
Das Politikfeld Innere Sicherheit

Jens Lanfer

- 1 Einführung
- 2 Politikfeld Innere Sicherheit: Aufgabenfelder im Überblick
 - 2.1 Das Aufgabenfeld ‚Polizei‘
 - 2.1.1 Typischer Programmmodus
 - 2.1.2 Typische Implementationsstruktur
 - 2.2 Das Aufgabenfeld ‚Verfassungsschutz‘
 - 2.2.1 Typischer Programmmodus
 - 2.2.2 Typische Implementationsstruktur
 - 2.3 Das Aufgabenfeld ‚Bevölkerungsschutz‘
 - 2.3.1 Typischer Programmmodus
 - 2.3.2 Typische Implementationsstruktur
- 3 Zwischenresümee: Aufgabenstrukturen des Politikfelds im Wandel
- 4 Strukturentwicklungen in den Aufgabenfeldern
 - 4.1 Videoüberwachung öffentlicher Räume
 - 4.2 Cyber-Sicherheit
- 5 Fazit

1 Einführung

Die politische Teilfunktion der Sicherheitsgewährleistung ist eine der ältesten des politisch-administrativen Systems. Nach Thomas Hobbes ist es die grundlegendste Konstitutionsbedingung des Staates überhaupt (Hobbes 2006), sodass der Gewährleistung und Herstellung von Sicherheit für das staatliche Handeln eine hohe Legitimationskapazität zukommt. Die Sicherheitsgewährleistung ist damit eine zentrale Aufgabe des modernen Staates und bringt das staatliche Gewaltmonopol öffentlich (sichtbar) zum Ausdruck. Die tatsächliche Anwendung von physischer Gewalt im Sinne eines körperlichen Zwangs und die Einschränkung von Grundrechten für die Sicherheitsgewährleistung (= Sicherheits-

herstellung) ist weit intensiver und häufiger als bei anderen staatlichen Aufgaben. Das politisch-administrative System erscheint der Bürgerschaft in der Sicherheitspolitik am eindrucklichsten als Staat; vor allem in Form des offen wahrzunehmenden „handelnden Staates“ (Groß 2008: 20) in Gestalt der Polizei. Insofern symbolisiert die Innere Sicherheit die Handlungsfähigkeit des Staates wie kein anderes Politikfeld und ist für die Legitimation (insbesondere die Output-Legitimation) des Staates insgesamt weiterhin und auch zunehmend von großer Bedeutung.

Die Gewährleistung von Sicherheit ist als staatliche Aufgabe nach innen und außen gerichtet. Zu unterscheiden sind demnach grundsätzlich zwei staatliche Teilfunktionen im Sinne der „Inneren“ und der „äußeren Sicherheit“ (vorher „Verteidigungspolitik“). Beide Teilfunktionen bilden entsprechend Politikfelder aus, die sich durch die jeweils spezifischen Problembe- und -verarbeitungsstrukturen über die Zeit evolutiv aus dem politischen System ausdifferenzieren. Sehr allgemein betrachtet ähneln sie sich strukturell auf vielfältige Weise, wie vor allem durch die regelmäßige Androhung und Anwendung staatsmonopolisierter physischer Gewalt. Beide Funktionen werden auch überwiegend durch staatliche Sicherheitsbehörden gewährleistet, sodass die allgemeinen Strukturen beider Politikfelder typisch staatszentriert sind und die Sicherheitsgewährleistung sowohl der inneren als auch der äußeren Sicherheit in Deutschland und in vielen anderen Staaten grundsätzlich „Hausgut der Exekutiven“ sind. So ist in Deutschland das Recht der Inneren Sicherheit entsprechend Verwaltungsrecht und nach Art. 33 Abs. 4 GG regelmäßig von Beamten wahrzunehmen (Gusy 2012: 248). Formal- institutionell sind jedoch beide staatlichen Funktionen bis auf wenige Ausnahmen (etwa die Bedingungen für den Einsatz der Bundeswehr im Inneren) strikt getrennt, auch wenn es zunehmend zu Verzahnungen der Problemperspektiven und damit zu Abstimmungen der Politikfeldstrukturen im Rahmen einer ‚erweiterten Sicherheitsgewährleistung‘ (grundlegend: Daase 2010) kommt.

Die weitere Beschreibung bezieht sich auf das Politikfeld der Inneren Sicherheit. Deren Teilfunktion ergibt sich aus der Abwehr von Gefahren für die nationale öffentliche Sicherheit und Ordnung und der strafrechtlichen Verfolgung von Verstößen. Auch wenn hieraus für den Staat hohe politische Legitimationskapazitäten hervorgehen, sind mit den staatlichen Sicherheitsaufgaben gleichzeitig auch hohe Legitimationsanforderungen verbunden. Denn neben der Sicherheitsherstellung *durch* den Staat umfasst diese Aufgabe auch (oder in modernen demokratischen Verfassungsstaaten sogar vorrangig) die Sicherheit *vor* dem Staat. Die Intensität und Häufigkeit der grundrechtsbeschränkenden Maßnahmen zur Herstellung von Sicherheit erfordern somit regelmäßig staatliche Ermächtigungsgrundlagen in Form eines Gesetzes und nicht lediglich durch exekutive Rechtsverordnungen oder Verwaltungsakte. Dadurch werden dem Staat ‚Hürden‘ gesetzt, die die Bürgerrechte vor einem übermäßigen und unverhältnismäßigen staatlichen Engagement schützen sollen. Es besteht also ein Spannungsverhältnis zwischen den zentralen Politikfeldwerten ‚Freiheit‘ und ‚Sicherheit‘. Sie oszillieren, ohne nach einer Seite aufgelöst werden zu können, sodass einzelne sicherheitspolitische Strukturen – mit größerer Reichweite vor allem Sicherheitsprogramme – zwischen den Anforderungen, die beide Wertprämissen stellen, ausbalanciert werden müssen. Insgesamt erscheint die Sicherheitsgewährleistung vor dem

Hintergrund dieses Wertduals sowohl als grundlegende staatliche Legitimationsgrundlage als auch gleichzeitig als hochsensibles Terrain staatlichen Engagements. Sie kennzeichnet sich somit durch eine nicht auflösbare und immer wieder neu auszuformende strukturelle Ambivalenz und kann deshalb metaphorisch treffend als ‚janusköpfig‘ bezeichnet werden (hierzu allgemein: Grunow 2009: 354). Durch diesen Grundkonflikt – oder mit anderen Worten: Problem- oder Kontingenzformel – des Politikfelds lässt sich das Wesen einer nationalen Sicherheitsgewährleistung immer zwischen den beiden sich wechselseitig ermöglichenden und beschränkenden Anforderungen einer *Herstellung von ‚kollektiver Sicherheit‘ (durch den Staat) und ‚individueller Sicherheit‘ (vor dem Staat)* verorten. An diesem Wertdual orientieren sich dann auch die Wertpräferenzen (Grundüberzeugungen) und konkrete Erwartungen und Interessen (Policy-Überzeugungen) politischer Akteure des Politikfelds, die deutungsmächtig das ausformen, was Sicherheit ist. Äquivalent zum Wertdual des Politikfelds strukturieren sich die Überzeugungen der Akteure im Politikfeldvergleich relativ übersichtlich durch zwei zentrale Akteurskoalitionen (allgemein Sabatier 2007, Sack 2013, Lanfer 2014), die gemäß ihren individuellen oder institutionellen Kernüberzeugungen einen von beiden Wertausprägungen stärker betonen und somit für einen politischen (Dauer-)Konflikt im Politikfeld sorgen.

Neben diesem Überzeugungskonflikt, durch den sich Problemperceptionen und Problemlösungen ideologisch gegenüberstehen, wird das Politikfeld auch durch einen Institutionenkonflikt geprägt. Dieser entzündet sich an einer strikten Institutionenabgrenzung im politischen Mehrebenensystem des Politikfelds zwischen den formalen legislativen und exekutiven Zuständigkeiten und Kompetenzen der politischen Ebenen (vor allem zwischen Bund und den Ländern, aber auch zwischen den Ländern und ihren Kommunen) zur Sicherheitsgewährleistung und der zunehmend erforderlichen Ressourcenverzahnung für die Aufgabenwahrnehmung.

