einschränkung. Deutlich wird aber auch, dass das Dilemma der mangelnden externen Festschreibung eines sinnvollen Umgangs mit Metadaten in Richtung der bereits in der Forschung skizzierten potentiell entstehenden Nachfragelücke zeigt (Ratcliffe 2008: 16). Es wird durch die Organisationen befürchtet, dass eine Scheu vor der Auswertung bestimmter Datentypen aufgrund von Unsicherheit, wie solche Aktivitäten retrospektiv – bei einer entsprechenden Regulierung der Metadatenverwendung – bewertet werden könnten, zu einer Nicht-Erfüllung des gesellschaftlichen Auftrages führen könnte. Organisation und Gesellschaft sind somit in dem, von der Theorie des Neuen Institutionalismus hervorgehobenen dauerhaft prozessualen Konstitutionsverhältnis befindlich, dessen Wechselseitigkeit immer sowohl Chance für das effektive Handeln als auch Gefahr für die Legitimität von Organisationen bedeutet. Dass die Organisationen die Bedrohung durch eine möglicherweise retrospektiv negativ ausfallende Bewertung ihres Verhaltens wahrnehmen, zeigt sich dadurch, dass sie sich zwar selbst keine Selbstbeschränkung auferlegt, jedoch eine Berücksichtigung bei kritischen Fällen befürwortet: "It was agreed that the conference should not seek to set any automatic limitations, but any such difficult cases would have to be considered by owning agency on a case-by-case basis" (ebd.).

Wie die Prüfung der ersten Annahme, der Wirkung kultureller Verbundenheit bereits ergeben hatte, wird durch die Organisationen der Zugang aller Partner zu möglichst vielen Daten fokussiert. Dies kann jedoch nicht nur auf kognitive Kongruenz, sondern auch auf die Interpretation der externen technischen Erfordernisse zurückgeführt werden. Denn auch wenn, wie oben diskutiert keine gesellschaftlich eindeutige Entscheidungsschablone für die Organisationen vorliegt, die von den exogenen technischen Bedingungen ausgehende Grundlage und Notwendigkeit für eine stark international vernetzte Datenauswertung ist vorhanden. Die adäquate Auswertung der Internetkommunikation ist nur durch die Datenweitergabe in internationale Datenbanken, die auch mit Informationen von Drittpartnern angefüllt werden, möglich, denn nur durch sie ist die Entdeckung globaler Muster und Beziehungen umsetzbar (National Security Agency 2003g). Denn die Daten können in den Systemen der NSA und der anderen Five-Eyes-Partnern dann zu komplexen Analysen über das Lebensumfeld einzelner Personen (‚Pattern of life'-Analysen) und zu Bewegungsprofilen reisender Individuen, deren Reiseverläufe miteinander korreliert werden können (ermöglicht durch das Programm ‚Co-Traveler'), verbunden werden (National Security Agency 2014c). Hierzu sind vor allem Daten, aber auch unterschiedliche, technisch höchst komplexe, Systeme notwendig, die miteinander kompatibel sind und sich verlässlich anwenden lassen. Da sich die

Organisationstechniken in Wechselwirkung zwischen Gesellschaft und Organisation entwickeln, darf jedoch nicht nur die Wirkung der Gesellschaft, sondern muss auch das Wissen der Organisationen hinsichtlich technischer Bedingungen und ihrer Bewältigung berücksichtigt werden. Daher erklärt sich die Binnenstruktur der Five Eyes vor allem durch die Erfahrung technisch sehr fähiger Organisationen. Diese Erfahrungen hängen untrennbar mit dem ‚Kulturobjekt Internet' zusammen. Die Basis der internationalen Vernetzungstechnologie wurde in den USA erarbeitet. Dieses technologische Grundlagenwissen spielt noch heute eine Rolle für die Effektivität der amerikanischen Sicherheitsdienste in der Internetaufklärung:

„Let's be blunt – the Western World (especially the US) gained influence and made a lot of money via the drafting of earlier standards. The US was the major player in shaping today's Internet. This resulted in pervasive exportation of American culture as well as technology" (National Security Agency 2014o).

Damit verbunden ist ein gewisser positiver Wettbewerbs- und Personalfaktor der amerikanischen Dienste. Dieser befreit jedoch nicht von der Notwendigkeit, nachrichtendienstliche Systeme ständig so weiterzuentwickeln, dass sie mit den allgemeinen technischen Möglichkeiten und ihren Weiterentwicklungen – und damit auch den Ausnutzungsmöglichkeiten dieser Strukturen durch Gefährder – mithalten können. Die Organisationen müssen die Technologie beherrschen und sich – in der Terminologie des Neuen Institutionalismus ausgedrückt – an die technische Umwelt anpassen. Dass die NSA dazu aus ihrer Sicht fähig ist, diese Einstellung ist eine zentrale geronnene Idee der NSA: „SIGINT prowess provides cyber advantage" (National Security Agency 2011c). Gleichzeitig befähigt das Wissen um die Funktionalität des Internets die amerikanischen Dienste, allen voran die NSA, dazu, Strukturen aufzubauen, die das nutzen können, was das Internet vor allem bereitstellt: Daten. Dadurch erklärt sich, warum die NSA und der britische Dienst GCHQ einen engen Schulterschluss suchen. Denn die geographische Lage der britischen Insel am Knotenpunkt wichtiger transkontinentaler Datenkabel, gepaart mit der beiderseitigen kognitiven Einstellung der Legitimität einer starken nachrichtendienstlichen Reichweite, hat den GCHQ zum größten Datensammler des Internetzeitalters gemacht: „GCHQ has massive access to international internet communication. We receive upwards of 50 Billion events per day (…and growing)" (Government Communications Headquarters 2014). Der Umgang mit technischer Unsicherheit in der Kooperationskonstellation Five Eyes ist also von den Phänomenen eines Nicht-Wissens über notwendige Grenzen des Datensammelns, dem Wissen über die funktionalen Mechanismen des Datensammelns gleichermaßen geprägt. Gleichzeitig

erkennen die Nachrichtendienste, dass sich die Pole Effektivität und Legitimität in einem ständigen Aushandlungsprozess befinden, in dem auch sie eine Roll einnehmen müssen:

> There is a constitutional expectation of privacy within the US. For communications data this is harder to quantify than for content. New procedures will permit a differentiation between content and communications data allowing for far greater data usage and advancing other related changes. A tension remains between the desires to minimize shared data containing US identifiers, and engaging more openly to support the foreign cryptologic mission" (National Security Agency 2007c).

Diese Aussage macht vier Punkte deutlich: Zum einen erkennen Organisationen allgemeine gesellschaftliche Einschränkungen, wie etwa durch die Norm der Privatheit und dieses Verständnis ist in diesem Sinne auch als ‚geronnen' zu bezeichnen, da beispielsweise die NSA dem obigen Zitat zufolge diese zumindest für die Inhaltsaufklärung routiniert durchsetzt. Lediglich, welche verfahrenstechnischen Lehren daraus zu ziehen sind, bleibt zunächst ungenau. Zweitens steht das Erkennen dieses generellen gesellschaftlichen Bedürfnisses nach möglichen Einschränkungen der alternativen Erklärung, dass Organisationen rein objektiv nach ihren eigenen ‚Organisationsinteressen' handeln wollen und würden, entgegen. Zwar ist drittens eine Präferenz der Organisationen zu diesem Handeln ablesbar. Sie können dieser jedoch nicht uneingeschränkt folgen, da sie um ihre Legitimität fürchten müssen. Viertens heben die Akteure aber durchaus narrativ hervor, dass mögliche (weitere) Einschränkungen auch für die gesellschaftliche ‚Mission' der Auslandsaufklärung hinderlich sein könnten. Anhand dieser empirischen Auswertung lässt sich auch vermuten, dass die Dienste diese Auffassung auch an Akteure außerhalb des nachrichtendienstlichen Spektrums, etwa an den mit Intelligence betrauten exekutiven Leitung in anderen Behörden, weitertragen und sich dadurch auch einen gewissen Handlungsrahmen erkämpfen können, was jedoch nicht im genuinen Untersuchungsrahmen der vorliegenden Arbeit liegt. Zentral hervorzuheben ist jedoch, dass die nachrichtendienstlichen Akteure durch die Diskussion nicht nur ihres Kooperationsrahmens, sondern auch ihres organisationalen Handlungsrahmen, sich im gesellschaftlichen Prozess des Umgangs mit Sicherheit und Technik wenn auch in diesem Material nicht nachweislich in den gesellschaftlichen Prozess einmischen, sie jedoch für sich selber eine habitualisierte Rolle im gesellschaftlichen und im internationalen System definiert haben, in dem sie sich als Daten- und wissensvernetzende Akteure, die eine Bedarfserfüllung nach Sicherheit erbringen, betrachten (National Security Agency 2004; National Security Agency 2006c). Diese Auseinandersetzung mit einem und die Einbettung in einen Kontext machen deutlich, dass es sich bei sicherheitsbehördlichem Handeln, selbst in der engsten Form der Kooperation, nur graduell um automatische Handlungsabläufe und Institutionalisierungsprozesse, und immer

auch um demonstrative Diskussionsprozesse handelt. Hierbei treten NSA und GCHQ besonders dominant auf, da sie technisch-strukturell eine besondere Stellung einnehmen, während die anderen Partner sich an sie anpassen. Darauf wird die Fallstudie, die die Beziehung zwischen diesen beiden Organisationen näher in die Betrachtung nimmt, noch weiter eingehen.

Für die Falluntersuchung der Five Eyes lässt sich indes zusammenfassen, dass sowohl die akteursbezogenen Aussagen der Theorie, wie in Tabelle 5 dargestellt, und die theoretischen Annahmen aus Tabelle 6 für die Art der Kooperationsbeziehung und deren Beeinflussung durch kulturelle Kongruenz und Inkongruenz bestätigt werden können. Die Akteure reflektieren und interpretieren ihre Einbettung in gesellschaftliche und technische Kontexte und nehmen hier sowohl fest habitualisierte Handlungen vor, diskutieren jedoch auch in einigen Bereichen ein geeignetes Vorgehen sowohl in organisationaler als auch in interorganisationaler Hinsicht. Zudem konnten die Annahmen für Kongruenz insofern bestätigt werden, als dass die Five Eyes weitreichende Modelle zur Beherrschung externer technischer Modelle ausprägen konnten, wobei diese teilweise zuerst von NSA und GCHQ entwickelt und dann an die anderen Gruppenmitglieder weitergegeben wurden. Die Kontinuität der Bedarfserfüllung und auch Möglichkeiten zur zukünftigen Bedarfserfüllung werden kooperativ eng gestaltet, was sich vor allem durch die Business vision ausdrückt. Die durch die Variable der technischen Unsicherheit ausgedrückten Schwierigkeiten im Abgleich von gesellschaftlicher Erwartungen und technischen Bedingungen werden in der Gruppe diskutiert und hier wird auch eine Präferenz formuliert, die der Einbettung in vertikale, gesellschaftliche Kontexte Rechnung trägt, die jedoch auch einen gewissen Erfolg der Kooperationsstrukturen garantieren soll.

4.1.4 Präsenz und Absenz: Wie viele Daten werden gespeichert, wie viele genutzt?

Aufgrund der Spezifität der ausgewerteten Dokumente müssen die Informationen, die in der Fallstudie dargelegt wurden, kritisch eingeordnet werden. Ziel ist es, die ausgewerteten Informationen hinsichtlich der Kategorien Intention und Sichtbarkeit einzuordnen und auf dieser Basis den zugrundeliegenden Kenntnisstand zu überprüfen. Das Prinzip der Intention soll herausstellen, welche Informationen in den Dokumenten enthalten sein könnten, um bewusst einige Vorgänge oder Einschätzungen hervorzuheben und andere unberücksichtigt zu lassen. Das Prinzip der Sichtbarkeit weist darauf hin, dass durch die Nachvollziehbarkeit einiger Vorgänge die Aufmerksamkeit des Beobachters unbeabsichtigt auf diese gelenkt werden kann und diese möglicherweise in der Folge als überproportional wichtig dargestellt werden zu Ungunsten der Fakten, die nicht oder weniger verarbeitet werden konnten, da sie – beabsichtigt oder nicht beabsichtigt – nicht (ausreichend) im ausgewerteten Material dargelegt wurden.

In den ausgewerteten Dokumenten für vorliegende Fallstudie tritt die Masse an Daten, die den Five Eyes zur Verfügung stehen und die Reichweite der Kooperation durch Datenbanken und Datenweiterleitungsstrukturen, die eine ständig hohe Zirkulation an Daten zwischen den Kooperationspartnern suggerieren, in den Vordergrund. Nicht nachvollziehbar wird jedoch, welchen Wert diese Menge an Daten für spätere Analysen haben, und wie viele Daten über welche Datenzugänge, Datenspeicher und Datenweiterleitungsstrukturen für die einzelnen Organisationen konkret nutzbar sind und genutzt werden sowie wie viele Daten nur auf Vorrat gespeichert, aber nicht analytisch ausgewertet werden. Es kann daher nicht präzisiert werden, wie viele Daten in der Kooperation der Five Eyes tatsächlich erhoben und ausgewertet werden und ob dahingehende Hervorhebungen der Organisationen der Intention geschuldet sind, sich selbst oder ihre Organisationsmitglieder zu motivieren. So wird auch gegenüber den ‚kleineren' Organisationen betont, dass sie wichtige Beiträge in der Unterstützung militärischer SIGINT und der Terrorismusabwehr leisten. Hier können die Informationen dadurch verzerrt werden, dass die Dokumente zu diesen Einschätzungen an die Five-Eyes-Partner zirkuliert werden können. Auch diesbezüglich kann also kritisch hinterfragt werden, ob die Darstellung dieser Daten einen Sachstand darstellen oder auch eine Reaktion bei möglichen Empfängern hervorrufen soll. Denn auch die Betonung der Wirksamkeit der ‚kleineren' Partner kann auch daraus intendiert sein, diese zu weiteren Anstrengungen zu animieren. Auch das tatsächliche Gefüge der Partner hinsichtlich einer möglichen Rollenverteilung zwischen führenden Organisationen und ‚Juniorpartnern' lässt sich letztlich nicht alleine aufgrund der ausgewerteten Dokumente beweisen, da ihre Anzahl dazu zu gering ist. Sie lassen aber dennoch zentrale Erkenntnisse über die Reichweite gemeinsamer Strukturen zu, die bislang nicht oder nur unzureichend bekannt waren.

Hinsichtlich der Ausführungen, durch die die Five Eyes die gesellschaftlichen Privatsphäre-Erwartungen als zu unspezifisch in Bezug auf neue Datentypen beschreiben und sie dadurch ihren Fokus nur auf Weiterleitung von Informationen lenken können, da ihnen konkrete institutionelle Vorgaben zur Limitierung fehlen, ist einschränkend zu bemerken, dass Dokumente zu den Weiterleitungsstrukturen der Five Eyes und zu den Verhandlungen der Funktionsweise eben solcher, sich notwendigerweise auf das Ziel ausrichten, eine möglichst wirksame Vernetzung zu ermöglichen. Denn die ausgewerteten Dokumente stellen Texte der Absprache von Informationsweiterleitungen dar. Auch ist es wahrscheinlich, dass sich Dokumente von Organisationen, die Daten beschaffen und auswerten sollen, vor allem auf diese Aspekte stützen. Daher muss der Beobachter angehalten werden, einen durch die Konzentration auf den Narrativ ‚mehr Daten, größere Weiterleitung, Konzentration auf Innovation und

Vernetzung‘ entstehenden Verdacht der Überbetonung des Datensammelns durch die Organisationen von einer Betrachtung ihrer gesellschaftlichen Aufgabe und dem Untersuchungszeitraum, der sehr nah am 11. September 2001 und der Anschlagserie in London 2005 anschließt, kritisch begleiten zu lassen. Auch muss hervorgehoben werden, dass die nachrichtendienstlich-kooperativen Vereinbarungen nicht auf organisationalen Alleingängen basieren, sondern durch bilaterale formale Regelungen auf Regierungsebene begleitet und geleitet sind. Gleichzeitig darf diese Hervorhebung nicht dazu führen, dass das Verhalten der Organisationen nur als logische Konsequenz jenseits jeglicher Eigenmotivation betrachtet wird. So können und sollten die Möglichkeiten der Ausspähung der Bürger der jeweils anderen Partner durchaus kritisch auf ihre gesellschaftliche Legitimation geprüft werden und Hinweise auf einen geheimdienstlichen Ringtausch der Daten zulassen, der gesellschaftlich kritisch diskutiert werden muss. Auf Grundlage der vorliegenden Dokumente alleine waren eindeutige Bewertungen zu Legitimität oder Nicht-Legitimität sowie zur Effektivität der Datenstrukturen nicht umfassend möglich, dies wird jedoch durch das Forschungsdesign vorliegender Arbeit ausdrücklich nicht angestrebt.

4.2 Die Kooperation zwischen NSA und GCHQ

Für die Kooperation von NSA und GCHQ sind indes viele Dokumente vorhanden, die auf die technische Innovationsleistung der beiden Partner schließen lassen, die auch für die anderen Five-Eyes-Partner nutzbar sind. Diese Erbringung von Innovationen muss jedoch gesondert betrachtet werden. Dadurch, dass die technischen Systeme dieser bilateralen Partnerschaft auch die Kooperation zwischen den Five Eyes maßgeblich effektiv gestalten, erscheint ein spezifischer Blick auf die Wirksamkeit dieser Strukturen sinnvoll. Wie sich zeigt, erarbeiteten NSA und GHCQ mit Systemen wie QUANTUMTHEORY und in besonderen Projekten, beispielsweise zur Entschlüsselung der Kommunikation der Plattform Tor oder in der Ausspähung der Kommunikation in virtuellen Videospielumwelten, Lösungen zur Erschließung verdeckter Kommunikation und zur weiteren Nutzung dieser Kommunikation, etwa für Manipulationen oder gezielte Netzwerkangriffe. Dabei eröffnet ihnen ihre kulturelle Kongruenz einen deckungsgleich großen Erfahrungs- und Handlungsraum. Ebenfalls deutlich wird, dass der Erfahrungsraum nicht nur durch die Gesellschaft institutionell ‚verliehen wird‘, sondern auch interorganisational sozial gebildet und prozesshaft weiterentwickelt wird. In diesem Prozess wir dann ebenfalls sichtbar, dass selbst die engste Kooperation nicht nur kongruente und kooperative Elemente, sondern durchaus auch kompetitive, dadurch aber innovative, Elemente beinhaltet und freisetzt. Abbildung 5 verdeutlicht die Wirksamkeit der

kulturellen Kongruenz und der Interpretation von Unsicherheit auf diese Kooperationsergebnisse.

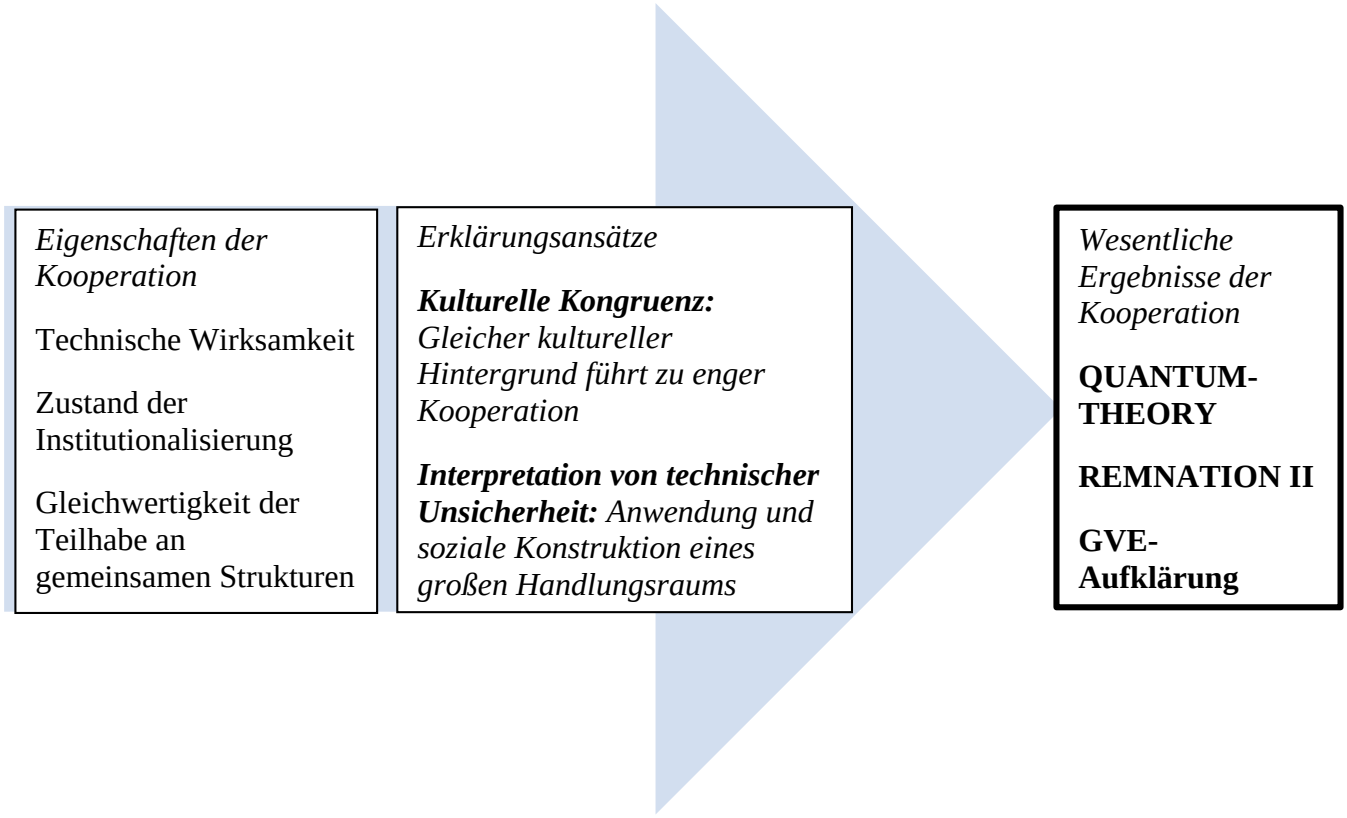


Abbildung 5: Erklärung der interorganisationalen Kooperation bei NSA und GCHQ.

Zunächst werden die gezielten Möglichkeiten der Netzwerküberwachung, die ein kleinteiliges Netz von Systemverknüpfungen zwischen NSA und GCHQ nötig machen, erklärt. Dabei offenbart sich eine hohe Wirksamkeit für die beteiligten Akteure, da sie durch diese Innovationen Daten gezielter sortieren, verknüpfen und zu weiteren nachrichtendienstlichen Aktivitäten, auch in Kooperation mit den Five Eyes, verwenden können (Abschnitt 4.2.1). Diese Ausgestaltung rührt maßgeblich von der kulturellen Kongruenz zwischen NSA und GCHQ her, deren Kooperationsbeziehung schon zur Zeit des Zweiten Weltkrieges fest institutionalisiert war. Aus dieser internalisierten Verbundenheit rekurriert bis heute eine dauerhafte und enge Kooperation, die sehr effektive Prozesse hervorbringt, die nicht nur technischer, sondern auch sozialer Art sind (Abschnitt 4.2.2.). Allerdings sind viele daraus entstehende Techniken auch auf die Interpretation von technischer Unsicherheit zurückzuführen, weshalb die Betrachtung beider als erklärend angenommener Variablen notwendig ist (Abschnitt 4.2.3). Wie viel die Snowden-Dokumente tatsächlich über die

Wirksamkeit und Erklärungen zur Funktionsweise der Techniken von GCHQ und NSA beitragen können, soll ebenfalls kritisch geprüft werden (Abschnitt 4.2.4).

4.2.1 Automatisierte Netzwerkaufklärung mit De-Anonymisierungsfunktion

Zunächst muss unter Berücksichtigung der Eigenschaften einer Kooperation die Wirksamkeit der Zusammenarbeit zwischen NSA und GCHQ dargelegt werden. Es wird angenommen, dass Organisationen Kooperationen dann als besonders wirkungsvoll betrachten, wenn eine Ausweitung an verfügbaren Informationen generiert wird und dadurch auch die verbesserte Möglichkeit, Daten zu verknüpfen und weiterzuleiten – und weitergeleitet zu bekommen – entsteht. Zwar wurde für die Five Eyes die Prämisse einer gleichwertigen und umfangreichen Kooperation bereits bestätigt. Allerdings müssen in der vorliegenden Fallstudie besonders die spezifischen Fähigkeiten der gezielten Aufklärung zur Datengenerierung – auch für die anderen Five-Eyes-Organisationen – behandelt werden, da festgestellt wurde, dass die bilaterale Allianz aus NSA und GCHQ die Gruppenkooperation entscheidend weiterentwickelt und so die besonderen Eigenschaften dieser Kooperation erklärt werden müssen. Dabei zeichnet sich diese spezifische Untersuchung der Beziehungen zwischen diesen Organisationen vor allem dadurch aus, dass beide Organisationen besondere Ergebnisse bei der (teilweise automatischen) Entdeckung verdächtiger Zielpersonen sowie bei Erschließung ihrer, auch verschlüsselten und anonymen, Kommunikation erzielen können. Wenn bei den Five Eyes bereits eine empirisch nachweisbare SIGINT-Kultur der Automatisierung der Signalaufklärung, einem hohen Grad der eigenen Fähigkeiten zur Erschließung der Internetkommunikation sowie Innovation und Forschung festgestellt werden konnte, so kann herausgestellt werden, das deren ‚Motor' der kooperative Entwicklungsaustausch zwischen NSA und GCHQ ist. Die technischen Lösungen werden sowohl von der NSA, als auch vom GCHQ erarbeitet und sind denen der anderen drei Kooperationspartner überlegen. Die durch die Techniken erschlossenen und verknüpften Daten können aber anschließend an ihre Partner weiterreichen. Nachfolgend muss für ein besseres Verständnis dieser Erkenntnisse eine Darlegung der technischen Systeme erfolgen.

Zur gezielten Aufklärung von Zielpersonen hat die NSA mit QUANTUMTHEORY ein komplexes Programm entwickelt, das dem GCHQ eine zentrale Rolle zuschreibt. Das Programm stellt eine innovative Möglichkeit zur gezielten Ausspähung von Datenpaketen dar. Da es nicht nur die Aufzeichnung von Metadatenströmen in Glasfaserkabeln ermöglicht, sondern darüber hinaus auch spezifische Optionen zum Hinweis auf auffällige Muster in großen Datenmengen sowie technische Einfallstore für weitere geheimdienstliche Ausspähmöglichkeiten in die Rechnersysteme verdächtiger Personen bereithält, kann es als

sehr gewinnbringend für die nachrichtendienstliche Arbeit bezeichnet werden. QUANTUMTHEORY ist dem Bereich der ‚Cyber Network Operations' (CNO) zuzurechnen. Die NSA subsumiert unter diesen Begriff sowohl bloße Extraktionen unterschiedlicher Datentypen aus Kommunikation, ohne das Eindringen in Rechnersysteme, deren Auswertung hinsichtlich darin verborgener Erkenntnisse über Zusammenhänge, Beziehungen und Schlussfolgerungen verfolgt wird (‚Digital Network Intelligence', DNI), aber auch den aktiven Eingriff in Rechnersysteme (‚Digital Network Exploitation', DNE) mit dem Ziel, die Beherrschung des Zielsystems zu erlangen, Daten zu entziehen oder zu manipulieren, Kommunikationsströme umzuleiten oder die Verschlüsselung klandestin zu schwächen (National Security Agency 2003e; 2003l).[67] QUANTUMTHEORY überwacht den Kommunikationsverkehr und kann, wenn es verdächtige Muster oder ihm bekannte Selektoren, also beispielsweise E-Mailadressen oder Telefonnummern entdeckt, die Kommunikation automatisch infiltrieren. Dabei wendet das System die Strategie des ‚Man on the Side' an. Der Begriff ist in Abgrenzung zur Angriffsmöglichkeit ‚Man In The Middle' zu sehen und erhält einen Mehrwert dadurch, dass sich ein Nachrichtendienstmitarbeiter technisch nicht zwischen Nutzer und das Medium – beispielsweise eine Website, welche dieser aufrufen will – stellt, sondern im technischen Sinne mit dessen Anfrage ‚mitläuft', da er den Kommunikationskanal und nicht die Kommunikation selbst infiltriert hat. Hierdurch erhält er einen Zeitvorteil und kann die Anfrage des Nutzers mit seinem eigenen getarnten Server schneller beantworten als der Service, der ursprünglich durch den Internetnutzer aufgerufen wurde (National Security Agency 2011b). Läuft eine Anfrage durch einen infiltrierten Kommunikationskanal, kann das System durch ‚passive Sensoren' automatisiert abfragen, ob es sich beim Nutzersystem um ein ungeschütztes System handelt, was einen verdeckten nachrichtendienstlichen Einbruch in dieses System erleichtert. Diese passiven Sensoren werden unter die Bezeichnung TURMOIL gefasst. TURMOIL ist an das Programm TURBINE angeschlossen, das wiederum ‚aktive Sensoren' beinhaltet. Erkennt TURBINE ein Zielsystem als mangelhaft geschützt, löst es

[67] Der GCHQ weist zusätzlich mit EFFECTS ein Programm zu Covert actions auf. Covert actions sind „agressive mission[s] (…), the secret manipulation of events abroad to advance a nation's interests" (Johnson 2003: 12). Die digitalen Maßnahmen, die der CHQ als "Information Operations" (ebd.) und "Online Covert Action" (ebd.) bezeichnet, haben zum Ziel, Gefährder und deren Netzwerke zu stören (Government Communications Headquarters 2014). Die betroffenen Personen wurden durch teilautomatisierte Auswertung identifiziert. Durch EFFECTS können Personen, etwa durch die Offenlegung ihrer Präferenzen beim Online-Pornographie-Konsum, möglicher sprachlicher Verfehlungen in privaten Nachrichten oder der Erzielung moralisch angreifbarer hoher Vergütungen für Vorträge eingeschüchtert oder erpresst werden. Auch andere Methoden wie die Manipulation des Bildschirms können eingesetzt werden. Online covert actions können nicht nur gegen Extremisten verwendet werden. Beispielhaft werden auch Hacker genannt. So hat der GCHQ im Rahmen der Operation WEALTH im Sommer 2011 mit EFFECTS die Strafverfolgungsbehörden unterstützt (National Security Agency 2014j). Die NSA begreift Hacker, ebenso wie Terroristen, als akute Bedrohungen der nationalen Sicherheit (National Security Agency 2014b).

automatisch eine Einleitung von Schadsoftware aus, die von ‚Implants'[68] eingebracht werden können. Diese aktiven Sensoren können sich in Satelliten, aber auch in Kabelverbindungen weltweit befinden (ebd.). In den ausgewerteten Dokumenten wird die, durch den GCHQ geleitete, Menwith Hill Station (MHS) in der Nähe von Harrogate (North Yorkshire), Großbritannien, als QUANTUMTHEORY-Koordinationsstelle zwischen NSA und GHCQ betrachtet und ist besonders wichtig in Bezug auf die passive Sensorik zum Hinweis auf relevante Datenpakete. MHS-Personal arbeitete mit NSA-Technikern vor allem an Lösungen, die durch TURMOIL protokollierten Datenpakete automatisiert zu sortieren und nach weiteren Angriffspunkten zu durchsuchen. Die hierfür entwickelte Lösung wird als DRAGGABLEKITTEN bezeichnet und baut eine ‚XKEYSCORE-Karte' auf, also eine Übersicht der gewonnen Informationen und Anknüpfungspunkte für den Analysten, welche die Informationen jedoch nicht nur darstellt, sondern auch nach Schlagworten durchsuchbar macht, sowie die Daten selbst gruppiert und nach Mustern durchsucht. Diese Übersicht bezieht sich jedoch nicht nur auf Inhaltswörter sondern auch auf systemische Kategorien, die eine weitere Aufklärung und Filtrierung möglich machen könnten. Somit stellt DRAGGABLEKITTEN gewissermaßen ein Lagebild der Internetkommunikation dar, von dem aus weitere Punkte angesteuert werden können. 2011 konnte die NSA 50 Prozent der durch Hotmail und 90 Prozent der durch Yahoo ausgeführten paketbasierten Internetkommunikation durch QUANTUMTHEORY zur gezielten Aufklärung nutzen: „This would not have been possible without XKEYSCORE providing a platform for analysis to mass-deploy packet-level processing" (National Security Agency 2011b).

XKEYSCORE bezeichnet allgemein eine Technik, Daten zu speichern und sie gleichzeitig nach relevanten Informationen und Hinweisen zu durchsuchen und zu sortieren. Das Programm kann Metadaten bis zu 90 Tage und Inhalte bis zu drei Tage speichern. Dadurch wird der Zugriff auf Kommunikationsdaten sowie auf E-Mails, Chatprotokolle und sogar Skype-Sitzungen inklusive Videoinhalte möglich. XKEYSCORE kann so viele Verknüpfungen zwischen Daten und damit zwischen Menschen ziehen, dass komplexe Analysen des gesamten direkten und indirekten Umfeldes einer Person möglich werden (National Security Agency 2014c). Das Programm erfasst auch verschlüsselte Kommunikation und markiert sie. So können Analysten

[68] Im Fall von QUANTUMTHEORY leitet das ‚Implant' QFIRE die Schadsoftware ein. Es nutzt dafür den Pfad zwischen Zielsystem und aufgerufener Webseite. So lädt das Rechnersystem der Zielperson die Schadsoftware unbemerkt herunter. Die Einleitung der Schadsoftware wird als QUANTUMINSERT bezeichnet. Zusätzlich zur Einschleusung von Schadcode kann die NSA eine Verbindungsanfrage des Nutzers auch zurücksetzen (QUANTUMSKY) sowie durch QUANTUMCOPPER Uploads und Downloads stören oder manipulieren (National Security Agency 2011b).

beispielsweise den Befehl „Show me all PGP usage in Iran“ (National Security Agency 2008b) ausführen, da verdeckte Kommunikation Hinweise darauf gibt, dass Informationen bewusst verborgen werden sollen und daher eine hohe geheimdienstliche Relevanz haben könnten. Die in XKEYSCORE gesammelten Daten sind in Echtzeit verfügbar, werden jedoch auch abgespeichert. Die Analyse mit XKEYSCORE kann sowohl „shallow“ (ebd.), also oberflächlich, erfolgen und ist dann mit gewöhnlichem Stöbern in Datensätzen nach bestimmten Stichworten vergleichbar, die Gesamtsumme an Informationen kann jedoch auch spezifisch nach Selektoren wie E-Mail und IP-Adressen durchsucht werden. Wichtigstes XKEYSCORE der NSA ist PRISM. [69] Auch der GCHQ verwendet ein eigenes XKEYSCORE mit dem Namen TEMPORA. Daher ermöglichen sich beide Kooperationspartner zu ihren jeweiligen Programmen Zugang, jedoch nicht in unbegrenztem Maße. PRISM stellt ein XKEYSCORE dar, dessen Besonderheit es ist, dass es Daten direkt von den Servern von US-Internetprovider und -firmen bezieht (National Security Agency 2013c). Die Kooperationen wurden unter Zustimmung der Betreiber in den Jahren 2007 bis 2012 gestartet (National Security Agency 2013a).[70] Die NSA erhält jedoch nicht nur über die Provider, die im Rahmen von PRISM mit der NSA zusammenarbeiten müssen, Informationen. Sie kann sich auch an den Kommunikationsstrukturen selbst verdeckten Zugang zu den Daten, die in die Rechenzentren der Unternehmen fließen, verschaffen. Die als Upstream bezeichnete Methode ist sprachlich der Erdölindustrie entlehnt und weist insofern eine Analogie auf, als dass die im Boden verlegten Glasfaserkabel als Quelle dienen.[71] PRISM ist laut NSA „the SIGAD[72] most used in NSA Reporting“ (National Security Agency 2013a). Im September 2003 wurden durch das Programm 400 Milliarden Metadaten aufgezeichnet, verarbeitet und gespeichert (National Security Agency 2012b).[73] PRISM stellt ein System zur gezielten Einzelüberwachung dar (Walsh/Miller 2016: 354; Schmid 2014a: 324). Bevor konkret Daten abgegriffen werden können, muss durch die NSA überprüft werden, ob die Überwachung geheimdienstlich notwendig ist, die Zielperson sich nicht in den USA aufhält und kein US-Bürger ist. Zuvor

[69] PRISM ist in seinen Grundzügen direkt nach dem 11. September 2001 unter dem Namen President’s Surveillance Program (PSP) entstanden. Vergleiche zur Entstehungsgeschichte National Security Agency 2009b.
[70] Die Zusammenarbeit mit Microsoft begann am 11.09.2007, mit Yahoo am 12.03.2008, mit Google am 14.01.2009, mit Facebook am 03.06.2009, mit PalTalk am 07.12.2009, mit YouTube am 24.09.2010, mit Skype am 06.02.2011, mit AOL am 03.03.2011, mit AOL am 31.03.2011 und mit Apple im Oktober 2012 (National Security Agency 2013a). Auch Metadaten und Inhalte von Skype-Gesprächen können über PRISM nachvollzogen werden (National Security Agency 2013e).
[71] Die Codenamen für die einzelnen Zugänge an den Glasfaserkabeln lauten FAIRVIEW, STORMBREW, BLARNEY und OAKSTAR (National Security Agency 2014i). Außerdem wurde daran gearbeitet, VoIP über FAIRVIEW und STORMBREW zugänglich zu machen (National Security Agency 2003c).
[72] Unter einem SIGAD lässt sich wohl, dem Kontext nach, eine spezifische Quelle eines technischen Datenzugangs begreifen.
[73] Die Medataten flossen in die MAINWAY-Datenbank für weitere Analyse und Speicherung.

liegen die Daten gewissermaßen in einem Schließfach (Johnson 2015). Die Auswertung der Dokumente ergibt ebenfalls, dass die NSA zwar die potentielle Möglichkeit, auf alle Metadaten und Inhalte zuzugreifen, die auf den Servern liegen vorhält, und in diesem Material nach Selektoren suchen kann. Vor einem tieferen Einblick muss der Analyst jedoch eine Überprüfung seines Vorhabens abwarten (National Security Agency 2013a). PRISM ist als XKEYSCORE im Gesamtsystem „XKS Central“ (National Security Agency 2012e) abrufbar. Das britische XKEYSCORE TEMPORA wird ebenfalls dort verknüpft und ist in der Lage, den gesamten, ihm zugänglichen, Internetverkehr – das ‚Full take‘ – für drei Tage und alle Metadaten für 30 Tage zu speichern (National Security Agency 2012d). Das System sortiert und beleuchtet ebenfalls selbständig relevante Informationen, was NSA und GCHQ als ‚Slice and dice‘ bezeichnen. Neben dem Sammeln von Daten steht auch hier die technische Bewertung von Informationen im Fokus. NSA-Analysten konnten durch ihren Zugang zu TEMPORA im Jahr 2012 „over 200 end-product reports“ (National Security Agency 2012e) erstellen und damit „critical support to SIGINT, defensive, and cyber mission elements“ (ebd.) leisten. Der GCHQ kann im Gegenzug auf PRISM zugreifen.

Eine reine Initative des GCHQ, an der die NSA nur mittelbar Teil hat, ist die Analyse von Metadaten aus Online-Rollenspielen, spezifisch genannt wird World of Warcraft:

> „By fusing information from different systems, databases, and resources GCHQ has correlated target entities WoW logon events and continues to uncover potential SIGINT value by identifying accounts, characters, and guilds related to Islamic Extremist Groups, Nuclear Proliferation and Arms Dealing” (National Security Agency 2012h).