Im Weiteren wird die Gewährleistung von Innerer Sicherheit durch die typischen Problem- und Problemlösungsstrukturen (Programmodus, Implementationsarrangements) der verschiedenen zentralen Aufgabenfelder Polizei, Verfassungsschutz und Bevölkerungsschutz vergleichend beschrieben. Auch wenn die Aufgabenfelder viele Strukturspezifika aufweisen, lassen sie sich durch die anleitende Politikfeldfunktion der Gewährleistung von Innerer Sicherheit und die dadurch ermöglichten Strukturverflechtungen als Teile des Politikfelds identifizieren. Erst vor dem Hintergrund der Aufgabenfelder können allgemeine Aussagen über den ‚Zustand‘ des Politikfelds insgesamt formuliert werden (Kapitel 2), um die grundlegenden Prozesse des gegenwärtigen Politikfeldwandels zu erfassen (Kapitel 3). Letztlich werden die Ambivalenzen der typischen Politikfeldstruktur und die sich vollziehenden Änderungsprozesse im Politikfeld exemplarisch an zwei Policies illustriert. Die Policy ‚Videoüberwachung öffentlicher Räume‘ bezieht sich dabei speziell auf den Wandel im Aufgabenfeld der Polizei und die Policy ‚Cyber-Kriminalität‘ tangiert sämtliche Aufgabenfelder und zeigt Potenziale für ein gänzlich neues Aufgabenfeld des Politikfelds (Kapitel 4).

2 Politikfeld Innere Sicherheit: Aufgabenfelder im Überblick

Die politische Funktion der Sicherheitsgewährleistung hat vielfältige sicherheitspolitische Aufgaben hervorgebracht, die seit Beginn der Bundesrepublik zu verschiedenen institutionellen Aufgabenfeldern im Politikfeld der Inneren Sicherheit geführt haben. Dies sind die Polizei, der Verfassungsschutz und der Bevölkerungsschutz. Sie unterscheiden sich hinsichtlich der für sie typischen Problem- und Problemlösungsstrukturen. Auf dieser Grundlage eint sie die teilweise aufgabenübergreifend tätigen politischen, administrativen und zivilgesellschaftlichen Akteure und Akteursnetzwerke sowie die miteinander mehr oder weniger stark verflochtenen sicherheitspolitischen Programme.¹ Die Strukturen der Aufgabenfelder und ihre Strukturverflechtungen werden im Weiteren beschrieben.

2.1 Das Aufgabenfeld ‚Polizei‘

Das Aufgabenfeld der Polizei unterteilt sich in Deutschland institutionell in die Polizeien der Länder und des Bundes. Es ist somit in staatlicher Hand. Auch wenn die amerikanischen und britischen Besatzungsmächte in der Nachkriegszeit die angelsächsische Polizeitradition etablieren wollten, indem sie zunächst die Sicherheitsgewährleistung stärker subsidiär als kommunale Aufgabe institutionalisierten (Lange/Frevel 2008: 128), setzte sich dieses Prinzip vor allem aufgrund der ausgeprägten deutschen Tradition einer staatlich organisierten Polizei (bereits im preußischen Landrecht im Jahr 1794 – Gusy 2012: 247) nicht durch. Während die Kommunen durch ihre ‚Ordnungsbehörden‘ von den meisten Ländern weiterhin mit der allgemeinen und abstrakten Gefahrenabwehr beauftragt und/oder weisungsgemäß verpflichtet werden (bspw. das Melde-, Ausländer-, Immissionschutzrecht, Bau- und Gewerbeaufsicht), verbleibt die Polizei in der Verwaltung der Länder.

Das Aufgabenfeld der Länderpolizeien bildet im Politikfeld quasi das „Rückgrat des staatlichen Gewaltmonopols“ (Groß 2008: 20). Neben dem Kulturbereich ist dieses sicherheitspolitische Aufgabenfeld die bedeutendste Kompetenz der Länder. Die Länder haben für die polizeilichen Aufgaben im Bereich der Gefahrenabwehr sowohl die Gesetzgebungs- als auch Aufgabenkompetenz. Beides wird in den Polizei- und Ordnungsgesetzen der Länder rechtlich geregelt. Der Bund hat hingegen die Gesetzgebungskompetenz für die

1 Die Aufgabenfelder lassen sich auch als *strukturelle Interdependenzunterbrecher* im Politikfeld beschreiben. Ein Aufgabenfeld bildet zwar eine Politikfeldstruktur zum gleichzeitigen Gebrauch in den beiden anderen Aufgabenfeldern, aber die Bedingungen, in welcher Weise die Struktur über das Aufgabenfeld hinaus im Politikfeld Anwendung findet, ist von den institutionellen und strukturellen Arrangements des bereitstellenden Aufgabenfelds abhängig. Über die drei hier relevanten Aufgabenfelder hinaus lässt sich diskutieren, ob und wie der Zoll (Lange/Frevel 2008: 123f.) und die kommunalen Sicherheitsbehörden (unter vielen etwa Lanfer 2012) in den Aufgabenfeldern eingebunden sind oder ob vor allem letztere nicht bereits ein eigenständiges Aufgabenfeld infolge einer neuen deutschen Sicherheitsarchitektur (vgl. Kap. 3 und 4) ausbilden. Diese sehr facettenreiche Fachdiskussion kann in diesem Beitrag aber nicht geführt werden.

Strafprozessordnung und regelt damit die polizeiliche Straftatenverfolgung. Der Aufgabenbereich ‚Polizei‘ differenziert sich somit funktional nach diesen beiden grundlegenden und voneinander institutionell relativ strikt abgegrenzten Bereichen aus. Die Abwehr von Gefahren bezog sich traditionell auf die *konkrete* Gefahrenabwehr. Insofern war und ist der materielle Kernpunkt der Polizeigesetze in allen Ländern „die polizeiliche Generalklausel: Die Polizeibehörden können die erforderlichen Maßnahmen treffen, um eine im einzelnen Falle bestehende Gefahr für die öffentliche Sicherheit und Ordnung abzuwehren.“ (Bäuerle 2008: 15 f.) Hingegen ist bei der Straftatenverfolgung der Verdacht einer Straftat Auslöser des polizeilichen Handelns. Es gilt das Legalitätsprinzip: Die Polizei muss bei Verdacht die Straftaten verfolgen. Dabei ist sie in ein justizförmiges Verfahren eingebunden und der Weisungsbefugnis durch die Staatsanwaltschaft als Herrin des Verfahrens unterworfen (ebd.: 15).

In allen Ländern haben sich Landeskriminalämter (LKÄ) gebildet, die wie die anderen Polizeibehörden den Innenministerien unterstellt sind. Die Landeskriminalämter unterstützen die nur in regionaler Zuständigkeit handelnden Kreispolizeibehörden bei der Kriminalitätsvorbeugung und Strafverfolgung, spezialpolizeilichen Aus- und Fortbildung, Kriminaltechnik sowie durch eine zentrale und einheitliche Informationserhebung, -verarbeitung, -auswertung und -steuerung von Kriminalitätsangelegenheiten.

Während die Sicherheitsherstellung im Aufgabenfeld ‚Polizei‘ somit bereits früh und dominant durch die Länder geleistet wurde und wird, haben sich auf der Bundesebene ergänzende Strukturen ausgebildet. Gegen die Vorbehalte der Alliierten zu Beginn der 1950er Jahre, die eine erneute zentralstaatliche Polizeimacht verhindern wollten, gründete sich der Bundesgrenzschutz mit dem politischen Motiv, einen Bürgerkrieg im Falle eines Angriffs durch eine ‚kommunistische Macht‘ abwehren zu können. Vor diesem Hintergrund wurde eine Polizei des Bundes als Bundesgrenzschutz (BGS) paramilitärisch ausgerüstet, die nunmehr als funktionales Äquivalent zur Bundeswehr für Aufgaben im Inneren fungierte, weil letztere hierfür nicht zur Verfügung steht (Lange/Frevel 2008: 116). Der BGS wurde in den 1970er Jahren verstärkt zu Großeinsätzen wie Demonstrationen hinzugezogen. Er re-organisierte sich im Zuge der deutschen Wiedervereinigung und europäischen Integration aufgrund des Wegfalls von ost- bzw. westdeutscher Grenzkontrollen infolge des sich stetig vergrößernden Schengen-Raums und erweiterte über die Zeit – aber insbesondere nach dem Terroranschlag in New York am 11. September 2001 – kontinuierlich seine bundespolizeiliche Kompetenzen. Von einer paramilitärischen Bundesbehörde mit einer Spezialaufgabe entwickelte sich der BGS im Laufe der Zeit zu einer zivilen Institution mit einem weiten und insbesondere die Länderpolizei unterstützenden Aufgabenspektrum. In diesem Sinne umfasst sein Aufgabenbereich die komplette Bandbreite polizeilicher Tätigkeit im Bereich der Gefahrenabwehr und Straftatenverfolgung. Zu seinen primären Aufgaben gehören aktuell „der grenzpolizeiliche Schutz des Bundesgebietes, die Gefahrenabwehr auf dem Gebiet der Bahnanlagen, der Schutz vor Angriffen auf die Sicherheit des Luftverkehrs, der Schutz von Bundesorganen, internationale Polizeieinsätze sowie die Unterstützung anderer Bundesbehörden“ (Schenck 2006: 36). Außerdem gehören zu den klassischen schutzpolizeilichen Aufgaben mittlerweile wie selbstverständlich auch die

Kriminalitätsbekämpfung, internationale Angelegenheiten sowie die europäische Zusammenarbeit (Lange/Frevel 2008: 118). Aufgrund dieses Aufgabenprofils entwickelte sich eine polizeiliche Bundesorganisation, die am 1. Juli 2005 auch konsequent in ‚Bundespolizei‘ (BPol) umbenannt wurde.

Das Bundeskriminalamt (BKA) ist eine Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei (Art. 73 Nr. 10a i. V. m. Art. 87 Abs. 1 GG) in Hoheit des Bundes. Es hat die Aufgabe, die Polizeien der Länder und des Bundes bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung wie international organisierten Rauschgift-, Waffen- und Falschgelddelikten und terroristischen Anschlägen gegen Verfassungsorgane des Bundes zu unterstützen (Lange/Frevel 2008: 119) und dabei alle relevanten Informationen zu sammeln und auszuwerten. In diesem Rahmen unterhält das BKA erkennungsdienstliche Einrichtungen (Fingerabdrucksysteme und DNA-Analysedatei) und erbringt forschend/ermittelnd polizeiliche Erkenntnisse in kriminalpolizeilichen Spezialgebieten und im Bereich der Kriminaltechnik. Hervorzuheben sind die Aufgaben des BKA im Bereich des internationalen Dienstverkehrs mit Polizeibehörden anderer Staaten, die im Zuge der europäischen Kooperation und Koordination von administrativen Sicherheitsherstellungen zunehmend wichtiger werden und bei denen dem BKA die exklusive Aufgabe einer zentralen nationalen Koordinationsstelle – vor allem auch im Hinblick auf die LKÄ – zukommt (Lisken/Lange 2000: 152-154).

Im Aufgabenfeld der Polizei sind die polizeilichen Kriminalstatistiken (PKS) von anleitender Bedeutung. Sie sollen die Problemperzeptionen und Problemlösungsorientierung objektivieren und bilden regelmäßig die Grundlage für die Erfolgszurechnung polizeilichen Handelns und Entscheidens. In der Tabelle 1 werden exemplarisch die Anzahl ausgewählter Straftaten im Zeitverlauf der Jahre 2009 bis 2014 und ihre jeweilige Aufklärungsquote sowie die Anzahl der Polizeibeamten der Jahre 2009 bis 2012 dargestellt. Die Auswahl der Straftaten bezieht sich einerseits auf die Straßenkriminalität, die in der Kommune zu Unsicherheitsgefühlen der Bürger führt (vgl. hierzu Kapitel 4.1) und andererseits auf Cybercrime im engeren Sinne (Kriminalität in Bezug auf die Informations- und Kommunikationstechnologie), die der Policy Cyber-Sicherheit zunehmende Relevanz im Politikfeld zukommen lässt (hierzu Kapitel 4.2). Insbesondere bei der IuK-Kriminalität im engeren Sinne (Cybercrime) besteht ein vergleichsweise sehr großes Dunkelfeld, weil die Straftaten häufig nicht zur Anzeige gebracht werden. Nach dem Bundeslagebild ‚Cybercrime‘ (Bundeskriminalamt 2014: 5, 2013: 10) sei von einem Dunkelfeld von 91 % aller Cybercrime-Straftaten auszugehen.

Tab. 1 Entwicklung der Anzahl ausgewählter Straftaten, die unter die Straßenkriminalität subsumiert werden können (sortiert nach Aufklärungsquote), der Höhe der jeweiligen Aufklärungsquote und der Anzahl von Polizeibeamten im Zeitraum der Jahre 2009–2014

	2009	2010	2011	2012	2013	2014
Vorsätzliche leichte Körperverletzung	369.709 90,3 %	372.950 90,5 %	374.367 90,8 %	383.928 90,6 %	378.747 90,9 %	374.576 91,1 %
Gefährliche und schwere Körperverletzung	149.301 82,2 %	142.903 82,3 %	139.091 82,5 %	136.077 80,7 %	127.869 82 %	125.752 81 %
Straftaten gegen die sexuelle Selbstbestimmung	49.084 79,7 %	46.869 78,9 %	47.078 79,5 %	45.824 78,6 %	46.793 79,5 %	46.982 78,5 %
Raubdelikte	49.317 52,6 %	48.166 52,6 %	48.021 52,7 %	48.711 51 %	47.234 51,7 %	45.475 51,6 %
Diebstahldelikte (ohne erschwerende Umstände)	1.235.880 43,8 %	1.233.812 42,9 %	1.290.502 40,8 %	1.281.299 39,2 %	1.298.545 38,1 %	1.322.144 37,5 %
Sachbeschädigung	775.547 25 %	700.801 25,5 %	688.294 25,2 %	673.704 24,7 %	621.699 25,1 %	601.112 24,9 %
Diebstahldelikte unter erschwerenden Umständen	1.108.766 14,9 %	1.067.974 15,1 %	1.113.279 15 %	1.098.426 14,8 %	1.084.198 14,8 %	1.117.916 14,7 %
Straßenkriminalität gesamt ²	1.435.655 18,7 %	1.352.897 18,6 %	1.382.949 17,7 %	1.357.134 17,4 %	1.309.807 17 %	1.342.905 16,5 %
IuK-Kriminalität im engeren Sinne (Cybercrime)	50.254 35,2 %	59.839 33 %	63.959 30 %	59.494 26,5 %	64.426 25,3 %	49.925 ³ 29,3 %

- 2 Als Straßenkriminalität definiert das Bundesministerium des Innern (2015: 60, Fn. 18) in der polizeilichen Kriminalstatistik die folgende Delikte: Vergewaltigung und sexuelle Nötigung; exhibitionistische Handlungen und Erregung öffentlichen Ärgernisses; Raub, räuberische Erpressung auf/gegen Geld- und Werttransporte; räuberischer Angriff auf Kraftfahrer; Raubüberfälle auf Straßen, Wegen und Plätzen; gefährliche und schwere Körperverletzung auf Straßen, Wegen und Plätzen; erpresserischer Menschenraub und Geiselnahme i. V. m. Raubüberfall auf Geld- und Werttransporte; Diebstahl an/aus Kraftfahrzeugen; Taschendiebstahl; Landfriedensbruch; Sachbeschädigung auf Straßen, Wegen und Plätzen; einfacher und schwerer Diebstahl von/aus Automaten; einfacher und schwerer Diebstahl von Mopeds und Krafträdern; einfacher und schwerer Diebstahl von Kraftwagen (einschließlich unbefugte Ingebrauchnahme).
- 3 Zur deutlichen Reduktion der Straftaten und Steigerung der Aufklärungsquote heißt es in der polizeilichen Kriminalstatistik für das Jahr 2014 (Bundesministerium des Innern 2015: 3): „In der Polizeilichen Kriminalstatistik (PKS) ist die Anzahl der auf Cybercrime entfallenden Straftaten für das Jahr 2014 gegenüber den Vorjahren im Bundesdurchschnitt deutlich geringer, zugleich sind die Aufklärungsquoten gestiegen. Diese statistischen Aussagen sind auf veränderte Erfassungsmodalitäten in der PKS zurückzuführen: Bis einschließlich 2013 erfasste die Mehrzahl der Länder Cybercrime-Delikte mit einem Schadensereignis in Deutschland (beispielsweise mit Schadsoftware befällener Rechner oder Betrugsopfer in Deutschland), auch wenn unbekannt war, ob sich die kriminelle Handlung im In- oder Ausland ereignet hatte. Für das Jahr 2014 wurde damit begonnen, Delikte der Cybercrime bundeseinheitlich nur noch in der PKS zu erfassen, wenn konkrete Anhaltspunkte für eine Tathandlung innerhalb Deutschlands vorliegen. Die Zahlen der PKS des Jahres 2014 zum Phänomen Cybercrime bilden insofern keine Bezugsgröße und keinen Vergleichsmaßstab für die zurückliegenden Jahre. Auf der Grundlage der für das Jahr 2014 ausgewiesenen Zahlen darf nicht auf eine rückläufige Bedrohung durch Straftaten der Cybercrime geschlossen werden.“

	2009	2010	2011	2012	2013	2014
Straftaten in Deutschland insgesamt	6.054.330	5.933.278	5.990.679	5.997.040	5.961.662	6.082.064
	55,6 %	56 %	54,7 %	54,4 %	54,5 %	54,9 %
Anzahl der Polizeibeamten	245.752	243.625	243.201	243.982	kein Beleg	kein Beleg

Quelle: Bundesministerium des Innern (2010, 2011b, 2012, 2013, 2014, 2015), Anzahl der Polizeibeamten nach Eurostat (2014)