Auch wenn die Überwachung eines Online-Rollenspiels als Maßnahme der Aufklärung von Gefährder-Netzwerken zunächst ungewöhnlich wirkt, scheint zumindest eine Erprobung für die beteiligten Dienste erfolgsversprechend zu sein. Die NSA geht davon aus, dass verdächtige Personen Online-Videocommunities, ‚Games and Virtual Environments‘ (GVEs), vor allem unter dem Gesichtspunkt der persönlichen Vernetzung und Kommunikation nutzen. Diese Umwelten machen es also möglich, Informationen zu E-Mailkennungen, VoIP, Chats, Proxy-Server und Web-Foren zu erhalten. In den Chats und Foren setzt der GCHQ auch HUMINT-Erfassung, beispielsweise durch eingeschleuste ‚Spieler‘, ein (National Security Agency 2012h). Doch nicht nur Videospielumwelten, sondern auch andere Plattformen im Internet bewerten GCHQ und NSA als wichtige Datenlieferanten. So haben beide den Workshop REMNATION II abgehalten, in dem es darum ging, Mitglieder des Anonymisierungsnetzwerk Tor zu enttarnen. Tor wirkt als Anonymisierungstool für den Sender von Datenpaketen, da diese Pakete durch so viele Server weitergeleitet werden, dass der Weg zwischen Sender und

Empfänger der Daten nicht mehr nachvollziehbar ist. Der Weg zwischen Sender und Empfänger verläuft über unterschiedliche Knotenpunkte (Nodes), an welchen die Datenpakete ihre Richtung ändern oder weiterfließen. Zentral sind der Node des Empfängers, ein mittlerer Node, der die Datenpakete auf unterschiedliche Serverstrukturen aufteilt und schließlich der Empfänger-Node. Einige dieser Nodes sind mit dem NSA-Netz verbunden oder sie kann zumindest darauf zugreifen. An dieser Stelle kann die Verquickung zwischen QUANTUMTHEORY und der Tor-Aufklärung gezeigt werden. Denn das erste System legt durch seine automatisierte Informationserschließung die Grundlage für die weitere Nutzung durch das zweite System.[74] Wird jedoch die Anonymisierung von Tor geknackt, geraten Unmengen neuer Selektoren in den Wirkungskreis genannter Systeme. Dies gestaltet sich jedoch schwierig, denn „all three Tor nodes in the circuit have to be in the set of nodes that we have access to“ (National Security Agency 2012h). Dadurch, dass dies nicht immer der Fall ist, bauen NSA und GCHQ auch darauf, durch infiltrierte Nodes eine Verlangsamung des ‚Traffics‘ zu erreichen, sodass der Service für die Nutzer unattraktiv wird. Außerdem verfolgten die Teilnehmer das Ziel, durch die eingenommenen Knotenpunkte die Datenpakete in eine gewünschte Richtung schicken zu können. Durch die Vielfalt der Initiativen, verschlüsselte, und in Online-Communities stattfindende Kommunikation aufzuklären, sowie durch den Zugang zu Daten, die über die Server der wichtigsten Internetunternehmen geleitet oder auf ihnen gespeichert werden, entsteht der NSA und dem GCHQ ein wichtiger Mehrwert im der Aufdeckung möglicher Gefährder und für die Erschließung von Daten, die dann an die Five Eyes weitergeleitet werden können. Gleichzeitig beweisen die dargestellten technischen Strukturen, dass der Handlungsraum für Organisationen sowohl eine Umweltkomponente aufweist, in dem er maßgeblich durch die Gesellschaft gewährt wird. Auf Organisationsebene ist der Handlungsraum aber auch ein sozialer Bereich des ‚Einander Zugriff Gewährens‘ und gemeinsam Entwickelns beziehungsweise des, durch einen diskursiven Austausch angestoßenen eigenständigen Entwickelns. Nachfolgend muss jedoch geprüft werden, ob NSA und GCHQ von diesen Technologien gleichwertig profitieren und ob ihre Kooperation den Prämissen ähnlicher SIGINT-Designs und Fähigkeiten durch eine kulturelle Kongruenz geschuldet ist.

[74] Einfacher wird es offenbar für die Analysten, wenn die Tor-Nutzer durch ihre E-Mailadresse oder in einem Web-Forum identifizierbar sind. Die NSA bezeichnet sie als „Dumb Users (EPICFAIL)“ (National Security Agency 2012h).

4.2.2 Kooperation auf Augenhöhe

Die Annahme für die Kooperation kulturell ähnlicher Partner ist, dass sie eine besonders enge Kooperation mit gleichwertigem Zugang und geronnenen Praktiken schaffen können. Da sie einen kongruenten Erfahrungsraum aufweisen, erreichen sie eine vergleichbare methodische und technische Reichweite. Weil beide Organisationen außerdem mit ähnlichen gesellschaftlichen Bedarfen nach weitreichenden technischen und methodischen Modellen konfrontiert sind, können sie diese Erwartungen durch ein hohes Niveau an (automatisierten) Fähigkeiten erfüllen, das sie auch zukünftig durch Innovationen und Forschung bereitstellen wollen (Peine/Sturm 2008; Klavehn/Müller 2008). Die kulturelle Kongruenz zeigt sich zwischen NSA und GCHQ zusätzlich darin, dass sie bei XKEYSCORE und TEMPORA ähnliche Ansätze verfolgen und diese Techniken durch einen eigenen großen Handlungsraum entwickeln konnten. Allerdings kann nicht nachgezeichnet werden, ob die Entwicklung der Systeme bereits in gemeinsamen Rahmen geplant wurde beziehungsweise wie und ob der Austausch in der Entwicklungsphase gegeben war und ob frühere Komponenten von der NSA auf den GCHQ übertragen wurden – oder umgekehrt. Jedenfalls garantieren sich die Partner gegenseitig einen relativ großzügigen Zugang zu ihren Strukturen. Zu TEMPORA haben 300 GCHQ-Mitarbeiter und 250-NSA-Analysten Zugang. Dieser enge Zustand der Institutionalisierung wird zusätzlich dadurch manifestiert, dass die NSA den TEMPORA-Zugang für diese Analysten als zusätzliche Datenbank in die Anwendung „XKS Central“ (National Security Agency 2012e) integriert hat. Allerdings ist die Nutzung von TEMPORA für NSA-Mitarbeiter nicht ohne ein „UK Legalities training“ (National Security Agency 2012e) möglich. Auch die Teilhabe an PRISM ist für GCHQ-Mitarbeiter nicht ohne weiteres durchführbar. Zwar hat die NSA dem GCHQ PRISM als ‚Olympic Option‘ zugänglich gemacht (National Security Agency 2012a). So hatte der GCHQ am 24. Mai 2012 im Kontext der olympischen Spiele in London vollen Zugriff auf PRISM erhalten. Bereits im Zeitraum vom 16. bis zum 22. Mai 2012 wurden jedoch 11.431 relevante Datenmitschnitte an den GCHQ übermittelt (National Security Agency 2012i). In der Folge arbeiteten beide Kooperationspartner daran, diese einmalige Nutzungsgenehmigung in eine dauerhafte Möglichkeit zu institutionalisieren:

> „Unsupervised access to FAA 702 data, in a manner similar to Olympics Option, remains on GCHQ’s wish list and is something its leadership still desires. NSA and SID leadership are well aware of GCHQ’s request for this data, and the steps necessary for approval. NSA leadership could be asked whether we’re still supportive of this initiative” (National Security Agency 2013g).

Diese Anfrage zeigt zweierlei: zum einen, dass ein gleichberechtigter Zugang zu den Systemen des Partners angestrebt wird. Andererseits muss auch solch eine Vertiefung erst ausgehandelt werden und entspricht keinem Automatismus. Diese Feststellung läuft der Vorstellung entgegen, NSA und GCHQ könnten sich als stark verbundene Akteure in ihrer geheimdienstlichen Arbeit grenzenlos vernetzen. Auch zeigt sich, dass eine kulturelle Kongruenz zwar für gemeinsame technische Entwicklungen notwendig ist und ähnliche Erfahrungshintergründe sowohl zur Entstehung kompatibler – ja fast schon identischer – Techniken und zur Integration von Partnerkomponenten Voraussetzung sind. Doch die Erarbeitung integrierender regulativer Verfahren zu diesen Systemen kann alleine dadurch nicht erzeugt werden – obwohl sie unter kultureller Kongruenz sicher leichter ist als in Konstellationen mit hoher Inkongruenz. Daher können zum einen die engen Strukturen zwischen NSA und GCHQ durch starke Kongruenz erklärt werden. Die Ähnlichkeit ist sogar so hoch, dass sehr ähnliche Einzelstrukturen vorhanden sind, die wie ein ‚Baukastensystem' kooperativ verbunden werden können. Zum zweiten kann durch die Falluntersuchung gezeigt werden, dass Kongruenz alleine nicht zu einer vollständigen, grenzenlosen Integration ‚fremder' Systeme in ein gemeinsames führt. Somit kann valide angenommen werden, dass die Kongruenz der Kultur zwar kooperationsvertiefend wirkt, der Bestand nationaler Kultur –und damit das inhärente Prinzip der Souveränität – aber ein grundlegend stabiles ist. Drittens kann anhand der Detailstudie der Kooperation von NSA und GCHQ verdeutlicht werden, dass Organisieren, und damit organisationale Kooperation, nicht nur aus organisationaler Einigung und Import von technischen Modellen, sondern auch aus, bewusster und unbewusster Co-Kreation von Handlungsmodellen besteht. Dabei muss es sich nicht um gemeinsamen Wissensaustausch mit dem Ziel, kooperativ zu arbeiten, handeln. Vielmehr findet Wissensaustausch immer dort statt, wo sich Organisationen – wo sich ihre Individuen – treffen. Diese Möglichkeit der Betrachtung der Meso-Ebene, bei der nicht nur die Anbindung zwischen Makrostrukturen und Organisation untersucht wird, sondern auch die Berührungspunkte von Individuen mit dieser Schnittstelle erforschbar werden, zeigt, dass nicht nur Kooperation, sondern auch Nicht-Kooperation oder schwache Kooperation eine soziale, und damit immanent kooperative, Komponente aufweist. Im Folgenden soll jedoch aufgezeigt werden, wie dies in einer sehr engen Kooperation aussieht. Dabei soll insbesondere herausgearbeitet werden, wie einzelorganisatorische geronnene Praktiken und interorganisational demonstrierte Handlungsabläufe in Wechselbeziehung stehen und damit stärker herausgearbeitet werden, dass Kooperation nicht nur von einer Einigung auf Kooperationsstrukturen, ihrer Vertiefung oder einem Import von Modellen basiert, sondern auch auf bilateraler Konstruktion unilateraler

Modelle. Zwar betont die NSA in einem Dokument, das “Second Party partnerships are extraordinarily close, and in some cases it is impossible to tell where one partner’s work ends and another’s starts” (National Security Agency 2012c). Der Austausch über die eigene organisationale Arbeit führt aber nicht automatisch zur Vergemeinschaftung von Modellen, sondern auch zur Entstehung eigener, wie die Abläufe im Workshop REMNATION II zeigen. Gleichzeitig wird deutlich, dass die Entwicklung neuer Modelle auch auf bewährten Handlungsweisen aufbaut. So ist die Entschlüsselung verdeckter Kooperation schon seit jeher eine Kernkompetenz der Geheimdienste und weist gerade zwischen NSA und GCHQ eine gewisse Tradition auf.

4.2.3 Anpassung an Kommunikationsentwicklungen: Innovation oder Fortführung der internalisierten kooperativen Kernkompetenz der Kryptoanalyse?

Es wurde angenommen, dass die Gleichwertigkeit der Partner hinsichtlich des Zugriffs auf bei Datenzugänge und damit ein fest institutionalisierter, hoher Datenaustausch mit einem übereinstimmenden kulturellen Kontext zu erklären ist. Diese Einflüsse können jedoch nur eine gewisse Vertiefung der Kooperation erklären, nicht aber die Art der Kooperationshandlungen. Eine tiefere Auseinandersetzung mit der Variable der technischen Unsicherheit offenbart jedoch, dass die NSA und der GHCQ gemeinsam ihre bereits traditionell in Kooperation durchgeführte Kernkompetenz der Kryptoanalyse weiterentwickeln und hier nicht nur effektive technische, sondern auch soziale Prozesse aufweisen.

Dies ist gerade in einer Organisationsumwelt nötig, in der die Organisationen sich ständig an Weiterentwicklungen allgemeiner technischer Strukturen anpassen müssen: „this generation’s challenge [is] mastering the cyberspace” (National Security Agency 2003f). Die Organisationen können aus ihrer Reaktion auf technische Unsicherheit jedoch nur dann einen Vorteil ziehen, wenn sie auch die Unsicherheit bezüglich einer späteren gesellschaftlichen Bewertung ihres eigenen Handelns berücksichtigen. Diese Annahme kann bewiesen werden, denn es ist feststellbar, dass NSA und GCHQ – trotzdem sie sich durch die bereits im Untersuchungsfall der Five Eyes ausgeführten Regelungen einen weiten Handlungsspielraum lassen – sich vor möglichen rückwärtigen Bewertungen illegitimen Verhaltens schützen und diese Notwendigkeit auch textualisieren. So zitiert die NSA die Bedenken des GHCQ wie folgt:

> „GCHQ and its sister intelligence agencies are challenged with their activities and operations being subject to increased scrutiny and oversight from their government (and public). As a result, closer attention is being paid to how UK-produced intelligence data is being used by NSA, and other partners” (National Security Agency (2012e).

Diese verstärkte Konzentration auf die legitime Verwendung von Daten, auch durch den Partner, lässt sich auch unter Verweis auf PRISM noch einmal unterstreichen. Zwar äußerte der GCHQ den Wunsch nach einer dauerhaften Teilhabe an dem Datensystem. Allerdings erbat sich die NSA als Antwort eine erneute Konsultation mit der höchsten Führungsebene, ob diese Initiative (weiterhin) unterstützt werden sollte (National Security Agency 2013g). Eine tiefe Kooperation kann also aufgrund der fehlenden Möglichkeit einer exakten Perzeption gesellschaftlicher Erwartungen nicht sofort und in jedem Fall – nicht einmal mit dem engsten Kooperationspartner – erfolgen. Auch in der Weiterleitung von GCHQ-Daten an andere Geheimdienste, mit denen die NSA Kooperationen aufweist, ist nicht ohne Einschränkungen möglich:

> „It is possible that Sir Iain [Lobban] may ask about what safeguards NSA may be putting in place to prevent UK data from being provided to others, the Israeli for instance, who might use that intelligence to conduct lethal operations" (National Security Agency 2013g).

Daher lässt sich mit vorliegender Fallstudie, die eine sehr enge Zusammenarbeit untersucht, nachweisen, dass die geheimdienstliche Kooperation selbst in der engsten und weitreichendsten formal und informell institutionalisierten Zusammenarbeit ein Spannungsfeld berücksichtigen muss. Zum einen muss sie einer effektiven Ausrichtung auf externe technische Entwicklungen zum Ziel besserer Aufklärung sowie, diesbezüglich, einem starken Datenaustausch entsprechen. Zum anderen muss sie auch der Tatsache, dass selbst im engsten Datenaustausch und einer Methodenteilhabe die Daten und Techniken trotzdem weiterhin derjenigen Organisation ‚gehören', die sie erschlossen und entwickelt hat und damit der Interpretation der Legitimitätsvorstellungen der Gesellschaft gerecht werden. Dieses Spannungsfeld verschärft sich bei kulturell sehr unähnlichen Kooperationspartnern, ist aber – wie dieser Fall zeigt – auch bei sehr ähnlichen und engen Partnern nachweisbar.

Der Untersuchungsfall NSA und GCHQ macht aber zusätzlich deutlich, dass die Organisationen selbst in der engsten Kooperation nicht nur einen gewissen unilateralen Handlungsraum wahren, sondern auch, dass Strukturen, selbst wenn sie nicht zu einer engen gemeinsamen Kooperation führen und wenn ihre kooperative Erarbeitung nicht ausdrücklich erwünscht ist, immer mit einer sozialen Auseinandersetzung mit den Strukturen der anderen Organisation einhergeht.[75] Wie bereits angedeutet wurde, versuchten sich die

[75] Im Untersuchungsfall Europol wird außerdem gezeigt, wie multilaterale Konstruktion erstens durch fehlenden Handlungsraum entsteht und, zweitens, dass sowohl unilaterale als auch multilaterale Strategien ebenfalls mit einzelorganisationaler Auseinandersetzung mit den Strukturen anderer Organisationen einhergeht. Da letztgenannter Faktor sowohl in kongruenten Kooperationskonstellationen (wie hier im Untersuchungsfall NSA

Kooperationspartner im Untersuchungszeitraum auch in unilateralen Strategien, um ein möglichst effektives Ergebnis zu erreichen. Damit ist nachweisbar, dass sich Organisationen in ihren Fähigkeiten einerseits aneinander orientieren, um effektiv kooperieren zu können. Andererseits reagieren die Organisationen in ihrer Anpassung jedoch auch auf die Techniken der Plattformen, die sie für ihren Erkenntnisgewinn ausspähen müssen und auf die Technik, die die andere Organisation zu dieser Ausspähung entwickelt hat (National Security Agency 2012h). Im Workshop REMNATION II versuchten sich beide Organisationen daher auch parallel – fern einer engen Abstimmung im Prozess – an geeigneten Methoden. Hierbei schien der GCHQ als erster erfolgreich gewesen zu sein, was die NSA dazu antrieb, aufzuschließen:

> „GCHQ has working version (QUICKANT). (…) NSA's version produced no obvious candidate selectors. Goal: Figure out if QUICKANT works, compare methodologies. Gathering data for additional tests of NSA's version" (National Security Agency 2012h).

Zusätzlich versuchte die NSA, gegenläufige Strategien zu der des Kooperationspartners zu entwickeln.

> „GCHQ has working QFD based on hard selectors (email, web forum, etc) but does not include cookies. Goal: NSA investigating own version (GREAT EXPECTATIONS) that would include cookies" (ebd.).

Auch die Vorleistung bei der Aufklärung von GVEs schien die NSA anzuspornen und zu einer stärkeren Eigenleistung auf diesem Gebiet zu animieren, anstatt sich nur auf die Fähigkeiten ihres Partners zu verlassen: „The SIGINT Enterprise needs to begin taking action now to plan for collection, processing, presentation, and analysis of these communications" (National Security Agency 2012h). Diese Ausführungen können als Beweise dafür gelten, dass die Einzelorganisationen, trotz ihrer engen Partnerschaft, auch und vor allem an den eigenen Bedingungen zur Steigerung von Fähigkeiten und geeigneten Reaktionsmustern auf eine komplexe und sich stets weiterentwickelnde technische Umwelt orientiert sind. Denn zum einen ist Kooperation – egal in welcher festen Institutionalisierung – immer eine zweitrangige Entscheidung der Organisationen, da sie in erster Linie ihrer Gesellschaft verpflichtet sind. Zum anderen können sich die Organisationen nicht blind darauf verlassen, dass die Lösung des Kooperationspartners effektiv ist, sondern selbst überzeugt sein, dass eine Technik den strukturellen Bedingungen angepasst ist. So müssen die Organisationen – schon alleine im Hinblick auf ihre Gesellschaft – darauf hinwirken, nicht alle Bereiche zu vergemeinschaften, sondern souverän zu sein. Daher sind eigene Entwicklung und Kooperation zwei maßgebliche

und GCHQ gezeigt) und in inkongruenten Kooperationskonstellationen (wie später im Fall Europol untersucht) auftritt, kann vermutet werden, dass es sich um einen allgemeinen Faktor organisationaler Praxis handelt.

Strategien von NSA und GCHQ, doch diese werden eben nicht synchron, sondern nur parallel verfolgt (National Security Agency 2008a). Diese Beobachtungen legen jedoch nahe, dass Kooperation und soziale Konstruktion nicht deckungsgleich sind und in einer späteren theoretischen Diskussion des internationalen interorganisationalen Kooperationsmodells möglicherweise stärker getrennt werden müssen. Denn auch wenn Organisationen in Teilbereichen nicht explizit miteinander kooperieren, sondern ‚nebeneinander arbeiten', ist eine soziale Wechselwirkung insofern beobachtbar, als dass sich Organisationen ständig in einer Abgrenzung oder Identifizierung mit den Praktiken anderer Organisationen befinden. Da Organisationen und ihre Handlungen damit nicht klar voneinander trennbar sind, stellt sich die Frage, inwieweit der Begriff Anpassung zu schärfen ist. Auch wenn keine Übernahme der Praktiken anderer Organisationen beobachtbar wäre, könnte ein Lernen am Beispiel anderer Organisationen stattfinden, dass Einfluss auf organisationales Handeln hat. Somit würde eine wissenschaftliche Untersuchung der organisationalen Umwelt von Sicherheitsbehörden, auch fernab der Vermutung einer Anpassung, umso zentraler.

Für die Falluntersuchung NSA und GCHQ lässt sich also zusammenfassen, dass die kulturelle Kongruenz und der stark habitualisierte gemeinsame Handlungsraum zu einer Kooperation führt, in der technische Systeme entstehen, die so stark kongruent und aufeinander aufbauend sind, dass die Techniken von NSA und GCHQ als Baukastensystem begriffen werden können. Zusätzlich konnte jedoch festgestellt werden, dass die Strukturen nicht vollständig vergemeinschaftet sind und ein solcher Zustand aufgrund der vorrangigen Bindung an die eigene Gesellschaft auch nicht geschaffen werden kann. Gleichzeitig kann vermutet werden, dass eine völlige Vergemeinschaftung auch aus Effektivitätsgründen nicht wünschenswert ist, da aus der, teilweise wettbewerbshaften, Abgrenzungen von den Strukturen des anderen, auch die Kreativität und Innovationskraft der Organisationen geweckt wird und zum Ausdruck kommen kann, was wiederum eine bessere Reaktion auf technische Bedingungen versprechen kann. Auch konnte gezeigt werden, dass Organisationen sich selbst in der Entwicklung eigener Praktiken stets miteinander in Austausch befinden und somit eine alleinig einzelorganisatorische Entstehung von Organisationshandlungen nicht angenommen werden kann. Vielmehr beschäftigen sich Organisationen immer mit dem Beispiel anderer und entscheiden dann, ob sie sich anpassen oder, in Abgrenzung eigene Praktiken entwickeln, die jedoch von den Handlungen der anderen inspiriert und damit nicht klar davon abzugrenzen sind. Damit konnten die Annahmen, die aus dem Neuen Institutionalismus herausgearbeitet und für den Untersuchungsgegenstand übertragen wurden, in diesem Fall bestätigt sowie um die vertiefende Beobachtung, dass eine Institutionalisierung der Kooperation in einigen Bereichen

und eine damit einhergehende Methodenkohärenz gleichzeitig auch von Methoden, die sich gerade von den Modellen besonders enger Partner abgrenzen, begleitet werden kann, da so Innovation gesteigert werden kann. Gleichzeitig bleibt die Tendenz, die daraus entstandenen erfolgreichen Handlungsmodelle wiederum dem besonders engen Kooperationspartner zugänglich zu machen, erhalten.

4.2.4 Präsenz und Absenz: Der Ehrgeiz der Analysten und die Lücken im Material

Da die ausgewerteten Dokumente nur einen Ausschnitt über die Aktivitäten von GCHQ und NSA darlegen konnten, sollen die vorangegangenen Erkenntnisse noch einmal hinsichtlich dessen kritisch bewertet werden, ob die in den Dokumenten ausgewiesenen Aussagen und Fakten aufgrund einer spezifischen Intention möglicherweise verzerrt sind oder ob die Einschränkungen durch das Material dazu geführt haben könnten, dass einige Zusammenhänge überproportional in den Vordergrund treten.

Einerseits ist hervorzuheben, dass die Dokumente über den Workshop REMNATION II nicht von der Leitungsebene, sondern offenbar von Analysten geschrieben wurden. Daher kann die Möglichkeit, dass auf dieser Ebene Informationen anders dargelegt werden, als dies den üblichen Organisationsnarrativen entspricht, in Betracht gezogen werden. So hat sich der Verfasser möglicherweise deshalb verstärkt auf divergente technische Strategien konzentriert, weil er diesem Umstand selbst eine starke Wichtigkeit zugesprochen hat. Es scheint zudem wahrscheinlich, dass die Konzentration auf die technologische Weiterentwicklung der NSA durch einen gewissen Ehrgeiz geprägt war und daher auch die narrative Aufbereitung der Ereignisse einen gewissen einzelorganisationalen Kampfgeist ausdrücken. Nicht ohne Grund lautet die Überschrift eines diesbezüglichen Dokuments wohl: „Tor stinks“ (National Security Agency 2012h).

Andererseits ist festzuhalten, dass die ausgewerteten Dokumente in der seit 1943 formal bestehenden Geschichte der Beziehungen von GCHQ und NSA einen vergleichsweise kurzen Zeitraum darstellen. Daher sind die in dieser Arbeit zitierten Aussagen als zeitgeschichtliche Momentaufnahmen zu sehen, die einerseits möglicherweise Entwicklungen geschuldet sind, die einen längeren – aber hier nicht abgedeckten – Zeitraum betreffen, oder andererseits, vielleicht gegenläufig zu vorherigen Entwicklungen stattfanden. Zugleich sind nur Informationen über einige wenige Projekte bekannt, sodass sich aus ihnen kein umfangreiches Bild über den Gesamtzustand der Kooperation ergeben kann. Auch kann nicht abschließend geprüft werden, ob die Einschränkungen hinsichtlich PRISM nicht vorrangig daher rühren, dass die NSA bei dieser Dateninfrastruktur mit Privatpartnern zusammenarbeitet und sie deren

Interessen schützen muss. Dies könnte die Teilhabe des GCHQ an dieser Struktur erschweren. Diese Folgerung ist aber in der Form nicht alleine über die Auswertung der Snowden-Dokumente nachvollziehbar.

4.3 Die Kooperation zwischen NSA und BND

Die NSA unterhält nicht nur zu ihren Five-Eyes-Partnern institutionalisierte Kooperationsarrangements. So reicht etwa die Kooperation zwischen US-amerikanischen und deutschen Diensten historisch weit zurück. Bereits die Wurzeln des heutigen BND, die Organisation Gehlen[76], wurden maßgeblich durch die US-Amerikaner aufgebaut und unterstützt (Ruffner 2007). Wie Abbildung 6 zeigt, lassen sich jedoch auch in jüngerer Zeit weitreichende gemeinsame Institutionen feststellen, die sich in einem gemeinsamen, personell gleichwertig besetzten, Analysezentrum und der Technikübertragung von XKEYSCORE an die Deutschen ausdrückt. Dies erscheint zunächst rätselhaft, denn zwischen NSA und BND zeichnet sich eine starke kulturelle Inkongruenz ab, die in der Kooperation der beiden Organisationen zunächst Hindernisse entfalten.

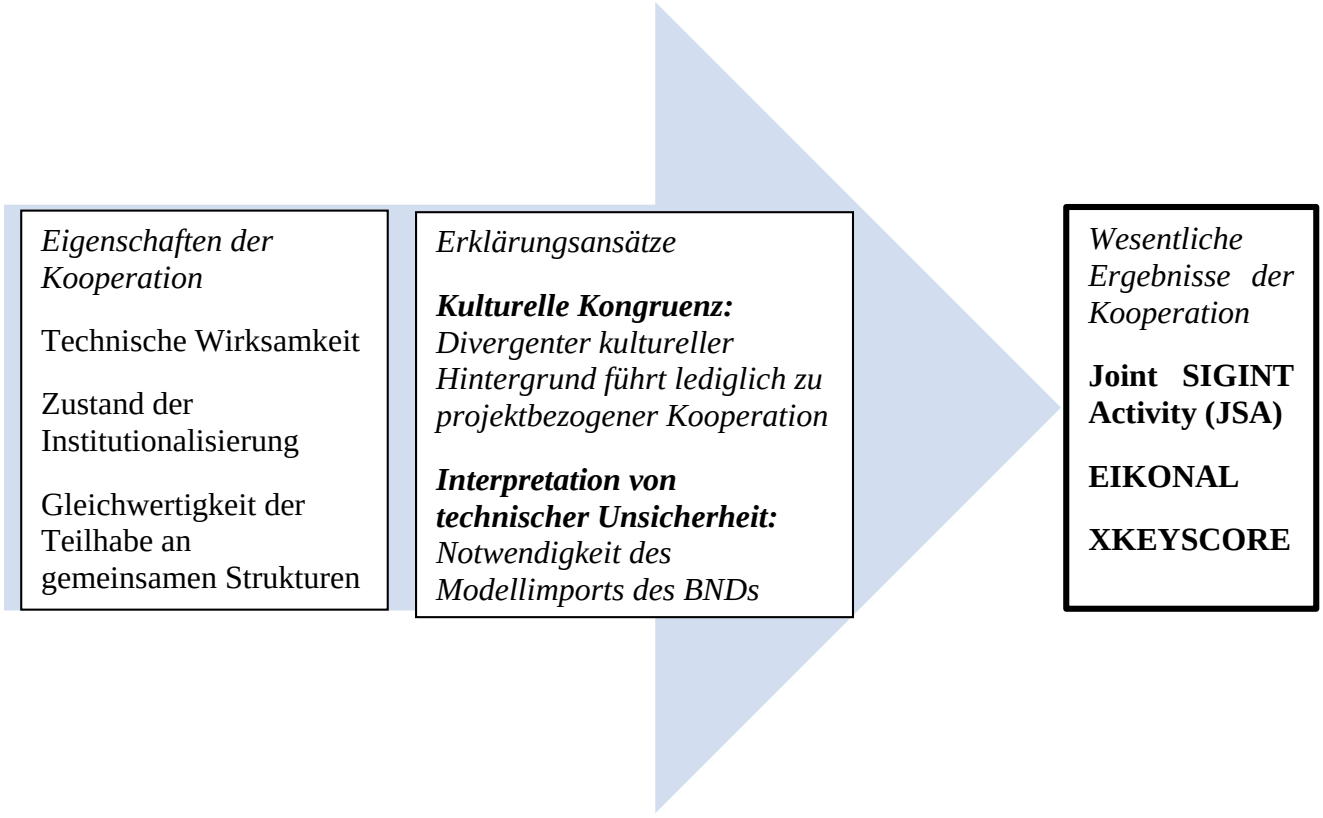


Abbildung 6: Erklärung der interorganisationalen Kooperation von NSA und BND.

[76] Der frühere Wehrmachtsgeneral Reinhard Gehlen wurde 1956 der erste Präsident des BND.

So sind zwar die gemeinsam erzielten Kooperationsergebnisse der NSA und des BNDs, die ‚Joint SIGINT Activity' (JSA) und die unter ihrem Dach zu verortende Operation EIKONAL, wirksame Instrumente zur militärischen SIGINT-Unterstützung und zur Terrorismusabwehr (Abschnitt 4.3.1). Allerdings lässt sich mit Hinblick auf die kulturellen Unterschiede, durch die der BND sich gegenüber der NSA vor allem technisch und methodisch anpassen muss, auch gewisse Hürden feststellen, die eine gleichwertige Teilhabe an Kooperationsstrukturen und eine dauerhafte Institutionalisierung der Kooperation erschwert (Abschnitt 4.3.2). Allerdings kann der BND durch seine Kooperation mit dem US-Dienst seine Reaktion auf die exogenen technischen Bedingungen deutlich verbessern, wovon auch die NSA profitiert. Die Snowden-Dokumente konnten für diese Zusammenhänge nur teilweise Erkenntnisse liefern, weshalb ihre Ausführungen durch die Zeugenaussagen und Einschätzungen im Rahmen des ‚NSA-Untersuchungsausschusses' ergänzt wurden. Dennoch soll kritisch geprüft werden, ob das Textmaterial ausreichend Aussagen trifft, um valide Erkenntnisse daraus abzuleiten (Abschnitt 4.3.4).

4.3.1 EIKONAL als Projekt der Joint SIGINT Activity

Vorliegende Arbeit geht davon aus, dass Kooperationen als besonders eng betrachtet werden können, wenn sie einen gleichwertigen Zugang zu einer wirksamen Struktur ermöglichen. Daher muss herausgearbeitet werden, welche Kooperationsstrukturen zwischen NSA und BND bestehen. Um Wirksamkeit zu erreichen müssen kooperative Strukturen Daten erschließen, Daten verknüpfen oder Daten weiterleiten, damit die Ziele eines möglichst weitreichenden, möglichst viele Daten verknüpfenden und vernetzenden Informationsbildes verwirklicht werden können. Ein gleichwertiger Zugang zeichnet sich dadurch aus, dass die Akteure die mit und in einer Struktur verbundenen Daten potentiell im gleichen Umfang nutzen können, also keinen unveränderlichen gesellschaftlichen oder technischen Hindernissen unterliegen, dies zu tun.

Zentral für die Kooperation zwischen der NSA und dem BND ist vor allem die Joint SIGINT Activity (JSA), die räumlich in der Mangfallkaserne im bayerischen Bad Aibling angesiedelt ist.[77] Gegründet wurde sie 2004 durch den damaligen NSA-Direktor Michael Hayden und den BND-Präsidenten August Hanning und ist damit Ausdruck einer gleichwertigen Initiative. Die

[77] „Seit 1988 ist der BND in Bad Aibling in der Mangfall-Kaserne untergebracht, anfangs noch neben Bundeswehreinheiten, die 2002 im Rahmen der Standortkonzentration abgezogen wurden. Im Gelände der Mangfall-Kaserne waren seit 1952 Militäreinheiten der US-Amerikaner stationiert. Die US-Amerikaner haben 2004 das Gelände der Stadt Bad Aibling zurückgegeben. In einer Vereinbarung mit der NSA kam man überein, ab 2004 in der Mangfall-Kaserne gemeinsam Auslandserfassung zu betreiben" (Bundestag 2017a: 761).

Mangfallkaserne beheimatet zudem die Special US Liaison Activity Germany (SUSLAG), welche als Dachorganisation des JSA betrachtet werden kann. Das SUSLAG ist mit dem NSA-Hauptsitz in Fort Meade, Maryland, sowie anderen NSA-Einrichtungen durch ein geschütztes Kommunikationsnetz, das NSANet verbunden (National Security Agency 2005b).[78] Die JSA war wichtiger Bestandteil der Operation EIKONAL, deren öffentliche Aufdeckung durch die Snowden-Dokumente ausgelöst und im NSA-Untersuchungsausschuss vertieft wurde. Die parlamentarischen Untersuchungen konnten durch viele Zeugenaussagen beteiligter BND-Mitarbeiter ein umfassendes Bild über diese Operation schaffen. Im Untersuchungszeitraum wurden durch NSA und BND im JSA jedoch mehrere gemeinsame Aufklärungsprojekte durchgeführt. Vor allem im Jahr 2005 fiel der Aufklärungsschwerpunkt des BND auf die Unterstützung deutscher Soldaten in Afghanistan sowie auf die Hilfeleistung für die SIGINT-Aktivitäten der Verbündeten im Gefechtsfeld (National Security Agency 2005b). Der Fokus lag zusätzlich auf Afrika und dem Irak und erbrachte im Jahr 2007 dreizehn Analyse-Produkte (National Security Agency 2007b). Darüber hinaus wurde in der JSA jedoch vorrangig Aufklärung und Analyse zur Terrorismusabwehr durchgeführt.

Auch die Operation EIKONAL, die 2004 startete, diente der Terrorismusabwehr. Bei EIKONAL handelte es sich jedoch, anders als bei der satellitenbasierten Mobilfunkaufklärung im Rahmen der militärischen Unterstützung des BND, um „eine Kabelerfassung bei einem deutschen Telekommunikationsunternehmen in den Jahren 2004 bis 2008“ (Bundestag 2017a: 706). 2004 bis 2005 lief EIKONAL im Probebetrieb. Der Wirkbetrieb begann im Frühjahr 2005 (Bundestag 2017a: 905). In diesem Zeitraum hat es weitere Initiativen dieser Art gegeben, die jedoch nicht zielführend waren. So heißt es im Bericht des NSA-Untersuchungsausschusses weiter:

> „Die unter dem Operationsnamen GLO… – unabhängig von der Zusammenarbeit des BND mit der NSA in Bad Aibling – mit einem anderen US-amerikanischen Nachrichtendienst[79] realisierte Kabelerfassung bei dem deutschen Tochterunternehmen eines US-amerikanischen Telekommunikationsdienstleisters war bereits im Jahr 2006 wieder beendet worden. (…) Eine Kooperation mit einem britischen Nachrichtendienst im SIGINT-Bereich[80], bei der eine Zusammenarbeit im Bereich der Kabelerfassung auf deutschem Staatsgebiet in Rede stand, wurde nicht realisiert, die entsprechenden Planungen noch im Jahr 2013 beendet“ (ebd.).

[78] Die JSA wird außerdem in den Snowden-Dokumenten mit einem eigenen Logo bedacht, die das US-amerikanische Wappentier, den Weißkopfseeadler, vor einer deutschen Flagge und mit dem Motto „Der Zeitgeist“ (National Security Agency 2014h) abbildet.

[79] Der BND kooperiert also nicht nur mit der NSA. Weitere Einzelheiten sind nicht bekannt.

[80] Es wird angenommen, dass es sich hierbei um den GCHQ handelt, weitere Details gehen weder aus dem Bericht des NSA-Untersuchungsausschuss (Bundestag 2017a) noch aus den untersuchten Dokumenten hervor.

Bei EIKONAL handelte es sich, allen Anscheins nach, um eine Datenerfassung an einem Glasfaserkabel im Raum Frankfurt am Main[81] unter Beteiligung von BND und NSA. Die Analyse der abgefangenen Kommunikation wurde vorrangig in der JSA durchgeführt. Bei der Erfassung habe es sich vor allem um Ausland-Ausland-Verkehre gehandelt, also um Kommunikation, deren Ende und Ausgangspunkt im Ausland lagen, aber per Kabel durch Deutschland geleitet wurden, sogenannte Transitverkehre. Diese Daten wurden in einer Überprüfung nach inländischen Kommunikationen untersucht und erst dann zu einer gemeinsamen Analyse zur Verfügung gestellt. Hierfür wurden spezielle Filtersysteme sowie eine anschließende manuelle Überprüfung angewandt (Bundestag 2017a: 887 ff.). Wie viele Daten die Operation EIKONAL konkret erbrachte, ist indes nicht bekannt.

Die Sichtung der Snowden-Dokumente lässt auch auf weitere Aufklärungsprojekte der NSA und des BNDs schließen, allerdings können hier die Zusammenhänge nicht lückenlos belegt werden. Das NSA-Partnerprojekt RAMPART-A startete 1992 und ist, gemeinsam mit WINDSTOP, dem britischen Zugangspunkt, Teil des Foreign Partner Access Projects. Das Projekt folgt einem institutionalisierten Ablauf: Die NSA unterstützt in dessen Rahmen sowohl Five-Eyes-Partner als auch Drittpartner mit Equipment, welches der Partner in seine Infrastrukturen einbaut. In der Folge findet eine gemeinsame Erfassung und Analyse statt (National Security Agency 2014e). Somit könnte es sich also bei EIKONAL um ein solches Projekt handeln, wobei nicht abschließend geklärt werden kann, ob sich EIKONAL unter das Programm RAMPART-A oder möglicherweise unter Zugangspunkte anderer Bezeichnung zusammenfassen lässt, die durch die Snowden-Dokumente nicht bekannt wurden. Ein Hinweis, dass Deutschland Teil des RAMPART-A sein könnte, kann sich aus der Festlegung der NSA, „Partner offensive tasking“ (ebd.) zu löschen, ergeben, da eine ähnliche Vereinbarung zumindest für die JSA vorliegt. Der Zusatz „The new capabilities will enable increased collection of communications available at each RAMPART-A site“ (ebd.) lässt zudem vermuten, dass es sich bei RAMPART-A um einen Covernamen für mehrere Datenzugänge

[81] Dabei handelt es sich aber nicht um den Netzwerknoten De-Cix, wie sowohl der private Betreiber, als auch die Bundesregierung bestätigten (Bundestag 2017a: 894). Frankfurt ist jedoch ein zentraler Punkt, an dem viele Kommunikationsverbindungen, unter anderem aus Osteuropa, dem arabischen Raum, aber auch Österreich und der Schweiz, zusammenlaufen (Bundestag 2017a: 895). Der Betreiber der Infrastruktur, die Deutsche Telekom AG, war über das Vorgehen informiert: „Der BND ist auf uns zugekommen. Wir waren mit dem BND schon vorher in Kontakt, weil wir durch Artikel 10 Gesetz respektive TKÜV schon verpflichtet worden waren, entsprechende G-10-Anordnungen umzusetzen. Im Zuge dessen kannten die uns also schon und dann sind die (…) so zwischen Spätfrühjahr, Anfang Sommer 2003 diesbezüglich auf uns zugekommen mit dem Ansinnen, dass sie halt über G 10 hinaus mehr haben wollten“ (Bundestag 2017a: 898). Die Ermächtigung der Überprüfung von Ausland-zu-Auslandkommunikation über die Infrastruktur eines privaten Betreibers hätte dieser, anders als bei G-10-Anordnungen, auch verweigern können (Bundestag 2017a: 897).

eines Partners oder mehrerer Partner handelt (National Security Agency 2014e). In einem Dokument, das um das Jahr 2013 entstanden sein muss,[82] heißt es zudem „RAMPART-A employs TURMOIL capabilities" (National Security Agency 2014a). Zwar interessierte sich der BND im Untersuchungszeitraum für die TURMOIL-Technik (National Security Agency 2006a). Allerdings kann dies nicht als ausreichender Beweis für eine Teilhabe des BNDs an RAMPART-A gewertet werden, selbst wenn Medienberichte dies klar in Betracht ziehen (Meister 2014).