2.1.1 Typischer Programmmodus

Das Aufgabenfeld ‚Polizei‘ im Politikfeld der Inneren Sicherheit ist so wie kein anderes rechtlich klar und eindeutig reguliert – jedenfalls dann, wenn sich die polizeilichen Maßnahmen auf konkrete Adressaten (vor allem zustandsstörende oder verdächtige Personen) beziehen. Auch wenn sich die polizeilichen Kompetenzen im Polizeirecht deutlich erweiterten, zeichnet es sich auch heute noch durch ein rechtliches Regime aus, das darauf ausgelegt ist, polizeiliche Willkür durch eine klare und zurechenbare rechtsstaatliche Fundierung (wie vor allem Gesetzesvorrang, Verhältnismäßigkeit, Bestimmtheit) zu verhindern, ihr Einschreiten auf die Abwehr konkreter Gefahren und im Verhältnis zu anderen Behörden mit einer nur subsidiären Zuständigkeit zu beschränken und dadurch die Freiheit des Einzelnen weitgehend zu sichern (Bäuerle 2008: 15). Dies hat seinen Grund vor allem darin, dass von keinem anderen Teil der Staatsgewalt „so weit gehende Zugriffsmöglichkeiten auf die grundrechtlich geschützten Bereiche der Bürgerinnen und Bürger“ bestehen (ebd.: 14). Die Balance zwischen Freiheit und Sicherheit zeichnet sich in Deutschland lange Zeit durch die relativ starke Betonung des Wertes der ‚individuellen Freiheit‘ bzw. der Sicherheit *vor* dem Staat aus. Wird das Legitimationsniveau der Polizei auf das gemessene Institutionenvertrauen reduziert, erreicht es regelmäßig hohe Werte. Als Programmmodus typisch sind für das Aufgabenfeld somit bis heute die *regulativen Programme* im Sinne von eindeutigen Ge- und Verbotsnormen der Polizeigesetze und der Strafprozessordnung, die das Handeln der Polizeien von Bund und Ländern relativ strikt konditionieren. Über die rechtliche Regulierung des hoheitlichen Handelns gegenüber einem bestimmten Adressaten hinaus waren und sind stets auch andere Programmformen wie insbesondere die Anreiz-, Informations- und Steuerungsprogramme von Bedeutung, die allerdings als Verwaltungsprogramme nur die Behörden binden und nur eine indirekte Wirkung auf die Adressaten polizeilichen Handels haben. Insofern gewährleisten und ergänzen sie administrativ die dominanten regulativen Programme. Sie beziehen sich einerseits überwiegend auf die organisatorischen Bedingungen zur polizeilichen Sicherheitsherstellung, wie aufgabenspezifische Prioritätensetzung und Koordination mit anderen Sicherheitsbehörden, und andererseits gegenüber den Adressaten vornehmlich auf Verhaltens- und Sicherheitshinweise für eine Straftatenvorbeugung (Eigentumssicherung, Opferschutz, Verkehrserziehung etc.).

2.1.2 Typische Implementationsstruktur

Bei der institutionellen Ausformung der Gefahrenabwehr sind die 16 Bundesländer vergleichbar. Sie übertragen der Polizei subsidiär die Abwehr von konkreten Gefahren, weil die originär zur Gefahrenabwehr zuständigen kommunalen Behörden aufgrund von mangelnden Ressourcen (insbesondere fehlenden Außendienstmitarbeitern) hierzu nicht oder nicht rechtzeitig in der Lage sind. Wesentliche Unterschiede zwischen den Ländern zeigen sich aber auf der Organisationsebene insbesondere zwischen jenen Ländern, die aus dem ehemaligen Preußen hervorgegangen sind und den süddeutschen Ländern. Erstere wenden das Trennsystem zwischen der aufgabenspezifisch eng gefassten polizeilichen Tätigkeit und den Ordnungsbehörden an. Vor allem in Nordrhein-Westfalen (NRW) zeigt sich diese Trennung deutlich durch zwei verschiedene Ermächtigungsgrundlagen (Polizeigesetz und Ordnungsbehördengesetz) für die Sicherheitsbehörden von Land und Kommunen. Letztere wenden ein Mischsystem an, das beide Aufgabenbereiche institutionell der Polizei zuordnet, diese aber organisatorisch voneinander trennt (Lange 2003: 228) – so etwa in Hessen durch das einheitliche Gesetz über die öffentliche Sicherheit und Ordnung (HSOG). Diese zunächst unscheinbar wirkende Unterscheidung kann jedoch bei der Gefahrenabwehr durchaus gewichtige Abweichungen bei der Implementationsstruktur im politischen Mehrebenensystem hervorbringen.

Die Länderpolizeien unterstehen in den Bundesländern den Landesinnenministerien bzw. den Innensenatoren. Die Polizeien der Länder unterteilen sich in den grundlegenden Sparten nach Schutz- und Kriminalpolizei. Weitere Unterteilungen erfolgen nach Spezialbereichen wie Autobahnpolizei, Wasserschutzpolizei und Bereitschaftspolizei (Lange/Frevel 2008: 128). Zwar variieren die konkreten organisatorischen Ausformungen je nach Bundesland stark, aber tendenziell konzentrieren sich die verschiedenen Bereiche in ähnlicher Weise in einer einheitlichen Behördenstruktur als „in den lokal ansässigen Kreispolizeibehörden oder im größeren geografisch angelegten Zuschnitt in Gestalt von Direktionen oder regionalen Polizeipräsidien.“ (Ebd.) Ähnliche Organisationsstrukturen finden sich auch bei der Bundespolizei, die an ihrer Spitze durch das Bundesministerium des Innern als oberste Bundesbehörde und ein Polizeipräsidium als Bundesoberbehörde mit Sitz in Potsdam organisiert ist. Die Aufgabe des Polizeipräsidiums ist die Dienst- und Fachaufsicht und die strategische Steuerung der ihr untergeordneten neun Bundespolizeidirektionen. Die operativen Aufgaben der Polizeidirektionen sind regional begrenzt bzw. orientieren sich an den Grenzen der Bundesländer. Ihnen unterstehen insgesamt 77 Bundespolizeiinspektionen (Lange/Frevel 2008: 118).

Das typische Implementationsarrangement des Aufgabenfelds ‚Polizei‘ kann folgendermaßen charakterisiert werden: Das Implementationsfeld zeichnete sich lange durch eine *stark homogene* Struktur aus, weil die Sicherheitsherstellung alleine von den Polizeien der Länder und des Bundes erfolgte. Gleichzeitig ist es *geschlossen*, weil die polizeilichen Maßnahmen gegenüber den Adressaten häufig ohne Beteiligung Dritter durchgesetzt werden. Beide Ausprägungen kennzeichnen die Be- und Verarbeitung der Sicherheitsherstellung als weitgehend staatszentriert. Zudem erfolgt die polizeiliche Aufgabendurchführung durch

eine klare hierarchische Über- und Unterordnung, beginnend bei den Innenministerien des Bundes oder der Länder bis in die regionale und örtliche Aufgabendurchführung in den Polizeiinspektionen. Diese ausgeprägte *vertikale Integration* der Implementation ermöglicht zudem eine ‚top down‘-Steuerung aus den Innenministerien, die durch regulative Rechtsnormen als auch interne Dienstanweisungen (bspw. VV PolG NRW) gesichert ist. Aber dennoch zeigen sich Möglichkeiten der Behördenleitungen und Polizeipräsidenten, Aufgabenschwerpunkte zu setzen. In diesem Rahmen kann sich die Polizeiarbeit häufig stark selbst steuern, indem sie je nach Organisation und Führung und vor allem abhängig von deren politischer Ressourcenausstattung (finanzielle Mittel, Einfluss auf die Politik, Journalisten, Sicherheitsexperten etc.) verschiedene formale und informale Koordinationen und Kooperationen verfolgt und die Prioritätensetzung für spezifische Sicherheitsprobleme und deren Lösungen infolge einer ausgeprägten administrativen Fachexpertise und auch mithilfe von ‚Fachbruderschaften‘ selbst prägt. Die Möglichkeit der Selbststeuerung ist hier im Vergleich zu Politikfeldern mit gleichartigen Implementationsarrangements, wie der Arbeitsmarktpolitik, sicherlich stärker gegeben. Aufgrund dieser mehr oder weniger starken und vor allem policy-abhängigen Autonomie polizeilicher Selbststeuerung lassen sich die vertikale Integration, Zentralität und Konzentration der polizeilichen Implementationsstruktur in den jeweiligen Ländern und im Bund nur als hoch einordnen und erreichen keine sehr hohen Ausprägungen oder sogar Extremwerte. Die Kontroll- und Steuerungsfähigkeit der Innenministerien ist entsprechend aufgrund der ausgeprägten kontext- und situationsbezogenen Selbstprogrammierung der Polizeiorganisationen und des Polizeipersonals begrenzt. Letztlich zeigt sich die Implementationsstruktur typisch *politikfern*. Durch die regulativen Programme und das stark ausgeprägte vertikal-integrierte und relativ ausgeprägte zentral-konzentrierte Arrangement erhöht sich zwar die politisch zielgenaue, zurechenbare und parlamentarisch kontrollierbare Programmierung. Sie führen aber auch dazu, dass sich die polizeiliche Aufgabenwahrnehmung gegen politische Einflüsse während der Implementation immunisieren. Das Implementationsfeld charakterisiert sich somit nicht nur als staatszentriert, sondern auch als ausgeprägt verwaltungsdominant (Lanfer 2012).

2.2 Das Aufgabenfeld ‚Verfassungsschutz‘

Ein weiteres Aufgabenfeld zur Gewährleistung von Innerer Sicherheit ist der Verfassungsschutz als inländischer ‚Geheimdienst‘.

Der sehr allgemeine Auftrag oder eher die Mission (Daun 2009: 64) des Verfassungsschutzes besteht „in dem Schutz der freiheitlich demokratischen Grundordnung, des Bestandes und der Sicherheit des Bundes und Länder“ (§ 1, Abs. 1 BVerfSchG) (ebd.). Ausgeformt wird dieser Anspruch durch Sammlung und Auswertung von sach- und personenbezogenen Informationen (Auskünfte, Nachrichten, Dokumenten) zu den folgenden gesetzlich festgelegten Aufgabenbereichen:

- „Verfassungsfeindliche oder die Sicherheit des Bundes oder eines Landes gefährdende Bestrebungen;
- sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht;
- Bestrebungen, die durch die Anwendung von Gewalt oder entsprechenden Vorbereitungshandlungen auswärtige Belange der Bundesrepublik gefährden;
- Bestrebungen gegen den Gedanken der Völkerverständigung, insbesondere gegen das friedliche Zusammenleben der Völker.“ (Murck 2009: 186)

In diesem Sinne erschöpft sich der Auftrag des Verfassungsschutzes in einer Informationsfunktion und dient als ‚Frühwarnsystem‘ für den Staat über solche Aktivitäten, die gegen die staatlich-institutionelle Ordnung gerichtet sind. Durch die Prozesse und Strukturen des Aufgabenfeldes werden Problemperceptionen erzeugt und allgemein Wissensbestände zur Sicherheitsgewährleistung geschaffen. Zur Aufgabenerfüllung verwendet der Verfassungsschutz auch „Methoden und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen“ (§ 8 BVerfSchG). Zudem haben die Behörden im Einzelfall Zugriff auf diverse vom Bund geführte Datenbanken (Ausländerzentralregister, Asylanten, Fahrzeugregister etc.) und können auch bei privatwirtschaftlichen Organisationen Auskünfte einholen (beispielsweise bei Luftfahrtunternehmen, Telekommunikationsdienstleistern, Kreditinstituten), wenn tatsächliche Anhaltspunkte für den Verdacht auf verfassungs- oder sicherheitsgefährdende Aktivitäten vorliegen (ebd.: 65).

Auch der Verfassungsschutz folgt dem relativ strikten föderalen Trennungsprinzip zwischen der Bundes- und der Landesebene im Politikfeld. Demnach unterhält jedes Land ein Landesamt für Verfassungsschutz (LfV). Sie sind dem jeweiligen Innenministerium unterstellt. Daneben besteht ein Bundesamt für Verfassungsschutz (BfV) des Bundesinnenministeriums. Während die Länder mit den Verfassungsschutzaufgaben betraut sind, darf der BfV grundsätzlich nur koordinierend tätig werden (Baumann 1997: 10), wenn das Sicherheitsproblem mehrere Bundesländer umfasst oder einen andersweiten Bundesbezug aufweist (Daun 2009: 65). Aber auch dann muss sich das Bundesamt mit den Landesämtern koordinieren bzw. erhält Auskünfte nur im Benehmen mit den Landesbehörden. Die Koordination erfolgt seit Anfang der 1970er Jahren insbesondere durch ein nachrichtendienstliches Informationssystem (NADIS) als ein elektronisches Aktenregister, das Daten zu bereits auffällig gewordenen Personen und Organisationen beinhaltet (Schütte 2006: 23).

Grundlegend für die Aufgabenerledigung des Verfassungsschutzes ist seine Trennung von der Polizei. Das Trennungsgebot geht auf den prägenden Einfluss der Alliierten (Polizeibrief vom 14.04.1949 an den Parlamentarischen Rat) zurück. Demnach darf der Verfassungsschutz keiner polizeilichen Dienststelle angegliedert werden (Kutscha 2006: 338), hat keine polizeilichen Zwangsanwendungsbefugnisse, gegenüber der Polizei keinerlei Weisungsbefugnisse und darf ihr auch nicht „im Wege der Amtshilfe um Maßnahmen ersuchen, zu denen es selbst nicht befugt ist.“ (§ 8 Abs. 3) In Abgrenzung zur Polizei lässt sich pointiert festhalten, dass die Polizei gegenüber der Öffentlichkeit ‚offen‘ und der Verfassungsschutz hingegen geheim handelt. Die Verfassungsschutzämter sammeln über

verdeckte Datenerhebungen ‚flächendeckende‘ Informationen etwa über extremistische oder terroristische Gruppierungen und Szenen (Landesamt für Datenschutz Bremen 2016). Dem LfV Bremen zufolge erfordere diese Informationserzeugung ein Vertrauensverhältnis zu den Informanten (V-Leute) als Mitglieder von verdächtigen und bereits straffällig gewordenen Gruppen und Organisationen. Dadurch werde ein exklusiver Zugang zu Informationsquellen ermöglicht. Um diese Aufgabe wahrnehmen zu können unterliegen die Verfassungsschutzämter dem Opportunitätsprinzip, wonach bei Erkenntnis von Straftaten eine Strafverfolgung zugunsten weiteren Erkenntnisgewinns nicht (unmittelbar) erforderlich ist bzw. im Ermessen der Behörde liegt. Demgegenüber handelt die Polizei nach dem Legalitätsprinzip. Sie muss bei Verdacht einer Straftat unmittelbar tätig werden. Schließlich liegt die Besonderheit des Verfassungsschutzes nach Gusy (2012: 231) auch darin, dass die Polizei nur begangene Straftaten aufklären oder bevorstehende verhindern, aber der Verfassungsschutz auch legalen Bestrebungen nachgehen dürfe.

2.2.1 Typischer Programmmodus

Der Programmmodus des Verfassungsschutzes ist im Vergleich zum regulativen Modus (Ge- und Verbote) hoheitlich-polizeilicher Maßnahmen nicht eindeutig. Die polizeiliche Aufgabenwahrnehmung macht aufgrund der Eingriffskompetenzen in die Grundrechte, die regelmäßig und intensiv zur Anwendung kommen, kleinteilige und konditionierbare Programme erforderlich, die auf politische und richterliche Kontrolle sowie Zurechenbarkeit und demokratische Transparenz ausgelegt sind. Diese Eingriffsformen stehen dem Verfassungsschutz jedoch nicht zur Verfügung. Zwar sind auch hier die Ge- und Verbote für die Tätigkeiten anleitend, sie beziehen sich jedoch auf die Mittel der gewählten Maßnahmen, die von der in der Regel juristisch ausgebildeten Führungsstruktur der Behörden (Grumke 2016) gesteuert und kontrolliert werden. Für die Aufgaben des Verfassungsschutzes typisch ist demnach eine Zweckorientierung: Was und in welcher Intensität als Gefahr erscheint und auf welche Art und Weise eine Problemlösung im Sinne der Informationserzeugung erfolgt, ist nicht im Vorfeld klar und kann somit auch nicht eindeutig oder gar abschließend rechtlich geregelt werden. Die Freiräume der Implementation sind letztlich weit und eröffnen ein breites Handlungsspektrum. Für die Informationserhebung, -verarbeitung und -auswertung sind regelmäßig Expertisen durch das fachwissenschaftliche Personal erforderlich, deren Tätigkeit nur durch interne Dienstanweisungen gesteuert wird. Die der Geheimhaltung gegenüber der Politik, den Bürgern und teilweise auch den Gerichten verpflichteten Arbeit des Verfassungsschutzes wird demnach dominant durch den *Steuerungsmodus* angeleitet.