Insoweit man Rückschlüsse auf EIKONAL sowie andere Operationen in der JSA Rückschlusse ziehen kann, handelt es sich hier um eine sehr wirksame Kooperation für beide Partner. Während die NSA sicherstellen konnte, dass der BND die Terrorismusabwehr für Deutschland und die hierfür benötigte Aufklärung globaler Kommunikation durch NSA-Technologie sowie -training bewerkstelligen und sie die abgefischten Daten nutzen konnte, profitierte der BND durch die Daten und die technische Unterstützung. Allerdings muss geprüft werden, ob und auf welche Weise die kulturellen Unterschiede zwischen den Organisationen eine, möglicherweise weitere, Vertiefung behinderten. Auch sollte betrachtet werden, ob die Divergenz ein die gemeinsamen Aktivitäten erschwerte.

4.3.2 Inkongruenz oder Abhängigkeit?

Vorliegende Arbeit folgt der Annahme, dass Kultur eine wichtige Voraussetzung für die Reichweite organisationalen Handelns und einen wichtigen Erfahrungsraum darstellt und deshalb vor allem Kooperationspartner, die einen ähnlichen kulturellen Hintergrund aufweisen, eng zusammenarbeiten können. Daher spannt eine ähnliche Kultur einen kompatiblen Handlungsraum auf, da nur in einer ausreichend offenen Organisationsumwelt innovative Lösungen erdacht werden können. Obwohl die Kooperation zwischen NSA und BND in der JSA im Rahmen der Operation EIKONAL weitreichend erscheint, kann angenommen werden, dass die Gleichwertigkeit und Institutionalisierung der Kooperation zwischen NSA und BND geringer ausgeprägt ist als zwischen der NSA und ihren Five-Eyes-Partnern, da mangelnde Erfahrungen und Befähigungen den BND einschränken und er daher auch nur von einer schwachen Position aus mit der NSA kooperieren kann.

Die kulturellen Unähnlichkeiten können darauf verdichtet werden, dass die NSA sich in einer expansiven, den strukturellen Bedingungen ihres Arbeitsumfeldes stets angepassten Weise

[82] da es Budgetplanungen enthält, die für das Jahr 2012 schon abgeschlossen und für das Jahr 2013 bereits angesetzt sind (vergleiche National Security Agency 2014a)

entwickeln kann, da ihre Gesellschaft eine größer Handlungsreichweite toleriert und verlangt (Peine/Sturm 2008). Zwar ist auch Deutschland den strukturellen Bedingungen internationaler Krisen und daraus folgenden Handlungsnotwendigkeiten ausgesetzt. Allerdings werfen Beobachter gerade der deutschen Gesellschaft und ihren politischen Entscheidungsträgern einen Mangel an strategischem Denken vor (Merten 2015; Krieger 2010: 805). Auf der einen Seite steht mit der NSA also ein Nachrichtendienst, der sich aufgrund seiner Ressourcenstärke und der unterstützenden Nachrichtendienstkultur zu einem der mächtigsten Nachrichtendienste entwickeln konnte und der außerdem in eine starke Gruppe der Geheimdienste der Anglosphäre eingebunden ist. Auf der anderen Seite operiert der BND in einer eher beschränkenden Nachrichtendienstkultur und ist diesbezüglich nicht so technisch innovativ und ressourcenstark wie die NSA und zudem noch einer starken Skepsis der deutschen Gesellschaft gegenüber einer starken außenpolitischen Rolle ausgesetzt, die sich nur langsam wandelt (Gauck 2014; Smidt 2008; Peine/Morisse-Schilbach 2008: 338). Aus der empirischen Analyse geht hervor, dass der BND im Untersuchungszeitraum aus eigener Kraft keine Kapazitäten zur methodischen Anpassung an strukturelle Bedingungen der SIGINT-Analyse vorweisen konnte und so bei der Reaktion auf diese gänzlich auf die Fähigkeiten der NSA angewiesen war (Bundestag 2017a: 728). Die Zusammenarbeit mit dem BND gestaltete sich jedoch trotz dessen offensichtlichen Bedarfs an Kooperationslösungen, vor allem aufgrund unterschiedlicher Transparenzverständnisse und zu erfüllenden gesellschaftlichen Institutionen, die wiederum Einfluss auf die technische Arbeitsweise des deutschen Auslandsnachrichtendienstes hatte, diffizil (National Security Agency 2013b).

Ausgehend von den Projekten in der JSA lässt sich indes zunächst kein objektives Ungleichgewicht darstellen. Personell waren NSA und BND in der JSA gleich ausgestattet. Dort arbeiteten zehn bis 15 BND-Mitarbeiter sowie ebenso viele NSA-Mitarbeiter unter deutscher Leitung (Bundestag 2017a: 767). Allerdings sind die gemeinsamen Regelungen, die die Zusammenarbeit in dem gemeinsamen Zentrum strukturieren, als nicht so weitreichend wie die der Five Eyes zu bewerten. So besteht zwar eine Vereinbarung für die JSA, die festlegt, dass keine deutschen sowie Five-Eyes-Nationalitäten oder Orte ausgespäht und keine europäische Wirtschaftsspionage praktiziert werden darf (Bundestag 2017a: 1286). Hierbei lässt sich also auf eine Regulierung schließen, da die Interessen von beiden Partnern, zumindest auf dem Papier, gewahrt werden. In den Snowden-Dokumenten findet sich zudem eine Liste derjenigen deutschen Selektoren, die von der Aufklärung ausgeschlossen werden sollen

(National Security Agency 2014f).[83] Die formale Abmachung für die JSA aus dem Jahr 2002 ist aber auch nicht mit einem generellen ‚Memorandum of Agreement', zum gegenseitigen Verzicht der Spionage, vergleichbar.[84] Generell ist festzuhalten, dass sich der Ausschluss der Ausspähung deutscher Bürger – ähnlich der Vereinbarungen mit den engeren Partnern, beispielsweise dem GCHQ – vermutlich nur auf die intendierte Aufklärung bezieht und deutsche Selektoren in der Datenbank anonymisiert werden, jedoch trotzdem als Hinweisgeber auf weitere Personen dienen konnten. Auch lässt sich nachweisen, dass die NSA unilateral gegen diese Vereinbarung verstoßen hat, indem sie die Kommunikation von Bundeskanzlerin Angela Merkel ausspähte (National Security Agency 2014p). So kann entweder davon ausgegangen werden, dass sich die Vereinbarung nur auf die Verarbeitung von Selektoren zur Metadatenanalyse erstreckte, oder dass die gezielte Spionage aus Sicherheitserwägungen durch eine Sonderklausel ausgenommen war. Denkbar ist aber auch, dass die NSA schlicht gegen diese formale Regel gehandelt hat. Es handelt sich bei der genannten Einschränkung jedenfalls eindeutig um eine weniger geronnene Praxis, als sie zwischen NSA und den Five Eyes festzustellen ist.

Als eine die Gleichwertigkeit des Zugangs zu gemeinschaftlich genutzten Daten und Strukturen zusätzlich schwer einschränkende Tatsache muss zudem festgehalten werden, dass Deutschland ein wichtiger Standort des US-Militärs ist. Wichtigste US-SIGINT-Einrichtung in Deutschland, ohne Beteiligung des BND, ist das European Security Center (ESOC)[85] in Darmstadt. In Zusammenarbeit mit Kooperationspartnern in Afrika[86] erhebt es Informationen zur Terrorismusabwehr. Durch die Aufklärungsaktivitäten sollten afrikanische Regierungen darin unterstützt werden, ihre Territorien effektiver gegen Terroristen schützen zu können. In diesem Rahmen kam es zum "capture or kill of over 40 terrorists" (National Security Agency 2005a). Somit ist das ESOC wichtiger Standort für die Terrorismusbekämpfung der NSA, denn zum

[83] Unter den 31 ausgeschlossenen Selektoren, hinter denen sich vor allem deutsche Organisationen verbergen, befinden sich unter anderem BASF, Mercedes Benz, die Bundeswehr, aber auch eher kurios anmutende, ausgeschlossene Organisationen, wie die Freiwillige Feuerwehr Ingolstadt (National Security Agency 2014f.).

[84] Jedoch wollte der BND-Präsident Gerhard Schindler in einem Austausch mit Keith Alexander für ein sogenanntes No-Spy-Abkommen genau an dieser Vereinbarung anknüpfen (Bundestag 2017a: 465). Es wurde jedoch letztlich nicht umgesetzt. Der Bericht des NSA-Untersuchungsausschusses erörtert die Gründe dafür ausführlicher (Bundestag 2017a: 444 ff.).

[85] Das European Security Center (ESC) wurde am 5. Juli 2006 in das European Security Operations Center (ESOC) umbenannt. Der Auftrag der militärischen und regionalen Aufklärung war bis 2013 gegeben (National Security Agency 2006b). Ob das ESOC darüber hinaus Bestand hatte, ist nicht bekannt. Damalige Foki lagen – neben der Terrorismusbekämfung – auf der Afrikanischen Union, der Energie-Sicherheit Nigerias, Zielen in Marokko, Algerien, Tunesien und Libyen (National Security Agency 2006b). Das ‚Hauptquartier' der NSA auf deutschem Boden wird auch als NSA/CSS Representative Europe (NCEUR) bezeichnet.

[86] Die NSA bezeichnet diese Kooperationspartner als "truly non-traditional customers (e.g., governments in Algeria, Mali, and Mauretania)" (National Security Agency 2005a)

einen soll der Terrorismus in afrikanischen Ländern selbst verhindert werden, zum anderen soll auch die Einreise von Terroristen aus dieser Region in westliche Länder bekämpft werden. Durch die Aufklärung von Netzwerken radikaler Einzelpersonen wollen die USA zusätzlich vermeiden, dass Ausländer in, vor allem nordafrikanische, Länder reisen und sich dort weiter radikalisieren, in Konflikten kämpfen und, dass diese nach Europa zurückkehren (National Security Agency 2013i). Neben dem ESC gibt es mit dem European Technical Center (ETC)[87] in Wiesbaden Mainz-Kastel noch eine weitere rein US-amerikanische Einrichtung. Das ETC dient als „communications hub" (National Security Agency 2011a) mit Partnern in Europa, Afrika und dem Nahen Osten und soll dabei vor allem Kommunikationssicherheit und SIGINT für militärische Zwecke zur Verfügung stellen (National Security Agency 2011a). Es ist zudem federführender Entwickler multilateraler Kooperationen mit europäischen SIGINT-Diensten, an denen auch Deutschland beteiligt ist. Ein solches multilaterales Forum stellen die SIGINT Seniors Europe (SSEUR) dar, an dem die Five Eyes, Deutschland, Belgien, Dänemark, Frankreich, Italien, die Niederlande, Norwegen, Spanien und Schweden teilnehmen und das sich vorrangig um Terrorismusabwehr kümmert (National Security Agency 2014m). Neben diesem Kreis hält die NSA ein weitreichendes Netz an bilateralen Kooperationen vor, was es diffizil gestaltet, die Bedeutung des Partners Deutschland für die NSA eindeutig herauszuarbeiten. Im Jahr 2012 führte die NSA Algerien, Österreich, Belgien, die Tschechische Republik, Dänemark, Äthiopien, Finnland, Frankreich, Deutschland, Griechenland, Ungarn, Indien, Israel, Italien, Japan, Jordanien, Südkorea, Mazedonien, die Niederlande, Norwegen, Pakistan, Polen, Rumänien, Saudi-Arabien, Singapur, Spanien, Schweden, Taiwan, Thailand, Tunesien, die Türkei, und die Vereinigten Arabischen Emirate (VAE) als Drittpartner (National Security Agency 2014k). Es ist also davon auszugehen, dass nicht nur der BND durch die NSA mit Training und Equipment zur Aufklärung globaler Kommunikationsnetzwerke ausgestattet wurde (National Security Agency 2003n). 2010 beispielsweise trafen sich NSA-Personal des Signals Intelligence Directorates (SID) und des Foreign Affairs Directorate (FAD)[88] zu einem „analytic course for NSA Third Party partners" (National Security Agency 2010a) im ETC. Ziel des Treffens war die Übereinbringung von Methoden und Begriffen für (gemeinsame) SIGINT-Aktivitäten. Die Meetinginhalte betrafen ein

[8787] Zusätzlich ist das ETC Aufklärungszentrum einer ‚Special source operation' unter der Coverbezeichnung OAKSTAR, die gemeinsam mit der polnischen Regierung durchgeführt wird. Der Zugriffspunkt liefert Informationen über die afghanische Armee, Kommunikation im Nahen Osten und Informationen von Teilen des afrikanischen Kontinents sowie europäische Kommunikation (National Security Agency 2014l).

[88] Das FAD ist eine spezielle Abteilung der NSA zur Anbahnung und Planung von Drittpartnerschaften (National Security Agency 2010a).

> "common understanding of the importance of SIGINT Development (SIGDEV) as a discipline, and a common definition of SIGDEV efforts. This effort enhanced the opportunities for SSEUR partners to work together more effectively to tackle mission areas of mutual interest – especially Afghanistan and Counterterrorism (CT) target sets" (ebd.).

Aus dieser Darlegung der unilateralen Präsenz der NSA in Deutschland einerseits, und andererseits, der breiten Ausrichtung auf Kooperationen mit vielen unterschiedlichen Partnern, lassen sich für die Kategorien der Enge und Gleichwertigkeit der Kooperation also Einschränkungen ableiten. Zum einen erwächst ein gutes Kooperationsverhältnis bei gleichzeitiger Militärpräsenz nicht auf gänzlich freiwilliger Basis, sondern aus einer historischen Pfadabhängigkeit heraus (Wolf 2013: 1042 f.). Hervorzuheben ist jedoch, dass sich daraus auch eine gewisse dauerhafte Institutionalisierung ergibt, die sich auf die Wirksamkeit der Kooperation positiv auswirken kann. Andererseits ist die NSA Dreh- und Angelpunkt vielfältiger institutionalisierter Kooperationspartnerschaften mit dem Fokus auf der Weiterbildung und technischen Ausstattung der Partner. Insofern kann die NSA ihre Kooperationsbereitschaft für einzelne Partner begrenzen, während sie selbst für die meisten Kooperationspartner sicherlich wichtigste Anlaufstelle ist. Daher ist ein Abhängigkeitsverhältnis, nicht nur für die Kooperation zwischen NSA und BND, wahrscheinlich. Auch wenn eine Orientierung an ähnlichen ordnungspolitischen Vorstellungen die Beziehungen zwischen Deutschland und den USA harmonisierend beeinflusst, kann auf Organisationsebene ein deutliches Ungleichgewicht attestiert werden (Jäger 2012: 149; Hacke 2011). Einige Autoren sprechen auch von einer Hegemonie, die die USA auf Deutschland – und damit auch auf seine Organisationen – ausübt (Katzenstein 2008: 157; Krieger 2010: 802).

Am deutlichsten wird diese Divergenz zwischen NSA und BND jedoch in Bezug auf unterschiedliche Erfahrungs- und Handlungsräume. Sie manifestiert sich in sich stark unterscheidenden formalen und informellen Verfahrensweisen und Fähigkeiten. Gerade in Bezug auf den gesellschaftlichen Konsens zu Rolle und Aktivitäten von Nachrichtendiensten besteht eine große Diskrepanz zwischen den USA und Deutschland, da der BND an größere Beschränkungen und ein stärkeres gesellschaftliches Bedürfnis nach parlamentarischer Kontrolle gebunden ist. Aus den Snowden-Dokumenten wird ersichtlich, dass sich diese Punkte bereits negativ auf das Kooperationsverhältnis ausgewirkt haben:

> "The Germans have previously approached NSA about using information derived from SIGINT in open court. CT is concerned that exposing SIGINT capabilities in German court threatens the ability to maintain the desired and planned for level of SIGINT cooperation" (National Security Agency 2013b).

So kann gezeigt werden, dass die Kooperation zwischen NSA und BND beiden Seiten zwar einen zusätzlichen Wert bringt und durchaus einen gewissen Zustand der Institutionalisierung, etwa durch eine gemeinsame Einrichtung mit gebündelten Analysefähigkeiten und einer Ausschlussklausel in der JSA, aufweist. Allerdings kann nicht von einer Gleichberechtigung im Sinne eines gleichwertigen Zuganges zu Informationen und Ressourcen gesprochen werden. Vielmehr besteht ein Verhältnis der Reziprozität, das dem BND durch die Kooperation einen organisational sinnvollen Mehrwert durch steigende technische Befähigung sichert, in dem jedoch die NSA – im Gegenzug – eine Zusicherung, auch zukünftig kooperativ und unilateral in Deutschland tätig werden zu können, erhält. Diesen Zusammenhang belegt auch die Aussage von T. B.,[89] Leiter des Sachgebiets JSA vom 1. November 2003 bis 30. September 2007, im NSA-Untersuchungsausschuss:

> „Der konkrete Nutzen für uns war, dass wir Zugang zu Material und Technik erhielten, die uns vorangebracht haben und dann eigentlich auch Dinge waren, die wir dann nicht selber von Grund auf neu entwickeln mussten, sondern auf einer bestimmten Basis aufsetzen konnten. Der Nutzen für den AND[90] war natürlich, dass sie weiterhin bestimmte Ressourcen innerhalb Deutschlands nutzen konnten“ (Bundestag 2017a: 766).

Die Wirksamkeit für den BND ergab sich herausragend durch die Übernahme der XKEYSCORE-Technologie von der NSA. Der US-amerikanische Dienst gab im Untersuchungszeitraum seine teilautomatisierte Metadatenanalysesoftware zunächst an den BND und später auch an das Bundesamt für Verfassungsschutz (BfV) weiter (National Security Agency 2013i). Gleichzeitig bedeutet das divergente Partnerschaftsverhältnis aber auch eine gewisse Beeinflussung der Tätigkeiten des BND durch die NSA und eine Einwilligung des BNDs in Strategien, die die NSA für die Weiterentwicklung der Kooperation entwickelt und damit auch den Ausbau der Tätigkeiten und Fähigkeiten des BNDs voranbringt. Zwar werfen Beobachter dem BND schon lange eine gewisse „Unterwürfigkeit“ (Krieger 2010: 802) gegenüber den amerikanischen Diensten vor. Es kann jedoch durch die Snowden-Dokumente erstmalig nachgewiesen werden, dass die NSA eine Veränderung der BND-Aktivitäten anstrebt, um die Kooperation durch Kompatibilität zu vertiefen: “Full use of current NSA DNI processing systems and analysis methodologies at JSA will be key to influencing the BND to alter their strategic DNI processing approach” (National Security Agency 2006a). Auch wird deutlich, dass die NSA einen direkten Zusammenhang zwischen der, in ihren Augen ineffektiven, Arbeitsweise des BND und dessen beschränkendem, kulturellen Handlungsraum

[89] Der volle Name des leitenden Beamten ist nicht bekannt, er wird in der Zeugenliste des NSA-Untersuchungsausschusses lediglich unter diesen Initialen geführt (Bundestag 2017a: 124).
[90] Allgemeine Abkürzung für einen ausländischen Nachrichtendienst (Bundestag 2017a: 1887).

– und vor allem die diesbezügliche Bindung an strenge Datenschutzvorschriften – sieht und daher adressiert, dass nur durch einen erweiterten Handlungsrahmen auch eine engere Kooperation zwischen NSA und BND ermöglicht werden kann:

> „The BND's inability to successfully address German privacy law (G-10) issues has limited some operations, but NSA welcomed German willingness to take risks and to pursue new opportunities for cooperation with the U.S, particularly in the CT realm" (National Security Agency 2013b)".

Diese Ausübung eines gewissen Einflusses auf den BND wird an dieser Stelle noch einmal besonders deutlich. Dies zeigt zwar einerseits, dass von einer faktischen Gleichwertigkeit der Partner nicht gesprochen werden kann. Gleichzeitig findet jedoch auch die einseitige Ausnutzung dieser Inkongruenz durch einen der Partner dort ihre Grenzen, wo der Kooperationspartner dieses Missverhältnis spürt und die Kooperation möglicherweise einschränkt. Auch die NSA registriert dieses Spannungsfeld und hebt hervor, dass eine gute Kooperation mit Drittpartnern nur dadurch gelingen könne, in dem eine „best fit" (National Security Agency 2003k) Lösung angestrebt werde, in der jedoch jedem Partner durchaus eine Rolle zugewiesen werden könne. Somit ist die Einschätzung des Verhältnisses zwischen NSA und BND divergent. Zum einen ist durchaus ein Abhängigkeitsverhältnis durch eine stärkere und schwächere Rolle festzustellen. Hervorzuheben ist aber auch, dass die NSA dem BND Technologien weitergibt und dabei einem Kooperationspartner, der lediglich ein Drittpartner ist, in einem nicht unwesentlichen Maße Unterstützung zukommen lässt. Gerade bei der Operation EIKONAL kann die Diskussion, ob es sich um eine ‚Best-Fit'-Lösung oder eine Abhängigkeit gehandelt hat, aber auch aus einem anderen Grund kritisch geführt werden. So ergibt sich aus der Aussage eines BND-Mitarbeiters der Nachweis, dass der BND sich an eine starke horizontale Erwartungserfüllung gegenüber der NSA gebunden sah: „Wir hatten das G-10-Aufkommen, und wir hatten das Routineaufkommen, das uns die Verpflichtungen erfüllen ließ gegenüber der NSA" (Bundestag 2017a: 1498 f.). Diese Einschätzung wird auch dadurch bestätigt, dass BND und NSA mit EIKONAL über vier Jahre sowohl Inland-Ausland-Verkehr (G-10-Verkehre), die jedoch einer spezifischen Behandlung nach dem G10-Gesetz bedurft hätten und durch den BND nicht an ausländische Nachrichtendienste weitergegeben hätten werden dürfen, als auch Transitverkehre, die der BND auch als Routineverkehre, also Kommunikation zwischen Ausland und Ausland, bezeichnet, aufklärte, was die Organisation damit rechtfertigte, dass sie gegenüber der NSA einen Ausgleich für deren technische Ausrüstung hätte erbringen müssen:

> „Es ist nur allgemein, auch gegenüber der G-10-Kommission, bei den Besuchen in Pullach darauf hingewiesen worden, dass der sogenannte Routineverkehr für den

> Bundesnachrichtendienst eine große Bedeutung hat, insbesondere auch deswegen, weil der Bundesnachrichtendienst damit seine Kooperationspartner bedienen kann und praktisch Gegenleistungen erbringen kann für das, was Partner dem Bundesnachrichtendienst geben“[91] (Bundestag 2017a: 4957).

Da also die Kooperation zwischen NSA und BND zwar von einer gewissen gleichwertigen Teilhabe, gleichzeitig jedoch von komplexen Abhängigkeiten und Beschränkungen geprägt ist, erscheint es zwar erwiesen, dass die kulturelle Divergenz das Kooperationsverhältnis zwischen NSA und BND erschwert. Allerdings können nicht alle Ausgestaltungen anhand dieses Zusammenhanges begriffen werden, da diese Variable zwar die Nicht-Existenz von gleichberechtigten Strukturen, nicht aber die Weitergabe von XKEYSCORE sowie die Anbahnung von EIKONAL ausreichend erklären kann. Daher wird nachfolgend geprüft, ob die beobachtbaren Zusammenhänge auch durch die Wahrnehmung von Unsicherheit hinsichtlich möglicher gesellschaftlicher Reaktionen auf technische Lösungen sowie durch die Interpretation interorganisationaler struktureller Notwendigkeiten in Bezug auf die Anpassungen an externe technische Strukturen erklärbar sind.

4.3.3 Die NSA als technischer Ausstatter des BNDs?

Die Organisationstheorie des Neuen Institutionalismus geht davon aus, dass für die Entwicklung und Aufrechterhaltung einer engen Kooperation sowohl eine organisationale Auseinandersetzung mit der gesellschaftlichen Ebene, als auch mit der interorganisationalen Ebene stattfinden muss. Gleichzeitig müssen die Organisationen prüfen, ob ihr Kooperationsarrangement ausreichend an die strukturellen Bedingungen ihrer exogenen technischen Umwelt angepasst ist. Die Unsicherheit hinsichtlich geeigneter Organisationslösungen für gegenwärtige und zukünftige Phänomene, für die die jeweiligen verwendeten Techniken möglicherweise nicht (mehr) ausreichend sind, stellt jedoch ein zentrales Problem für Organisationen dar. Denn darauf bezogene technische Lösungen werden durch die Notwendigkeit, dass diese gegenwärtig und zukünftige Legitimitätsbewertungen berücksichtigen müssen, verkompliziert.

Die Snowden-Dokumente zeigen, dass beide Organisationen die Lücke zwischen BND und NSA hinsichtlich ihrer technischen Fähigkeiten, aber auch die grundsätzlich mangelhafte technische Basis des BNDs in der Erbringung seiner eigenen Aufklärung, als Gründe für die Ausgestaltung der Kooperation thematisieren. Der BND operierte zum Zeitpunkt der Übertragung von XKEYSCORE mit veralteten NSA-Systemen: “BND analysts discussed their

[91] Diese Aussage stammt von Joachim Mewes, der von August 2001 bis September 2008 Leiter verschiedener Referate der Abteilung 6 im Bundeskanzleramt war (Bundestag 2017a: 579 f.).

processing architecture, which is largely based on NSA's old P25 and P26 GRANDMASTER prototypes" (National Security Agency 2006a). Diese Zitierstelle beweist sowohl, dass die Fähigkeiten des BND nicht mehr zeitgemäß waren, als auch, dass die NSA den BND schon vor dem Untersuchungszeitraum mit Technik versorgt hatte. Durch die Dokumente nachweisbar ist auch, dass der BND – im Rahmen der Diskussion seiner damaligen in Verwendung stehenden Techniken – 2006 durch Demonstration der US-amerikanischen Systeme Einblick in diese erhielt. 2007 stellte er dann eine Anfrage nach der Übertragung dieser Technologien im Rahmen des JSA (National Security Agency 2007b). Vorangegangen war auch beim BND die Einsicht, dass die Technik den aktuellen Entwicklungen nicht mehr angemessen war. So berichtete Hartmut Pauland, ehemaliger Leiter der Abteilung Technische Aufklärung (TA) beim BND, gegenüber dem NSA-Untersuchungsausschuss, innerhalb des BND habe man die Bedeutung von Metadaten zur Kommunikationsaufklärung zwar erkannt, habe jedoch nicht über die entsprechenden Kompetenzen und Mittel verfügt, diese zu verarbeiten „weil wir ja gemerkt haben, dass wir technisch einfach nicht up to date sind. Das war eine Diskussion, die auch schon in 2012 gelaufen hat, weil man mit diesem metadatenzentrierten Ansatz eben überhaupt noch nicht zurechtkam bzw. nicht die entsprechenden Mittel und Fähigkeiten hatte" (Bundestag 2017a: 728).[92] Auch beim BfV war die Wahrnehmung technischer Mängel einer Anfrage an die NSA nach neuen methodischen Möglichkeiten vorangegangen:

> „[Wir haben] als Inlandsnachrichtendienst erhebliche Probleme bei der technischen Informationsgewinnung. Dies sind weniger rechtliche als technische Probleme; denn wir haben die gesetzliche Grundlage nach dem G 10-Gesetz, einzelfallbezogene Telekommunikationsüberwachung zu betreiben. Wir haben vielfach das technische Problem, die Daten, die wir aufgrund einer G 10-Anordnung erhalten, technisch lesbar zu machen und auswerten zu können. Unsere Anlage für die Telekommunikationsüberwachung muss mit Blick auf die Übertragungsprotokolle und Codierungen der Hersteller von Telekommunikations-Apps permanent ertüchtigt werden. Dies ist eine unglaubliche Herausforderung" (Bundestag 2017a: 616).

Die Bedingungen der Kooperation zwischen NSA und BND waren also deshalb schlecht, da die Partner weder in organisationaler Reichweite und in ihrem Erfahrungsraum, noch hinsichtlich der notwendigen Anpassung an die strukturellen Bedingungen einen engen Zustand der Kooperation erreichen konnten. Daher war die Übertragung von XKEYSCORE die einzige Möglichkeit, eine Kooperation zu ermöglichen, die zwar Gleichwertigkeit nicht zu schaffen im Stande ist, aber eine effektive Wirksamkeit garantiert. Da sich die NSA eine effektive Terrorismusabwehrkooperation nur auf der Grundlage der Einbeziehung des Inlandsdienstes BfV versprach, wurde es verstärkt miteinbezogen (National Security Agency 2014n). Dadurch

[92] Die grammatikalischen Fehler in dieser Aussage bilden die Darstellung in der Zitierstelle ab.

mussten sowohl BND als auch BfV mit XKEYSCORE ausgestattet werden (Bundestag 2017a: 617):[93]

> „Ich hatte die Amerikaner so verstanden, dass sie Sorge hatten, dass wir nicht in der Lage sind, unsere Arbeit richtig zu machen. Hierdurch wären auch nationale US-amerikanische Interessen in Deutschland und die Stabilität Deutschlands als Bündnispartner gefährdet“,

so Hans-Georg Maaßen, der von August 2012 bis November 2018 Präsident des BfV war (Bundestag 2016a: 620).

Eine Interpretation des BND dahingehend, inwieweit die Verwendung von XKEYSCORE und der Durchführung der Operation EIKONAL gesellschaftlich rückwirkend negativ bewertet werden könnte, fiel also dadurch nicht schwer ins Gewicht oder wurde nicht berücksichtigt, da die Möglichkeiten konkreten Handelns für den BND ohne diese technologischen Verbesserungen gar nicht gegeben gewesen wären. Ergänzend muss angeführt werden, dass sich ein auf diese Weise verkompliziertes Bild auch aus den tatsächlichen retrospektiven Kritiken und den Folgen daraus ergibt. So wurde die Beteiligung des BND an EIKONAL zwar in rückwärtiger Betrachtung einerseits als zu invasiv beurteilt, denn der Bericht des NSA-Untersuchungsausschusses kam letztlich zu dem Ergebnis, dass der BND selbst keine vollständige Kontrolle über das gemeinsame Projekt hatte, da die verwendete Technologie zur Auswertung der Routineverkehre, also der Ausland-zu-Auslandkommunikation von der NSA gestammt habe und dieser somit

> „Zugriff auf verschiedene Stellschrauben des Systems [hatte] und (…) diese durch von ihm gelieferte Updates beliebig ändern[94] [konnte] sodass die Durchschaubarkeit des Systems für den BND immer wieder aufgehoben wurde (…) Als Folge davon hatte die NSA Zugriff auf sog. G 10-geschütztes Material, also Kommunikationsdaten von Deutschen bzw. aus Deutschland. Der Bericht benennt dies im Übrigen an vielen Stellen nicht in der Möglichkeitsform, wie es BND-ZeugInnen (…) nachträglich vor dem Ausschuss behaupteten. Der Bericht spricht nicht von potentiellen G 10-Daten-Abflüssen sondern von tatsächlichen“ (Bundestag 2017a: 1512).

[93] Nach Angabe des Zeugen im NSA-Ausschuss, Folker Berfuß, Gruppenleiter der Abteilung 6 des BND, habe Keith Alexander selbst im Januar 2011 das erste Angebot an den BfV, XKEYSCORE nutzen zu können, unterbreitet. Die formale Anfrage des BfV nach XKEYSCORE wurde 2013 gestellt. „The BfV Vice President formally requested the XKEYSCORE software from DIRNSA to further enable the BfV to achieve its mission goal of countering terrorist activities in Germany” (National Security Agency 2013i). Der BND hat dabei als Makler fungiert, eine Rolle, die dem Dienst stets zufalle, wenn es um die Kooperation des BfV mit Auslandsnachrichtendiensten im SIGINT-Bereich gehe (Bundestag 2017a: 623). Seit Mitte 2011 stand zur weiteren Vertiefung der Gespräche zudem ein NSA-Verbindungsbeamter zur Verfügung, der ab Anfang 2012 einen Raum auf dem Gelände des BfV in Berlin bezogen hat (Bundestag 2017a: 624).

[94] Der Zeuge Breitfelder hatte jedoch darauf verwiesen, dass nur Technik der NSA eingesetzt wurde, die für die Experten des BND transparent war und dass die NSA auch keinen direkten Zugriff auf die Informationen hatte (Bundestag 2017a: 894).

Problematisch war die Operation vor allem durch technische Gründe. Da bei der Ausleitung von ‚paketvermittelten Verkehren', der ‚IP-Erfassung', anders als bei der Erschließung leitungsvermittelter Telefonkommunikationen, eine Unterscheidung zwischen Ausland-und-Ausland oder Inland-und-Ausland kaum möglich ist, entstehen ‚Mischverkehre'. Hierbei geriet der BND in drei Dilemmata: Erstens musste er hinsichtlich der exogenen strukturellen Bedingungen, die aus der aufzuklärenden Kommunikationsstruktur entstanden, den Aufklärungsauftrag bewältigen. Zweitens konnte er sich aufgrund mangelnder Präzedenzfälle nicht an Strategien orientieren, wie mit Mischverkehren umzugehen sei. Die strukturelle Bindung an die NSA in der JSA kann als dritter Faktor betrachtet werden, den der BND mitberücksichtigen musste. Denn es ist nicht zu vernachlässigen, dass die NSA offenbar deutsche Behörden generell mit Technik ausstattet. So zeigte der BND beispielsweise bereits 2006 Interesse an TURMOIL (National Security Agency 2006a). Aber auch die Strafvollzugsbehörden fragen offenbar bei der NSA um Lösungen an. So zeichnen die NSA-Dokumente einen Besuch von Klaus-Dieter Fritsche, Staatssekretär im Bundesministerium des Innern[95] nach, bei dem er nach einer Ausspähungsmöglichkeit von Skype-Gesprächen gefragt habe. Die NSA verwies sie – wie sie betont „once again" (National Security Agency 2013b) an CIA und FBI. Hervorgehoben werden muss also, andererseits, dass die NSA als zentraler Ausstatter der deutschen Sicherheitsorgane zu betrachten ist.[96] Daher wurden zwar die Ausmaße der Operation EIKONAL rückblickend kritisiert, nach Abflauen der Affäre wurde mit der BND-Reform 2017 jedoch der gesetzliche Handlungsraum so weit erweitert, dass die Anwendung von XKEYSCORE – welches der BND in Zusammenhang mit EIKONAL erhalten hatte – legitimiert wurde (Wetzling 2017; Diehl/Meiritz 2016).

Zusammenfassend kann festgehalten werden, dass die kulturelle Inkongruenz zu einem Handlungsraum führte, der durch starke Diskussion legitimer Verfahrensweise und dominante Demonstration geeigneter Modelle durch die NSA geprägt war. Auf dieser Grundlage verlief die Kooperation im JSA sehr eng und durchaus gleichwertig, allerdings konnte diese Reichweite nicht – zumindest nicht nachweisbar – auch auf andere Initiativen übertragen werden. Da ihm keine anderen Methoden zur Verfügung standen, passte sich der gesellschaftlich und technisch beschränktere Kooperationspartner, der BND, an die

[95] Fritsche war von 2009 bis 2013 als Staatssekretär im Bundesministerium des Innern tätig. Seit Januar 2014 ist er Staatssekretär im Bundeskanzleramt und dort als Koordinator für die Nachrichtendienste des Bundes zuständig.
[96] Wie Daun (2011a: 75) durch Interviews mit ehemaligen BND-Mitarbeitern herausfand, hatte der BND bereits in Zeiten des Kalten Krieges den technischen Erwartungen der US-Amerikaner nicht standgehalten. Damals hatten sie versucht, den BND mit relevanten Rohdaten zu versorgen, die er aufgrund mangelnder technischer Ausrüstung jedoch nicht ausreichend analysieren konnte.

Organisation mit der größeren Reichweite, die NSA, an. Damit konnten die Annahmen, die aus dem Neuen Institutionalismus herausgearbeitet und für den Untersuchungsgegenstand übertragen wurden, in diesem Fall bestätigt werden.

4.3.4 Präsenz und Absenz: Das Schlaglicht der Abhängigkeit?

Die Snowden-Dokumente weisen im Hinblick auf die Kooperation zwischen NSA und BND vielfältige Hinweise auf. Dort wird auf die Hindernisse und Einschätzung hinsichtlich der Fähigkeiten und der kulturellen Unähnlichkeit des BNDs ausführlich eingegangen, weshalb nicht davon ausgegangen wird, dass in den Papieren absichtlich einige Sachverhalte deutlicher dargestellt wurden als andere. Auch konnten durch die Aussagen im Bericht zum NSA-Untersuchungsausschuss einige Feststellungen, die in den Snowden-Dokumenten zu finden waren, zusätzlich bekräftigt werden. Trotzdem lassen die Papiere einige Blindstellen, vor allem, was die Notwendigkeit einer engen Partnerschaft auch für die NSA betrifft. So könnte für die – vergleichsweise enge – Kooperation auch eine Rolle gespielt haben, dass die Attentäter des 11. Septembers 2001 ihr Vorhaben maßgeblich von Deutschland aus geplant haben. Auch weisen die Papiere Desiderate hinsichtlich der tatsächlichen terroristischen Anschlagsgefahr in Deutschland auf, die eine Aufrüstung des BNDs und BfVs möglichwerweise umso dringlicher machte. Ebenfalls unterbetrachtet ist, dass der BND zwar in der Metadatenaufklärung klare Defizite aufwies. Allerdings lässt sich vermuten, dass der deutsche Auslandsnachrichtendienst in anderen Bereichen einen klaren Mehrwert für die NSA oder andere US-amerikanische Dienste bieten konnte. So wies Daun (2011a: 187 ff.) durch Interviews mit BND- und CIA-Mitarbeitern nach, dass der BND die CIA 1991 durch die starke Präsenz deutscher Unternehmen und Ingenieure im Irak mit wichtigen Quellen unterstützen konnte. Auch im Irakkrieg, sowie in dessen Vorfeld,[97] kooperierten USA und Deutschland auf geheimdienstlicher Basis. Zudem muss berücksichtigt werden, dass das ‚Logistikzentrum der CIA' in Frankfurt am Main maßgeblich für die Versorgung der CIA-Operationen im Irakkrieg genutzt wurde. Auch für die Kommunikationsaufklärung in Bagdad – unter anderem lieferte der BND Informationen über Gespräche im irakischen Führungsbereich – sowie die Übermittlung von GPS-Daten, mithilfe der die US-Amerikaner versehentliche Angriffe auf kriegsvölkerrechtlich gestützte Einrichtungen vermeiden konnten, übernahm die BND-Zentrale in Pullach. Diese Ausführungen zeigen also, dass zur Einschätzung eines gleichberechtigten oder Abhängigkeitsverhältnisses zwischen NSA und BND die Untersuchung der Operation

[97] Die amerikanische Regierung stützte ihre Argumentation eines Einmarsches im Irak vorrangig auf einen irakischen Überläufer, der sich dem BND angedient hatte. ‚Curveball' erwies sich jedoch als unseriöse Quelle, was zu Verstimmungen im deutsch-amerikanischen geheimdienstlichen Verhältnis führte (Drogin 2007).

EIKONAL sowie der Abläufe in der JSA alleine nicht ausreichen. Jedoch konnten die vorangegangenen Untersuchungen insofern einen Mehrwert beibringen, da Informationen über eben diese Strukturen zuvor nicht bekannt waren. Auch wurden erst durch die Auswertung der durch Edward Snowden entwendeten Dokumente konkrete Einrichtungen, Mitarbeiterzahlen und die Details der technischen Unterstützung des BNDs durch die NSA in ihrer gesamten Tragweite bekannt.

4.4 Europäische Polizeikooperation: Europol

Europol ist eine Agentur der EU zur Koordination und Information der europäischen Polizeikooperation und soll eine größere Reichweite an polizeilichen Strategien, Informationen und vor allem eine Stärkung des Datenaustauschs zwischen den Ermittlungsbehörden der Mitgliedsländer, aber auch mit Drittstaaten, ermöglichen. Zwar sind die gemeinsamen Strukturen vielgestaltig und grundsätzlich technisch wirksam, jedoch auch Einschränkungen aufgrund unterschiedlicher Organisationsdesigns und einer, daraus folgend, divergenten Nutzung Europols und Hemmnissen in der Vertiefung der Nutzung gemeinsamer Datenbanken unterworfen. Daher soll geprüft werden, ob die Variablen der kulturellen Inkongruenz und der Interpretation von Unsicherheit die Wirksamkeit und den Zustand der Institutionalisierung des Europol Information System (EIS), der Dateien zu Analysezwecken (AWF) und der Secure Information Exchange Network Application (SIENA) erklären können (Abbildung 7).

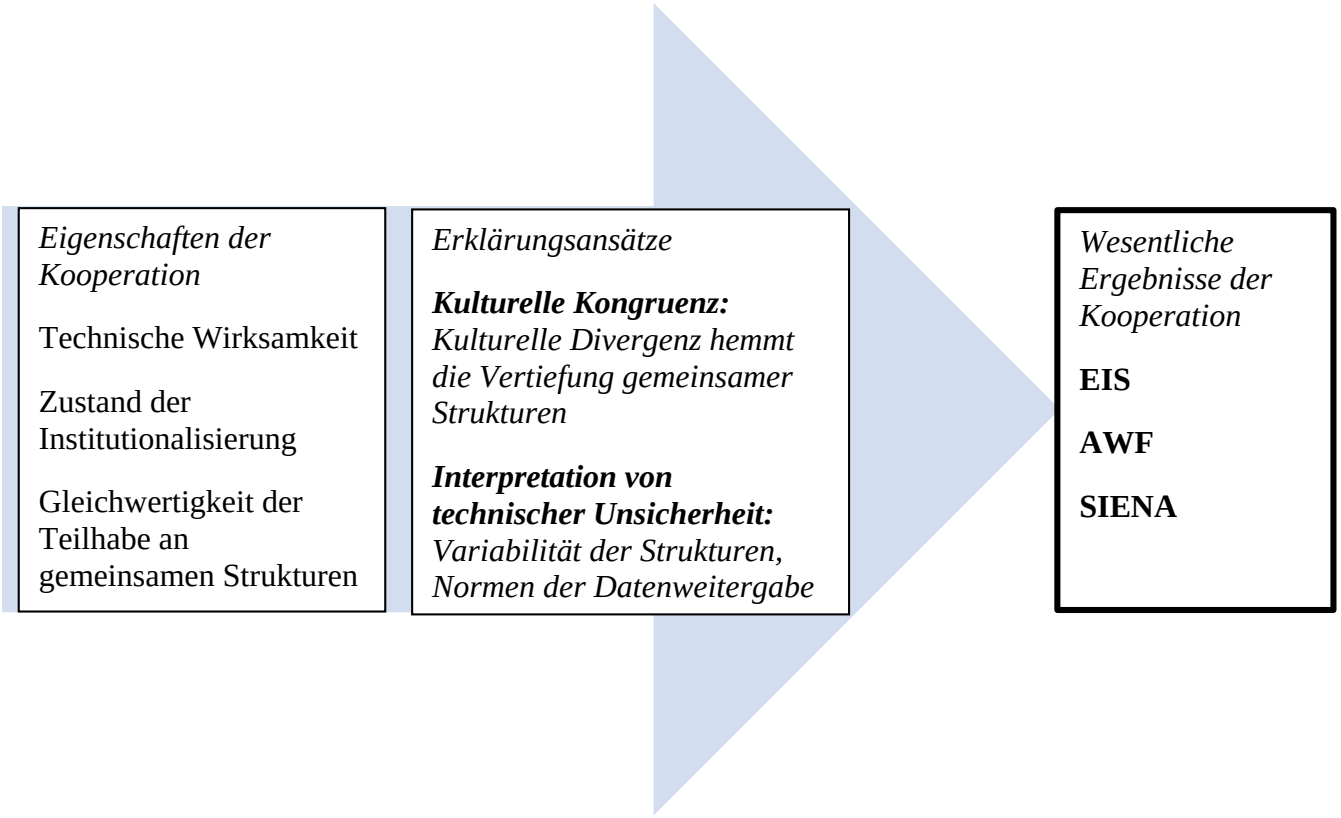


Abbildung 7: Erklärung der interorganisationalen Kooperation bei Europol.

Europol ist ein europäisches Informationssystem der Polizeikooperation mit einer spezifischen Geschichte, die zu einem besseren Verständnis der Entwicklungen und Zusammenhänge zunächst dargelegt werden soll. Anschließend wird geprüft, inwiefern die, bereits genannten, Instrumente Europols hinsichtlich eines strukturellen Datenaustausches überhaupt eine wirksame Struktur darstellen (Abschnitt 4.4.2). Gezeigt werden kann, dass die kulturellen Unterschiede Schwierigkeiten bezüglich eines gleichwertigen und effektiven Engagements aller Mitgliedsstaaten erzeugen (Abschnitt 4.4.3). Dabei wird auch beleuchtet, ob Europol gerade durch diese Variabilität für die teilnehmenden Organisationen von Nutzen sein kann, da die Agentur auch als Übermittlerin von Methoden fungiert. Dabei werden auch in diesem Fall die Anpassungstendenzen bei kultureller Divergenz aufgezeigt (Abschnitt 4.4.4). Zwar ist für den Untersuchungsfall genug Textmaterial vorhanden, da Europol eine umfassende Berichterstattung pflegt. Allerdings muss kritisch darauf eingegangen werden, dass die Dokumente nicht nur für den Dienstgebrauch angefertigt sind, sondern vielmehr auch eine Außendarstellung erreichen sollen. Daher müssen auch hier – möglicherweise verzerrende – Effekte berücksichtigt werden (Abschnitt 4.4.5). Da Europol mit sehr vielen unterschiedlichen Akteuren zusammenarbeitet liegt der Fokus folgender Auswertung darauf, inwiefern Europol im Untersuchungszeitraum seine Struktur hinsichtlich des Ziels einer engen Kooperation

wechselseitig mit den zentralen Kooperationspartnern der Agentur – den Mitgliedsstaaten der EU – vertiefen, verbessern und, im Sinne einer gleichwertigen und effektiven Nutzung durch die Mitgliedsländer, gestalten konnte.

4.4.1 Entstehungs- und Vertiefungsgeschichte Europols

Die Geschichte der vertieften europäischen Polizeikooperation ist vor allen im Zusammenhang der Notwendigkeit einer besseren grenzübergreifenden Polizeiarbeit in Westeuropa zur Aufklärung von transnationalen Straftaten wie Schmuggel, aber auch zur Eindämmung der Vorbereitung, Verschleierung und Durchführung des internationalen und regionalen Terrorismus zu sehen. Bereits 1956 legte der Europarat mit einem Auslieferungsübereinkommen und einem Übereinkommen über die Rechtshilfe in Strafsachen, das von Deutschland, Belgien, Dänemark, Griechenland, Italien, Luxemburg, Österreich und Schweden unterzeichnet wurde und, mit einiger Verzögerung, am 1. Januar 1977 in Kraft trat, die Grundlage für die europäische polizeiliche Zusammenarbeit (Schober 2017: 24 ff.). Ebenfalls zu diesem Zweck wurde 1976 der Vorläufer von Europol, die ‚TREVI-Gruppe',[98] gegründet (Europäisches Parlament 2017). Sie erhielt ihren Stellenwert vor allem dadurch, dass sich das internationale Polizeinetzwerk Interpol nicht bereit erklärt hatte, die zentrale Verfolgung von politisch motivierten Straftaten, unter welche Terrorismus fällt, zu ermöglichen (Deflem 2007b; Deflem 2006; Aden 1998: 77).[99] Bereits in den 1970er Jahren verübten jedoch linksterroristische und separatistische Gruppierungen Sprengstoff- und Brandanschläge, Raubüberfälle, Entführungen und Tötungsdelikte in Deutschland, Italien, Frankreich und Spanien. Bereits die TREVI-Gruppe arbeitete deshalb an Fragen einer verbesserten einsatztaktischen Ausbildung und der Ausstattung von Spezialkräften, sowie einer engeren Zusammenarbeit der einzelstaatlichen Behörden beim Schutz des zivilen Luftverkehrs zur Verhinderung von Flugzeugentführungen, befasste sich zusätzlich aber auch mit operativen Aspekten einer grenzüberschreitenden Lagebewältigung (Schober 2017: 30 ff.). [100] Eine zweite Begründung lieferte später der Wegfall der europäischen Grenzen. Der freie Personenverkehr sorgte für die Möglichkeit und Notwendigkeit, Ausgleichsmaßnahmen in Form von europäischen „quasi-staatlichen Polizeistrukturen" (Aden 1998: 42) zu schaffen, und beförderte

[98] Die Abkürzung TREVI steht für Terrorismus, Radikalisierung, Extremismus und internationale Gewalt (Segell 2004: 83).
[99] In den Teilnehmerstaaten gab es unterschiedliche Ansichten darüber, ob und welche terroristischen Aktionen gerechtfertigt waren, beispielsweise, ob separatistische Gewalt – etwa in Spanien – als politische Straftat behandelt werden sollte.
[100] Während die strategischen Analysen von Europol das Ziel haben, generelle Trends und Muster zu erkennen, beruhen die operativen Analysen auf personenbezogenen Daten (Daun 2005b: 145).

die europäische Polizeikooperation.[101] In der Folge wurde das Schengener Informationssystem (SI) als erste gemeinsame Datenbank eingeführt, das seit 2013 in seiner Nachfolgestruktur SIS II existiert. TREVI diente also bereits in einer frühen Phase der europäischen Polizeikooperation zur technischen Vereinheitlichung und Koordinierung des Informationsaustausches, konzentrierte sich jedoch einzig auf Informationen, die direktes polizeiliches Handeln aufgrund einer Straftat erforderlich machten und nicht auf darüber hinaus gehende Erkenntnisse (Aden 1998: 79). Die TREVI-Gruppe entwickelte sich jedoch über die Jahre weiter und schuf den Austausch von Verbindungsbeamten, ein geschütztes Fernmeldenetz und eine Verwaltungsstruktur. Am 1.11.1993 wurde die Organisationsstruktur der TREVI-Gruppe mit Inkrafttreten des Maastrichter Vertrages in den Rahmen der ‚European Drug Unit (EDU)/Europol' – die sich ab dem 29. Oktober 1993 im Wirkbetrieb befand – überführt und in das Rahmenwerk der Europäischen Gemeinschaften, genauer in die ‚dritte Säule' der Polizeilichen und Justiziellen Zusammenarbeit der EU, integriert. Der Vertrag schrieb die drei Elemente der europäischen Polizeikooperation, die gremienbasierte Abstimmung zwischen den mitgliedsstaatlichen Regierungen zur Verhütung und Bekämpfung bestimmter Kriminalitätsformen, die direkte Zusammenarbeit der mitgliedstaatlichen Polizeien, sowie die direkte Zusammenarbeit der mitgliedstaatlichen Polizeien über und mittels Europol fest (Schober 2017: 189). Das am 26. Juli 1995 durch die Innen- und Justizminister der EU-Mitgliedsstaaten unterzeichnete Europol-Übereinkommen regelte den Mandats- und Zuständigkeitsbereich Europols und machte diesen an den regelungstechnischen Kriterien Zielstellung (Stärkung der Leistungsfähigkeit der für die Verbrechensbekämpfung zuständigen Behörden), phänomenologischer Arbeitsgegenstand (dieser ist von der Nennung von Kriminalitätsphänomenen und ihrer qualitativen Komponente abhängig), Internationalität des Tatgeschehens (Erheblichkeit für mehrere Mitgliedsstaaten) und Organisationsgrad der Kriminalitätsform fest (Schober 2017: 242 ff.). Das Tampere-Programm, das vom

[101] Europol ist nicht die einzige Form der Polizeikooperation. Informeller Austausch besteht im deutsch-niederländisch-belgischen Grenzgebiet seit 1979 mit NEBEDEAG-POL, seit 1979 in der Police Working Group on Terrorism (PWGOT) als Forum der Spezialdienststellen der Terrorismusbekämpfung von Deutschland, Belgien, Frankreich, Italien, Luxemburg, den Niederlanden, Finnland, Norwegen, Österreich und Schweden, im Club der Fünf für die polizeiliche Terrorismusbekämpfung Deutschlands, Frankreichs, Italiens, Österreichs und der Schweiz und in der Quantico-Gruppe, die seit Ende der 1970er Jahre unter Leitung des FBIs jährlich Treffen auf Führungsebene in Kooperation mit Frankreich, Großbritannien, Deutschland, Italien, Schweden, Kanada und Australien durchführt (Aden 1998: 75 ff.). 2016 wurde außerdem die Verstärkung der grenzüberschreitenden Bekämpfung der Eigentumskriminalität zwischen Deutschland – speziell Nordrhein-Westfalen – den Niederlanden und Belgien durch die ‚Aachener Erklärung' ausgerufen, die die Durchführung gemeinsamer Auswerte- und Analyseprojekte, die gemeinsame Beteiligung an Sicherheitsforschung, etwa in der vorbeugenden Polizeiarbeit sowie den Austausch von effektiven Ermittlungsmodellen beinhaltet (Bundesministerium des Innern 2016). Parallel wird diese multilaterale Initiative auch von einer EU-Initiative begleitet (Rat der Europäischen Union 2016).

Europäischen Rat am 15. und 16. Oktober 1999 beraten wurde, stellte dann die Weichen für eine Schaffung des ‚Raums der Freiheit, der Sicherheit und des Rechts' und vereinbarte eine gemeinsame Asyl- und Migrationspolitik, einen europäischen Rechtsraum, unionsweite Kriminalitätsbekämpfung, Sondermaßnahmen zur Geldwäsche und ein stärkeres gemeinsames außenpolitisches Handeln im Bereich Justiz und Inneres (Möllers 2012: 11). Die Erklärung des Rates der Innen- und Justizminister der EU zur vollen Unterstützung der USA beim Kampf gegen den internationalen Terrorismus am 20.09.2001 legte das Fundament für die vergrößerten Anti-Terrorbemühungen Europols und stärkte die Verbindung zu Drittstaaten, allen voran der USA: Am 6. Dezember wurde eine strategische Partnerschaft zwischen den amerikanischen Strafvollzugsbehörden und Europol zur Terrorismusbekämpfung geschlossen (Segell 2004: 89). Am 28. November 2002 wurde die Organisation Europol – und dadurch auch ihre Rolle zur Gewährleistung einer effektiven Zusammenarbeit zwischen den Mitgliedsstaaten – durch das Protokoll zur Änderung des Europol-Übereinkommens gestärkt und in einen neuen Rechtsakt überführt, was die Organisation zusätzlich zur Zentralstelle zur Bekämpfung der Euro-Fälschung machte. Auch haben Europol-Bedienstete seitdem die Möglichkeit, aus eigener Initiative heraus oder auf Ersuchen der Mitgliedsstaaten, Ermittlungsgruppen auf nationaler Ebene zu unterstützen (Schober 2017: 461 ff.). Im Nachgang der Terroranschläge in Madrid am 11. März 2004[102] wurde schließlich auf EU-Ebene die Counterterrorism Task Force (CTTF) gegründet, welche jedoch nur Kompetenzen der Analyse und des Informationsaustauschs und keine operativen Fähigkeiten aufweist (Kaunert 2010: 665). Allerdings hat die CTF die Aufgabe, relevante Erkenntnisse zu sammeln und einer strategischen und operativen Analyse zu unterziehen, Systeme zu entwickeln und zu nutzen, um Daten aus dem Arabischen ins Englische zu übersetzen, einen Lagebericht zu erstellen und zu zirkulieren und Listen mit konkreten Personen und operativen Vorschlägen, gegen diese vorzugehen, zu erarbeiten (Segell 2004: 89). Ein weiterer integrativer Meilenstein war das Haager Programm von 2004 mit einem Aktionsplan und konkreten Maßnahmen zur Umsetzung der europäischen Kooperation in der inneren Sicherheit. Es legte die Prioritäten bei der Schaffung des gemeinsamen Raumes der Freiheit, der Sicherheit und des Rechts für fünf Jahre fest. Im Zentrum standen die Ausrichtung an Datenschutzgrundrechten, aber auch die Verbesserung des Informationsaustausches, unter anderem nach dem Grundsatz der Verfügbarkeit, insbesondere in der Terrorismusbekämpfung und der Bekämpfung grenzüberschreitender Kriminalität sowie der Kriminalprävention. Wichtigstes Ziel war die Schaffung eines Prozesses, in dem die Organisationen der

[102] Die Terroranschläge in Spanien können als Beschleuniger der polizeilichen Integration Europas betrachtet werden (Daun 2005b: 149).

Mitgliedsstaaten den Sicherheitsbehörden anderer Mitgliedsstaaten und Europol alle Informationen zur Verfügung stellen sollen, die diese zur Verhütung, Aufdeckung und Untersuchung von Straftaten benötigen (Zöller 2011: 65). Mit dem Lissaboner Vertrag ist die rechtliche Grundlage von Europol 2007 in das europäische Gemeinschaftsrecht eingegangen. Die Mitgliedsstaaten und die Kommission sollen nun im Konsensverfahren Initiativen zur (Weiter-)entwicklung Europols einbringen (Piquet 2017: 1194). Weitere integrationsbezogene Prioritäten wurden 2009 im Stockholmer Programm formuliert, das die Zusammenarbeit in den Bereichen innere und öffentliche Sicherheit, Terrorismusbekämpfung, Bekämpfung der Organisierten Kriminalität, Migration sowie Harmonisierung von Teilbereichen des Familien-Zivil- und Erbrechts zum Ziel hatte und das unter anderem die Schaffung gemeinsamer Mindestnormen und die Stärkung wirksamer Strategien in der gemeinsamen Strafverfolgung und Kriminalprävention forderte, deren Umsetzung jedoch in Teilen bis heute andauert (Möllers 2012: 18 f.). Der Beschluss des Rates vom 6. April 2009 zur Einrichtung des Europäischen Polizeiamts zielte dann darauf ab, die Möglichkeiten von Europol zur – auch operativen – Unterstützung der Mitgliedsstaaten zu erweitern, ohne dem Personal Vollzugsgewalt zu übertragen (Europäischer Rat 2009). Seit dem 1. Januar 2010 hat Europol den Status einer Agentur der Europäischen Union. Dadurch wird Europol nicht mehr durch die Mitgliedsstaaten finanziert, sondern aus dem Gemeinschaftshaushalt. Das Europäische Parlament ist damit Haushaltsbehörde und budgetierungs- und kontrollbefugt (Europol 2009).[103] In Folge der Terroranschläge am 13. November 2015 in Paris macht der Rat der EU den Vorstoß, den Informationsaustausch zu verstärken. So wurde die Kommission ersucht, „einen Gesetzgebungsvorschlag vorzulegen, um Europol in die Lage zu versetzen, systematisch die Europol-Datenbanken mit dem SIS II abzugleichen“ (Rat der Europäischen Union 2015: 2). Die aktuell gültige Europol-Verordnung, die am 1. Mai 2017 in Kraft getreten ist, sieht die Erarbeitung von Datenübermittlungs*pflichten* für die Mitgliedsländer vor, hebt aber gleichzeitig die Notwendigkeit der Zweckbegrenzung der Verarbeitung personenbezogener Daten nach dem Prinzip der Erforderlichkeit hervor, stärkt die Zusammenarbeit Europols auch mit dezentralen Polizeibehörden auf Mitgliedsländerebene und strebt die Öffnung der Europol-Informationssammlung für Eurojust und das Europäische Amt für Betrugsbekämpfung (OLAF) an.

[103] Einige unter Europol subsumierte nationale Ermittlungsstellen sehen die Auslagerung der Budgetkompetenz an das Europäische Parlament nicht etwa als Machteinbuße, sondern als positiv, da man sich nun auf das Kerngeschäft der Polizeiarbeit konzentrieren könne (Piquet 2017: 1195).

4.4.2 Die Wirksamkeit Europols als Informationsspeicher der Ermittlungsbehörden der Mitgliedsländer

Obwohl durch die Darlegung der Geschichte Europols bereits weitreichende Hinweise darauf erbracht wurden, dass die Agentur zentraler Wissensspeicher und Koordinationsstelle der europäischen Polizeikooperation ist, soll nachfolgend die Wirksamkeit der Kooperation dahingehend geprüft werden, welche Datenbanken und Datenweiterleitungsstrukturen Europol konkret aufweist. Europol hält mit seinen Verbindungsbeamten sowie den nationalen Kontaktstellen, den ‚National Units' (NEU), zentrale Elemente der Informationsweiterleitung vor. Für die Reichweite und den informationellen Mehrwert von Europol spielen jedoch vor allem die zentralen Datenspeicher und Analysesysteme eine Rolle. Nachfolgend werden erstens das Europol Information System (EIS), zweitens die Arbeitsdateien zu Analysezwecken (Analysis Work Files, AWFs) mit ihren Analysepunkten (APs), sowie drittens, die Datenübermittlungsstruktur SIENA, die sowohl Mitgliedsstaaten als auch Drittstaaten nutzen können, vorgestellt.

Das Europol Information System (EIS), auch „Europol-IS" (Manske 2001: 105) genannt, ist die zentrale Datenbank Europols und gleicht, von den Ermittlungsbehörden in den EU-Mitgliedsländern eingespeiste, Daten automatisch mit bereits vorhandenen Datensätzen im EIS sowie in den APs, die noch vorgestellt werden sollen, ab (Europol 2013). Europol-Mitarbeiter, die zu Europol entsendeten Beamten der Mitgliedsstaaten, sowie die zu Europol geschickten Experten für bestimmte Kriminalitätsarten und Ermittlungsbereiche, können auf die im EIS gespeicherten Daten zugreifen sowie weitere Informationen hinzufügen und dadurch Hinweise auf Muster in unterschiedlichen Mitgliedsländern und Kriminalitätsbereichen oder zu länderübergreifenden Delikten ableiten und weitergeben. Die Organisationen der Mitgliedsländer nutzen das EIS vor allem, um bei ihrer Ermittlungstätigkeit nach möglichen Treffern in der Datenbank zu forschen. Seit 2017 werden zudem innerhalb der High Level Expert Group (HLG) on Information Systems and Interoperability, einer Expertengruppe der Europäischen Kommission, Möglichkeiten entwickelt, auch Kreuztreffer zu ermöglichen, also innerhalb einer Suchmaschine als ‚One Stop Shop' Treffersuchen in unterschiedlichen Datenbanken – beispielsweise parallel in SIS II, dem EIS sowie im Visa-Informationssystem (VIS) – durch eine zentrale Anwendung zu ermöglichen. Dieser Punkt ist in der Initiative ‚Automation of Data Exchange Processes' (ADEP) der Europäischen Kommission, welche die Entwicklung einer technischen Anwendung zur Durchsuchung vernetzter Datenbestände aller Mitgliedsländer vorsieht, wenn ein rechtlich zulässiger Grund für diese Informationserhebung

vorliegt, prominent vorgesehen. Die Europäische Kommission schlägt das EIS hierfür als zentrale Struktur vor. An das EIS angeschlossen ist außerdem das Europol Analysis System (EAS), das es den eingangs genannten berechtigten Personen erlaubt, Inhalte des EIS zu Analyseprodukten zu bündeln und diese zu teilen. Es können aber auch Informationen aus dem EAS in das EIS übertagen werden, um diese Informationen auch dort zugänglich zu machen (Europol 2011b). Mit dem EAS können zusätzlich Daten aus spezifischen Projekten, wie etwa Check the Web,[104] dem Terrorist Finance Tracking Program (TFTP)[105] sowie aus Analysepunkten (APs), des AWFs, wie etwa Travellers[106] und Hydra[107], zusammengeführt werden. Daraus lassen sich weitere Erkenntnisse zu begangenen Straftaten ableiten, entstehen aber auch Informationen über Finanzierung von Terrorismus, kommunikativer und informationeller Vorbereitung extremistischer und krimineller Vergehen, Reiseverläufen von Kriminellen und Extremisten und den jeweiligen strukturellen Zusammenhängen. Die Möglichkeit der Verknüpfung aller vorhandenen Daten zur Herausarbeitung bestimmter Muster ist jedoch nicht den Behörden der Mitgliedsstaaten, sondern bislang nur der zentralen Abteilung für operative und strategische Auswertung bei Europol möglich. Angeschlossene Drittstaaten und Mitgliedsländer können nur nach Treffern in der Datenbank suchen. Anders als das SIS, das nur Informationen zu Personen, nach denen entweder zum Ziel der Festnahme, der Auslieferung, der Einreiseverweigerung, der Gefahrenabwehr, der verdeckten Registrierung, der Aufenthaltsermittlung oder zu Sachen, die zur Sicherstellung oder Beweissicherung im Strafverfahren gesucht werden, bereithält – sogenannte harte Daten – erlaubt das EIS jedoch auch die Speicherung von weichen Daten, die auch personenbezogene Merkmale sensibler Natur von Zeugen und anderen Tatbeteiligten enthalten dürfen (Bundestag 2016b). Diese Möglichkeit war vor der Entstehung Europols für die Mitgliedsländer der EU nicht gegeben, weshalb die Polizeiagentur und ihr Informationssystem einen deutlichen Mehrwert für die polizeiliche Kooperation darstellen (Europol 2012: 4). Seit 2014 machen sich die

[104] Der AP Check the Web hat die Kontrolle extremistischer Inhalte im Internet zum Ziel. Im weiteren Verlauf vorliegender Arbeit wird darauf noch eingegangen.

[105] Das TFTP ist auch unter dem Namen SWIFT-Programm bekannt und wurde zwischen den USA und Europol nach dem 11. September 2001 geschlossen, um den Zahlungsverkehr zur potentiellen Finanzierung von Terrorangriffen zu überwachen. Das US-amerikanische Finanzministerium kann dabei über Europol Finanzauskünfte über europäische Konten anfordern und umgekehrt (Europäische Kommission 2017; Kaunert/MacKenzie 2012; Ripoll Servent/MacKenzie 2011; Europol 2011a; 2011c; Connorton 2007). Das SWIFT-Programm war vor der Umwandlung in ein offizielles Abkommen am 27.07.2007 einer informellen Praxis gefolgt, an der laut Medienberichten die CIA beteiligt war (Lichtblau/Risen 2008).

[106] Der AP Travellers koordiniert seit 2015 gemeinsame Ermittlungen und Datenanalysen zu Personen, die sich dem islamistischen Terror in Syrien und dem Irak angeschlossen haben und nun möglicherweise nach Europa (zurück) reisen könnten (Europol 2018b).

[107] Hydra ist der Name für den Auswerteschwerpunkt zum Thema islamistischer Terrorismus und soll Attentate gegen Leib, Leben, Eigentum oder Eingriffe in die persönliche Freiheit und verwandte Straftatbestände aufklären oder verhindern (Europol 2018b).

Mitgliedsstaaten und Drittstaaten über das EIS zudem Listen über ‚Foreign Terrorist Fighters' (FTFs), also Personen, die sich dem islamistischen Terrorismus anschließen, zugänglich (Europol 2017b). Europol fungiert über das EIS auch als Kontaktknoten zu Drittstaaten, anderen EU-Agenturen wie Frontex, und zu anderen externen Datenbanken, wie etwa dem SIS II, der Fingerabdruck-Datenbank für Asylbewerber (EURODAC), dem VIS, dem Informationssystems des OLAFs, Finanzfahndungsstellen, Vermögensabschöpfungsstellen und Plattformen gegen Cyber-Kriminalität sowie zu dem durch Interpol entwickelten System I-24/7, was die Wirksamkeit von Europol für unterschiedliche Akteure der Sicherheitspolitik durch den Schnittstellencharakter der Agentur steigert.

Ein weiteres datafiziertes Verfahren zur Zusammenarbeit bei Europol stellen die AWFs dar (Petri 2001: 62 f.). Sie bilden ein Informationssammlungssystem zu verschiedenen Deliktarten, das sich dazu eignet, in spezifischen Kriminalitätsbereichen zusätzliche Informationen, die entweder durch strategische Einschätzungen oder durch operative Erkenntnisse Aufmerksamkeit erlangt haben, zentral bereitzustellen und übergreifend auszuwerten, um so die operative Unterstützung in Ermittlungsfällen der Mitgliedsländer, sowie deren Ermittlungen zu erleichtern. In den AWFs befinden sich gleichzeitig harte und weiche Informationen (Europol 2012: 4). Die Erlaubnis, Daten in die AWFs einzugeben, haben Europol-Mitarbeiter, Verbindungsbeamte und Sachverständige, die ein anerkanntes Interesse an dem Analyseprojekt haben, und Experten, die an Europol entsandt sind. Zusätzlich können interessierte Mitgliedsstaaten eine Abfrage tätigen, insofern sie eine Betroffenheit geltend machen können. An die AWFs angeschlossen ist das ‚Indexsystem'. Dieses Dateisystem ermöglicht es nationalen Verbindungsbeamten, festzustellen, ob ihnen die in den AWFs gespeicherten Informationen zur Ermittlungstätigkeit der nationalen Behörden nützlich sein könnten. Das Indexsystem stellt somit einen Überblick über den Inhalt der AWFs dar. Neben den Verbindungsbeamten der Mitgliedsstaaten bei Europol können darauf berechtigte Europol-Mitarbeiter zugreifen. Dieser Datensatz soll nur begrenzte Informationen enthalten, und somit nur ein Minimum an personenbezogenen Daten vorhalten (Petri 2001: 62f). Bei den AWFs lassen sich zwei Hauptdateien unterscheiden. Die AWF Counter Terrorism (CT) wird auch als europäisches Datenfundament für den Staatsschutz bezeichnet (Bundestag 2014). Außerdem besteht noch die AWF der Schweren und Organisierten Kriminalität (AWF SOC). Beiden AWFs sind APs zugeordnet, also unterschiedliche Themenbereiche, die sich unter die AWFs subsumieren lassen. Bei der AWF CT sind dies die Informationsplattform Check the web, Nicht-islamistischer Terrorismus, islamistischer Terrorismus, Seepiraterie und Austausch von Zahlungsverkehrsdaten zwischen der EU und den USA im Rahmen des TFTPs. Die AWF SOC

beinhaltet 20 APs, darunter Menschenhandel, Organisierte Kriminalität/Rocker, Schleusung, verschiedene Rauschgift-Kategorien, Kinderpornografie, Zigarettenschmuggel und Waffenhandel. Europol, EU-Institutionen oder die Organisationen der Mitgliedsländer können die Erstellung von APs anregen, die sich mit einem thematischen oder regionalen Phänomen beschäftigen und die dann wieder zu spezifischeren Bereichen untergliedert werden können (Europol 2016a). So befinden sich im AP Cyberkriminalität beispielsweise Daten zu Phishing-Attacken im E-Banking. Die formale Öffnung und Schließung eines solchen APs obliegt jedoch Europol. Die Notwendigkeit der APs wird zusätzlich alle zwei Jahre überprüft. Mitgliedsländer oder Drittstaaten, die ein operatives Abkommen hinsichtlich des Beitritts zu einem AP geschlossen haben, können Teil einer Analysegruppe werden. Im Fall einer konkreten Ermittlung innerhalb des Themenbereiches können zusätzlich ‚Target Groups' gebildet und dann gegen Zielpersonen vorgegangen oder weitere ermittlungsrelevante Schritte geplant werden (Europol 2012: 5ff). Deutschland ist mit Ausnahme des APs zu Waffenkriminalität und Waffenhandel an alle Analyseprojekte als Teilnehmer assoziiert (Bundestag 2014). Ob sich Deutschland diesem AP nach dem Amoklauf in München am 22.07.2016 angeschlossen hat oder anschließen möchte, ist nicht bekannt. Das Bundeskriminalamt sprach sich in seinem Bundeslagebild Waffenkriminalität 2016 jedoch für europäische Rechtsharmonisierung aus und sah ein besonderes Gefahrenpotenzial durch den Waffenhandel, vor allem auf illegalen Online-Marktplätzen (Bundeskriminalamt 2016: 14).

Eine weitere wichtige Struktur Europols ist SIENA. SIENA startete am 1. Juli 2009 und ist eine zentrale Datenweiterleitungsmöglichkeit zwischen Europol-Analysten und -Experten und den Sicherheitsbehörden auf Ebene der Mitgliedsstaaten, Drittstaaten sowie zu Interpol. Über sichere Leitungen können alle genannten Parteien auf die Europol-Datenbanken zugreifen. Deutschland hat die Roadmap[108] zu SIENA entwickelt (Bundestag 2008). Das von SIENA unterstützte universelle Datenformat UMF soll die Übertragung von Informationen einfacher machen, denn die Daten werden strukturiert auf ein allgemein lesbares und verwertbares Format aufbereitet und ermöglichen parallele Abfragen bei allen angeschlossenen Behörden. Mit der Technologie UMF3 sind sogar Trefferanfragen eines Mitgliedslandes direkt bei einem anderen Mitgliedsland möglich (Europol 2013). Europol stellt hier lediglich den Verbindungsservice zur Verfügung, den sogenannten REST-Service, der intern bei Europol QUEST genannt wird und der seit 2017 im Wirkbetrieb ist (Bundestag 2017b: 3). Drittstaaten, die seit 2006 an SIENA beteiligt sind, sind Albanien, Australien, Island, Kanada, Kolumbien, Liechtenstein,

[108] Roadmaps bezeichnen Initiativen der Mitgliedsländer oder der Kommission zur Weiterentwicklung Europols.

Mazedonien, Republik Moldau, Monaco, Montenegro, Norwegen, Serbien, Schweiz und die USA. Großer Mehrwert wird vor allem den durch SIENA entstehenden Verbindungen zwischen Europol, Eurojust, Interpol[109], Australien, Kanada, Norwegen, der Schweiz und den USA zugeschrieben, da die zugänglichen Informationen damit den Aktionsradius von Europol und der EU verlassen können und auch die Einbindung von Informationen auch aus diesen Räumen ermöglichen (Europol 2011d: 13). Einen indirekten Anschluss an SIENA – der Zugang besteht nur, wenn eine Betroffenheit geltend gemacht werden kann – haben Bosnien und Herzegowina, Russland, Türkei, Ukraine sowie verschiedene EU-Behörden, darunter die Europäische Zentralbank, Frontex, das EU Intelligence Center (INTCEN), aber auch das UN Office on Drugs and Crome und die World Customs Organization (Bundestag 2016a). Über SIENA kann zusätzlich Informationstransfer so stattfinden, dass nur einige wenige Mitglieder Zugang erhalten, etwa dann, wenn eine operative Abstimmung zur Terrorabwehr nur zwischen bestimmten beteiligten Ermittlern und Spezialeinheiten vonnöten ist. SIENA ist also gleichzeitig ein Werkzeug zum Teilen relevanter Informationen mit einem, nach unterschiedlichen Reichweiten ausgewählten Teilnehmerkreis und ein generell ansteuerbarer Knotenpunkt für interne und externe Akteure. Es wird unter Hervorhebung des UMF-Formats als „Instrument der nächsten Generation“ (Europol 2011d: 12) bezeichnet, obwohl diese Schaffung einer verbindenden Kommunikationsstruktur bereits mit der Gründung von Europol geplant war. Zukünftig soll SIENA verstärkt auch in die (teilweise regionalen) Initiativen Maritime Analysis and Operations Centre – Narcotics, Zoll, Passenger-Information Units und Financial Intelligence Units eingebunden werden. Auch der ATLAS-Verbund der polizeilichen Spezialeinheiten soll SIENA nutzen und damit eine stärkere Angliederung an Europol erfahren.[110]

Alle drei Informationssysteme, das EIS, die AWFs und SIENA, beziehen ihre Wirksamkeit von einer Steigerung der Daten, die sich in und mit ihnen verknüpfen lassen oder die durch sie weitergeleitet werden können. Am deutlichsten können diese Zahlen für das EIS belegt werden. Während das System 2006 weniger als 50.000 Eintragungen erfasste, beliefen sich die Zahlen im Dezember 2012 schon auf knapp unter 200.000 Informationen zu Personen und Sachen. Auch die Auflistungen zu FTFs stiegen an. Während zur Einführung am 31.12.2014 nur 18

[109] Interpol und Europol arbeiten außerdem daran, ihre Strukturen für mehr Interoperabilität aneinander anzupassen (Europol 2015: 28).

[110] Der ATLAS-Verbund ist eine Gemeinschaft polizeilicher Spezialeinheiten und soll im European Counter Terrorism Center (ETCT) bei Europol ein dauerhaftes Sekretariat erhalten. Allein 2017 wurden 65 Treffen und Übungen durchgeführt. Das feste Sekretariat soll den Wechsel der Führung mit den EU-Ratspräsidentschaften vermeiden. Bislang sind jedoch nicht alle ATLAS-Mitglieder zugleich auch an Europol beteiligt (Monroy 2017).

Datensätze verfügbar waren, vergrößerte sich die Zahl zum 15.02.2016 auf 3.857 an (Europol 2017b). Die AWFs umfassen derzeit 30 APs zu unterschiedlichsten Themen wie Schleusung, Heroin, organisierte Einbruchskriminalität, die Finanzierung von Terrorismus, Cyberkriminalität, Diebstahl geistigen Eigentums, Geldwäsche, Menschenhandel, Cannabis und, unter dem AP Check the Web, Maßnahmen zur Entfernung und Archivierung von illegalen Internetinhalten (Videos, Audiodateien, Textveröffentlichungen), die zur Terrorismuspropaganda verwendet werden. Seit der Einführung von CtW 2007 wurden bereits 10.000 Dokumente und Personendaten gespeichert. Im Zusammenhang mit CtW wurde bei Europol 2015 auch die ‚Meldestelle für Internetinhalte', die Internet Referral Unit (EU IRU), gegründet (Europol 2016c). Sie wird operativ tätig und durchsucht das Internet nach Inhalten, die sie für unangemessen oder zumindest fragwürdig hält. Dahinter steht zwar das Ziel, extremistische Propaganda zu verhindern – hierzu arbeitet die EU IRU auch mit dem Europol-Terrorismusabwehrzentrum ECTC zusammen – allerdings wurden die Tätigkeiten auch auf Informationen, die illegale Einwanderung und den Schmuggel von Migranten betreffen, ausgeweitet (Vieth 2017). Eine Pressemitteilung von Europol vom 22. Juli 2016, welche eine Einjahresbilanz der IRU zieht, hält fest, dass die IRU binnen eines Jahres 11.000 Benachrichtigung an 31 Online-Plattformen versendet hat. 91,4 Prozent der beanstandeten Inhalte wurden entfernt. Zukünftig sollen die Online-Plattformen darin unterstützt werden, verdächtige Inhalte selbst zu erkennen und zu entfernen. Die Verfolgung der Urheber der Inhalte wird dann gemeinschaftlich zwischen der IRU und den privaten Betreibern der Portale geleistet (Europol 2016b). Auch die Nutzung von SIENA ist in Steigerung begriffen. 2016 waren bereits 90 Prozent der EU-Mitgliedsländer an Europol angeschlossen. Ein Pilotprojekt zwischen Europol und BKA ermöglicht zudem den Zugang der deutschen Landeskriminalämter an SIENA.

4.4.3 Kooperation ohne Kooperationsbereitschaft?

Die Annahme für die Kooperation kulturell ähnlicher Partner ist, dass sie eine besonders enge und stabile Kooperation mit gleichwertigem Zugang schaffen können und dass, umgekehrt, eine Inkongruenz dies behindert. Gleichzeitig würde eine Kooperation unter den Bedingungen kultureller Kongruenz sich in gleichwertigen Zugang zu den genannten Techniken und Datensammlungen darstellen, während eine Inkongruenz gerade dies verhindert. Die Analyse der Datensammel- und Datenweiterleitungssysteme Europols zeigt, dass unterschiedliche Organisationsdesigns auf Ebene der Mitgliedsländer eine einheitliche und umfassende Nutzung dieser Hilfsmittel zur Bekämpfung transnationaler organisierter Kriminalität und Terrorismus

teilweise erschweren. Diese Schwierigkeiten sollen nachfolgend dargestellt werden. Sie zeigen sich darin, dass das Prinzip der Weiterleitung von Daten, die für mehrere Mitgliedsorganisationen wichtig sein könnten, nicht von allen Organisationen gleich stark befolgt wird, da die zentralisierte Datenkooperation in Europa keine internalisierte Praxis darstellt. Dadurch ergeben sich inkongruente Teilnahme- und Mitentwicklungsstufen, da einige Mitgliedsstaaten und ihre Organisationen Europol und seine Funktionen weiterentwickeln, während andere Staaten und ihre Ermittlungsbehörden sich nur schrittweise anschließen und auch ihre nationalen Strukturen nur teilweise für Europol öffnen. Diese Inkongruenz führt, wie weiterhin gezeigt werden soll, zu heterogenen Parallelstrukturen.