Dennoch tritt der Verfassungsschutz auch öffentlich in Erscheinung. Er veröffentlicht regelmäßig Verfassungsschutzberichte, durch die verfassungsfeindliche Gruppierungen und Organisationen beschrieben und bewertet werden. Zudem engagieren sich die Ämter in der politischen Bildungsarbeit, indem sie Informationsmaterial zur Verfügung stellen und Informationsveranstaltungen an Schulen durchführen (kritisch: Wiedemann 2013, Kohlstruck 2013). Diese Programme sind typisch dem *persuasiven Modus* (Informations- und Überzeugungsprogramme) zuzurechnen.

2.2.2 Typische Implementationsstruktur

Das Implementationsarrangement lässt sich als stark ausgeprägt *homogen* und *in einem sehr hohen Ausmaß geschlossen* charakterisieren. Erstere Einschätzung beruht entsprechend darauf, dass die Verfassungsschutzämter in ihrer Aufgabenerfüllung weitestgehend auf sich selbst bezogen sind und durch das Trennungsgebot eine Zusammenarbeit mit den Polizeibehörden der Länder und des Bundes nicht erfolgt. Letzteres ergibt sich grundlegend daraus, dass die Behörden geheim und getarnt arbeiten. Eine partielle Öffnung besteht jedoch hinsichtlich der sogenannten ‚V-Leute‘ als inoffizielle und bezahlte Informanten außerhalb der Behörde, die über verfassungsfeindliche Aktivitäten berichten. Zudem bezieht sich die Aufgabe des Verfassungsschutzes auf die Verfassungsschutzämter der jeweiligen Länder und des Bundes selbst, sodass ein *Höchstwert an Zentralität und Konzentration* für die Implementation erreicht wird. Die Geheimhaltung der Arbeitsweise und der erzeugten Informationen führt nicht nur zu einer Selbststeuerung der Implementation, sondern macht einen (kritischen) öffentlichen Diskurs unmöglich und behindert eine politische Kontrolle durch die Parlamente grundlegend. Die Parlamente können ihre Kontrollfunktion nur über die hierfür eingesetzten parlamentarischen Kontrollkommissionen oder durch entsprechende Gremien nachkommen, die als ständige Ausschüsse tagen (Striegel 2013: 83). Dies kann allerdings nur dann gelingen, wenn die Kontrollierbarkeit der Ämter und die Kontrollfähigkeit durch die Kommission hinreichend gewährleistet sind. Beides erscheint jedoch nur in einem geringen Maße möglich: Die Kontrollierbarkeit ist mindestens unzuverlässig, weil die Kommissionen, Ausschüsse und Gremien strukturell grundsätzlich auf solche Informationen angewiesen sind, die von den zu kontrollierenden Ämtern deutungsmächtig selbst ausgewählt und bereitgestellt werden (Baier 2009: 118; Gusy 2008: 39). Zudem erfolgt „die parlamentarische Kontrolle nahezu überall nach dem Prinzip: *multa, non multum*.“ (Gusy 2008: 39), und dadurch über verschiedene, miteinander unverbundene und formal unterschiedlich ausgestaltete parlamentarische Kontrollen, die je andere Aspekte der geheimdienstlichen Aufgabenwahrnehmung in den Blick nehmen (ebd.). Diese fragmentierte Kontrolle wird der stark auf eine Organisation konzentrierten Implementationsstruktur nicht gerecht und mindert die Kontrollierbarkeit zusätzlich. Darüber hinaus erscheint die Kontrollfähigkeit häufig nicht effektiv möglich, weil den Politikern grundsätzlich die fachliche Expertise und Zeitkapazitäten fehlen, aus den durch die Ämter selbst zur Verfügung gestellten Berichten, Akten und Verwaltungsvorgänge gezielt Widersprüche zu erkennen. Die parlamentarischen Kontrollausschüsse haben darüber hinaus keine Instrumente, um effektive Wirkungen ihrer Kontrolltätigkeit herbeizuführen. Einerseits fassen sie in der Regel keine Beschlüsse und andererseits sind die Kommissionsmitglieder auch zur Verschwiegenheit gegenüber der eigenen Fraktion und sogar ihren Stellvertretern verpflichtet. Die Folge ist, dass wichtige Informationen über Versäumnisse oder Skandale der Ämter vornehmlich durch investigative Recherchen von Journalisten erzeugt und öffentlich gemacht werden, durch die erst relevante Impulse und Inhalte für die Kontrollkommissionen geliefert werden und damit aber gleichzeitig die parlamentarische Kontrollfähigkeit öffentlich in Frage gestellt wird (Striegel 2013: 86-87; Gusy 2008: 39). Durch die mangelnde Kontrollierbarkeit/Steuerbarkeit

und Kontrollierfähigkeit/Steuerungsfähigkeit zeigt sich insgesamt auch ein *Höchstwert an Politikferne* für die Implementationsstruktur.

Die Intransparenz und die mangelnde rechtliche Kodifizierung und Konditionierbarkeit der Arbeit der Verfassungsschutzämter erscheint ursächlich für ein geringes Institutionenvertrauen der Bürger insbesondere im Vergleich zur Polizei.

2.3 Das Aufgabenfeld ‚Bevölkerungsschutz‘

Der Bevölkerungsschutz als das dritte hier vorzustellende Aufgabenfeld des Politikfelds umfasst „alle Aufgaben und Maßnahmen der Kommunen und Länder im Katastrophenschutz sowie des Bundes im Zivilschutz (...) (und – *der Verf.*) somit alle nicht-polizeilichen und nicht-militärischen Maßnahmen zum Schutz der Bevölkerung und ihrer Lebensgrundlagen vor Katastrophen und anderen schweren Notlagen sowie vor den Auswirkungen von Kriegen und bewaffneten Konflikten (...) und) Maßnahmen zur Vermeidung, Begrenzung und Bewältigung der oben genannten Ereignisse.“ (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011: 7) Der Bevölkerungsschutz bildet ein komplexes Aufgabenfeld, das sich durch eine politikfeldtypisch klar voneinander abgegrenzte, föderale Zuständigkeit zwischen Bund, Ländern und Kommunen auszeichnet (Lange/Endreß 2013: 13).

Institutionell unterteilt sich der Bevölkerungsschutz in Zivilschutz- und Katastrophenschutz. Der *Zivilschutz* umfasst den Schutz der Bevölkerung im Verteidigungsfall bei Angriffen von ‚Außen‘ und gegen Gefahren, die beim Freiwerden von Kernenergie oder durch ionisierende Strahlen entstehen (Art. 73 Abs. 1 Nr. 1, 14 GG). Die Gesetzgebung und Aufgaben des Zivilschutzes liegen bei der Bundesebene. Den Ländern ist der Zivilschutz als Bundesauftragsangelegenheit auferlegt (Art. 87b Abs. 1 GG) (Pohlmann 2013: 250). Die zentralen Akteure sind hier das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und die Bundesanstalt Technisches Hilfswerk (THW), die beide zum Geschäftsbereich des Bundesministeriums des Inneren gehören.

Das THW wird vor allem für die Bewältigung von Aufgaben des Zivilschutzes und unterstützend für den Katastrophenschutz der Länder eingesetzt. Wechselbeziehungen zu Verwaltungseinheiten anderer Politikfelder sind aufgrund des allgemeinen und weitreichenden Charakters des Aufgabenbereichs vielfältig und zahlreich. Insbesondere hinsichtlich der Informationsbereitstellung und -verarbeitung zur Vorbeugung von Naturkatastrophen bestehen Beziehungen zu den Bundesanstalten für Gewässerkunde, Seeschifffahrt und Hydrographie und Deutscher Wetterdienst und zur Wasser- und Schifffahrtsverwaltung, die sämtlich dem Bundesministerium für Verkehr, Bau und Stadtentwicklung zugeordnet sind sowie zum Umweltbundesamt, das sich im Geschäftsbereich des Bundesministeriums für Umwelt, Naturschutz und Reaktionssicherheit befindet. Wechselbeziehungen zu anderen Sicherheitsbehörden außerhalb des Bevölkerungsschutzes bestehen vor allem zur Bundespolizei und Bundeswehr.

Bundesweit engagieren sich zudem zivilgesellschaftliche Organisationen (Verbände, Vereine) mit umfangreichen materiellen und personellen Ressourcenausstattungen, die

teilweise durch die Ausbildung von Einsatzkräften, aber insbesondere durch die Ressourcenbereitstellung zur Bewältigung von Einsatzlagen maßgebliche Kapazitäten im Bevölkerungsschutz bereithalten. Hierunter fallen vor allem der Arbeiter-Samariter-Bund, die Deutsche Lebens-Rettungs-Gesellschaft, das Deutsche Rote Kreuz, die Johanniter-Unfall-Hilfe und der Malteser Hilfsdienst. Sie sind zwar bundesweit organisiert, aber nicht nur auf dieser Ebene und auf den Zivilschutz beschränkt. Insofern engagieren sie sich auch und insbesondere für den weit aufgabenintensiveren Katastrophenschutz der Länder und darüber hinaus vor allem im Politikfeld der Sozialpolitik (vgl. hierzu Köhling in diesem Band). Zudem stellen verschiedene weitere Verbände, Vereine, Initiativen, Privatunternehmen sowie Forschungsinstitutionen und -verbünde auf Bundesebene Informationen für den Bevölkerungsschutz zur Verfügung.