Zwar stellt die EU ein integrierendes Organisationskonstrukt dar, dass die Unterschiede zwischen einigen Mitgliedsländern zumindest überlagern kann (Manners 2008). Allerdings muss festgehalten werden, dass gerade in der Außen- und Sicherheitspolitik der Souveränitätsvorbehalt der Mitgliedsländer eine Integration der sicherheitspolitischen Maßnahmen in den europäischen Rahmen maßgeblich behindert und dass der Kulturraum Europa kein kongruentes Konstrukt ist, sondern immer ein dynamisches politisches Projekt war (France/Whitney 2013).[111] So zeigen sich Souveränitätsvorbehalte durch eine mangelnde Bindung nationaler Ermittler an die formalen Strukturen Europols, was dafür sorgt, dass die Angebote der Polizeiagentur vielfach nicht genutzt werden und Ermittlerteams sich lieber bilateral oder informell mit ihren Kollegen aus anderen Ländern vernetzen (Aden 1998: 99; Fägersten 2010b: 519). So sind die Eintragungen in das EIS und die Zahlen der Nutzung SIENAs zwar steigend. Aber Europol ist weiterhin darauf angewiesen, die Mitgliedsländer dazu zu motivieren, Europol als „channel of first choice for law enforcement information sharing across the EU“ (Europol 2017c: 4) zu nutzen. Ausgedrückt mit dem Lebenszyklus der Norm, der Feststellungen zum Zustand der Institutionalisierung ermöglicht, handelt es sich bei Europol also (noch) nicht um eine Struktur, die habitualisiert genutzt wird. Anders als in der nachrichtendienstlichen Gruppe der Five Eyes können die Ermittlungsbehörden der EU-Staaten in ihrer Kooperation also nicht auf eine zurückliegende interorganisationale Erfahrung des zentralisierten Datenaustauschs zurückblicken und daher bemühen sich einige beteiligte Ermittlungsbehörden sowie Europol selbst, um eine Diskussion und Demonstration dazu, dass die habituelle Durchführung einer solchen Kooperation sinnvoll wäre. Somit befinden sich die Polizeiagentur und ihre Kanäle noch in der Phase der Verbreitung und Demonstration von

[111] Die Gründe dafür könnten gerade darin liegen, dass Europa keine gemeinsame Gesellschaft im eigenen Sinne vorweisen und entwickeln kann (Offe 2001).

Normen. Unterstützung erhält Europol auch von der Europäischen Kommission, aber auf Mitgliedsländerebene vor allem von Deutschland, Frankreich und Großbritannien. Während die EU-Kommission durch Berichte und durch Mitteilung an den Rat die Vertiefung in der grenzüberschreitenden Zusammenarbeit und die Propagierung der Nutzung von EIS und SIENA als zentrale Instrumente anstrebt (Europäische Kommission 2012), können Mitgliedsländer Europol vor allem dadurch stärken, dass sie die Instrumente der Agentur demonstrativ nutzen und weiterentwickeln. Europol ermöglicht über das EIS beispielsweise bei einem Fahrzeughalterabgleich mobil Daten gleichzeitig in der nationalen, der Europol-Datenbank sowie im Schengensystem abzufragen. In Frankreich besitzen sechzig Prozent aller Polizeifahrzeuge solche mobilen Datenterminals (Segell 2004: 84). Deutschland etwa hat die Weiterentwicklung von SIENA durch das UMF-Messaging-Format maßgeblich in die Hand genommen, während Großbritannien die Arbeit der Behörde durch die Integration der Konzepte der erkenntnisgeleiteten Polizeiarbeit und der vorhersagenden Polizeiarbeit maßgeblich geprägt hat. Deutschland, Frankreich und Großbritannien können daher als entscheidende Nutzer und Weiterentwickler Europols betrachtet werden, während für andere Mitgliedsländer Europol weniger zentral ist. Fägersten (2010a: 101 f.) spricht in diesem Zusammenhang von unterschiedlichen „cooperative design[s]“ der Mitgliedsländer. Diese fehlende geronnene Praxis der europäischen Polizeikooperation sowie die divergenten kooperativen Designs lassen sich auf konkrete technische Unterschiede bei der Nutzung von Europol zuspitzen. So ist es seit 2012 zwar theoretisch möglich, dass eine Dateneingabe in dem nationalen System der Ermittlungsbehörden automatisch zu einer Eingabe im EIS führt. Dies entspräche einer Schnittstellenlösung, wie sie etwa für die deutsche Datenbank INPOL-neu existiert. Viele Länder nutzen jedoch nur eine Client-Anwendung, das heißt, dass die Ermittler das EIS als zusätzliche Datenbank auf ihrem Computer aufrufen können, Daten aber nicht direkt übernommen werden. Da nicht alle Europol-Mitglieder die Schnittstellen-Möglichkeit, sondern aufgrund divergierender Rechtsrahmen, Datenverarbeitungskulturen und damit unterschiedlicher IT-Systeme nur die Client-Lösung nutzen, ist zumindest mittelfristig keine zentrale Stärkung der Struktur des EIS und keine gleichwertige Nutzung durch die Mitgliedsländer zu erwarten (Manske 2001: 106).

Aden (1998: 99) sieht die mangelnde Nutzung der Europol-Datenstrukturen auch dadurch begründet, dass Polizeipraktiker lieber mit Kollegen, die ihnen persönlich bekannt sind, zusammenarbeiten als mit zentralen kooperativen Datenstrukturen. Ebenso würden kooperative Ermittlungen dadurch erschwert, dass den Polizisten im europäischen Raum die Orientierung an einer verlässlichen Autorität und klare Führungsstrukturen fehlen würden (Aden 1998: 202).

Da Ermittlungsbehörden deshalb vorrangig an ihre staatlichen Strukturen gebunden bleiben und sich europäisch nicht an eine befehligende Struktur gebunden sehen, bleiben die verbindenden Strukturen wie das EIS und SIENA rein künstliche Überbauten und keine habituellen Kontaktknoten. Daher bemüht sich Europol, zumindest Übermittler polizeilicher Arbeitsprinzipien zu sein und somit zumindest durch eine gewisse Kompatibilität eine stärkere Interaktion zu erreichen. Beispiele hierfür sind das Intelligence led policing und das Predictive policing. Ersteres Prinzip des Datenmanagements, das zur Verbesserung der Erkenntnisse im Staatsschutz dienen soll, betont bereits die Relevanz der Gefahrenabwehr (Ratcliffe 2008: 6). Deren Zentralität wird durch das Predictive policing weiter ausgebaut. Das Predictive policing wurde Ende 2005 durch die PREVENT-Strategie der EU[112] eingeführt. Letzteres beinhaltet sogar Instrumente zur Erkennung und Bewältigung problematischer Verhaltensweisen und die Bekämpfung von Aufstachelung und Anwerbung von Einzelpersonen (Burczyk 2017). Medienberichten zufolge testet die nordrhein-westfälische Polizei die verhindernde Polizeiarbeit seit 2010 für den Gebrauch auf Landesebene. Seit 2014 laufen auch Testreihen in Bayern, Hessen, Baden-Württemberg, Niedersachsen, Hamburg und Berlin. Zusätzlich wird der Einsatz in Rheinland-Pfalz, Sachsen, Brandenburg und Schleswig-Holstein geprüft (Diehl/Kartheuser 2018). Das European Cyber Crime Center (EC3) von Europol bezeichnete das Konzept bereits 2014 als „an important application of Big Data in the area of law enforcement“ (Europol 2014) unter der Überschrift „The future is already here“ (ebd.). Aber auch hier wirkt die Diversität polizeilicher Umsetzungen in unterschiedlichen Ländern erschwerend, sodass es zwar bei einer Hervorhebung des Konzeptes, aber durchaus zu weitreichenden Unterschieden in deren Anwendung kommt (Casey 2010; Ratcliffe 2008).

Selbst wenn also die Einigung auf ein Prinzip[113] oder eine Methodik erreicht worden ist, garantiert dies noch nicht dessen Umsetzung, da (noch) keine dementsprechend kongruente habituelle Praxis vorhanden ist. Es wird daher deutlich, dass die kulturelle Inkongruenz sich in der Nutzung von Europol nicht (nur) dadurch manifestiert, dass kulturelle Unterschiede zu einer rechtlichen Diversität führen, obwohl dies auch einen wichtigen Faktor darstellt (Fägersten 2010a; 2010b). Denn es ist seit Jahren Bestreben der EU, den Rechtsrahmen zu harmonisieren. Bereits seit dem Stockholmer Programm 2009 verständigen sich die Mitgliedsländer über eine verstärkte Zusammenarbeit in den Bereichen innere und öffentliche Sicherheit und die Schaffung gemeinsamer Mindestnormen (Möllers 2012: 18 f.). Es ist vielmehr nachweisbar,

[112] PREVENT ist eine der vier Säulen der EU-Terrorismusbekämpfungsstrategie, die der Europäische Rat Ende 2005 verabschiedet hat.
[113] Ein Prinzip ist nichts anderes als eine Norm. In den Dokumenten wird dieser Begriff jedoch häufiger genutzt.

dass die Umsetzung des Ziels der effektiven Nutzung Europols und der Verstärkung europäischer Strukturen mit dem durch die Gesellschaft geschaffenen Handlungsrahmen der Ermittlungsbehörden korreliert. So sticht beispielsweise das deutsche BKA in der aktiven Nutzung und Weiterentwicklung Europols hervor (Deutsche Welle 2017),[114] weil mit der Novelle des BKA-Gesetzes vom 7. Juli 1997 der deutsche Handlungsrahmen, um mit Europol zusammenzuarbeiten und diese Ebene weiterzuentwickeln, gestärkt wurde, indem beispielsweise die Rolle der deutschen Polizeien in der internationalen und polizeilichen Zusammenarbeit in der Strafverfolgung und der Gefahrenabwehr explizit definiert wurde (Schober 2017: 302 f.). Daher kann das BKA sich zumindest in der inneren Sicherheit weitgehend auf gesellschaftliche Rückendeckung verlassen. Eine starke Bindung an nationale Gesetzgeber und Regierung ist vor allem für Polizeibehörden zentral, da sie das Hoheitsrecht der Gewaltausübung innehalten, und dieser Schulterschluss eine wichtige Voraussetzung dafür, dass die Polizeiorganisationen auf internationaler Ebene überhaupt zusammenarbeiten dürfen und hier eine Übereinkunft ihrer Befugnisse erreichen können. Wie kongruent Polizeibehörden also miteinander kooperieren können, hängt maßgeblich von der nationalen Sicherheitskultur ab, die – stärker als bei den Nachrichtendiensten – nicht nur lediglich eine gewisse Reichweite bereitstellen muss, sondern diese klar durch politische Botschaften ausdefinieren und durch eindeutige öffentliche Unterstützung durch die Regierung demonstrieren muss. So beteuerte der damalige französische Präsident Jacques Chirac schon 1993: „Die Polizeikräfte brauchen einen klaren politischen Willen. Sie müssen sich geleitet fühlen, sie brauchen das Gefühl, unterstützt und geschützt zu werden“ (Aden 1998: 203).[115] Sind die Positionen hinsichtlich Kooperation also nicht kongruent, dann auch, weil der politische Handlungsrahmen der Organisationen entweder in unterschiedliche Richtungen zeigt oder bei einigen Organisationen stärker ausdefiniert ist als bei anderen (Tekin 2017). So resultiert aus dem – klar auf die Vertiefung und Harmonisierung der europäischen Polizeikooperation ausgerichteten – Handlungsrahmen des BKAs, eine aktive Rolle, aus der sogar eine Erwartungshaltung auch an andere Staaten, entsteht (Schober 2017: 303). Gleichzeitig ist diese Aktivität aber eingebettet in die deutsche Sicherheitskultur, vorrangig multilaterale Regelungen zu schaffen, die nicht vorrangig auf Zentralisierung, sondern lediglich auf eine gewisse Normeinigung zielen

[114] Das BKA ist jedoch nicht nur multilateral bei Europol, sondern auch in der bilateralen Polizeikooperation sehr aktiv. Seit 2016 besteht ein Memorandum of Understanding zwischen Deutschland und den USA, das einen verstärkten Austausch zwischen dem Federal Bureau of Investigation (FBI) und dem BKA über Gefährder vorsieht (Bundestag 2016c).

[115] Anders als im geheimdienstlichen Bereich, in dem sich die deutsche Regierung zurückhält, die Möglichkeiten und Grenzen des Arbeitens konkret öffentlich zu diskutieren, wird die Rolle der Polizeien gerade deshalb stärker politisch betrachtet, weil sie für die Gesellschaft sichtbarer sind und auch exekutive Gewalt anwenden können.

(Katzenstein 2008). Da dieser Kontext jedoch nicht in Bezug auf alle Staaten in der Form gegeben ist, kann man im Fall von Europol nicht von einer engen, gleichwertigen Kooperation sprechen, sondern lediglich von Strukturen der Interaktion, die sich erst handlungspraktisch entwickeln und demonstriert werden müssen und durch die entsprechenden Gesetze eine gesellschaftliche Basis erhalten müssen (Frevel/Kuschewski 2007).

4.4.4 Anpassung aus Effektivitätsgründen

Der Neue Institutionalismus hebt hervor, dass sowohl der gesellschaftlich-kulturelle Kontext, als auch die Bedingungen externer technischer Strukturen und daraus entstehende Handlungszwänge gleichermaßen für die Entstehung fester Organisationsstrukturen – und damit auch Kooperationsstrukturen – sorgen. Der Faktor einer nur unzureichend vorhandenen gesellschaftlichen Ausdifferenzierung der Reichweite europäischer Polizeikooperation führt somit zwar dazu, dass eine technische Harmonisierung und Zentralisierung nicht vollumfänglich möglich ist. Daher soll nachfolgend gezeigt werden, dass die Zwänge, hinsichtlich transnationaler Kriminalität auch den Austausch diesbezüglicher Erkenntnisse über Grenzen hinweg verlässlich zu organisieren, die europäische Polizeikooperation in der Form strukturiert, als dass variable, aber dennoch verlässlich ansteuerbare Strukturen der Interaktion erarbeitet werden, Verfahren des Datenaustauschs festgelegt werden, Methoden übertragen werden und die Kompatibilität von Methoden vorangetrieben wird.

Zunächst soll näher dargestellt werden, dass die Europol, auf die Divergenz des Anschlusses und der Nutzung der EIS-Struktur eingehend, das EIS als Schnittstelle zu anderen bilateralen Strukturen anbietet. Im konkreten polizeilichen Anwendungsfall sieht diese Einbindung folgendermaßen aus:

> „Bei einer grenzübergreifenden schweren Straftat oder organisierter Kriminalität könnten Informationen zu einer Person oder einer Strafsache sowohl im Europol-Informationssystem als auch im SIS, an das alle Mitgliedstaaten der EU angeschlossen sind, abgerufen werden, und im Trefferfall könnten Folgeersuchen über die Europol- oder SIRENE-Kanäle übermittelt werden. Zu biometrischen Daten könnte ein Informationsaustausch nach dem Prümer Beschluss stattfinden; an den sich nach einem ‚Treffer'-Folgeersuchen im Rahmen der schwedischen Initiative mittels SIENA anschließen könnte" (Europäische Kommission 2012: 7).

Aus diesem Zitat lässt sich neben der Komplexität des Ineinandergreifens der Strukturen ein vielschichtiger Mehrwert für nationale Ermittlungsbehörden ableiten. Erklärend hierzu müssen die genannten Kanäle näher beschrieben werden: Die SIRENE[116]-Büros sind an das SIS

[116] Die SIRENE-Büros sind in den gleichen Organisationen angesiedelt, die auch als Verbindungsbüros für Europol fungieren, in Deutschland im Bundeskriminalamt (BKA).

angeschlossen und können im Fall eines Treffers in der Datenbank weitere Informationen bei anderen Ermittlungsbehörden anfordern. Der Beschluss von Prüm umfasst die Übermittlung von DNA-Profilen, Fingerabdrücken, Daten aus nationalen Fahrzeugregistern an andere Vertragsstaaten zum Zweck der Ermittlung von Straftaten, der Verhinderung von Straftaten und der Aufrechterhaltung der öffentlichen Sicherheit. Die schwedische Initiative wiederum legte Regeln und Fristen für den Austausch von Informationen und Erkenntnissen zur Durchführung von Ermittlungen und zum polizeilichen Erkenntnisgewinn fest (Europäische Kommission 2012: 3 f.). So stellt Europol zwar keine zentrale Plattform der europäischen Polizeikooperation dar, bietet aber vor allem durch ihren Schnittstellencharakter zusätzlichen Nutzen, der immer weiter ausgebaut wird. Europol kann so beispielsweise durch die zusätzliche Möglichkeit, strukturierte Muster in den APs zu erkennen und Analyseprodukte oder spezifische Informationen über SIENA zu teilen, eine Art variable Meta-Ebene der Polizeikooperation anbieten, deren Mehrwert nicht zentralisiert ist, sondern gezielt angesteuert werden muss. Gleichzeitig kann das EIS variabel mit Daten bestückt werden und jeder Anwender und Mitgliedsstaat behält Verfügungsgewalt darüber, ob er Daten bei EIS einträgt oder nicht und ob er automatische Uploads zulässt. So bestehen auch ‚opt-out-Möglichkeiten' für den Zugang, sowie einige Datentypen, weshalb beispielsweise Deutschland keine DNA-Daten auf EIS hoch lädt (Bundestag 2014: 15).

Der Interpretation, dass die Souveränität der Mitgliedsstaaten und ihrer Organisationen nicht veräußert werden soll, schließt sich damit die Erkenntnis an, dass ein Europa ohne kontrollierte Grenzen den Datenaustausch zur Verhinderung schwerer Straftaten benötigt. Dies zeigt sich zum einen im sogenannten Prinzip der Verfügbarkeit, auf das gleich noch weiter eingegangen werden soll, und zum anderen in der Norm der Interoperabilität, die in der EU immer stärker institutionalisiert wird. Deutschland hat 2005 den Vertrag von Prüm ins Leben gerufen, der außerhalb der Agenturstrukturen als multilateraler Vertrag gestaltet wurde, jedoch ein Prinzip ins Feld führte, das als eine zentrale Europol-Norm betrachtet werden kann. Das Prinzip der Verfügbarkeit wurde parallel durch die schwedische Initiative für Europol entwickelt und steht dafür, dass die Strafverfolgungsbehörden der Europol-Mitgliedstaaten Zugang zu Datenanwendungen anderer Mitgliedstaaten erhalten sollen, wobei die Bedingungen für die Bereitstellung von Informationen für ersuchende Mitgliedsstaaten nicht strenger sein dürfen als die auf nationaler Ebene. Dieses Prinzip der schwedischen Initiative bildet seither die Grundlage für die parallelen Treffersuchen, die durch das standardisierte Datenformat des UMFs ermöglicht werden und die Schwierigkeit, dass durchsuchbare Daten zum Trefferabgleich zunächst in das EIS eingegeben werden müssen, umgehen soll. Durch dieses

Verfahren werden ausländische Polizeiorganisationen inländischen im Prozess des Datenaustausches gleichgesetzt. Die schwedische Initiative wird seit 2006 umgesetzt. Der Vertrag von Prüm[117] integriert das Prinzip der Verfügbarkeit und schafft durch die Möglichkeit, direkt auf die DNA-Analyse-Dateien sowie das elektronische Register mit Kraftfahrzeug- und Kraftfahrzeughalterdaten der anderen Unterzeichnerstaaten zugreifen können, konkrete Anwendungsfälle für die schwedische Initiative (Kietz/Maurer 2006). Obwohl Deutschland die Verhandlungen zum Vertrag vorgenommen und dabei ausdrücklich die Anbindung an Europol zunächst ausgeklammert hat, hat sich die Bundesrepublik anschließend maßgeblich dafür eingesetzt, dass der Vertrag auf Beschluss des Rates vom 23. Juni 2008 in den EU-Rechtsrahmen überführt wurde und Europol nun als technischer Übermittler der unter Prüm übermittelten Daten fungiert (Bundestag 2007: 3). Das Prinzip der Verfügbarkeit im Vertrag von Prüm und in der schwedischen Initiative drückt also vier Punkte aus: erstens wird durch die Akteure berücksichtigt, dass der Austausch von Daten nicht ausschließlich zentral über das EIS erfolgen muss, sondern auch in multilateralen Strukturen erfolgen kann. Zweitens ist das Prinzip der Verfügbarkeit ein sowohl in der Europol-Struktur als auch der bilateralen Kooperationsstruktur generell zu beachtendes, und kann so als eine durch Diskussion entstandene Norm verstanden werden. Drittens wird dadurch ausgedrückt, dass sich national erhobene Daten zu internationalen kriminell oder politisch motivierten Straftaten nicht vollständig trennen lassen, da sie nur in ihrer Gesamtheit Aufschluss über diese Aktivitäten geben und somit Zugriffsrechte und Weiterleitungspflichten gegeben sein und geschaffen werden müssen. Viertens entsteht durch das Prinzip der Verfügbarkeit aber auch die Notwendigkeit, eine sicher Datenübermittlung zu schaffen, weswegen die Norm der Interoperabilität sich zu einer diskutierten Norm entwickelt, unter der Beispielsweise die Datenbanken Eurodac, VIS und SIS für Kreuztrefferanfragen auf eine gemeinsame technische Plattform gehoben werden sollen, auf die auch Europol und die Ermittlungsbehörden der EU-Mitgliedsstaaten Zugriff haben sollen und die bei der EU-IT-Behörde LISA einen physischen Standort erhalten soll. Zwar stehen dort die Server mit den Daten von SIS, VIS und Eurodac voneinander getrennt und weisen keine physischen Verbindungen auf, Doch durch eine gemeinsame Suchmaske können die Server parallel durchsucht werden. So entsteht ein One

[117] Dem Vertrag von Prüm sind nach deutschem Vorschlag Belgien, Spanien, Frankreich, Luxemburg, die Niederlande und Österreich, später auch Finnland, Slowenien, Ungarn, Norwegen, Bulgarien und Rumänien beigetreten. Die Informationen, die aus erfolgreichen Trefferabgleichen gezogen werden können, müssen nach dem Prümer Vertrag zusätzlich an Europol und Eurojust weitergeleitet werden, sofern sich die Straftaten auf deren Zuständigkeitsbereich beziehen und zwei oder mehrere Staaten betreffen (Europäische Kommission 2012: 3).

Stop Shop für Ermittlungsbehörden, der jedoch nur harte Daten[118], sowie, zukünftig, ein Register für Ein- und Ausreisen von Nicht-EU-Bürgern, ein sogenanntes Entry-Exit-System beinhalten soll (Brühl 2018).

Zusammenfassend lässt sich jedoch festhalten, dass die theoretischen Aussagen der Theorie im Fall Europol bestätigt werden können. Die Akteure interpretieren ihre Einbettung in gesellschaftliche und technische Kontexte, konnten aber aufgrund der kulturellen Divergenz und der generell fehlenden Erfahrung einer multilateralen Makrostruktur der Polizeikooperation keine habituellen Handlungsmuster entwickeln. Gleichzeitig erkennen sie den Handlungsbedarf aufgrund externer technischer Bedingungen, beispielsweise, die Mobilität Krimineller sowie die Anwerbung für terroristische Gruppen im Internet grenzübergreifend, und damit zentralisiert, überwachen zu müssen und aufgrund fehlender Grenzkontrollen und sehr mobiler Gefährder einen generellen und verlässlichen Datenaustausch zu garantieren. So entwickeln einige Akteure, darunter Europol selbst, aber auch Ermittlungsbehörden der Mitgliedsländer, Methoden und Verfahren, um diese Effektivität sowohl in die Handlungspraxis der einzelnen Organisationen zu integrieren, als auch einen verlässlichen und kompatiblen Kooperationsmodus zu entwickeln.

4.4.5 Die Intentionalität der Berichterstattung Europols

Europol muss als Agentur der EU bestimmten Berichtspflichten nachkommen. Zu den regelmäßigen Veröffentlichungen zählen Jahresberichte, Strategien, aber auch Informationsprodukte zu den unterschiedlichen Expertenzentren Europols. Zusätzlich informiert die Organisation beständig durch Pressemitteilungen. Eine solch dichte Berichterstattung ist einerseits für die Wissenschaft ein nützliches Instrument. Allerdings muss kritisch berücksichtigt werden, dass Europol als einzige in vorliegender Arbeit vorgestellte Art der Kooperation eine eigene Akteurshaftigkeit besitzt (Kaunert 2010). Diese Vergrößerung der eigenen Rolle wird auch dadurch unterstützt, dass die Europäische Kommission die Stärkung der EU-Organisationen forciert und die Wirksamkeit der Strukturen Europols auch vor diesem Hintergrund herausstellt. Daher sind die Informationen, die Europol bereitstellt, ebenfalls auf eine Intention, die sich bei der ersten Durchsicht nicht erschließt, kritisch zu prüfen. So arbeitet Europol selbst darauf hin, dass die Mitgliedsländer ihre Zusammenarbeit mit der Polizeiagentur verstärken. Daher ist davon auszugehen, dass Informationen zu einer mangelnden Bereitschaft

[118] Auch die Güte diese Daten soll verbessert werden. So streben einige Mitgliedsstaaten, darunter Deutschland, an, gemeinsame Mindestnormen für kriminaltechnische Tätigkeiten ‚vom Tatort bis in den Gerichtssaal' aufzustellen und durchzusetzen (2016d).

sich möglicherweise nicht aus den öffentlichen Dokumenten ergeben, da Europol eine positive Außenwahrnehmung unterstützen möchte. Auch lässt sich die Aufmachung der Informationen in den Europol-Veröffentlichungen im Lichte der Feststellung vorliegender Arbeit, dass durch Europolstrukturen eine gesteigerte Interaktion jenseits politischer Diskussionen über Vertiefungen im Sinne einer Supranationalität erreicht werden soll, herausstellen. So ist die Berichterstattung durch Informationsblätter zu technischen Abläufen geprägt, wodurch die Gefahr besteht, dass der Betrachter diese Haltung unreflektiert übernimmt. Deshalb wurde die Untersuchung auch auf deutsche Bundesdrucksachen, die Europol betreffen, sowie Sekundärquellen ausgeweitet und die Stichhaltigkeit der erbrachten Erkenntnisse dadurch gefestigt. Trotzdem kann – selbst bei umfassender Berichterstattung – nicht ausgeschlossen werden, dass relevante Informationen verborgen geblieben sind. Erschwert werden treffende Aussagen zusätzlich dadurch, dass nicht alle Dokumente, die Europol produziert, öffentlich sind. So fertigt Europol auch Berichte für den Europäischen Rat oder den Rat der EU an, die der Öffentlichkeit nicht zugänglich sind.

5. Fazit und Ausblick

> "Wir fühlen uns von Freunden umgeben, wissen aber kaum, wie wir umgehen sollen mit diffusen Sicherheitsrisiken wie der Privatisierung von Macht durch Terroristen oder Cyberkriminelle. Wir beschweren uns, zu Recht, wenn Verbündete bei der Gefahrenabwehr über das Ziel hinausschießen. Und doch ziehen wir es vor, auf sie angewiesen zu bleiben, und zögern, eigene Fähigkeiten zur Gefahrenabwehr zu verbessern. Aus all dem folgt: Die Beschwörung des Altbekannten wird künftig nicht ausreichen! Die Kernfrage lautet doch: Hat Deutschland die neuen Gefahren und die Veränderungen im Gefüge der internationalen Ordnung schon angemessen wahrgenommen? Reagiert es seinem Gewicht entsprechend?"
>
> *Joachim Gauck*

Vorliegende Arbeit hat mit dem Neuen Institutionalismus eine neue Perspektive auf die internationale Kooperation von Sicherheitsbehörden angestrebt. Dabei konnten wichtige Schlüsse gezogen werden, die nachfolgend zunächst hinsichtlich der ermittelten empirischen Ergebnisse vorgestellt werden, die in der Form zuvor noch nicht erbracht wurden und daher die eingangs aufgeworfenen Forschungsbedarfe füllen können (Abschnitt 5.1). Gleichzeitig muss kritisch diskutiert werden, wo die Grenzen dieses Analysefokus liegen und wo weitere Forschung angesichts bestehender Lücken ansetzen sollte (Abschnitt 5.2). Anschließend werden die erbrachten Erkenntnisse dahingehend hinterfragt, ob Gesellschaft und nationale Kultur sich von der Reflexion der Legitimität der Sicherheitsbehörden entfernen und ob die Gründe dafür in der Komplexität technologischer Entwicklungen zu finden sind (Abschnitt 5.3).

5.1 Das Spannungsfeld zwischen Legitimität und Effektivität aus empirischer Sicht

Im Zentrum der Betrachtung standen gesellschaftlich bedingte und durch die Organisationen interpretierte Grenzen für das Handeln von Sicherheitsorganisationen, die als beeinflussend für Kooperationsarrangements betrachtet wurden. Dies gründete sich darauf, dass Kultur als Erfahrungs- und Handlungsraum verstanden wurde, in dem Organisationen agieren können und der sich auf ihr Verhalten sowohl beschränkend als auch unterstützend auswirken kann, je

nachdem, wie viel Raum ihnen die Gesellschaft für ihre Reichweite zugesteht und wie kongruent dieser Rahmen für unterschiedliche Organisationen, die zusammenarbeiten (wollen), ist. Dabei wurde festgestellt, dass der kulturelle Erfahrungsraum Auswirkungen auf das jeweilige Organisationsdesign der Organisationen hatte – also auf deren Möglichkeiten, enge Kooperationsdesigns zu gestalten – und daher auch die Zusammenarbeit zwischen Organisationen maßgeblich beeinflusst, vor allem, wo diese aus unterschiedlichen kulturellen Erfahrungsräumen stammten. Diese Kongruenz oder Inkongruenz bestimmte die Ergebnisse in den jeweiligen Fallstudien. In der Kooperation der Five Eyes konnten die Akteure ihre Kooperation so fest institutionalisieren, dass eine, auch in die Zukunft gerichtete, gemeinsame Entwicklung umgesetzt werden konnte. Dabei konnten sich die Five Eyes auf internalisierte Institutionen stützen, die etwa besagten, dass generell alle Informationen geteilt werden dürfen, wo dies explizit nicht die Bindung an die eigene Gesellschaft berührt. In der Zusammenarbeit von GCHQ und NSA führte die Kongruenz dazu, dass die Organisationen – teilweise auch in Abgrenzung zueinander – ihre Fähigkeiten derart innovativ entwickeln und bündeln konnten, dass diese Weiterentwicklung der kooperativen Kernkompetenz Kryptoanalyse zum Motor für die weitere Gruppe der Five Eyes werden konnte. Der Fall der Kooperation zwischen NSA und BND war von großer Inkongruenz geprägt. Um ein fest institutionalisiertes Kooperationsarrangement zu erreichen, musste daher eine Übertragung der Technologie des Kooperationspartners erfolgen, um eine gewisse Kompatibilität zu erreichen. In dieser Untersuchung zeigte sich bereits eine Tendenz, die auch in der Fallstudie zur europäischen Polizeikooperation bei Europol offenbar wurde, dort aber anders ausgeprägt war. War der kulturelle Hintergrund zwischen NSA und BND zu divergent, wurde sich vorrangig auf die Auseinandersetzung mit diesen Unterschieden konzentriert und debattiert, was nötig war, um eine effektive Kooperation zu ermöglichen, was schließlich einzig über eine Technologieübertragung realisierbar war. Auch bei Europol ließen sich Unterschiede der kooperierenden Organisationen feststellen, die die Kooperationspartner jedoch nicht hinsichtlich einer Überwindung dieser Unähnlichkeit diskutierten, da das Fehlen einer habitualisierten Bereitschaft zur Nutzung supranationaler zentralisierter Polizeistrukturen eine so zentrale Divergenz darstellte, dass sich die Mitgliedsstaaten nicht auf eine Anpassung, sondern lediglich auf eine Steigerung der Interaktion durch technische Lösungen verständigten. In der Sprache des Neuen Institutionalismus konnten sie also eine strukturelle Äquivalenz nicht erreichen, da die Institution der zentralisierten Kooperation auf der Ebene der Gesellschaften nicht übergreifend entstanden war. In der Interpretation der Notwendigkeit der Reaktion auf exogene strukturelle Bedingungen, für die die Gesellschaften keine Erfahrungswerte und,

daraus folgend, auch keine regulativen Grenzen oder handlungsleitenden Institutionen anbieten konnte, wurde eine technische Vernetzung vorgenommen, die die Wahrnehmung gesellschaftlicher Grenzen mit der Notwendigkeit technischer Interaktion übereinbrachte. Durch diese Erkenntnisse lassen sich zentrale Desiderate füllen, die durch den ausgewerteten Literaturstand nicht geschlossen werden konnten. So konnte der Nachweis erbracht werden, dass die gesellschaftlichen Institutionen hinsichtlich des angemessenen Verhaltens von Sicherheitsbehörden kulturell geprägt und daher meist – mit Ausnahme kulturell kongruenter und erfahrungsgeschichtlich gewachsener Kooperation – divergierend sind, was die bi- und multilaterale Kooperation stark beeinflusst. Trotzdem sind für komplexe Phänomene oft keine handlungsleitenden Beschreibungen angemessenen Verhaltens vorhanden. Die Frage, ob die Organisationen ihr Kooperationsarrangement hinsichtlich dieser Gemengelage einzig nach der Interpretation von Möglichkeiten zu legitimem Handeln oder doch größtenteils nach technischer Effektivität ausgestalteten, konnte insofern beantwortet werden, als dass beide Bereiche – die der Kongruenz der Erwartungen und die der Kompatibilität der technischen und methodischen Strukturen zur Bewältigung von Komplexität – für die Kooperation zentral sind und Dimensionen ausdrücken, nach denen sich Organisationen in ihrer Kooperation ausrichten. Zwar kann es aus theoretischer Perspektive unbefriedigend anmuten, dass nicht geklärt werden kann, welche der beiden Variablen eine größere Auswirkung aufweist. Aus der empirischen Beobachtung wird jedoch deutlich, dass selbst in der Hervorhebung größter Notwendigkeit effektiver Maßgaben die Organisationen hervorheben, dass der Auftrag legitim erbracht werden muss, da die Gesellschaften sonst die Form der Kooperation als illegitim empfinden, retrospektiv nicht unterstützt und so womöglich auch zukünftig nicht (in der angewandten Form) akzeptieren wird (Morisse-Schilbach/Peine 2008). Ebenfalls konnte festgestellt werden, dass selbst in Kooperationskonstellationen, in denen kein enger Zustand der Institutionalisierung besteht, wie im Fall Europol, gegenseitige Zugriffsrechte und Weiterleitungspflichten – im Gegensatz zu ad-hoc-Kooperationen – garantiert werden, um die Kooperation stabil zu gestalten. Eine bis zu einem gewissen Grad normative Form des Organisierens der Kooperation wird also immer gewählt, um eine Kompatibilität hinsichtlich der Methoden und Strukturen der Kooperationspartner zu erreichen, wo dies möglich ist. Ihre Ausgestaltung und die Tiefe der Institutionalisierung hängen aber wiederum genau von der Größe der Kompatibilität als Faktor ab und Akteure interpretieren sie dahingehend, ob eine tiefere institutionelle Verbundenheit oder nur eine technische Interaktion vorliegt oder angemessen ist. Bei einer Interaktion bei starker Divergenz traten außerdem stärker interorganisationale Bedingungen zutage, die auch einen gewissen interorganisationalen Zwang

darstellen können. So sind Organisationen, die keine eigenen Mittel aufgrund mangelnder kultureller Erfahrungsräume entwickeln können, auf die Übertragung durch andere Organisationen angewiesen, die dann entweder eine stärkere Anpassung oder eine größere Übermittlung von Informationen fordern können. Hier kann das durch die Akteure interpretierte gesellschaftliche Spannungsfeld zwischen Legitimität und Effektivität also für einen organisationalen Zielkonflikt sorgen. Denn zur effektiven Erfüllung des gesellschaftlichen Auftrages nach Sicherheit benötigen die Organisationen auch eigene Methoden und Strukturen. Wo sie nicht vorhanden sind, bietet Kooperation die Möglichkeit, sie zu erhalten. Gleichzeitig könnte eine Weiterleitung großer Datenmengen zum Ausgleich für eine diesbezügliche Methodenübernahme gesellschaftlich retrospektiv als illegitim bewertet werden. Aus der Sicht der Organisationen ist eine solche Kooperationshinwendung jedoch zwangsläufig, denn ohne diese Gegenleistung kann auch die Technologie nicht übertragen werden, die sie letztlich jedoch vor allem basierend auf ihrem gesellschaftlichen Auftrag dringend benötigen.

Die Interpretation gesellschaftlicher Erwartungen konnte in vorliegender Arbeit als zentrale theoretische Prämisse identifiziert werden, die zugleich empirisch beobachtbar ist. Auch machte diese Fokussierung eine erweiterte Betrachtung der Dualität zwischen Akteur und Struktur, die in ihrer Festlegung nach Giddens (1984) eine der Grundlagen des Neuen Institutionalismus darstellt, möglich. Denn auf den ersten Blick suggeriert die Orientierung des Akteurs an einer, ihm übergeordneten, Struktur, dass er durch diese Rückbindung eine Versicherung dahingehend erhält, welche Handlungen er wählen kann um Legitimität zu erhalten. Es kann jedoch durch die vorliegende Untersuchung bewiesen werden, dass diese Rückversicherung nicht immer gelingt. Dieser Umstand ergibt sich schon aus der ‚Verfeinerung des Institutionsbegriffs' in vorliegender Arbeit, in der die Institution als habitualisierte Form einer Norm begriffen wurde. Der Lebenszyklus der Norm definiert aber deutlich, dass die erste Phase einer Norm ihre Entstehung ist. Es ließ sich jedoch feststellen, dass handlungsleitende Normen für viele komplexe Phänomene, denen sich Sicherheitsbehörden ausgesetzt sehen, noch gar nicht vorhanden sind und die Organisationen einen Mangel an Präzedenzfällen, etwa für den Umgang mit sensiblen Metadaten, interpretierten und daraufhin die Vereinbarung trafen, aufgrund fehlender Richtungsweisung von Fall zu Fall zu entscheiden. Gleichzeitig veranlasste die Reaktion auf die technischen Bedingungen des Internets die Five Eyes dazu, auch neue Regelungen für den generellen Umgang mit internationalen Datenströmen zu erarbeiten. So entwickelten beispielsweise NSA und GCHQ eine Verfahrensweise zur Verwendung britischer Daten, die bei Verdacht ebenfalls ausgewertet werden dürfen. Zusätzlich erlaubt diese enge Kooperation den Geheimdiensten der Anglosphäre, sich auch in

der Gruppe fest institutionalisiert weiterzuentwickeln, was dadurch geschieht, dass die stärkeren Akteure ihre Technologie und methodischen Weiterentwicklungen auch an die schwächeren Gruppenmitglieder weiterreichen und eine insgesamt kongruente Weiterentwicklung angestrebt wird. Die Vorgehensweise, Methoden in der Gruppenstruktur weiterzureichen, lässt sich auch bei Europol beobachten. Akteure, die von ihrer Initiative überzeugt sind, holen nach und nach weitere Unterstützer durch das Versprechen hinzu, dass durch eine diesbezügliche Interaktion die komplexen Bedingungen der Überwachung transnationaler Kriminalität besser bewältigt werden können. Hierbei steht die Bewältigung der Divergenz der Nutzung gemeinsamer Strukturen im Vordergrund, weshalb die Akteure sich nicht vordergründig auf die Entwicklung zentraler Strukturen konzentrierten, sondern variable Strukturen zuließen, dafür aber Methoden und Normen zur Datenweitergabe entwickelten und demonstrieren. Europol stellte dann sowohl in multilateralen Initiativen, die durch Mitgliedsländer gestartet wurden, als auch innerhalb der Kooperation unter Europol, eine wichtige Schnittstelle dar, um den effektiven Datenaustausch zu gewährleisten. Damit realisierten die Mitgliedsländer eine normengeleitete Kooperation aus Effektivitätsgründen auch dort, wo aufgrund von Souveränitätsvorbehalten und divergenten Handlungsräumen keine internalisierten Praktiken zur zentralisierten Polizeikooperation vorhanden waren.[119] Die Bindung vorrangig an die eigene Gesellschaft, bei einem gleichzeitigen Verständnis dafür, dass Anpassungen zugunsten des Ziels der Kompatibilität notwendig sind, ist für die Polizeikooperation – wie es auch für gesellschaftliche Bindung der Geheimdienste zu attestieren ist – somit eine unverrückbare und nicht zu vernachlässigende Institution der Kooperation. Die Untersuchung der europäischen Polizeikooperation weist aber auch große Gemeinsamkeiten zum Fall der Kooperation zwischen NSA und BND auf. Zwar bestehen eklatante Unterschiede zwischen dem US-amerikanischen und dem deutschen Nachrichtendienst insoweit, als dass sie von unterschiedlichen gesellschaftlich gewünschten Reichweiten ihrer Handlungen geprägt sind. Der BND konnte aufgrund seines kulturellen Hintergrundes keine derart weitreichenden Technologien erschaffen und anwenden, wie die NSA dazu in der Lage war. Trotzdem konnten im Zusammenwirken der Akteure in der Kooperation durch den BND methodische Verbesserungen erreicht werden, die ihn zur NSA kompatibler werden ließen, ohne dass er sich gänzlich gegen gesellschaftliche Erwartungen stellen musste. Zwar wurden die Umstände, unter denen der deutsche Auslandsnachrichtendienst an die Methodik XKEYSCORE gelangt war, retrospektiv kritisiert.

[119] Auch Funda Tekin (2017) hat dieses ‚Spannungsfeld zwischen Problemlösungsinstinkt und Souveränitätsreflex' bereits beschrieben, ohne dabei jedoch spezifisch auf Europol einzugehen.

Die Anwendung der Technologie wurde jedoch rückwirkend gesetzlich legitimiert, woraus aus Sicht des Neuen Institutionalismus die Schlussfolgerung erwächst, dass die Gesellschaft erkannt hat, dass der BND nur durch diese methodische Anpassung die Nachfrage nach Sicherheit erfüllen konnte. In der Untersuchung der Entwicklungen bei Europol konnten ähnliche Zusammenhänge attestiert werden. Auch wenn die Zentralisierung von Polizeikompetenzen zur Bekämpfung transnationaler Bedrohungen unter dem Dach der europäischen Polizeiagentur Grenzen durch die divergente Bereitschaft einer vertieften Polizeikooperation bei den Ermittlungsbehörden der Mitgliedsländer erfahren hat, so entstand doch durch die Zusammenwirkung der unter Europol subsumierten Mitgliedsländer eine Kooperation, die zwar keiner Verbundenheit, entspricht, in der aber die Interaktion zwischen ihnen dadurch gesteigert werden konnte, dass mittels SIENA und UMF technische Strukturen sowie Verfahrensweisen geschaffen wurden, die zwar keine institutionalisierte Struktur darstellen, aber einen kompatible und gleichwertigen Austausch und dadurch eine Steigerung der Effektivität erreichen konnten.

Daher konnte die empirische Untersuchung zeigen, dass es in allen Kooperationsarrangements zumindest zu einer gewissen Form der Institutionalisierung, im Sinne einer gemeinsamen Struktur und einer Anpassung der Kooperationspartner an, an diese Struktur gebundene, Handlungsmodelle kam. Sowohl geheimdienstliche als auch polizeiliche Akteure konstruierten im Untersuchungszeitraum 2002 bis 2017 weitreichende Kooperationsarrangements, um entweder Daten zu erschließen, Daten zu verknüpfen oder Daten weiterzuleiten. Diese Vorhaben ließen sich als koordiniertes Handeln identifizieren und sind daher im Sinne der IB auch als Kooperation zu betrachten (Keohane 1984). Sie dienten dem Zweck, durch interorganisationale Zusammenarbeit ein möglichst weitreichendes (durch viele Daten), ein möglich verständliches (durch Verknüpfung unterschiedlicher Datentypen, die dann zu Erkenntnissen führen können) und ein möglichst vernetztes (wenn andere Akteure Daten erhalten, können sie entweder ihr eigenes Erkenntnisbild schärfen, oder dem weiterleitenden Akteur zusätzliche Informationen zukommen lassen, um dessen Wissen zu vergrößern) Maß zu erreichen. Die Gruppe der Geheimdienste der Anglosphäre, die Five Eyes, generierten ihre Daten zunächst über spezielle Zugänge an Glasfaserkabeln. Ein solches Projekt trägt den Namen WINDSTOP und ermöglicht es, Daten aus internationalen Kommunikationsstrukturen aufzuschließen, die dann an alle Five-Eyes-Organisationen weitergeleitet werden können. Eine Struktur zur Weiterleitung dieser Daten sowohl an andere US-Geheimdienste als auch an die Partnerorganisationen ist ICREACH. Die Struktur ermöglicht die Weiterleitung von Daten der NSA an andere US-Dienste sowie die Five-Eyes-Partner „to the maximum extent possible“

(National Security Agency 2008d). Nicht immer werden Daten jedoch über, den anderen Kooperationspartnern bekannte, Verfahren erschlossen. Wenn Quellen oder Methoden vor den Partnern geschützt werden sollen, können Daten über TICKETWINDOW geteilt werden. Durch diese Überwindung der Sensibilität der geheimdienstlichen Kooperation – die immer das Risiko beinhaltet, dass eigene streng geschützte Fähigkeiten und Zugänge offenbar werden könnten – konnte die Menge der, den Five Eyes zugänglichen, Informationen und Daten gesteigert werden. Der Zusammenhang zwischen Methoden der Datenerschließung und einer effektiven Kooperation wird aber auch durch ein Verständnis der komplexen Programme, vor allem der NSA und des GCHQs, deutlich. QUANTUMTHEORY, das Programm zur automatisierten Speicherung und Sortierung von Daten sowie zum Hinweis auf ungeschützte Aufklärungszielsysteme, zeigt, dass Datenerschließung nicht nur mit einer Datenquelle, sondern vor allem mit, möglichst automatisierten, Datensortierungsprogrammen einhergeht, die dem Analysten einen Teil seiner Bewertungs- und Verknüpfungsarbeit bereits abnimmt. Dabei orientieren sich Methoden und Techniken an der Datenorganisationsform eines One Stop Shops für Informationen, in dem alle relevanten Daten bereits durch das System kategorisiert werden und vom Analysten nur noch angewählt werden müssen. Auch bei Europol wird dieses Vorhaben durch das EIS verfolgt. Zusätzlich entstand auch hier durch SIENA eine Datenweiterleitungsstruktur, die eine Weitergabe von sensiblen Informationen ermöglicht, ohne dass diese in einer gemeinsamen Datenbank gespeichert werden müssen.

Dadurch sind die untersuchten Geheimdienste sowie die Akteure in der europäischen Polizeikooperation faktisch dort technisch miteinander verbunden, wo dies nicht aufgrund der Bindung an die Gesellschaft begrenzt werden muss. Es konnte jedoch beobachtet werden, dass die materiellen, technischen Verbindungen zudem in einigen Fällen auch von immateriellen Anpassung, etwa durch die Weitergabe des metadatenzentrierten Ansatzes durch die NSA an den BND, begleitet wurden. Somit werden materiellen Verbindungen in den Kooperationsbeziehungen immer auch von immateriellen Normen, zumindest von deren Entstehen, begleitet. Während die europäische Polizeikooperation durch die Beschränkung, keine zentrale supranationale Kooperationsstruktur aufbauen zu können, gehemmt war, konnte sie aufgrund der Notwendigkeit, sich an die sicherheitstechnischen Erfordernisse eines internationalen Kommunikationsraums sowie eines grenzenlosen Raums Europa anzupassen, die immateriellen Institution der Zugriffsrechte der Ermittlungsbehörden auf die Datenpools anderer Länder schaffen. Daher lässt sich die Frage aufwerfen, ob die interorganisationale Kooperation lediglich durch die Vertiefung von Strukturen aufgrund diesbezüglich vorhandener internalisierter Kooperationsmodi und einem gemeinsamen oder ähnlichen

Handlungsraum geprägt ist, oder ob es sich nicht vielmehr um weitreichendere Normdiffusionsprozesse handelt, die traditionell in der Politikwissenschaft eher als von internationalen Organisationen ausgehend betrachtet wurden. Es lässt sich dann jedoch kritisch diskutieren, ob Sicherheitsbehörden diese Rolle überhaupt legitim einnehmen dürfen.

Durch die strukturierte Hervorhebung der in vorliegender Arbeit erbrachten empirischen Erkenntnisse offenbart sich also dreierlei: Erstens kann die gesellschaftliche Sphäre nie die alleinige Ebene sein, von der aus sich Kooperation betrachten lässt, da sie interorganisationale Interpretations- und Anpassungsprozesse nicht berücksichtigt. Kooperation – und damit auch die Forschung – muss damit immer eine vertikale Bindung von Organisationen an die Gesellschaft, gleichzeitig aber die horizontale Bindung der Organisationen aneinander berücksichtigen. Zweitens offenbart sich in der interorganisationalen Verbindung eine Gefahr für liberale Gesellschaften. Denn sie können zwar Vorgaben zum allgemeinen Handlungsraum ihrer Organisationen machen, in der Kooperation wirken jedoch auch starke interorganisationale Anpassungsprozesse, die sich aus dem Zusammentreffen von unterschiedlich fähigen und ‚gewohnten' Organisationen entwickeln und auf die die Gesellschaften keinen Einfluss nehmen können, da sie für den interorganisationalen Austausch nur eine abstrakte Ebene, die interpretiert werden muss, und keinen Diskussionspartner darstellen. Drittens können Gesellschaften, dieser Betrachtung nach, selbst in einen Zielkonflikt geraten. Denn wenn sich aus der Kooperation auch effektivere Lösungen für ihre eigenen Organisationen ergeben könnten, sind Gesellschaften, sowohl im Einzelfall als auch generell, dazu angehalten zu überlegen, inwieweit sie ihre Organisationen bei dieser Anpassung zu mehr Kompatibilität in der internationalen Kooperation unterstützen oder begrenzen wollen.

5.2 Grenzen der Betrachtung

Die vorliegende Perspektive auf die Kooperation von Sicherheitsbehörden hat für sich in Anspruch genommen, den analytischen Blick auf diese zu weiten. Durch die Hervorhebung, dass Organisationen nicht durch Eigeninteressen, sondern vor allem durch die Interpretation der Erwartungen ihrer Gesellschaften motiviert, aber auch beschränkt sind, konnte ein Analyseansatz genutzt werden, der bislang in der Untersuchung nachrichtendienstlicher und polizeilicher Kooperation noch nicht verwendet wurde. Mit der Abkehr von der ontologischen Vorstellung eines rationalen Akteurs konnte die Untersuchung einen wissenschaftlichen Mehrwert durch die Betonung der Einbettung des Akteurs in ihm vorgelagerte Strukturen gewinnen. Dadurch konnte die Studie über bereits bekannte Ansätze der Forschung zu Nachrichtendiensten und anderen Sicherheitsbehörden hinausgehen. Durch die Anwendung auf

die internationale Kooperation konnte darüber hinaus auch der Anwendungsbereich des Neuen Institutionalismus erweitert werden. Dabei ging der Fokus der Betrachtung auch über bekannte Ansätze der strategischen Kulturforschung hinaus, da Kultur nicht als stabile Größe, sondern vielmehr in ihrer dynamischen Qualität behandelt wurde (Siedschlag 2006; Farrell 1998). So wurde angenommen, dass kulturelle Variablen zwar zu (unterschiedlichen) Erfahrungsräumen führen. Allerdings wird Erfahrung nicht nur durch Kultur bewirkt, sondern kann auch im interorganisationalen Austausch erworben werden. Dadurch wurde nachweisbar, dass kulturelle Kongruenz und Inkongruenz sich zueinander prozessual verhalten. Durch einen Konsens über die Unähnlichkeit kann dann eine Anpassung in Teilbereichen erreicht werden. Bei Europol zeigte sich, dass eine Absage an eine strukturelle Zentralisierung des Datenaustauschs aufgrund zu divergenter kooperativer Designs keine grundsätzliche Einschränkung darstellte. Eher diente diese Wahrnehmung der Divergenz selbst als Grundlage für einen Handlungsraum, der zwar eine Trennlinie zwischen den einzelnen Datenbanken zieht und die Datenhoheit der Ermittlungsbehörden berücksichtigt, trotzdem aber Raum für eine Anpassung lässt. Die Feststellung, dass kulturelle Inkongruenz und Kongruenz sich in methodischen und strukturellen Angleichungen prozessual verändern können, wenn sie auch gleichzeitig immer wichtige Bezugsgrößen bleiben, erfordert aber auch eine Reflexion dahingehend, dass auch Institutionalisierungsprozesse schwierig beobachtbar sein können, vor allem dann, wenn einige wichtige Zustände bereits vor dem untersuchten Zeitraum erreicht wurden. So entwickelten sich die tiefsten nachrichtendienstlichen Partnerschaften, die in dieser Arbeit untersucht wurden, bereits vor Jahrzehnten. Damals war diese Entstehung, ebenso wie dies für die Entwicklungen in dieser Arbeit nachgewiesen werden konnte, vermutlich genauso von einer Interpretation gesellschaftlicher Grenzen und eines antizipierten technischen Handlungsbedarfs auf der anderen Seite ausgelöst. So arbeiteten US-amerikanische Dienste und der Vorläufer des britischen Nachrichtendienstes GCHQ schon während des Zweiten Weltkriegs an gemeinsamen Dechiffrierlösungen und wurden auch in anderen technischen Bereichen arbeitsteilig aktiv (Herman 2002: 202). Diese Zusammenarbeit wurde bald auch auf Kanada ausgedehnt und schloss darauffolgend Neuseeland und Australien mit ein (Rudner 2006). Die kulturelle Kongruenz zeigt sich bei diesen Organisationen zwar durchaus dadurch, dass ähnliche gesellschaftliche Bedingungen dafür sorgen, dass die Nachrichtendienste einen vergleichbar großen Handlungsspielraum haben. Letztendlich lässt sich jedoch im Untersuchungszeitraum nicht eindeutig feststellen, ob dieser kulturell bedingte Handlungsrahmen oder die Pfadabhängigkeit bezüglich der kongruenten Zusammenarbeit seit dem Zweiten Weltkrieg, für die Ergebnisse im Untersuchungszeitraum vorliegender Arbeit eine

wichtigere Rolle spielen. Allerdings wird vermutet, dass eine derart weitreichende Struktur der Kooperation, in der die Organisationen nahezu in einem Ringtausch miteinander verbunden sind, ohne eine gewisse kulturelle Kongruenz – und ein sich damit entwickelndes kollektives Selbstbild – nicht denkbar wäre. Gerade in der Geheimdienstforschung drängt sich jedoch der Verdacht auf, dass die Organisationen nur auf die ihnen eigene Weise handeln, weil sie generell einen großen gesetzlichen Handlungsrahmen aufweisen sowie sich durch einen Informationsvorsprung auch der parlamentarischen Kontrolle entziehen können. Dennoch wurde in der Analyse deutlich, dass die Akteure auf ihren gesellschaftlichen Kontext Bezug nehmen und sich durchaus nach ihm ausrichten sowie in weitreichende Entscheidungen, wie gemeinsame Operationen oder neue Regelungen im Datenaustausch, auch die Regierungen eingebunden sind. Die gesellschaftliche Einbettung und die dadurch notwendige kulturelle Kongruenz kann also als valider Einflussfaktor auf die untersuchten Kooperationsarrangements betrachtet werden. Allerdings lassen sich diese kulturellen Faktoren aus einer holistischen Perspektive nie gänzlich von der Tragweite vorangegangener relationaler Begebenheiten, die Wirkungen bis in die Gegenwart aufweisen, loslösen. Auch birgt die Betonung der Wechselseitigkeit von Akteur und Struktur die Schwierigkeit, dass keine verlässlichen und generalisierbaren Kausalketten gebildet werden können. Trotzdem bietet der Neue Institutionalismus eine relevante Perspektive auf politisch relevantes Akteurshandeln und kann gegebenenfalls auch durch eine stärkere Herausarbeitung der Kategorie der Pfadabhängigkeiten noch weiter präzisiert und empirisch auf weitere Problemfelder angewandt werden.[120] Darüber hinaus kann die Dualität von Akteur und Struktur in zukünftiger Forschung noch weiter geschärft werden. Der Akteur wird im Neuen Institutionalismus vor allem als von der Struktur beeinflusst betrachtet. Er kann zwar auch auf sie zurückwirken, aber nur, wenn er nach deren ‚Spielregeln' spielt. Die Auswertung vorliegender Arbeit hat jedoch auch ergeben, dass sich moderne Gesellschaften – die als die maßgebliche Struktur in dieser Darlegung gelten – mit den möglichen Wirkungen weitreichender Sicherheitsmaßnahmen auf gesellschaftliche,

[120] Die Verbindung der unterschiedlichen Formen des Neuen Institutionalismus – des soziologischen Institutionalismus, des historischen Institutionalismus, des rational-choice-Institutionalismus (Hall/Taylor 1996) und des, seltener verwendeten, diskursiven Institutionalismus – ist indes nichts Ungewöhnliches. So kann der historische Institutionalismus mit dem soziologischen, sowie der soziologische und der historische Institutionalismus mit dem diskursiven Institutionalismus kombiniert werden (Carstensen/Schmidt 1996). Die Verbindung vom rational-choice-Institutionalismus ist jedoch nur mit dem historischen Institutionalismus möglich, denn er geht von einem positivistischen Wissenschaftsverständnis aus, das mit der Annahme des ‚Homo sociologicus' des soziologischen und diskursiven Institutionalismus nur eingeschränkt kompatibel ist. Die Annahme der Pfadabhängigkeit des historischen Institutionalismus ist jedoch sowohl mit den Einschätzungen einer eingebetteten Rationalität als auch einer Objektivität von Akteuren vereinbar. Zusätzlich zu diesen institutionalistischen Analyseansätzen auf Akteursebene kann auf systemischer Ebene die World-Polity-Theorie als institutionalistische Theorie eingeordnet und komplementär verwendet werden (Meyer et al. 2005/Finnemore 1996; 1995).

traditionelle Institutionen nicht (mehr) auseinandersetzen (können), da die potentiellen Einschränkungen, welche durch diese Maßnahmen entstehen, nur auf einer komplexen technischen Ebene zu fassen sind, die die Gesellschaften nicht reflektieren oder die ihnen kognitiv in ihrer Wirkung nicht begreifbar sind. So werden zwar durch die Regierungen Diskussionen darüber geführt, ob sicherheitspolitische Engagements weitreichend(er) oder beschränkt(er) ausgestaltet werden sollen (Hegemann 2018; Gauck 2014). Wie diese Realisierung im Rahmen zeitgemäßer, komplexer technischer Methodik aussieht oder aussehen soll, über diese Frage herrscht jedoch kein gesellschaftlicher Konsens. Vielmehr haben die Veröffentlichungen der durch Edward Snowden entwendeten Papiere die Gesellschaften alarmiert, aber keine weitreichenden Diskussionen über Lösungs- oder Veränderungsprozesse angestoßen (Dörr/Diersch 2017). Die Auseinandersetzung vorliegender Arbeit mit der Wirkung technischer Unsicherheit, die auch durch mangelnde gesellschaftliche Institutionen für aktuelle und zukünftige technische Bedingungen entsteht, deren effektive Bearbeitung durch die Organisationen jedoch gesellschaftlich vorausgesetzt wird, zeigt jedoch vier Entwicklungen auf: Erstens reagieren Organisationen in jedem Fall auf neue technische Herausforderungen, da dies in ihren gesellschaftlichen Auftrag fällt. Ist kein gesellschaftlicher Konsens zu erwünschten Verhaltensweisen diesbezüglich abrufbar, beziehungsweise stehen keine geeigneten Handlungsräume zur Verfügung, um adäquate Lösungen hierzu zu entwickeln, führt das in den Organisationen zweitens zu einer Interpretation eines zu eingeschränkten Handlungsraums, der ihren Auftrag, Sicherheit und Informationen – gerade in der Kooperation – bereitzustellen, behindert. Drittens wenden sich Organisationen bei einer Wahrnehmung einer zu großen eigenen Beschränkung für die Lösung ihrer methodischen Probleme dann an ihre Kooperationspartner, was deswegen eine Anpassung der Organisation an ihre Kooperationspartner mit sich zieht, da die Übernahme von Kooperationslösungen eine gewisse methodische und strukturelle Kompatibilität voraussetzt und benötigt. Dies wiederum führt, viertens, dazu, dass die Gesellschaft in einen weiteren Konflikt gerät, da sie diese Entwicklung zwar hinsichtlich einer Steigerung der Effektivität gutheißen müsste, jedoch über die Bestimmung der legitimen Mittel ihrer Organisation die Autorität verliert, beziehungsweise ihren Einfluss deswegen nicht wahrnimmt, weil sie mangels Erfahrung mit vergleichbaren Phänomenen nicht weiß, welche Mittel sie für angemessen und erstrebenswert hält. Diskutiert werden muss bei dieser Anmerkung jedoch, ob sich dadurch, dass die Gesellschaft in vorliegender Arbeit als diffuse Gruppe betrachtet wurde, deren Einfluss empirisch nur durch die Interpretation ihrer Erwartungen durch die Organisationen betrachtet wurde, Einschränkungen für die Analyse ergaben, obwohl dieses Vorgehen im Sinne des Neuen

Institutionalismus legitim und gebräuchlich ist (Senge/Hellmann 2006: 23). Eine darüberhinausgehende Betrachtung könnte die öffentliche Meinung als zusätzliche Variable oder die Interdependenz zwischen Regierungsentscheidungen und Entwicklungen auf interorganisationaler Kooperationsebene als weiteren Aspekt in die Betrachtung nehmen und etwa untersuchen, inwieweit Entscheidungen zu einer verstärkten Kooperation Ausdruck symbolischen Handelns sind oder einer globalen Norm folgen (Hegemann/Kahl 2012; Feldman/March 1981; Meyer/Rowan 1977). Trotzdem wird angenommen, dass die Betrachtungsweise vorliegender Arbeit einen Mehrwert zur wissenschaftlichen Erforschung von Sicherheitskooperation erbringen konnte, da die empirische Untersuchung ergab, dass die Akteure ihr eigenes Handeln und auch die Aktivitäten und Strukturen ihrer Kooperationspartner immer im Hinblick auf ihre und deren gesellschaftliche Einbettung reflektieren. Auch wenn die Verbindung zwischen gesellschaftlichen Bedarfen und Aufträgen aufgrund der Wahl eines konstruktivistischen Analyseansatzes nicht in ihrer Kausalität für das Organisations- und Kooperationshandeln, sondern lediglich in ihrer Maßgeblichkeit gezeigt werden konnte, geht vorliegende Arbeit davon aus, dass die Ergebnisse in den unterschiedlichen Fallstudien nicht gänzlich durch die Wahl des Modells eines rationalen Akteurs erklärbar wären. Denn gesellschaftliche Institutionen, die von Kultur beeinflusst sind, sind durchaus nicht nur reine Anreizstrukturen für die untersuchten Akteure. In vielen Fällen ist nachweisbar, dass einige Akteure sich eine stärkere Interaktion untereinander aufgrund von bürokratischen Interessen durchaus wünschen würden, wie dies im Material etwa von BND, NSA, aber auch vom BKA, ausgedrückt wird. Sie können sich jedoch nur in diese Richtung bewegen, wenn sie eine Rechtfertigung dieser Initiative unter Rückbezug auf ihre Gesellschaft wahrnehmen können beziehungsweise hier nicht an eindeutige Grenzen stoßen. Hervorzuheben ist jedoch auch, dass die Fragmentierung des Materials die Untersuchungen der nachrichtendienstlichen Kooperation erschwert hat. Somit sind alternative Erklärungen so lange nicht gänzlich auszuschließen, bis ein vollständiger Blick auf die Vorgänge im geheimdienstlichen Bereich im Untersuchungszeitraum durch eine Archivöffnung erreicht werden kann. Auch kann nie ausgeschlossen werden, dass die institutionellen Bindungen einer Organisation nicht durch – diesen zuwiderhandelnde – Einzelpersonen oder Gruppen umgangen werden und so Entwicklungen zutage treten, die der gesellschaftlichen Bindung widersprechen. Hierbei ist jedoch zu berücksichtigen, dass gesellschaftliche Institutionen kontrafaktische Gültigkeit besitzen, weswegen eine Zuwiderhandlung ihre generelle Wirkung nicht obsolet macht (Brummer/Oppermann 2014: 56; Kratochwil/Ruggie 1986: 767-768). Dadurch, dass die Auswertung sich auf Dokumente bezog, die zum Großteil einem intersubjektiven

Organisationsnarrativ entsprechen, wurde beabsichtigt, diese potentiellen individuellen Strategien implizit anzusprechen und deren mögliches Wirken zu diskutieren. Es kann jedoch nicht gänzlich ausgeschlossen werden, dass die Verknüpfung von organisationalen Handlungen und ihrer gesellschaftlichen Relevanz lediglich einem absichtlichen strategischen Narrativ entspricht, der mögliche abweichende Strategien bewusst verbergen soll. Diese Manipulation ist gerade in Bezug auf die Untersuchung geheimdienstlicher Aktivitäten, zu denen auch die gezielte Täuschung zählt, nie ganz zu verhindern, sodass sich diese Problematik auch mit einem anderen analytischen Fokus oder einer divergierenden Untersuchungsmethode – etwa Einzelinterviews – ergeben hätte. Zugleich hat vorliegende Arbeit versucht, die Reliabilität, Objektivität und Validität der erbrachten Aussagen dadurch zu stärken, dass auch etwaige Unsicherheiten und Einschränkungen explizit herausgestellt wurden. Durch diese reflektierte Auseinandersetzung mit dem Textmaterial und den dort abgebildeten Vorgängen gerät nicht nur die Autorin vorliegender Arbeit, sondern letztlich auch deren Leser sowie Wissenschaftler, die die Untersuchungen in den behandelten Fällen vertiefen oder weiterführen wollen, in die Pflicht „to struggle to figure out the ‚big picture'" (Rappert 2010: 583). Somit erhebt vorliegende Arbeit lediglich den Anspruch, eine überprüfbare analytische Anwendung deduktiver Erklärungen an verfügbares Material vorgenommen und die Erkenntnisse daraus kritisch eingeordnet zu haben. Eine holistische Erklärung sowie die Ableitung von Gesetzmäßigkeiten für Kooperationsverhalten bei Sicherheitsorganen sind jedoch nicht möglich und wurden explizit nicht angestrebt. Herausgearbeitet werden konnte jedoch das Spannungsverhältnis zwischen Legitimität und Effektivität, wobei beide Interpretationsbereiche einander in der Form verbunden sind, dass sie beide Dimensionen des organisationalen Handelns darstellen. Handeln Sicherheitsbehörden nicht effektiv, handeln sie auch nicht legitim. Handeln sie nicht legitim, kann ihre Aktivität nicht als gesellschaftlich erfolgreich gewertet werden, da die Organisationen dann ihre Verbindung zur Gesellschaft aufgekündigt haben. Gleichzeitig müssen Gesellschaften eine Sensibilität dafür entwickeln, dass sich Organisationen in der Reaktion auf externe technische Bedingungen – selbst wenn sie aus divergierenden kulturellen Kontexten stammen – angleichen (müssen), auch wenn Organisationen aus einem ähnlichen kulturellen Hintergrund dabei weitreichender agieren können als divergente Organisationen, und in letzteren Fällen nur technische Lösungen einer besseren Kompatibilität erreicht werden können. Gerade dieses Ergebnis kann jedoch angesichts der Grundrechtssensibilität sicherheitsorganisatorischer Aktivität kritisch diskutiert werden. Dabei muss thematisiert werden, ob die Tendenz einer steigenden technischen

Anpassung nicht vor allem von internationalen Kommunikationsstrukturen ausgeht und diese möglicherweise gar einen allgemeinen globalen gesellschaftlichen Wandel auslöst.

5.3 Der allgemeine Einfluss technischer Entwicklungen

Vorliegende Arbeit ist der Blickrichtung des Forschungsstandes gefolgt, wonach sowohl Nachrichtendienste als auch Polizeibehörden sich in Zeiten komplexer und internationaler Bedrohungslagen mit einem deutlich ansteigenden Aufklärungsbedarf konfrontiert sehen, den sie alleine aus nationalen Strukturen heraus nicht bewältigen können (Gill/Phythian 2012; Fägersten 2010a; 2010b; Gill 2006). Diese Annahme wurde dadurch erweitert, dass die Befähigung durch die Gesellschaft – in Form eines Auftrages zur Kooperation – die Praxis der Zusammenarbeit zwar auslösen, nicht aber vollständig erklären kann. Denn wenn von Gesellschaften ausgegangen wird, die sich hinsichtlich ihrer, kulturell beeinflussten, Institutionen unterscheiden, dann wird deutlich, dass der Auftrag der Gesellschaft für jede Organisation – da es sich jeweils um eine spezifische Gesellschaft und eine ebenso speziell geartete Organisation handelt – andere Bedingungen hervorbringt. In der internationalen Kooperation kann dies zu Hindernissen führen, die Beachtung erfahren müssen. Deren Berücksichtigung wurde dadurch nachgewiesen, dass Organisationen versuchen, mögliche (retrospektive) gesellschaftliche Bewertungen ihres Handelns zu interpretieren, bevor sie ihre Kooperation vertiefen oder während sie diese durchführen. Diese Feststellung alleine konnte jedoch unterschiedliche Kooperationsarrangements nicht ausreichend erklären, denn eine Ausrichtung eines Handelns kann bei technischen Organisationen nicht das Handeln alleine erklären, sondern nur deren Richtung festlegen. Denn Aktivitäten müssen nicht nur legitime Ziele – im Sinne eines Auftrages ihrer Gesellschaft unter den von ihnen genannten Bedingungen – erfüllen, sondern auch technisch adäquate Mittel wählen. Diese müssen so gestaltet sein, dass sie den technischen Erfordernissen der Aufgabenerfüllung gerecht werden. Somit erhalten auch exogene technische Strukturen Einfluss auf die Ausprägung von Kooperationsarrangements. So hat die technische Entwicklung des Internets, die vorrangig in den USA erfolgte, bis heute Einfluss auf die Rolle der NSA in ihren Kooperationspartnerschaften (Naughton 2016; National Security Agency 2014o). Hervorzuheben ist aber, dass die technischen Erfordernisse des internationalen Kommunikationsumfeldes – dem Internet, der damit verbundenen Software und seiner vernetzten Hardwarekomponenten – eine generelle Herausforderung für Organisationen aller Art darstellen, die in Zukunft noch steigen wird. Gerade staatliche, traditionell an ein Staatsgebiet und eine eigene Rechtsprechung gebundene, Akteure geraten hierbei in

Handlungszwänge. Denn das Internet ist weder territorial begrenzt noch maßgeblich staatlicher Autorität unterworfen, da sich die Infrastruktur vor allem in privater Hand befindet und so viele globale Komponenten auf eine so komplexe Weise zusammenwirken, dass eine nationale Fragmentierung nicht möglich ist (Dörr/Diersch 2018; Diersch/Schmetz 2017; Wolf 2013; Kitchin 1998). Dadurch sind die Daten der Kommunikationsstruktur erstens dort uneingeschränkt abschöpfbar, wo keine privatwirtschaftlichen Interessen anderer Länder beschnitten werden, zweitens Kommunikation Nutzer jeglicher Nationalitäten erreichbar, da ihre Datenübertragung globale Wege nimmt und daher an unterschiedlichen Punkten mitgeschnitten werden kann, und drittens alle Anwendungen und Plattformen, die über das Internet genutzt werden können und in denen Nutzer Informationen veröffentlichen, auch für die Sicherheitsbehörden verwendbar. Nicht alle Kommunikationen erbringen jedoch sofort Informationen über die Personen, mit denen sie verknüpft sind. Denn ein wesentliches Merkmal des Internets ist die Anonymität (Diersch/Schmetz 2017). Daher müssen, viertens, E-Mailadressen und Pseudonyme in Sozialen Netzwerken, aber auch gezielt verborgene persönliche Beziehungen, die etwa über Serverstrukturen wie Tor verschlüsselt werden, mit realen Personen in Verbindung gebracht werden. Auf diese vier Bedingungen müssen sich sowohl Nachrichtendienste als auch kooperierende Polizeien ausrichten und dabei auch traditionelle, physische Beziehungsgeflechte zwischen potentiellen Gefährdern, etwa über Transportrouten geschmuggelter Waren, Menschen oder Waffen, nicht aus den Augen verlieren. Es sind jedoch gerade die neuen Technologien, die in den Gesellschaften auf Unentschiedenheit dahingehend treffen, in welchem Maße sie durch staatliche Sicherheitsbehörden genutzt werden sollen. Dies ist vor allem deshalb der Fall, da nicht in ausreichendem Maße Präzedenzfälle zur Ausrichtung der Organisationen an diesen Technologien und daraus potentiell resultierenden unerwünschten gesellschaftlichen Folgen vorhanden sind (Dörr/Kowalski 2018). Daraus ergibt sich, wie bereits festgestellt wurde, jedoch keine Verzagtheit dieser Organisationen. Vielmehr können sie diese gar nicht entstehen lassen, da sie an die Erwartung ihrer Gesellschaften, keine Nachfragelücke entstehen zu lassen, gebunden sind. Daher erarbeiten sie nachweislich, trotz fehlender Kategorisierung von legitimen Zielen und Mitteln durch die Gesellschaft, effektive Lösungen, da diese nach ihrer Interpretation im Sinne der Gesellschaft benötigt werden. Wo es ihnen ihr kultureller Handlungsraum erlaubt, entwickeln sie diese besonders innovativ und orientieren sich dabei vor allem an den globalen Kommunikationsstrukturen und ihren Funktionen selbst, wobei sie durchaus auch technische Eingrenzungen als Ausdruck ihrer Interpretation genereller gesellschaftlicher Legitimitätserwartungen vornehmen. Die gesellschaftliche Tendenz jedoch,

die Aufklärung neuer Kommunikationstechnologien durch Sicherheitsbehörden nicht grundlegend zu diskutieren und die Auslotung zentraler Mittel dadurch vor allem den Organisationen selbst zu überlassen, muss kritisch diskutiert werden. Denn wenn Organisationen lediglich einen Auftrag erhalten, auf exogene Bedingungen zu reagieren und dabei gegebenenfalls nur marginale technische Einschränkungen in der Nutzung ihrer Mittel vorzunehmen, sie sich die Methoden vorrangig unter Rückbezug auf die aufzuklärenden Kommunikationsstrukturen wählen und dabei zusätzlich interorganisationalen Erwartungen nach der Weitergabe möglichst vieler Informationen, zum Ausgleich für etwaig erhaltene Technologien, folgen, entsteht potentiell eine Art Managementsystem, das einzig dem Faktor der effektiven Problemlösung folgt und Fragen der Grundrechtssensibilität ausblendet, beziehungsweise ihr keine Taten folgen lässt. Diese Vorgänge sind nicht alleine auf Seiten der Organisationen zu kritisieren, denn sie sind lediglich in das Gefüge eingebettet und wirken auf dieses zurück. Jedoch lässt sich vor allem über das Verhalten der Gesellschaft urteilen, die Alltagssicherheit, Verhältnismäßigkeit der Sicherheitsbehörden und die Freiheit der Internetnutzung gleichermaßen fordert, ohne die, diesen Kategorien innewohnenden, Zielkonflikte zu reflektieren und zu einer Abwägung zu bringen. Zwar besteht durchaus ein latentes gesellschaftliches Unbehagen über die transatlantische und europäische Überwachung der Kommunikationsstrukturen. Dieses beißt sich jedoch mit einer Erwartungshaltung des umfassenden Sicherheitsmanagements durch Geheimdienste und Nachrichtendienste. Dadurch entsteht ein Mythos der „perfect manageability“ (Dunn Cavelty/Mauer 2009: 139) aller Bedrohungen, der letztendlich jedoch von den Gesellschaften als solcher entlarvt werden muss, um einen Ausweg aus dem zu finden, was Dunn Cavelty und Mauer an gleicher Stelle als Teufelskreis bezeichnen. Solange der gesellschaftliche Glaube nach absoluter Sicherheit besteht, gleichzeitig aber die Gründe für deren Nicht-Existenz sowie der Protest über zu weitreichende Überwachung den Sicherheitsbehörden selbst angelastet werden – und nicht ihrer eigenen Weigerung zu einer umfassenden lösungsorientierten und Grenzen setzenden Debatte – solange kann einerseits kein ehrlicher Diskurs über die soziale Erwünschtheit von globaler Internetüberwachung (und deren Begrenzung) geführt werden. Andererseits gerät darüber der Austausch dazu zu kurz, wo die Ursachen für Sicherheitsvorfälle tatsächlich liegen und wie ihnen adäquat begegnet werden kann. Denn Gesellschaften überwiegend außer Acht lassen, ist die Tatsache, dass die Motivation für Gefährder vor allem in ihrem Bewusstsein der Exklusion aus der gesellschaftlichen Gemeinschaft und einer damit verbundenen Wahrnehmung der (globalen) Ungerechtigkeit besteht. Diesen Anstoß und seine Dynamisierung kann die Gesellschaft alleine durch die Nutzung und Duldung einer

sicherheitsbehördlichen Produktionskette der Daten und Informationen über diese Individuen und ihre Lebens- und Radikalisierungsverläufe nicht bekämpfen, wenn sie solche Hinweise nur zur Gefahrenverhinderung überwachen will, ihre Ursachen aber nicht hinterfragt und zu beseitigen sucht.

Literatur- und Quellenverzeichnis

1. Snowden-Dokumente

Fundstelle: ‚NSA-Archive' der American Civil Liberties Union, https://www.aclu.org/nsa-documents-search

National Security Agency (2014a): "*Special Source Accesss; Foreign Partner Access*", veröffentlicht: 18.06.2014.

National Security Agency (2014b): "*NSA Overview Briefing*", 13.05.2014.

National Security Agency (2014c): "*Running Strategic Analytics Affecting Europe and Africa*", 18.06.2014.

National Security Agency (2014d): "*The Cryptologic Provider of Intelligence from Global High Capacity Telecommunications Systems*", veröffentlicht am 18.06.2014.

National Security Agency (2014e): "*RAMPART-A Special Source Operation Extra Slides*", veröffentlicht 18.06.2014.

National Security Agency (2014f): "*JSA Restrictions*", veröffentlicht am 18.06.2014.

National Security Agency (2014g): "*NSA Technology directorate analysis of converged data*", veröffentlicht am 12.03.2014.

National Security Agency (2014h): "*Logo of NSA BND Cooperation*", veröffentlicht am 18.06.2014.

National Security Agency (2014i): "*FAA702 Operations and PRISM Collection Details*", 13.05.2014.

National Security Agency (2014j): "*NSA Background Slight re SIGINT Assessment Report on Radicalization*", veröffentlicht am 22.05.2014.

National Security Agency (2014k): "*Approved SIGINT Partners and FAD FY12 CCP Funding of Partners*", veröffentlicht am 13.05.2014.

National Security Agency (2014l): "*OAKSTAR: International Cooperation*", veröffentlicht am 13.05.2014.

National Security Agency (2014m): "*Report on the NSA-BND Cooperation known as Joint SIGINT Activity (JSA)*", veröffentlicht am 18.06.2014.

National Security Agency (2014n): "*BND NSA Talking Point Topics Proposal*", veröffentlicht am 18.06.2014.

National Security Agency (2014o): "*NSA Powerpoint Re US Gains in Relation to the Developing Internet*", veröffentlicht am 26.05.2014.

National Security Agency (2013a): "*Prism Overview Powerpoint Slides*", April 2013;

National Security Agency (2013b): "*Information Paper NSA Relationship with Germany*", 17.01.2013.

National Security Agency (2013c): "PRISM Powerpoint Slides re Data Acquisition", 13.04.2013.

National Security Agency (2013d): "*SSO Expands PRISM Skype Targeting Capability*", 03.04.2013.

National Security Agency (2013e): "*New Skype Stored Capability for PRISM*", 03.04.2013.

National Security Agency (2013f): "*PRISM Microsoft Skydrive Collection*", 08.03.2013.

National Security Agency (2013g): "*Lobban NSA Visit Precis*", 30.04.2013.

National Security Agency (2013h): "*NSA Intelligence Relationship with Canada's Communications Security Establishment Canada (CSEC)*", 03.04.2013.

National Security Agency (2013i): "*NSA's Counterterrorism Relationship with the BND and the BfV*", 08.05.2013.

National Security Agency (2013j): "*Menwith Hill Station Leverages XKEYSCORE for QUANTUM Against Yahoo and Hotmail*", 12.03.2013.

National Security Agency (2012a): "*PRISM Operations Highlight*", verfasst nach dem 24.05.2012.

National Security Agency (2012b): "*PRISM Based Reporting June 2011-May 2012*", 13.06.2012.

National Security Agency (2012c): "*Classification Guide for SIGINT Material Dating from 16 August 1954 – 31 December 1967*", 25.04.2012.

National Security Agency (2012d): "*GCHQ report on Capability of TEMPORA project*", Mai 2012.

National Security Agency (2012e): "*Report on NSA's Access to Tempora*", 19.09.2012.

National Security Agency (2012f): "*CSEC Targets Brazilian Ministry of Mines and Energy*", 01.01.2012.

National Security Agency (2012g): "*Report on Analytic Modernization Outreach Campaign's Success*", 13.04.2012.

National Security Agency (2012h): "*Tor stinks*", 01.06.2012.

National Security Agency (2012i): "*PRISM Operations Highlight: Olympic Support – GCHQ Using PRISM Access*", 24.05.2012.

National Security Agency (2011a): "*NSA Communications Hub in Europe is modernized*", 20.10.2011.

National Security Agency (2011b): "*QFIRE*", 03.06.2011.

National Security Agency (2011c): "*SCS Pacific SIGDEV Conference 2011*", 1. April 2011.

National Security Agency (2010a): "*First-Ever Formal SIGINT Development (SIGDEV) Training is Provided to SIGINT Seniors Europe (SSEUR) Partners*", 25.10.2010.

National Security Agency (2010b): "*CIA Colleagues Enthusiastically Welcome NSA Training*", 21.09.2010.

National Security Agency (2010c): "*Social Convergence*", 01.05.2010.

National Security Agency (2009a): "*Third Party Relationships*", 15.09.2009.

National Security Agency (2009b): "*Draft NSA IG Report*", 24.03.2009.

National Security Agency (2008a): "*NSA Video Games Paper*", 01.01.2008.

National Security Agency (2008b): "*XKEYSCORE Powerpoint*", 25.02.2008.

National Security Agency (2007a): "*SID Analysts Can Now Unminimize Incidentally Collected UK Contact Identifiers*", 16.05.2007.

National Security Agency (2007b): "*US, German SIGINTERs Increase Cooperation on African Targets*", 13.12.2007.

National Security Agency (2007c): "*Sharing SIGINT Metadata on ICREACH*", 27.09.2007.

National Security Agency (2007d): "*Sharing Communications Metadata Across the U.S. Intelligence Community*", 15.05.2007.

National Security Agency (2007e): "*Intelligence Community (IC) Reach Team*", 25.08.2007.

National Security Agency (2007f): *SID can now unminimize UK phone data*", 01.01.2007.

National Security Agency (2006a): "*German, NSA SIGINTers Share DNI Processing Knowledge*", 22.05.2006.

National Security Agency (2006b): "*European Security Center to become the ESOC*", 11.09.2006.

National Security Agency (2006c): "*Encouraging Innovation*", 27.04.20016.

National Security Agency (2005a): "*Forward Production at NCEUR*", 14.01.2005.

National Security Agency (2005b): "*One-Year-Anniversary for SUSLAG*", 10.06.2005.

National Security Agency (2004): "*Generally Speaking: Driving History*", 03.05.2004.

National Security Agency (2003a): "*SIGINT Directors to Collaborate Virtually*", 10.09.2003.

National Security Agency (2003b): "*Second Party SIGINT Directors Hold Virtual Meeting*", 19.12.2003

National Security Agency (2003c): "*FAIRVIEW and STORMBREW – Live on the Net*", 19.11.2003.

National Security Agency (2003d): "*JESI: Don't Lose That Number*", 25.08.2003.

National Security Agency (2003e): "*DNE, DNI, and CNE (repost)*", 30.12.2003.

National Security Agency (2003f): "*MG Quirk and Mr. Black Speak to Analytic Boot Camp Graduates*", 27.08.2003.

National Security Agency (2003g): "*TICKETWINDOW Second party Collection Sharing*", 07.11.2003.

National Security Agency (2003h): "*Second Party Bilaterals Held in Hawaii*", 02.10.2003.

National Security Agency (2003i): "*SIDs Antipodal Colleagues*", 08.10.2003.

National Security Agency (2003j): "*Chef's Choice: Third Parties*", 30.09.2003.

National Security Agency (2003k): "*Message from MG Quirk on Foreign Affairs*", 31.07.2003.

National Security Agency (2003l): "*Digital Network Exploitation (DNE), Digital Network Intelligence (DNI) and Computer Network Exploitation (CNE)*", 16.07.2003.

National Security Agency (2003m): "*CATAPULT – A bilateral data port*", 08.05.2003.

National Security Agency (2003n): "*The Partnership Dissemination Cell. Information Sharing with Third Party SIGINT Partners (Repost)*", 01.12.2003.

2. Literatur

Aden, Hartmut (1998): „*Polizeipolitik in Europa. Eine interdisziplinäre Studie über die Polizeiarbeit in Europa am Beispiel Deutschlands, Frankreichs und der Niederlande*", Opladen: Westdeutscher Verlag.

Agrell, Wilhelm/Treverton, Gregory F. (2015a): "Introduction: The Odd Twins of Uncertainty", in: Dies. (Hg.): "*National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*", Oxford: Oxford University Press, S. 1-12.

Agrell, Wilhelm/Treverton, Gregory F. (2015b): "Framing the Divide", in: Dies. (Hg.): "*National Intelligence and Science: Beyond the Great Divide in Analysis and Policy*", Oxford: Oxford University Press, S. 12-40.

Aldrich, Richard J. (2009): „Global Intelligence Co-Operation versus Accountability: New Facets to an Old Problem", *Intelligence and National Security, 24*(1), S. 26-56.

Aldrich, Richard J. (2004): „Transatlantic Intelligence and Security Cooperation", *International Affairs, 80*(3), S. 733-755.

Aldrich, Richard J. (2002): "Dangerous Liaisons. Post-September 11 Intelligence Alliances", in: *Harvard International Review, 24*(3), S. 50-54.

Alvesson, Mats/Karreman, Dan (2000): „Varieties of discourse: On the study of organizations through discourse analysis", *Human Relations, 35*(9), S. 1125-1149.

Anckar, Carsten (2008): „On the Applicability of the Most Similar System Design and the Most Different Systems Design in Comparative Research", *International Journal of Social Research Methodology, 11*(5), S. 389-401.

Argomaniz, Javier (2011): "T*he EU and Counter-Terrorism. Politics, polity and policies after 9/11*", Abingdon/New York: Routledge.

Baitsch, Christof/Nagel, Erik (2014): "Organisationskultur – Das verborgene Skript der Organisation", in: Wimmer, Rudolf/Meissner, Jens. O./Wolf, Patricia (Hg.): *Praktische Organisationswissenschaft. Lehrbuch für Studium und Beruf*, zweite Aufl., Heidelberg: Carl-Auer Verlag, S. 267-288.

Battilana, Julie (2006): „Agency and Institutions: The Enabling Role of Individuals' Social Position", *Organization 13*(5), S. 653-676.

Becker, Sven/Gude, Hubert/Horchert, Judith u.a. (2014): „Hier sitzt die NSA in Deutschland", http://www.spiegel.de/netzwelt/netzpolitik/nsa-dokumente-von-snowden-enthuellen-standorte-in-deutschland-a-975611.html , *Der Spiegel*, 18.06.2014 [Zugriff: 05.04.2018].

Becker-Ritterspach, Florian A. A./Becker-Ritterspach, Jutta C. E. (2006): "Isomorphie und Entkoppelung im Neo-Institutionalismus", in: Senge, Konstanze/Hellmann, Kai-Uwe (Hg.): *Einführung in den Neo-Institutionalismus. Mit einem Beitrag von W. Richard Scott*, Wiesbaden: Springer VS, S. 102-117.

Behr, Rafael/Ohlemacher, Thomas (2009): "Einleitung", in: Dies. (Hg.): *Offene Grenzen – Polizieren in der Sicherheitsarchitektur einer post-territorialen Welt*, Frankfurt: Verlag für Polizeiwissenschaft, S. 7-12.

Bell, Duncan (2012): „The project for a new Anglo century: race, space, and global order“, in Katzenstein, Peter J. (Hg.): *Anglo-America and its Discontents: Civilizational Identities beyond West and East*, Abingdon/New York: Routledge, S. 33-55.

Berger, Peter L./Luckmann, Thomas (1977): "*Die gesellschaftliche Konstruktion der Wirklichkeit. Eine Theorie der Wissenssoziologie*", Frankfurt: Fischer.

Bigo, Didier (2006): "Globalized (in)Security: the Field and the Ban-opticon", in: Bonelli, Laurent/Guittet, Emmanuel-Pierre/Olsson, Christian/Tsoukala, Anastassia (Hg.): *"Illiberal Practices of Liberal Regimes: The (In)Security Games"*, Paris: Centre d'Etudes sur les conflits, S. 5 – 49.

Boekle, Henning/Rittberger, Volker/Wagner, Wolfgang (1999): "Normen und Außenpolitik. Konstruktivistische Außenpolitiktheorie und deutsche Außenpolitik nach der Vereinigung, *Zeitschrift für Politikwissenschaft, 11*(1), S. 71-103.

Boer, Monica, den/Hillebrand, Claudia/Nölke, Andreas (2008): "Legitimacy under Pressure: The European Web of Counter-Terrorism Networks", *JCMS, (46)*1, S. 101-124.

Boer, Monica den/Bruggemann, Willy (2007): "Shifting Gear: Europol in the Contemporary Policing Era", *Politique Européenne, 23*(3), S. 77-91.

Bossong, Raphael (2017): "*Die EU-Zusammenarbeit beim Kampf gegen den internationalen Terrorismus. Fortschritte seit 2015 und zukünftige Prioritäten*", Berlin: Stiftung Wissenschaft und Politik.

Brady, Hugo (2008): "Europol and the European Criminal Intelligence Model: A Non-state Response to Organized Crime", *Policing: A Journal of Policy and Practice, 2*(1), S. 103-109.

Brimmer, Esther (2006): „From Territorial Security to Societal Security: Implications for the Transatlantic Strategic Outlook", in: Dies. (Hg.): "*Transforming Homeland Security. U.S. and European Approaches"*, Washington: Center for Transatlantic Relations, S. 23-42.

Brosziewski, Achim (2015): "Unsicherheit als ein Grundkonzept der Organisationssoziologie", in: Apelt, Maja/Senge, Konstanze (Hg.): „*Organisation und Unsicherheit*", Wiesbaden: Springer VS, S. 17-34.

Brühl, Jannis (2018): „Neue Macht für die obskurste Behörde der EU“, *Sueddeutsche.de*, https://www.sueddeutsche.de/digital/fluechtlinge-eurodac-eu-datenbanken-migration-ueberwachung-kriminalitaet-1.4219070 [Zugriff: 30.01.2019].

Brummer, Klaus/Oppermann, Kai (2014): „*Außenpolitikanalyse*“, München: Oldenbourg.

Bundeskriminalamt (2016): „*Waffenkriminalität. Bundeslagebild 2016*“, Wiesbaden.

Bundesministerium des Innern (2016): „*Pressemitteilung zur ‚Aachener Erklärung‘*“, 31.10.2016, https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2016/10/drei-laendergipfel-wohnungseinbruchdiebstahl.html; Zugriff: 16.02.2018].

Bundestag (2017a): “Beschlussempfehlung und Bericht des 1. Untersuchungsausschusses gemäß Artikel 44 des Grundgesetzes“, *Drucksache 18/12850*, 23.06.2017.

Bundestag (2017b): „Standardisierung europäischer Informationssysteme“, *Drucksache 18/11661*, 23.03.2017.

Bundestag (2016a): „Austausch geheim eingestufter Informationen unter europäischen Geheimdiensten, Polizeien und Militärs“, *Drucksache 18/7246*, 13.01.2016.

Bundestag (2016b): „Unterschiedliche EU-Datensammlungen über sogenannte ausländische Kämpfer“, *Drucksache 18/8324*, 03.05.2016.

Bundestag (2016c): „Datenabgleich des BKA mit dem US-Terrorist Screening Center – Memorandum of Understanding“, *Drucksache 18/8866*, 08.07.2016.

Bundestag (2016d): „Mindestvorschriften und Mindestnormen der EU-Mitgliedsstaaten für kriminaltechnische Tätigkeiten „vom Tatort bis zum Gerichtssaal“, *Drucksache 18/7707*, 25.02.2016.

Bundestag (2014): „Neustrukturierte Arbeitsdateien zu Analysezwecken (AWF) bei der EU-Polizeiagentur Europol“, *Drucksache 18/571*, 19.02.2014.

Bundestag (2008): „Interoperabilität von Datenbanksystemen im Bereich der Inneren Sicherheit“, *Drucksache 16/9987*, 15.07.2008.

Bundestag (2007): „*Prümer Vertrag und die europäische Integration*“, Drucksache 16/3994, 02.01.2007.

Burczyk, Dirk (2017): "Wunderwaffe ‚Deradikalisierung': Prävention im Dschungel von Polizei und Geheimdiensten", *CILIP 113*, September 2017.

Buuren, Jelle van (2014): „Analyzing international Intelligence Cooperation. Institutions or Intelligence Assemblages?", in: Duyvesteyn, Isabelle/de Jong, Ben/von Reijn, Joop (Hg.): "*The Future of Intelligence. Challenges in the 21st century"*, Abingdon/New York: Routledge, S. 80-93.

Carstensen, Martin B./Schmidt, Vivien A. (2016): „Power through over and in ideas: conceptualizing ideational power in discursive institutionalism", in: *Journal of European Public* Policy, 23(3), S. 318-337.

Casey, John (2010): "Implementing Community Policing in different Countries and Cultures", *Pakistan Journal of Criminology*, *2*(4), S. 55-70.

Collier, David/LaPorte, Jody/Seawright, Jason (2008): "Typologies: Forming Concepts and Creating Categorical Variables", in: Box-Steffensmeier, Janet M./Brady, Henry E./Collier, David (Hg.): "*The Oxford Handbook of Political Methodology*", Oxford/New York: Oxford University Press, S. 152-173.

Cooper, Jeffrey R. (2005): "*Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*", Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency, [Zugriff: 13.03.2018].

Christe-Zeyse, Jochen (2007): „Von Profis, Bürokraten und Managern – Überlegungen zu einer Theorie innerorganisationalen Widerstandsverhaltens in der Polizei", in: Ohlemacher/Thomas, Mensching, Anja/Werner, Jochen-Thomas (Hg.): „*Empirische Polizeiforschung VIII: Polizei im Wandel? Organisationskultur(en) und –reform"*, Frankfurt: Verlag für Polizeiwissenschaft, S. 175-202.

Clark, Robert M. (2013): „Intelligence Analysis. A Target-Centric Approach", 4. Aufl., London: Sage.

Clough, Chris (2004): "Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation", *International Journal of Intelligence and Counterintelligence, 17*(4), S. 601-613.

Daase, Christopher (2012): „Sicherheitskultur als interdisziplinäres Forschungsprogramm", in: Daase, Christopher/Offermann, Philipp/Rauer, Valentin (Hg.): „*Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr*", Frankfurt/Main: Campus, S. 23-44.

Daase, Christopher (2010): „Wandel der Sicherheitskultur“, *Aus Politik und Zeitgeschichte (APuZ), 50*(2010), S. 9-16.

Daase, Christopher (2009): „Der erweiterte Sicherheitsbegriff“, in: Ferdowsi, Mir A. (Hg.): „*Internationale Politik als Überlebensstrategie*“, München: Bayerische Landeszentrale für politische Bildungsarbeit, S. 137-153.

Daun, Anna (2011a): „*Auge um Auge? Intelligence-Kooperation in den deutsch-US-amerikanischen Beziehungen*“, Wiesbaden: Springer VS.

Daun, Anna (2011b): „Nachrichtendienste in der deutschen Außenpolitik“, in: Jäger, Thomas/Höse, Alexander/Oppermann, Kai (Hg.): „*Deutsche Außenpolitik*“, 2. Aufl., Wiesbaden: Springer VS, S. 171-197.

Daun, Anna (2005a): „Die deutschen Nachrichtendienste“, in: Jäger, Thomas/Daun, Anna (Hg.): „*Geheimdienste in Europa: Transformation, Kooperation und Kontrolle“*, Wiesbaden: Springer VS, S. 56-77.

Daun, Anna (2005b): „Intelligence-Strukturen für die multilaterale Kooperation europäischer Staaten“, *Integration, 28*(2), S. 136-149.

Davis, Jack (2002): „Sherman Kent and the Profession of Intelligence Analysis“, *Central Intelligence Agency, Sherman Kent Center*, http://www.dtic.mil/dtic/tr/fulltext/u2/a526587.pdf [04.06.2018].

Davies, Philip (2002): „Ideas of Intelligence. Divergent National Concepts and Institutions”, *Harvard International Review, 3(24*), S. 62-66.

Deflem, Mathieu (2007a): „Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective“, *Justice Quarterly*, *23*(3), S. 336-359.

Deflem, Mathieu (2007b): „International Police Cooperation Against Terrorism: Interpol and Europol in Comparison“, in: Durmaz, Huseyin/Sevinc, Bilal/Yayla, Amet Sait/Ekici, Siddik (Hg.): “*Understanding and Responding to Terrorism”*, NATO Security Through Science Series, *19*, S. 17-25.

Deflem, Matthieu (2006): “Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective”, *Justice Quarterly 3*(23), S. 336-359.

Deutsche Welle (2017): "*BKA und Europol verlangen europaweite Vernetzung*", http://www.dw.com/de/bka-und-europol-verlangen-europaweite-vernetzung/a-41213676 [Zugriff 19.02.2018].

Diehl, Jörg/Kartheuser, Boris (2018): „Predictive Policing: Ich weiß, was du heute tun wirst", *Spiegel Online*, http://www.spiegel.de/panorama/justiz/kriminalitaet-in-deutschland-polizei-setzt-auf-computer-vorhersagen-a-1188350.html, 27.01.2018 [Zugriff: 07.03.2018].

Diehl, Jörg/Meiritz, Annett (2016): „Reform: BND darf künftig manchmal immer fast alles vielleicht", *Spiegel Online*, http://www.spiegel.de/politik/deutschland/bnd-reform-des-deutschen-geheimdienstes-im-eiltempo-a-1101891.html, 08.07.2016 [Zugriff: 04.03.2018].

Diersch, Verena/Schmetz, Martin (2017): „Vom Cyberfrieden", in: Jacob, Daniel/Thiel, Thorsten (Hg.): „*Politische Theorie und Digitalisierung*", Baden-Baden: Nomos, S. 297-312.

Diersch, Verena (2017): "Die Dienste", in: Thomas Jäger (Hg.): „*Die Außenpolitik der USA. Eine Einführung*", Wiesbaden: Springer VS, S. 65-84.

DiFabio, Udo (2008): "Sicherheit in Freiheit", *NJW 2008*, S. 421-425.

DiMaggio, Paul J./Hargittai, Eszter/Neumann, W. Russel/Robinson, John P. (2001): „Social Implications of the Internet", *Annual Review of Sociology, 27*, S. 307-336.

DiMaggio, Paul J. (1988): „Interest and Agency in Institutional Theory", in: Zucker, Lynn G. (Hg.): "*Instiutional Patterns and Organizations. Culture and Environment*", Cambridge: Ballinger, S. 3-22.

DiMaggio, Paul J./Powell, Walter W. (1983): "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields", *American Sociological Review, 48*(2), S. 147-160.

DiMaggio, Paul J./Powell, Walter W. (1991): "Introduction", in: Dies. (Hg): "*The New Institutionalism in Organizational Analysis*", Chicago/London: The University of Chicago Press, S. 1-38.

DiMaggio, Paul (1988): "Interest and Agency", in: Zucker, Lynne G. (Hg): "*Institutional Patterns and Organizations. Culture and Environment*", Cambridge: Ballinger, S. 3-21.

Dimitriu, George/Duyvesteyn, Isabelle (2014): „Conclusions: it may be 10 September 2001 today", in: Duyvesteyn, Isabelle/de Jong, Ben/von Reijn, Joop (Hg.): "*The Future of Intelligence. Challenges in the 21st century"*, Abingdon/New York: Routledge, S. 149-161.

Dörr, Julian/Diersch, Verena (2018): „Eine neue industrielle Revolution? Die Veränderung des Eigentums angesichts von Internet und Digitalisierung", in: Kirchdörfer, Rainer/Hennerkes, Brun-Hagen/Heidbreder, Stefan/Goldschmit, Nils (Hg.): „*Eigentum. Warum wir es brauchen, was es bewirkt, wo es gefährdet ist*", Freiburg: Herder, S. 265-276.

Dörr, Julian/Kowalski, Olaf (2018): „Vom Tal auf die Insel? Vom Kalifornischen Liberalismus zur Sozialutopie Seasteading", *Aus Politik und Zeitgeschichte (APuZ), 68* (32-33), S. 16-21.

Dörr, Julian/Diersch, Verena (2017): "Zur Rechtfertigung von Whistleblowing: Eine ordnungstheoretische und legitimitätstheoretische Perspektive der Whistleblower-Fälle Carl von Ossietzsky und Edward Snowden", *Zeitschrift für Politik, 64*(4), S. 468-492.

Drogin, Buy (2007): „*Curveball. Spies, Lies, And The Man Behind Them: The Real Reason America Went To War In Iraq*", New York: Ebury.

Dreher, Jochen (2016): "The Social Construction of Power: Reflections beyond Berger/Luckmann and Bordieu", *Cultural Sociology, 10*(01), S. 53-68.

Dunn Cavelty, Myriam/Mauer, Victor (2009): "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence", *Security Dialogue, 40*(2), S. 123-144.

Ebers, Mark/Gotsch, Wilfried (2006): „Institutionenökonomische Theorien der Organisation", in: Kieser, Alfred/Ebers, Mark (Hg.): „*Organisationstheorien"*, 6. Aufl., Stuttgart: Kohlhammer, S. 247-308.

Edeling, Thomas (1999): „Einführung: Der Neue Institutionalismus in Ökonomie und Soziologie", in: Edeling/Thomas/Jann,Thomas/Wagner, Dieter (Hg.): „*Institutionenökonomie und Neuer Institutionalismus. Überlegungen zur Organisationstheorie*", S. 7-15.

Elman, Colin (2005): „Explanatory Typologies in Qualitative Studies of International Politics", *International Organization, 59* (Spring 2005), S. 293-326.

Ericson, Richard v./Shearing, Clifford D. (1986): "The Scientification of Police Work", in: Böhme, Gernot/Stehr, Nico (Hg.): "*The Knowledge Society. The Growing Impact of Scientific Knowledge on Social Relations"*, Dordrecht et al.: D. Reidel.

Europäische Kommission (2017): "*Security Union: Commission Reports on the Implementation of the EU-US TFTP and PNR Agreements*", Pressemitteilung, 19.01.2017.

Europäische Kommission (2012): „Stärkung der Zusammenarbeit der Strafverfolgungsbehörden in der EU: Das Europäische Modell für den Informationsaustausch", *Mitteilung der Kommission an das Europäische Parlament und den Rat*, 7.12.2012.

Europäisches Parlament (2017): „*Fact Sheets on the European Union – Police Cooperation*", http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_4.2.7.html [26.03.2018]

Europol (2018a): "*EU Policy Cycle – EMPACT*".

Europol (2018b): „*Europol Analysis Projects*".

Europol (2017a): "*European Union Serious and Organised Crime Threat Assessment. Crime in the age of Technology*".

Europol (2017b): "*Europol Information System (EIS). A system for information on serious international crime*", 01.09.2017.

Europol (2017c): "*Europol Programming Document 2017 – 2019*", 17.01.2017.

Europol (2016a): "*Europol Review 2016-2017*".

Europol (2016b): "*Europol Strategy 2016-2020*".

Europol (2016c): "*EU Internet Referral Unit. Year One Report – Highlights*".

Europol (2015): "*Consolidated Annual Activity Report 2015*", 12.05.2016.

Europol (2014): "*EU Policy Cycle Infographic*".

Europol (2013): "*EIS Leaflet*".

Europol (2012): "*New AWF Concept Guide for MS and Third Parties*", 31.05.2012.

Europol (2011a): "*Terrorist Finance Tracking Program (TFTP). The EU-US TFTP Agreement*".

Europol (2011b): „*Europol Work Programme 2012*", 09.08.2011.

Europol (2011c): "*Europol Activities in relation to the TFTP Agreement – Information Note to the European Parliament*", 08.04.2011.

Europol (2011d): "*Europol-Jahresbericht 2011. Allgemeiner Bericht über die Tätigkeiten von Europol*", Luxemburg: Amt für Veröffentlichungen.

Europol (2009a): „*Europol Work Programme 2010*", 7.09.2009.

Evera, Stephen, van (1997): "*Guide to Methods for Students of Political Science*", Ithaca: Cornell University Press.

Fägersten, Björn (2010a): „*Sharing Secrets: Explaining International Intelligence Cooperation*", Lund: Lund University.

Fägersten, Björn (2010b): "Bureaucratic Resistance to International Intelligence Cooperation – The Case of Europol, *Intelligence and National Security, 25*(4), S. 500-520.

Farrell, Theo (1998): "Culture and Military Power", *Review of International Studies, 24*, S. 407-416.

Feldman, Martha S./March, James G. (1981): "Information in Organizations as Signal and Symbol", *Administrative Science Quarterly, 26* (2), S. 171-186.

Fingar, Thomas (2011): "*Reducing Uncertainty. Intelligence Analysis and National Security*", Stanford: Stanford University Press.

Finnemore, Martha/Sikkink, Kathryn (1998): "International Norm Dynamics and Political Change", *International Organization, 52*(4), S. 887-917.

Finnemore, Martha (1996): "Norms, Culture, and World Politics: Insights from Sociology's Institutionalism", *International Organization 50*(2), S. 325-347.

Finnemore, Martha (1995): „*National Interests in International Society*", Ithaca: Cornell University Press.

France, Olivier, de/Witney, Nick (2013): "*Europe's Strategic Cacophony*", Paris: European Council on Foreign Affairs.

Frevel, Bernhard/Kuschewski, Philipp (2007): „Polizei zwischen Kernaufgaben und Kooperationsnotwendigkeit. Ein Werkstattbericht zum Forschungsprojekt ‚Kommunale Sicherheit in Mittelstädten'", in: Ohlemacher/Thomas, Mensching, Anja/Werner, Jochen-

Thomas (Hg.): „*Empirische Polizeiforschung VIII: Polizei im Wandel? Organisationskultur(en) und –reform*“, Frankfurt: Verlag für Polizeiwissenschaft, S. 153-174.

Friedland, Roger/Alford, Robert R. (1991): „Bringing Society Back In“, in: Powell, Walter W./DiMaggio, Paul J. (Hg): „*The New Institutionalism in Organizational Analysis”*, Chicago: University of Chicago Press, S. 232-266.

Friederichs, Hauke (2016): „Der Stärkste steigt aus“, *Zeit Online*, 01.08.2016, https://www.zeit.de/politik/2016-08/grossbritannien-sicherheitspolitik-brexit-eu [05.06.2018].

Fry, Michael G./Hochstein, Miley (2008): „Epistemic Communities: Intelligence Studies and International Relations“, *Intelligence and National Security*, 8(3), S. 14-28.

Gauck, Joachim (2014): „Deutschlands Rolle in der Welt. Anmerkungen zu Verantwortung, Normen und Bündnissen. Rede anlässlich der Eröffnung der 50. Münchner Sicherheitskonferenz am 31. Januar 2014, *Zeitschrift für Außen- und Sicherheitspolitik, 2014*(2), S. 115-122.

George, Alexander L./Bennett, Andrew (2005): “*Case Studies and Theory Development in the Social Sciences*”, Cambridge: MIT Press.

Giddens, Anthony (1984): “*The Constitution of Society. Outline of the Theory of Structuration*”, Berkeley, Los Angeles: University of California Press.

Gill, Peter (2006): “Not Just Joining the Dots but Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2011”, *Policing & Society*, *16*(1), S. 27-49.

Gill, Peter/Phythian Mark (2012): “*Intelligence in an Insecure World*”, Cambridge: Polity Press.

Göhler, Gerhard (1990): “Einleitung”, in: Göhler, Gerhard/Lenk, Kurt/Schmalz-Bruns, Rainer (Hg.): „Die Rationalität politischer Institutionen: Interdisziplinäre Perspektiven“, Baden-Baden: Nomos, S. 9-14.

Government Communications Headquarters (2014): “*EFFECTS Definition*”, veröffentlicht 22.05.2014.

Gray, Sidney J. (1988): „Towards a Theory of Cultural Influence on the Development of Accounting Systems Internationally“, *ABACUS, 24*(1), S. 1-15.

Greenwald, Glenn (2014): „*Die globale Überwachung: Der Fall Snowden, die US-amerikanischen Geheimdienste und ihre Folgen*“, München: Droemer Knaur.

Gukenbiel, Hermann (1995): “Institution und Organisation, in: Korte, Hermann/Schäfers, Bernhard (Hg.): „*Einführung in die Hauptbegriffe der Soziologie*“, Opladen: Leske und Budrich, S. 95-110.

Hacke, Christian (2011): „Vernetzte Sicherheit: Intention und Wirklichkeit“, in Meier-Walser, Reinhard/Wolf, Alexander (Hg.): „Neue Dimensionen Internationaler Sicherheitspolitik“, *Berichte & Studien der Hanns Seidel Stiftung 93,*München: HSS S. 45-58.

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

Harnisch, Sebastian (2008): “Demokratie und Geheimdienste: Dilemmata ungezügelter Exekutivgewalt”, Morisse-Schilbach, Melanie/Peine, Anke (Hg.): „*Demokratische Außenpolitik und Geheimdienste. Aspekte eines Widerspruchs in Deutschland, Großbritannien, Israel, USA und Frankreich im Vergleich*“, Berlin: Dr. Köster, S. 95-130.

Hasenclever, Andreas/Mayer, Peter/Rittberger, Volker (1997): “*Theories of international regimes*”, Cambridge: Cambridge University Press.

Hastedt, Glenn P./Skelley, Douglas B. (2009): “Intelligence in a turbulent World: Insights from Organizaton Theory”, in: Gill, Peter/Marrin, Stephen/Phythian, Mark (Hg.): “*Intelligence Theory. Key Questions and Debates“*, Abingdon/New York: Routledge, S. 112-130.

Hegemann, Hendrik (2018): „Toward ‚normal‘ Politics? Security, Parliaments and the Politicisation of Intelligence Oversight in the German Bundestag”, *The British Journal of Politics and International Relations, 20*(1), S. 175-190.

Hegemann, Hendrik/Kahl, Martin (2012): “Politische Entscheidungen und das Risiko Terrorismus”, in: Daase, Christopher/Offermann, Philipp/Rauer, Valentin (Hg.): „*Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr*“, Frankfurt/Main: Campus S. 159-182.

Hellmann, Kai-Uwe (2015): „Wenn der Nebel des Krieges aufzieht. Anmerkungen zur Transformation der Bundeswehr“, in: Apelt, Maja/Senge, Konstanze (Hg.): „*Organisation und Unsicherheit*“, Wiesbaden: Springer VS, S. 195- 212.

Herman, Michael (2003): "*Intelligence Power in Peace and War"*, 2. Aufl., Cambridge: Cambridge University Press.

Herman, Michael (2001): "*Intelligence Services in the Information Age. Theory and Practice*", London: Frank Cass.

Hofstede, Geert (2001): "Cultural Consequences", Thousand Oaks: Sage Publications.

Hofstede, Geert (1991): "Cultures and Organizations: Software of the Mind", *Human Resource Development Quarterly, 4*(3), S. 319-325.

House of Lords European Union Committee (2008): "*29th Report of Session 2007-08 – Europol: Coordinating the Fight against Serious and Organized Crime. Report with Evidence*", 12.11.2008, https://publications.parliament.uk/pa/ld200708/ldselect/ldeucom/183/183.pdf [13.06.2018].

Huey, Laura J. (2002): "Policing the Abstract: Some Observations on Policing Cyberspace", *Canadian Journal of Criminology*, S. 243-254.

Hulnick, Arthur S. (2014): "The Future of the Intelligence Process. The End of the Intelligence Cycle?", in: Duyvesteyn, Isabelle/de Jong, Ben/von Reijn, Joop (Hg.): "*The Future of Intelligence. Challenges in the 21st century*", Abingdon/New York: Routledge, S. 47-57.

Hulnick, Arthur S. (2011): "What's wrong with the Intelligence Cycle", in: in: Loch K. Johnson (Hg.): "*Intelligence. Critical Concepts in Military, Strategic & Security Studies, Volume I: The Collection and Analysis of National Security Intelligence"*, S. 235-255.

Inkster, Nigel (2016): "Brexit, Intelligence and Terrorism", *Survival, 58*(3), S. 23-30.

Jobs, Eva (2014): „Ursprung und Gehalt von Mythen über Geheimdienste", *Aus Politik und Zeitgeschichte 64*(18-19/2014), S. 42-26.

Jäger, Thomas (2015): „Die Verzahnung von Sicherheitsgefahren", in: Ders. (Hg.): „*Handbuch Sicherheitsgefahren*", Wiesbaden: Springer VS, S. 1-9.

Jäger, Thomas (2012): "Die Bedeutung der transatlantischen Beziehungen für die deutsche Außenpolitik", in: Meier-Walser, Reinhard/Wolf, Alexander (Hg.): „Die Außenpolitik der Bundesrepublik Deutschland. Anspruch, Realität, Perspektiven", *Berichten & Studien der Hanns Seidel Stiftung 95*, S. 149-160.

Jäger, Thomas (2002): „Die Rückkehr des Sicherheitsstaates“, *Blätter für deutsche und internationale Politik“, 9*(2002), S. 1037-1040.

Jäger, Thomas/Daun, Anna (2005): “Die Koordination der Nachrichtendienste im Ländervergleich: USA, Großbritannien, Frankreich, Deutschland, Schweden, Australien und Kanada”, in: Borchert, Heiko (Hg.): *„Verstehen, dass sich die Welt verändert hat: Neue Risiken, neue Anforderungen und die Transformation der Nachrichtendienste“*, Baden-Baden: Nomos, S. 57-75.

Jakobsen, Peter Viggo/Ringsmose, Jens (2015): „Size and Reputation – Why the USA has valued ist ‚special relationships‘ with Denmark and the UK differently since 9/11“, *Journal of Transatlantic Studies, 13*(2), S. 135-153.

Jervis, Robert (1976): “*Perception and Misperception in International Politics*”, Princeton: Princeton University Press.

Johnson, Loch K. (2015): “A Conversation with James R. Clapper, Jr., The Director Of National Intelligence in the United States”, *Intelligence and National Security 30*(1), S. 1-25.

Johnson, Loch K./Aldrich, Richard J./Moran, Christopher/Marrett, David M./Hasted, Glenn/Jervis, Robert (2014a): “An INS Special Forum: Implications of the Snowden Leaks”, *Intelligence and National Security 29*(6), S. 793-810.

Johnson, Loch K. (2014b): “The development of intelligence studies”, in: Dover, Robert/Goodmann, Michael S./Hillebrand, Claudia (Hg.): “*Routledge Companion to Intelligence Studies*”, Abingdon/New York: Routledge, S. 3-22.

Johnson, Loch K. (2003): “Bricks and Mortar for A Theory of Intelligence”, *Comparative Strategy, 22*(1), S. 1-28.

Katzenstein, Peter J. (2008): „Coping with Terrorism: Norms and internal Security in Germany and Japan“, in: Ders. (Hg.): “*Rethinking Japanese Security. Internal and External Dimensions*”, London: Routledge, S. 157-184.

Katzenstein, Peter J. (1996):” Introduction: Alternative Perspectives on National Security”, in: Ders. (Hg.): “*The Culture of National Security. Norms and Identity in World* Politics”, Ithaca: Cornell University Press, S. 1-32.

Katzenstein, Peter J. (2012a): “The West as Anglo-American”, in: Ders. (Hg.): “*Anglo-America and its Discontents: Civilizational Identities beyond West and East*”, Abingdon/New York: Routledge, S. 1-30.

Katzenstein, Peter J. (2012b): “Many Wests and Polymorphic Globalism”, in: Ders. (Hg.): “*Anglo-America and its Discontents: Civilizational Identities beyond West and East*”, Abingdon/New York: Routledge, S.207-247.

Kaunert, Christian/Léonard, Sarah/MacKenzie, Alex (2012): “The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the case of PNR and SWIFT”, *European Security 21*(4), S. 474-496.

Kaunert, Christian (2010): „Europol and EU Counterterrorism: International Security Actorness in the External Dimension“, *Studies in Conflict & Terrorism, 33*(7), S. 652-671.

Kean, Thomas H./Hamilton, Lee H./Ben-Veniste, Richard (2004): “The 9/11 Commission Report”, New York: W.W. Norton.

Kent, Sherman (1966): „*Strategic Intelligence for American World Policy*“, Princeton: Princeton University Press.

Keohane, Robert O. (1989): “Neoliberal Institutionalism: A Perspective on World Politics”, in: Ders. (Hg.): “*International Institutions and State Power: Essays in International Relations Theory”*, Boulder: Westview, S. 1-20.

Keoane, Robert O. (1984): “*After Hegemony: Cooperation and Discord in the World Political Economy”*, Princeton: Princeton University Press.

Kietz, Daniela/Ondarza, Nicolai von (2016): “*Sicherheit delegieren. EU-Agenturen in der inneren und äußeren Sicherheit*“, Berlin: Stiftung Wissenschaft und Politik.

Kietz, Daniela/Maurer, Andreas (2006): “*Von Schengen nach Prüm. Sogwirkungen verstärkter Kooperation und Anzeichen der Fragmentierung in der EU*“, Diskussionspapier der FG1, 2006/07. Mai 2006, Berlin: Stiftung Wissenschaft und Politik.

King, Gary/Keohane, Robert O./Verba, Sidney (1994): „*Designing Social Inquiry. Scientific Inference in Qualitative Research*”, Princeton: Princeton University Press.

Kitchin, Rob (1998): „*Cyberspace. The World in the Wires*“, Chichester et al: John Wiley & Sons.

Klatetzki, Thomas (2006): "Der Stellenwert des Begriffs 'Kognition' im Neo-Institutionalismus", in: Senge, Konstanze/Hellmann, Kai-Uwe (Hg.): „*Einführung in den Neo-Institutionalismus. Mit einem Beitrag von W. Richard Scott*", Wiesbaden: Springer VS, S. 48-61.

Klavehn, Christoph/Müller, Michael (2008): „Exekutive Allmacht – Öffentliche Ohnmacht? Britische Außenpolitik und die Instrumentalisierung der Nachrichtendienste im Vorfeld des Irak-Krieges von 2003", in: Morisse-Schilbach, Melanie/Peine, Anke (Hg.): „*Demokratische Außenpolitik und Geheimdienste. Aspekte eines Widerspruchs in Deutschland, Großbritannien, Israel, USA und Frankreich im Vergleich*", Berlin: Dr. Köster, S. 199-230.

Köcher, Renate (2016): "Das Sicherheitsgefühl der Deutschen erodiert", Faz.net, 24.08.2016, http://www.faz.net/aktuell/politik/kampf-gegen-den-terror/terror-angst-der-deutschen-nimmt-laut-allensbach-studie-zu-14402481.html?printPagedArticle=true#pageIndex_0 [26.06.2018].

Krasner, Stephen D. (1983): „*International Regimes*", Ithaca: Cornell University Press.

Krause, Joachim (2018): "Sicherheit", in: Voigt, Rüdiger (Hg.): „*Handbuch Staat. Band 2"*, S. 1559-1568.

Kratochwil, Friedrich V./Ruggie, John G. (1986): „International Organization: A State of the Art on an Art of the State", *International Organization, 40(*4), S. 753-775.

Kretschmann, Andrea (2017): "Soziale Tatsachen. Eine wissenssoziologische Perspektive auf den 'Gefährder'", *Aus Politik und Zeitgeschichte (APuZ), 67* (32-33), S. 11-16.

Krieger, Wolfgang (2018): „Geheimdienst", in: Voigt, Rüdiger (Hg.): „*Handbuch Staat. Band 1"*, S. 727-736.

Krieger, Wolfgang (2014): "*Geschichte der Geheimdienste. Von den Pharaonen bis zur NSA*", 3. Aufl., München: C.H. Beck.

Krieger, Wolfgang (2010): „The German Bundesnachrichtendienst (BND): Evolution and Current Policy Issues", in: Loch K. Johnson (Hg.): "*The Oxford Handbook of National Security Intelligence"*, Oxford: Oxford University Press, S. 790-805.

Krücken, Georg (2006): "World Polity Forschung", in: Senge, Konstanze/Hellmann, Kai-Uwe (Hg.): „*Einführung in den Neo-Institutionalismus. Mit einem Beitrag von W. Richard Scott"*, Wiesbaden: Springer VS, S. 139-149.

Kühne, Eberhard (2012): "*Informationsverarbeitung und Wissensmanagement der Polizei beim Aufbruch in eine digitalisierte Welt*", Frankfurt: Verlag für Polizeiwissenschaft.

Lange, Hans Jürgen/Schenck, Jean Claude (2004): „*Polizei im kooperativen Staat*", Wiesbaden: Springer VS.

Lefebvre, Stéphane (2003): „The Difficulties and Dilemmas of International Intelligence Cooperation", *International Journal of Intelligence and Counterintelligence, 16*(4), S. 527-542.

Lichtblau, Eric/Risen, James (2006): "Bank Data is Sifted by U.S. in secret to block terror", *The New York Times*, http://www.nytimes.com/2006/06/23/washington/23intel.html , 23.05.2006 [Zugriff: 23.03.2018].

Lowenthal, Mark M. (2017): „*Intelligence. From Secrets to Policy*", 7. Aufl., Los Angeles: CQ Press.

MacDonald, David/O'Connor, Brendon (2012): "Special Relationships. Australia and New Zealand in the Anglo-American World", in: Katzenstein, Peter J. (Hg.): "*Anglo-America and its Discontents: Civilizational Identities beyond West and East*", Abingdon/New York: Routledge, S. 176-204.

Maguire, Mike (2000): "Policing by risks and targets: Some dimensions and implications of intelligence-led crime control, *Policing and Society 9*, S. 315-336.

Mahoney, James/Thelen, Kathleen (2010): "A Theory of Gradual Institutional Change", in: Dies. (Hg.): "*Explaining Institutional Change. Ambiguity, Agency, and Power"*, Cambridge: Cambridge University Press, S. 1-37.

Mallinckrodt, Marie v./Reimers, Ariane (2016): "Streit über Wege der Terrorbekämpfung. Mehr Sicherheit durch Datenaustausch?", *Tagesschau*, https://www.tagesschau.de/inland/datenaustausch-in-europa-101.html, 03.04.2016 [Zugriff: 20.02.2018].

Manners, Ian (2008): „The Normative Ethics of the European Union", *International Affairs, 84*(1), S. 45-60.

Manske, Mirko (2000): "Das 'Europol-Informations-System' (Europol-IS)", *Kriminalistik, 2001*(2), S. 105-108.

March, James G./Olsen, Johan P. (1976): "Organizational Choice under Ambiguity", in: March, James G./Olsen, Johan P. (Hg.): "*Ambiguity and Choice in Organizations"*, Bergen, S. 10-23.

Marrin, Stephen (2011): „*Improving Intelligence Analysis. Bridging the Gap between Scholarship and Practice*", Abingdon/New York: Routledge.

Maschewski, Felix/Nosthoff, Anna-Verena (2018): "Passivität im Kostüm der Aktivität. Über Günther Anders' Kritik kybernetischer Politik im Zeitalter der „totalen Maschine", *Behemoth, 11*(1), S. 8-25.

Massey, Doreen (2005): "*For Space*", London: Sage Publications

Mayer, Jonathan/Mutchler, Patrick/Mitchell, John C. (2015): "Evaluating the privacy properties of telephone metadata", *Proceedings of the National Academy of Sciences of the United States of America, 113*(20), S. 5536-5541.

Meister, Andre (2014): "RAMPART-A: Die NSA schnorchelt mehr als 3 Terabit pro Sekunde von Glasfasern ab – und der BND macht mit (Updates)", https://netzpolitik.org/2014/rampart-a-die-nsa-schnorchelt-mehr-als-3-terabit-pro-sekunde-von-glasfasern-ab-und-der-bnd-macht-mit/ , 19.06.2014 [Zugriff: 05.04.2018].

Mense-Petermann, Ursula (2005): „Das Verständnis von Organisation im Neo-Institutionalismus. Lose Kopplung, Reifikation, Instituion" in: Senge, Konstanze/Hellmann, Kai-Uwe (Hg.): „*Einführung in den Neo-Institutionalismus. Mit einem Beitrag von W. Richard Scott"*, Wiesbaden: Springer VS, S. 62-74.

Merten, Ulrike (2015): „Der gesellschaftliche Diskurs über die Sicherheitsvorsorge in Deutschland", *Europäische Sicherheit und Technik, 2015*(8), S. 14-15.

Meyer, John W./Boli, John/Thomas, George M. (2005): "Ontologie und Rationalisierung im Zurechnungssystem der westlichen Kultur", in: Meyer, John W. (Hg): *Weltkultur. Wie die westlichen Prinzipien die Welt durchdringen*, Frankfurt am Main: Suhrkamp, S. 17-46.

Meyer, John W./Rowan, Brian (1977): "Institutionalized Organizations: Formal Structure as Myth and Ceremony", *American Journal of Sociology, 83*(2), S. 340-363.

Monroy, Matthias (2017): "EU stärkt Netzwerk von Spezialeinheiten", *CILIP*,1.11.217, https://www.cilip.de/2017/11/01/eu-staerkt-netzwerk-von-spezialeinheiten/ [Zugriff: 16.02.2018]

Möllers, Rosalie (2012): „*Polizei in Europa. EUROPOL und FRONTEX im Raum der Freiheit, der Sicherheit und des Rechts*“, Frankfurt/Main: Verlag für Polizeiwissenschaft.

Morisse-Schilbach, Melanie/ Peine, Anke (2008): “Demokratische Außenpolitik und Geheimdienste – ein Widerspruch? Forschungsstand, Begriffe, Thesen“, in: Dies. (Hg.): „*Demokratische Außenpolitik und Geheimdienste. Aspekte eines Widerspruchs in Deutschland, Großbritannien, Israel, USA und Frankreich im Vergleich*“, Berlin: Verlag Dr. Köster, S. 9-40.

Münkler, Herfried (2002): „*Die neuen Kriege*“, Lübeck: Rowohlt.

Naughton, John (2016): „The evolution of the Internet: From military experiment to General Porpuse Technology“, *Journal of Cyber Policy 1*(1), S. 5-28.

Nešković, Wolfgang (2015): „*Der CIA-Folterreport: Der offizielle Bericht des US-Senats zum Internierungs- und Verhörprogramm der CIA*“, Frankfurt/Main: Westend .

Offe, Claus (2001): “Gibt es eine europäische Gesellschaft? Kann es sie geben?“, *Blätter für deutsche und internationale Politik, 2001*(4), S. 423-435.

Omand, David (2014): “The cycle of intelligence” in: Dover, Robert/Goodmann, Michael S./Hillebrand, Claudia (Hg.): “*Routledge Companion to Intelligence Studies”*, Abingdon/New York: Routledge, S. 59-70.

Omand, David/Bartlett, Jamie (2012): „Introducing Social Media Intelligence (SOCMINT)”, *Intelligence and National Security 27*(6), S. 801-823.

Omand, David (2010): “*Securing the State*”, Oxford: Oxford University Press.

Pauly, Louis W./Reus-Smit, Christian (2012): “Negotiating Anglo-America: Australia, Canada, and the United States”, in: Katzenstein, Peter J. (Hg.): “*Anglo-America and its Discontents: Civilizational Identities beyond West and East*”, Abingdon/New York: Routledge, S. 127-151.

Paoli, Letizia (2014): „How to Tackle (Organized) Crime in Europe: The EU Policy Cycle on Serious and Organized Crime and the New Emphasis on Harm”, *European Journal of Crime, Criminal Law and Criminal Justice 22*, S. 1-12.

Pechstein, Matthias/Koenig, Christian (2000): “*Die Europäische Union*”, 3. Aufl., Tübingen: Mohr Siebeck.

Peine, Anke/Morisse-Schilbach, Melanie (2008): "Demokratische Außenpolitik und Geheimdienste – Zusammenfassung und Ausblick", in Dies. (Hg.): „*Demokratische Außenpolitik und Geheimdienste. Aspekte eines Widerspruchs in Deutschland, Großbritannien, Israel, USA und Frankreich im Vergleich*", Berlin: Dr. Köster, S. 337-344.

Peine, Anke/Sturm, Constanze (2008): „Die Vereinigten Staaten von Amerika: Eine Supermacht zwischen Freiheitsideal und hegemonialer Vorherrschaft", in: Morisse-Schilbach, Melanie/Peine, Anke (Hg.): „*Demokratische Außenpolitik und Geheimdienste. Aspekte eines Widerspruchs in Deutschland, Großbritannien, Israel, USA und Frankreich im Vergleich*", Berlin: Dr. Köster, S. 265-298.

Petri, Thomas Bernhard (2001): „*Europol. Grenzüberschreitende polizeiliche Tätigkeit in Europa*", Baden-Baden, Nomos.

Piquet, Agathe (2017): „Supranational Activism and Intergovernmental Dynamics: the European Police Office as a supranational opportunist?, *Journal of Contemporary European Research, 13*(2), S. 1186-1207.

Power, Michael (2004): „*The Risk Management of Everything. Rethinking the Politics of Uncertainty*", London: Demos.

Rappert, Brian (2015): "Sensing Absence: How to See what Isn't There in the Study of Science and Security", in: Rappert, Brian/Balmer, Brian (Hg.): "Absence in Science, Security and Policy: From Research Agendas to Global Strategy", London et al: Palgrave MacMillan.

Rappert, Brian (2014): "Present Absences: Hautings and Whirlwinds in '-Graphy'", Social Epistemology, Vol. 28(1), S. 41-55.

Rappert, Brian (2010): "Revealing and concealing secrets in research: the potential for the absent", *Qualitative Research 10*(5), S. 571-587.

Ratcliffe, Jerry H. (2008): "Intelligence-Led Policing", Milton: Willan.

Rat der Europäischen Union (2016): „*Draft European Initiative to Prevent and Combat Organised Domestic Burglary*", 8.03.2016.

Rat der Europäischen Union (2015): "*Schlussfolgerungen des Rates der EU und der im Rat vereinigten Mitgliedstaaten zur Terrorismusbekämpfung*", Pressemitteilung 848/15,

http://www.consilium.europa.eu/de/press/press-releases/2015/11/20/jha-conclusions-counter-terrorism/ [Zugriff: 16.02.2018]

Rathmell, Andrew (2010): „Towards postmodern Intelligence“, *Intelligence and National Security 3*(17), S. 87-104.

Ratzel, Max-Peter (2008a): “Das Europäische Polizeiamt. Teil 1“, *Kriminalistik 2008*(1), S. 27-37.

Ratzel, Max Peter (2008b): “Oral evidence, 24 June 2008”, in: House of Lords European Union Committee (Hg.): *“29th Report of Session 2007-08 – Europol: Coordinating the Fight against Serious and Organized Crime. Report with Evidence”*, 12.11.2008, https://publications.parliament.uk/pa/ld200708/ldselect/ldeucom/183/183.pdf [13.06.2018], S. 78-114.

Richelson, Jeffrey T. (2009): “Technical Collection in the Post-September 11 World”, in: Treverton, Jeffrey T./Agrell, Wilhelm (Hg.): “*National Intelligence Systems. Current Research and Future Prospects”*, Cambridge: Cambridge University Press, S. 147-175.

Richelson, Jeffrey T. (1990): “The Calculus of Intelligence Cooperation”, *Intelligence and Counterintelligence*, 4(3), S. 307-323.

Richelson, Jeffrey T./Ball, Desmond (1985): “*The Ties that Bind. Intelligence Cooperation between the UKUSA Countries – the United Kingdom, the United States of America, Canada, Australia and New Zealand*”, North Sydney et al: Allen & Unwin.

Ripoli Servent, Adriana/MacKenzie, Alex (2011): “Is the EP Still a Data Protection Champion? The Case of SWIFT”, *Perspectives on European Politics and Society 12*(4), S. 390-406.

Rudner, Martin (2006): “The Historical Evolution of Canada’s Foreign Intelligence Capability: Cold War SIGINT Strategy and its Legacy”, *Journal of Intelligence History*, *6*(1), S. 67-83.

Ruffner, Kevin C. (2007): “*Forging an Intelligence Partnership: CIA and the Origins of the BND, 1949-56, Volume II*”, Central Intelligence Agency.

Schaller, Christian (2016): „*Kommunikationsüberwachung durch den Bundesnachrichtendienst. Rechtlicher Rahmen und Regelungsbedarf*“, Berlin: Stiftung Wissenschaft und Politik.

Schmid, Gerhard (2014a): „Kommunikationsüberwachung als Werkzeug beim Kampf gegen den Terrorismus“, in: Hansen, Stefan/Krause, Joachim (Hg.): *Jahrbuch Terrorismus 2013/2014*, Berlin: Budrich, S. 325-344.

Schmid, Gerhard (2014b): „Abhören in der Premiumklasse“, in: *Zeitschrift für Außen- und Sicherheitspolitik, 2014*(1), S. 11-21.

Schneckener, Ulrich (2013): „Bedingt abwehrbereit: Politische und administrative Reaktionsmuster auf das ‚Terrorrisiko‘“, in: Daase, Christopher/Engert, Stefan/Junk, Julian (Hg.): „*Verunsicherte Gesellschaft – Überforderter Staat. Zum Wandel der Sicherheitskultur*“, Frankfurt/Main: Campus, S. 35-56.

Schober, Konrad (2017): „*Europäische Polizeizusammenarbeit zwischen TREVI und Prüm. Mehr Sicherheit auf Kosten von Freiheit und Recht?*“, Heidelberg: C.F. Müller.

Schuster, Leo (2000): “Europäisierung der Polizeiarbeit. Ein ebenso schwieriges wie schicksalhaftes Problem“, *Kriminalistik 2000*(2), S. 74-82.

Scott, Len V./Jackson, Peter D. (2004): „The Study of Intelligence in Theory and in Practice“, in: Dies. (Hg.): “*Understanding Intelligence in the Twenty-First Century: Journeys in Shadows*”, Abingdon/New York: Routledge, S. 139-169.

Scott, W. Richard (2014): “*Institutions and Organizations. Ideas, Interests, and Identities*”, 4. Aufl., London: Sage Publications.

Scott, W. Richard (1991): “Unpacking Institutional Arguments”, in: Powell, Walter W./DiMaggio, Paul J. (Hg): *“The New Institutionalism in Organizational Analysis”*, Chicago/London: The University of Chicago Press, S. 164-182.

Scott, W. Richard/Meyer, John W. (1983): “The Organization of Societal Sectors”, in: Dies. (Hg.): *“Organizational Environments: Ritual and Rationality”*, Beverly Hills: Sage, S. 129-153.

Segell, Glen M. (2004): “Intelligence Agency Relations between the European Union and the U.S.”, *International Journal of Intelligence and Counterintelligence, 17*, S. 81-96.

Seidel, Christoph (2015): „Ungewissheit, Vielfalt, Mehrdeutigkeit – Eine Heuristik unsicherer Umwelten“, in: Apelt, Maja/Senge, Konstanze (Hg.): „*Organisation und Unsicherheit*“, Wiesbaden: Springer VS, S. 35-50.

Senge, Constanze (2011): "*Das Neue am Neo-Institutionalismus. Der Neo-Institutionalismus im Kontext der Organisationswissenschaft*", Wiesbaden: Springer VS.

Senge, Constanze (2006): „Zum Begriff der Institution im Neo-Institutionalismus", in: „*Einführung in den Neo-Institutionalismus. Mit einem Beitrag von W. Richard Scott*", Wiesbaden: Springer VS, S. 35-47.

Senge, Konstanze/Hellmann, Kai-Uwe (2006): „Einleitung", in: Dies. (Hg.): „*Einführung in den Neo-Institutionalismus. Mit einem Beitrag von W. Richard Scott"*, Wiesbaden: Springer VS, S. 7-34.

Sheptycki, James W. E. (1998): „The Global Cops Cometh: Reflections on Transnationalization, Knowledge Work and Policing Subculture", *The British Journal of Sociology, 49(*1), S. 57-74.

Siedschlag, Alexander (2006): "Strategische Kulturanalyse: Deutschland, Frankreich und die Transformation der NATO", in: Ders. (Hg.): "*Methoden der sicherheitspolitischen Analyse. Eine Einführung*", S. 21-48.

Siedschlag, Alexander (2000): „*Politische Institutionalisierung und Konflikttransformation. Leitideen, Theoriemodelle und europäische Praxisfälle*", Opladen: Leske und Budrich.

Sims, Jennifer (2006): „Foreign Intelligence Liaison: Devils, Deals, and Details", *Journal of Intelligence and Counterintelligence, 19*, S. 195-217.

Smidt, Wolbert K. (2008): „Nachrichtendienst-Kultur in der Demokratie: Defizite, Fragen, Forderungen", in: Morisse-Schilbach, Melanie/Peine, Anke (Hg.): „*Demokratische Außenpolitik und Geheimdienste. Aspekte eines Widerspruchs in Deutschland, Großbritannien, Israel, USA und Frankreich im Vergleich*", Dr. Köster, S. 143-157.

Splendid Research (2016): „Quantified Wealth Monitor 2016: Wichtigkeit von Datenschutz", https://www.splendid-research.com/de/statistiken/item/datenschutz-fuer-mehrheit-wichtig.html [26.06.2018].

Sterbling, Anton (2009): "Entgrenzung von Sicherheitsräumen und Entstehung von 'Gewaltmärkten'", in: Behr, Rafael/Ohlemacher, Thomas (Hg.): „*Offene Grenzen. Polizieren in der Sicherheitsarchitektur einer post-territorialen Welt. Ergebnisse der XI. Tagung des Arbeitskreises Empirische Polizeiforschung*", Frankfurt/Main: Verlag für Polizeiwissenschaft, S. 113-128.

Stetter, Stephan (2017): „Soziologische Ansätze in den Internationalen Beziehungen“, in: Sauer, Frank/Masala, Carlo (Hg.): „*Handbuch Internationale Beziehungen*“, 2. Aufl., Wiesbaden: Springer VS, S. 257-282.

Tekin, Funda (2017): „Differenzierte Integration im Raum der Freiheit, der Sicherheit und des Rechts im Spannungsfeld von Problemlösungsinstinkt und Souveränitätsreflex“, *Integration 2017*(4), S. 263-275.

Tönnesmann, Wolfgang/ Alemann, Ulrich von (1995): „Grundriss: Methoden in der Politikwissenschaft“, in Dies. (Hg.): „*Politikwissenschaftliche Methoden. Grundriß für Studium und Forschung“*, Opladen: Westdeutscher Verlag, S. 17-140.

Treverton, Gregory F. (2014): “The future of intelligence. Changing threats, evolving methods”, in: Duyvesteyn, Isabelle/de Jong, Ben/von Reijn, Joop (Hg.): “*The Future of Intelligence. Challenges in the 21st century”*, Abingdon/New York: Routledge, S. 27-38.

Treverton, Gregory F. (2001): “Reshaping National Intelligence in an Age of Information, *RAND Studies in Intelligence*: Cambridge University Press.

Türk, Klaus (1999): “Organisation und moderne Gesellschaft. Einige theoretische Bausteine“, in: Edeling/Thomas/Jann,Thomas/Wagner, Dieter (Hg.): „*Institutionenökonomie und Neuer Institutionalismus. Überlegungen zur Organisationstheorie*“, S. 43-80.

Uhrlau, Ernst (2009): “Modernisierung und Zukunftsfähigkeit. Die Strukturreform des Bundesnachrichtendienstes“, *Zeitschrift für Außen- und Sicherheitspolitik, 2009*(2), S. 449-453.

Ulbert, Cornelia (1997): „Ideen, Institutionen und Kultur. Die Konstruktion (inter-) nationaler Klimapolitik in der BRD und in den USA“, *Zeitschrift für Internationale Beziehungen, 4*(1), S. 9-40.

Valkenburg, Govert/van der Ploeg, Irma (2015): “Materialities between Security and Privacy: A constructivist account of Airport Security Scanners”, *Security Dialogue, 46*(4), S. 326-344.

Vieth, Kilian (2018): „Im Internet sind alle Ausländer. Was der BND darf, geht zu weit“, n-tv.de, 02.06.2018, https://www.n-tv.de/politik/Was-der-BND-darf-geht-zu-weit-article20460297.html [04.06.2018]

Vieth, Kilian (2017): „Die Internetpolizei. Wie Europol gegen unliebsame Internetinhalte vorgeht“, *CILIP 112*, März 2017.

Wahl, Thomas (2010): „The European Union as an Actor in the Fight against Terrorism“, in: Wade, Marianne/Maljevic, Almir (Hg.): "*A War on Terror? The European Stance on a New Threat, Changing Laws and Human Rights Implications*", Wiesbaden: Springer VS.

Walgenbach, Peter (2006): „Neoinstitutionalistische Ansätze in der Organisationstheorie“, in: Kieser, Alfred/Ebers, Mark (Hg.): „*Organisationstheorien*“, Stuttgart: Verlag Kohlhammer, 6. Aufl., S. 353-402.

Walsh, Patrick F./Miller, Seumas (2016): „Rethinking ‚Five Eyes' Security Intelligence Collection Policies and Practice Post Snowden“, *Intelligence and National Security, 31*(3), S. 345-368.

Warner, Michael (2013): "*The past and future of the intelligence cycle", in: Phythian, Mark (Hg.): "Understanding the Intelligence Cycle"*, Abingdon/New York: Routledge, S. 9-20.

Wendt, Alexander (1992): "*Anarchy is what States make of it*", International Organization, 46(2), S. 391-425.

Westerfield, H. Bradford (1996): „America and the World of Intelligence Liaison“, *Intelligence and National Security, 11*(3), S. 523-560.

Wetzling, Thorsten (2017): "*Germany's Intelligence Reform: More Surveillance, modest Restraints and inefficient Controls*", Berlin: Stiftung Neue Verantwortung.

Wieck, Hans-Georg (2008): „Demokratische Außenpolitik und Geheimdienste – ein Widerspruch? Anmerkungen aus der Praxis“, in: Morisse-Schilbach, Melanie/Peine, Anke (Hg.): „*Demokratische Außenpolitik und Geheimdienste. Aspekte eines Widerspruchs in Deutschland, Großbritannien, Israel, USA und Frankreich im Vergleich*“, Berlin: Dr. Köster, S. 43-62.

Wiefelspütz, Dieter (2007): "*Die Abwehr terroristischer Anschläge und das Grundgesetz. Polizei und Streitkräfte im Spannungsfeld neuer Herausforderungen*“, Frankfurt: Verlag für Polizeiwissenschaft.

Wolf, Joachim (2013): „Der rechtliche Nebel der deutsch-amerikanischen ‚NSA-Abhöraffäre'. US-Recht, fortbestehendes Besatzungsrecht, deutsches Recht und Geheimabkommen“, *Juristenzeitung, 2013*(21), S. 1039-1046.

Ziedler, Christopher (2016): „Die Wirkungen des BREXIT auf die Sicherheitspolitik. Weniger abwehrbereit“, *Stuttgarter-Zeitung.de*, 21.06.2016, https://www.stuttgarter-zeitung.de/inhalt.die-wirkungen-des-brexit-auf-die-sicherheitspolitik-weniger-abwehrbereit.448097f8-d95f-4179-89e9-55a49759fab0.html [05.06.2018].

Zilber, Tammar B. (2006): „The Work of the Symbolic in Instiutional Processes: Translations of Rational Myths in Israeli High Tech“, *Academy of Management Journal 2*(49), S. 281-303.

Zöller, Mark A. (2011): “Der Austausch von Strafverfolgungsdaten zwischen den Mitgliedsstaaten der Europäischen Union“, *Zeitschrift für Internationale Strafrechtsdogmatik 2011*(2). S. 64-69.

Zucker, Lynne G. (1983): “Organizations as Institutions”, *Research in the Sociology of Organization 2*, S. 1-47.

3. Nachweis der Motti

Kapitel 1:
Thomas de Maizière, von 2013 bis 2018 Bundesminister des Innern. Zitiert nach Mallinckrodt/Reimers 2016.

Kapitel 2:
Wolbert K. Smidt, bis 2001 Erster Direktor des Bundesnachrichtendienstes. Zitiert nach Smidt 2008: 149.

Kapitel 3:
Doreen Massey, Humangeographin. Zitiert nach Massey 2005: 9.

W. Richard Scott, US-amerikanischer Soziologe und Wegbereiter des Neuen Institutionalismus. Zitiert nach Scott 2014: 126.

Kapitel 4:

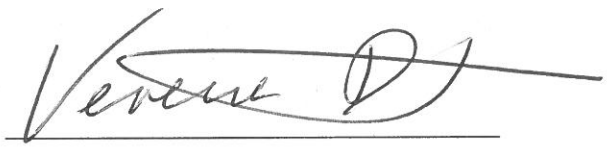
Ohne Verfasser. Zitiert nach National Security Agency 2012g.

Kapitel 5:

Joachim Gauck, von 2012 bis 2017 Bundespräsident. Zitiert nach Gauck 2014: 117.

Ich erkläre hiermit, dass ich die vorgelegte Arbeit ohne Hilfe Dritter und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus anderen Quellen direkt oder indirekt übernommenen Aussagen, Daten und Konzepte sind unter Angabe der Quelle gekennzeichnet. Niemand hat von mir unmittelbar oder mittelbar geldwerte Leistungen für Arbeiten erhalten, die im Zusammenhang mit dem Inhalt der vorgelegten Dissertation stehen. Die Arbeit wurde bisher weder im In- noch im Ausland in gleicher oder ähnlicher Form einer anderen Prüfungsbehörde vorgelegt. Ich versichere, dass ich nach bestem Wissen die reine Wahrheit gesagt und nichts verschwiegen habe.

Köln, den 7. Februar 2019



Verena Diersch

LEBENSLAUF

Name:	Verena Diersch
Adresse:	Erfurter Str. 34, 51103 Köln
Telefon:	01 63/ 6 39 83 08
E-Mailadresse:	verena.diersch@gmail.com
Staatsangehörigkeit:	deutsch
Geburtsdatum:	16.11.1987

Akademischer Werdegang:

2013 - 2019	Promotion in Politikwissenschaft bei Prof. Dr. Thomas Jäger, Lehrstuhl für Außenpolitik und Internationale Politik, Universität zu Köln, Note 1,0 Dissertationsthema: **„**‘Culture, Cooperation, Capabilities‘ – internationale Geheimdienstkooperation und europäische Polizeikooperation im Spannungsfeld von Legitimität und Effektivität“
2007-2013	Diplomstudium Politikwissenschaft an der Hochschule für Politik, angeschlossenes Institut der Ludwig-Maximilians-Universität München, Note: 2,19 Studienschwerpunkt: Internationale Beziehungen Thema der Diplomarbeit: „Cyberwar und Kalter Krieg im Vergleich“

Beruflicher Werdegang:

seit Oktober 2013:	Wissenschaftliche Mitarbeiterin am Lehrstuhl für Außenpolitik und Internationale Politik, Prof. Dr. Thomas Jäger, Universität zu Köln Redaktionsleitung Social Media der *Zeitschrift für Außen- und Sicherheitspolitik (ZfAS)*
Dezember 2013 – Mai 2013:	Werkstudentin für den technisch-wissenschaftlichen Dienstleister iABG mbH, Ottobrunn
Oktober 2011 – Dezember 2011:	Praktikum im Brüsseler Büro der Stiftung Wissenschaft und Politik (SWP)
2006 – September 2013:	Freiberufliche journalistische Tätigkeit beim Musikbranchenmagazin „Musikmarkt“, München sowie Starnberger Merkur
März 2011 – April 2011:	Praktikum Hanns Seidel Stiftung, München Organisatorische Leitung Expertenworkshop „Cyberwar“

Auslandsaufenthalte und Stipendien:

13.02.2017 - 07.04.2017	Forschungsaufenthalt an der Cornell University, Ithaca, bei Prof. Dr. Peter J. Katzenstein
13.02.2017 – 07.04.2017	Stipendium der Heinrich Hertz-Stiftung für auswärtigen Forschungsaufenthalt
2016	Kongressreisenstipendium des Deutschen Akademischen Austauschsdienst für die International Studies Association's (ISA) Annual Convention, Atlanta, USA
2015	Kongressreisenstipendium des Deutschen Akademischen Austauschsdienst für die International Studies Association's (ISA) Annual Convention, New Orleans, USA

Publikationsverzeichnis:

Monographien und Sammelbände

- Verena Diersch, Stephan Liedtke, Thomas Jäger (Hrsg.): „*Die Geheimdienste der USA. Organisation, Strategie und die NSA-Affäre*", Zürich: Orell Füssli (geplant für Frühjahr 2020).

Beiträge in Sammelbänden

- Verena Diersch (2018): „Nationale und internationale Cybersicherheitspolitik. Ein Spannungsfeld", in: Thomas Jäger, Anna Daun, Dirk Freudenberg (Hrsg.): „*Politisches Krisenmanagement. Reaktion, Partizipation, Resilienz*", Wiesbaden: Springer VS, S. 163-179.
- Verena Diersch, Julian Dörr (2018): „Eine neue industrielle Revolution? Die Veränderung des Eigentums angesichts von Internet und Digitalisierung", in: Rainer Kirchdörfer, Brun-Hagen Hennerkes, Stefan Heidbreder, Nils Goldschmidt (Hrsg.): „*Eigentum: Warum wir es brauchen, was es bewirkt, wo es gefährdet ist*", Freiburg: Herder, S. 265-275.
- Verena Diersch (2017): „Die Dienste", in: Thomas Jäger (Hrsg.): „*Die Außenpolitik der USA. Eine Einführung*", Wiesbaden: Springer VS, S. 65-84.
- Verena Diersch, Martin Schmetz (2017): „Vom Cyberfrieden. Wieso wir Frieden kennen müssen um den Cyberkrieg zu verstehen", in: Daniel Jacob, Thorsten Thiel (Hrsg.): „*Politische Theorie und Digitalisierung"*, Baden-Baden: Nomos, S. 299-316.

Journal-Beiträge

- Verena Diersch, Julian Dörr (2017): „Zur Rechtfertigung von Whistleblowing: Eine ordnungsethische und legitimitätstheoretische Perspektive der Whistleblower-Fälle Carl von Ossietzky und Edward Snowden", *Zeitschrift für Politik, Vol. 64*(4), S. 468-492.

Rezensionen und Berichte

- Verena Diersch (2016), Rezension für Dieter Deiseroth, Annegret Falter (2014): „Whistleblower in der Sicherheitspolitik. Preisverleihung 2011/2013", Berlin: Berliner Wissenschaftsverlag, *Zeitschrift für Außen- und Sicherheitspolitik (ZfAS), Vol. 2*/2016, S. 289-291.
- Verena Diersch (2015), Rezension für Wolfgang Krieger (2014): „Geschichte der Geheimdienste", München: C.H. Beck, *Politische Studien der Hanns Seidel Stiftung, Vol. 460,* S. 114-116.
- Verena Diersch (2015): „Bericht über den Cyber Security Summit 2014 der Münchner Sicherheitskonferenz und der Deutschen Telekom in Bonn", *Zeitschrift für Außen- und Sicherheitspolitik (ZfAS), Vol. 01*/2015, S. 133-137.

- Verena Diersch (2014), Rezension für The President's Review Group on Intelligence and Communications Technologies (2014): „The NSA Report. Liberty and Security in a changing World", *Zeitschrift für Außen- und Sicherheitspolitik (ZfAS), Vol. 3*/2014, S. 417-419.
- Verena Diersch (2014): „Bericht über den Cyber Security Summit 2013 der Münchner Sicherheitskonferenz und der Deutschen Telekom in Bonn", *Zeitschrift für Außen- und Sicherheitspolitik (ZfAS), Vol. 01*/2014, S. 67-73.

Vorträge und Konferenzbeiträge:

- Vortrag „Entscheiden und Handeln in der internationalen Politik – Supranationale Institutionen und die Grundlagen der transatlantischen Beziehungen", Lehrgespräch im Rahmen der Fortbildungsmaßnahme „Internationale Beziehungen – Organisationen und Kooperationen im Überblick" der Bundesakademie für öffentliche Verwaltung (BAKöV) beim Bundesministerium des Innern, für Bau und Heimat, Berlin, 05.11.2018
- Vortrag beim Cyber Security Slam der Universität Bonn, „'Don't Mess with your Big Brother' – Die NSA-Affäre aus deutscher Sicht", 30.01.2018, Bonn
- Konferenzbeitrag „Digital Network Intelligence", Creating and Challenging the Transatlantic Intelligence Community, internationale Kooperationsveranstaltung des Woodrow Wilson Centers, des German Historical Institute (GHI) und der International Intelligence History Association (IIHA), Washington, D.C., USA, 29.03.2017
- Konferenzbeitrag (mit Julian Dörr) „The Dark Side of Market Power? The Political Logic of Market Dominance in the Digital Economy", International Studies Association's (ISA) Annual Convention, Baltimore, USA, 25.02.2017
- Konferenzbeitrag "Cyberspace as a Realm for Intelligence Cooperation – Is Technology the driving Factor?", International Studies Association's (ISA) Annual Convention, Baltimore, USA, 22.02.2017
- Vortrag „'Mad Cyber'? Akteure, Fähigkeiten und Problemlagen im Cyberspace aus Sicht der Internationalen Politischen Ökonomie" für das Seminar Universität und Bevölkerungsschutz des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK), Akademie für Krisenmanagement, Notfallplanung und Zivilschutz (AKNZ), Ahrweiler, 22.09.2016
- Vortrag „Cyber War, für likeminds: german-turkish junior expert initiative, Köln, 25.05.2016
- Vortrag "Der Cyber-Terrorismus und die Antwort der europäischen Sicherheitspolitik" für die Konrad Adenauer Stiftung, Aachen, 25.04.2016
- Konferenzbeitrag mit Martin Schmetz, Universität Frankfurt: "On Cyberpeace. Why we must know Peace to understand Cyberwar", International Studies Association's (ISA) Annual Convention, Atlanta, USA, 17.03.2016
- Vortrag "Die strategische Cyber-Überwachung der NSA und ihrer Partner" in einer Kooperationsveranstaltung des Kolloquiums für Zeitgeschichte, Prof. Dr. Constantin Goschler, und des Kolloquiums zur Geschichte der USA, Prof. Dr. Michael Wala, Ruhr-Universität Bochum, 20.01.2016
- Vortrag "Cyberidentitäten und Cybersicherheitspolitik", Seminar Universität und Bevölkerungsschutz des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe (BBK), Ahrweiler, 20.10.2015
- Vortrag „Die Bedrohung durch Cyber-Angriffe und die Antwort der europäischen Sicherheitspolitik", Seminar „Wie weit soll sich Europa in internationale Konflikte einmischen?" der Konrad Adenauer Stiftung, Villa La Collina, Cadenabbia, 29.09.2015
- Konferenzbeitrag „The framing of Cybersurveillance", 2015 Annual Convention of the International Intelligence History Association (IIHA), Zagreb, 09.05.2015
- Vortrag "Krieg im Netz" für Haus Neuland, Bielefeld, 28.04.2015
- Vortrag "Der Cyberspace als Kriegsschauplatz – Gefährdungseinschätzung und Sicherheitsstrategien der westlichen Staaten" für die Karl Arnold Stiftung, Königswinter, 21.04.2015

- Vortrag „Der Cyber-Terrorismus und die Antwort der europäischen Sicherheitspolitik“ für das Europa-Seminar der Konrad Adenauer Stiftung, Hürtgenwald-Vossenack, 20.04.2015
- Konferenzbeitrag “Do Corporations outpower Governments? – TNCs, States and Power in International Cybersecurity, International Studies Association’s Annual Convention, New Orleans, USA, 21.02.2015
- Konferenzbeitrag “Cyber Strategy: United Kingdom, Estonia and Germany”, International Studies Association’s (ISA) Annual Convention, New Orleans, USA, 18.02.2015
- Konferenzbeitrag (mit Mischa Hansel, Universität Gießen, und Simon Ruhnke, Universität zu Köln) „European Cyber Strategies and Capabilities“, Copenhagen Conference – War in the 5th Domain, Kopenhagen, Dänemark, 05.11.2014
- Konferenzbeitrag “Akteure und Institutionen der Cybersicherheitspolitik”, Vierte Offene Sektionstagung Internationale Politik der DVPW, Magdeburg, 26.09.2014
- Vortrag „Cyber War“ für die Summer School der Akademie der Bundeswehr für Information und Kommunikation, Strausberg, 09.09.2014
- Vortrag „Europas Antwort auf den Cyber-Terrorismus“ für das Europa-Seminar der Konrad Adenauer Stiftung, Bildungszentrum Eichholz, 02.09.2014
- Vortrag „Die ‚Cyber-Beziehungen‘ zwischen USA und China“ an der Professur für Internationale Beziehungen mit dem Schwerpunkt Weltordnungspolitik Prof. Dr. Reinhard Wolf, Universität Frankfurt, 02.07.2014
- Vortrag „Cybersicherheitspolitik – Cybersicherheit im Spannungsfeld von Geheimdiensten, Datenschutz und Wirtschaftspolitik“, Abendgespräch des Jean-Monnet-Lehrstuhls für Europäische Politik Prof. Dr. Daniel Göler, Universität Passau, 29.04.2014

Lehrverzeichnis

Bachelorvorlesung

Sommersemester 2019	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Internationale Politik“
Wintersemester 2018/2019	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Außenpolitik“
Sommersemester 2018	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Internationale Politik“
Wintersemester 2017/2018	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Außenpolitik“
Sommersemester 2017	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Internationale Politik“
Wintersemester 2016/2017	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Außenpolitik“
Sommersemester 2016	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Internationale Politik“
Wintersemester 2015/2016	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Außenpolitik“
Sommersemester 2015	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Internationale Politik“

Wintersemester 2014/2015	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Außenpolitik“
Sommersemester 2014	Mitarbeit in der Vorlesung „Grundzüge der Internationalen Beziehungen: Einführung in die Internationale Politik“
Wintersemester 2013/2014	Mitarbeit in der Vorlesung: „Grundzüge der Internationalen Beziehungen: Einführung in die Außenpolitik“

Seminare im Bachelor und Master

Sommersemester 2019	Master-Seminar „Internationale Klima- und Umweltpolitik als Herausforderung für die politische Praxis und die politikwissenschaftliche Analyse“
Wintersemester 2018/2019	Bachelor-Seminar „Intelligence – Nachrichtendienste in Theorie und Praxis“
Sommersemester 2018	Master-Seminar „Aktivität und Kooperation von Sicherheitsbehörden im Kontext politikwissenschaftlicher Forschung“
Wintersemester 2017/2018	Master-Seminar „Nachrichtendienste in der Außenpolitik und der Internationalen Politik“
Sommersemester 2017	Bachelor-Seminar „Cyber(sicherheits)politik“
Wintersemester 2016/2017	Bachelor-Seminar „Intelligence – Nachrichtendienste in Theorie und Praxis“
Sommersemester 2016	Bachelor-Seminar „Cyber(sicherheits)politik“
Wintersemester 2015/2016	Bachelor-Seminar „Intelligence – Nachrichtendienste in Theorie und Praxis“
Sommersemester 2015	Bachelor-Seminar „Cybersicherheitspolitik“
Wintersemester 2014/2015	Bachelor-Seminar „Intelligence – Nachrichtendienste in Theorie und Praxis“
Sommersemester 2014	Bachelor-Seminar „Cybersicherheitspolitik“
Wintersemester 2013/2014	Bachelor-Seminar „Die Rolle der Nachrichtendienste in Theorie und Praxis“

Köln, den 19.07.2019

Verena Diersch