Das Ziel des *Katastrophenschutzes* ist hingegen der Schutz von Leben, Gesundheit und Eigentum und die Hilfestellung bei Schadensereignissen infolge von Naturkatastrophen und durch technologische oder industriell bedingte Großschadensereignisse infolge von Unfällen oder dem Versagen von technischen oder sozialen Infrastrukturen (Lange/Endreß/Wendekamm 2012: 22, 30f.), die für Aufrechterhaltung der gegenwärtigen Wirtschafts- und Sozialstruktur unentbehrlich sind (insbesondere Kommunikation, Verkehr, Energie, Währung, Gesundheit). Für den Katastrophenschutz sind die Länder zuständig (Art. 30, 70, 83 GG). Sie behalten auch dann ihre Zuständigkeiten, wenn mehrere Länder gefährdet oder betroffen sind (ebd.: 31). Auf Antrag/Anfrage der Länder kann in diesem Fall auch der Bund koordinierend tätig werden, aber auch dann verbleibt die operative Verantwortung bei den einzelnen Ländern.

Zuständig für den Katastrophenschutz der Länder sind die Katastrophenschutzbehörden: „die Landräte in den Kreisen und die Oberbürgermeister in den kreisfreien Städten, die für den Katastrophenschutz zuständigen Ministerien oder Senatsverwaltungen sowie gegebenenfalls die mittleren staatlichen Verwaltungsebenen“ (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2011: 16). Durch die (Land-)Kreise und (kreisfreien) Städte als Katastrophenschutzbehörden greift im Katastrophenschutz die Garantie der kommunalen Selbstverwaltung (Art. 28 Abs. 1 GG) und erweitert das politische Mehrebenensystem des Bevölkerungsschutzes um die Ebene der Kommunen. Die Abbildung 1 bildet den Aufbau des staatlichen Krisenmanagements modellförmig ab.

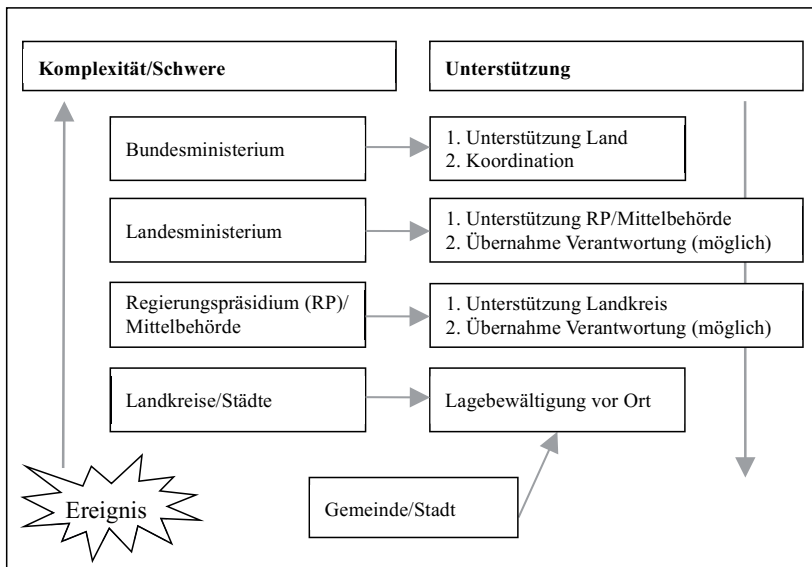


Abb. 1 Aufbau des staatlichen Krisenmanagements im Mehrebenensystem des Aufgabenfelds
 Quelle: Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2010: 2

Im Katastrophenschutz bestehen enge Wechselbeziehungen zu den *Länderpolizeien* und *Feuerwehren*. Die Länderpolizeien unterstützen im Rahmen ihrer Amtshilfe die Katastrophenschutzbehörden subsidiär (Lange/Endreß/Wendekamm 2012: 74). Die Feuerwehren der Länder werden qua Weisung der Landesebene durch die Kommunen bereitgestellt. Während lediglich 102 Berufsfeuerwehren in Deutschland eingerichtet sind, unterhält grundsätzlich jede Kommune auch eine Freiwillige Feuerwehr, die gemäß den kommunalen Erwägungen an verschiedenen kommunalen Orten vertreten sind (ebd.: 76f.). Entsprechend der verschiedenen Organisationsstrukturen in den Ländern werden weitere staatliche Akteure einbezogen wie beispielsweise in NRW das Landesamt für Natur, Umwelt und Verbraucherschutz sowie die Landesbetriebe ‚Straßenbau‘ und ‚Wald und Holz‘.

Der Bevölkerungsschutz findet seine Identität vor allem im Schutz einer allgemeinen kritischen Infrastruktur. Hiermit wird im Bevölkerungsschutz ein komplexes System von technischen Basisstrukturen und sozioökonomischen Dienstleistungsstrukturen⁴ bezeich-

4 Die *technischen Basisinfrastrukturen* beziehen sich auf die Energieversorgung, Informations- und Kommunikationstechnologie, Transport und Verkehr, (Trink-)Wasserversorgung und Abwasserentsorgung und die *sozioökonomischen Dienstleistungsstrukturen* umfassen das Gesundheitswesen und die Ernährung, Notfall- und Rettungswesen und allgemein die Katastrophenhilfe als auch öffentliche Institutionen wie die Parlamente, Regierungen, öffentliche Verwaltung, Justizeinrichtungen, das Finanz- und Versicherungswesen und die Medien und Kulturgüter (Bundesministerium des Innern 2009: 5).

net, deren interdependentes Verhältnis insgesamt die Verletzlichkeit (Vulnerabilität) einer nationalen Gesellschaft zum Ausdruck bringt. Dabei befinden sich einerseits mehr als 80 % dieser Infrastrukturen im Eigentum privater Unternehmen, deren Gewährleistungsfunktion in Krisen- und Katastrophenzeiten jedoch andererseits dem Staat zukommt (ebd.: 99). Dabei hat der Staat im Verteidigungs- und Katastrophenfall verschiedene Kompetenzen, um privatwirtschaftliche Leistungen in Anspruch zu nehmen (Überblick bei ebd.: 99f.). Darüber hinaus ergibt sich ein zunehmender Bedarf für ‚Public Privat Partnerships‘ als Formen der institutionalisierten kooperativen Zusammenarbeit zwischen Staat und den verschiedenen Wirtschaftsunternehmen, um die Kapazitäten des Bevölkerungsschutzes zu gewährleisten.

Die Beschreibung des Aufgabenfeldes zeigt, dass das allgemein politikfeldtypische Trennprinzip auch in der institutionellen Aufgabenverteilung zwischen dem Zivilschutz des Bundes und den Katastrophenschutz der Länder Anwendung findet. Es bezieht sich nicht nur auf die Legislative der beiden Ebenen, die etwa durch weisungsmäßige Auftragsangelegenheiten die Implementationsstrukturen der Länder in Anspruch nehmen, sondern – im Vergleich zu anderen Politikfeldern ein eher seltener Fall – auch auf die Exekutive (Gusy 2013: 212). Nach Gusy (ebd.) ist zu betonen, dass dies nicht zugleich ein Verbot der Zusammenarbeit zwischen Bund und den Ländern bedeutet, sondern nach Art. 35 GG gerade im Hinblick auf den kooperativen Bundesstaat vielmehr das Gegenteil der Fall ist. Es bestehen grundgesetzliche Unterstützungspflichten zwischen Bund und Ländern sowohl konkret für einen Katastrophenfall (Art. 35 Abs. 2, S. 3 GG) als auch allgemein im Bereich der Amtshilfe (Art. 35 Abs. 1 GG). Dadurch ergeben sich vielfältige Kooperationsnotwendigkeiten zwischen der Bundes- und Länderebene vor allem dann, wenn es um die wechselseitige Ressourcenbereitstellung für die Aufgabenerledigung geht. Nach Pohlmann lässt sich die Gesamtstruktur dadurch bilanzieren, dass der Bund die Länder dazu verpflichtet, für seinen zunehmend bedeutungslos werdenden Zivilschutz die Kapazitäten des Katastrophenschutzes einzubringen (Prinzip des „Doppelnutzens“). Die hierdurch verursachten Kosten werden vom Bund getragen. Gleichzeitig engagiert sich der Bund aber im Katastrophenschutz im Rahmen seiner Amts- und Katastrophenhilfe weitaus stärker und hat damit eine erhebliche Bedeutung (Pohlmann 2013: 252). Die Länder erhalten auf Antrag/Anfrage Unterstützung von der Bundesebene vor allem durch das THW (Lange/Endreß/Wendekamm 2012: 31), die Bundeswehr und Bundespolizei sowie andere Verwaltungseinheiten (Art. 35 Abs. 2, Satz 2 GG). Aber auch hier zeigt sich, dass mit diesem weitreichenden Engagement der Bundesebene keine bundespolitischen Steuerungskompetenzen einhergehen. Nach Gusy (Gusy: 213 f.) kann somit geschlossen werden:

„Was funktionell segmentär sauberlich abgegrenzt werden kann – nämlich der Schutz der Zivilbevölkerung gegen Katastrophen militärischen oder nicht-militärischen Ursprungs –, ist ressourcenmäßig schwerer teilbar (...) Es sind weitgehend dieselben oder doch vergleichbare Fachkompetenzen, Logistiken und Sachmittel, welche für beide Arten von Katastrophen vorgehalten werden müssen. Hier wird das Trennprinzip zwar nicht unmöglich, aber doch möglicherweise sinnlos. Dies gilt erst recht dann, wenn beide Seiten einander zu Unterstützung und Amtshilfe (Art. 35 GG) verpflichtet sind.“

2.3.1 Typischer Programmmodus

So wie die beiden anderen Aufgabenfelder des Politikfelds zeigt sich auch beim Bevölkerungsschutz zunächst eine klare rechtliche Zuständigkeit der verschiedenen Behörden mit Zivil- und Katastrophenschutzaufgaben im politischen Mehrebenensystem. Weil die Kommunen durch die kommunale Selbstverwaltungsgarantie die Organisationen und das Personal für den Katastrophenschutz bereithalten, müssen sie einerseits ein Krisenmanagement verfolgen, das die konzeptionellen, organisatorischen und verfahrensmäßigen Voraussetzungen schafft, um im Ereignisfall konkrete Gefahren und Schadensfolgen durch eine Katastrophe abwenden zu können. Die politisch-administrativen Programme, die zur Erfüllung dieser Aufgaben eingesetzt werden, folgen dem *Leistungsmodus*. Demnach finanziert die Kommune Personal, Gebäude, technische Ausrüstung etc., um für die Katastrophenhilfe geeignete Infrastruktureinrichtungen bzw. die erforderlichen Kapazitäten im Rahmen ihrer Zuständigkeit bereitzuhalten. Gleichzeitig müssen die Kommunen politisch-administrative Strukturen (zuständiges/verantwortliches Personal, Kommunikationswege, Ausführungsprogramme) für die Aufgabenerfüllung im Katastrophenfall formal einsetzen. Diese Verwaltungsprogramme im Sinne von *regulativen Programmen* (Ge- und Verbote) regeln das Katastrophenmanagement formal-institutionell. Davon zu unterscheiden sind die operativ-taktischen Strukturen, Prozesse und Verfahren, die von den professionellen Organisationen der Katastrophenhilfe bei der Bewältigung von Gefahren und Schadensfolgen im Katastrophenfall angewendet werden. Es sind insbesondere technische und medizinische ‚Alarmprogramme‘, die je nach Organisation hoch standardisiert bzw. stark konditioniert funktionieren und Abläufe perfektionieren und beschleunigen. Die Implementation durch die Katastrophenbehörde bezieht sich damit weniger auf die punktuelle Ziel- und Mittelformulierung durch regulative Vorgaben, wie operative Anweisungen, Instruktionen und Direktiven für den Einzelfall, sondern vornehmlich auf *regulierende Programme* im *Steuerungsmodus*.

Bei einem Katastrophenfall beziehen sich die Steuerungsprogramme auf die strategische Führung der Katastrophenschutzbehörden der Kommunen, der Länder und in Ausnahmefällen des Bundes. Eine effektive Steuerung muss die verschiedenen organisierten Einzelprogramme zeitnah miteinander verzahnen. Die Akteure müssen jeweils in ihrer Verflechtung sowohl zweckorientiert (insbesondere bei einer konkreten Gefahrenabwehr zum Schutz von bedeutender Rechtsgüter und für den Infrastrukturerhalt und die -instandsetzung), als auch konditionierbar (wie logistische und technische Unterstützung, Verpflegung und Unterkunft für und Kommunikationsbedingungen mit der betroffenen Bevölkerung) gesteuert werden. Dies sind besonders anspruchsvolle Bedingungen für die strategische Führung und für die erwartete Programmkapazität in einem komplexen administrativen Netzwerk der Katastrophenhilfe im Mehrebenensystem des Aufgabenfeldes: Welche Art an Katastrophenhilfe wird in welchem Umfang wo, wann und wie lange benötigt?

Nach Mintzberg (1979: 349) kann das professionelle Handeln im Bevölkerungsschutz, hier vor allem: Katastrophenschutz, grundsätzlich dadurch beschrieben werden, dass das Personal durch eine spezialisierte Wissensgrundlage und regelmäßiges Training hoch

standardisiert und geregelt Aufgaben wahrnimmt. Gleichzeitig ist für ein solches Arrangement typisch, dass die Organisationen und die einzelnen Helfer aufgrund ihrer hohen Spezialisierung typischerweise relativ unabhängig voneinander arbeiten (ebd.). Die Organisationsbeziehungen zur Gefahrenabwehr strukturieren sich somit grundlegend durch eine ‚Adhocracy‘ im Sinne organischer, eigendynamischer und dadurch wenig formalisierter Abstimmungen zwischen jeweils hoch professionalisierten und spezialisierten Tätigkeiten (ebd.: 432). Dies hat regelmäßig Vorteile, weil die Anforderungen an die Gefahrenabwehr vor allem je nach Gefahr, Situation, Kontext und Ressourcen hoch variabel sind und die Adhocracy gleichsam spontan situations- und kontextabhängig Innovationen für die Problemlösung hervorbringen kann. Dies wäre durch eine strikt zentrale und konzentrierte Steuerung nicht möglich. Gleichzeitig besteht jedoch der Anspruch an eine zentrale strategische Steuerung der Katastrophenschutzbehörden je nach Komplexität/Schwere des (erwarteten) Schadensereignisses (vgl. Abbildung 1), um die Leistungen der verschiedenen Organisationen möglichst effektiv und effizient zu koordinieren. In diesem Sinne kann sich die ausgeprägte Selbststeuerung der Organisationsnetzwerke auch nachteilig auf die Gefahrenabwehr auswirken, weil die Akteure zwar jeweils situativ und einzelfallbezogen effektiv handeln, in einer Gesamtbetrachtung aber die angestrebten Wirkungen (Impact, Outcome) aufgrund redundanter und mithin ineffizienter sowie nicht kompatibler Strukturen verfehlen. Der Steuerungsmodus im horizontalen und vertikalen Mehrebenensystem des Bevölkerungsschutzes ist geprägt durch diese Ambivalenz. Sie bewegen sich zwischen operativer und strategischer Steuerung und müssen beiden Anforderungen sachlich, sozial und zeitlich gerecht werden. Mit anderen Worten: Sie müssen dem Problem gerecht werden, das sich aus der Gleichzeitigkeit interaktionsorientierter Vertrauens- und Wissensgenerierung für nicht planbare ‚Ausnahmesituationen‘ und formaler Rahmensteuerung für eine effektive Schnittstellenkoordination ergibt. Hier müssen Mechanismen greifen, die zwischen beiden Ansprüchen (eigendynamisch-operativ und strategisch-formalisierend) vermitteln. Dies kann nur dann gelingen, wenn durch Übungen und Szenarien in der Aus- und Fortbildung verschiedene Gefahren und Schäden simuliert werden. In diesem Rahmen werden Strukturen, Prozesse, gemeinsame Standards (beispielsweise anschlussfähige Begriffe, Anweisungen und Lagebeurteilungen) entwickelt und verbindlich standardisiert, um zugleich operative und strategische Handlungsgrundlagen zu schaffen.

Neben diesen verschiedenen Programmformen, die insgesamt durch den staatlichen Steuerungsmodus aufeinander zu beziehen sind, finden aufgrund der hohen Bedeutung von Verbänden und speziellen Diensten im Katastrophenschutz, die auf vornehmlich ehrenamtliche Mitglieder angewiesen sind (Wendekamm/Matzke 2015), auch *persuasive Programme*, aber auch *Anreizprogramme* Anwendung. Durch sie versucht der Staat das ehrenamtliche Engagement als tragendes Element des Bevölkerungsschutzes zu fördern.

2.3.2 Typische Implementationsstruktur

Die Steuerungsprogramme als dominanter Programmmodus sind Ausdruck des typischen Implementationsarrangements, das sich in *stark ausgeprägter Weise heterogen* und *relativ offen* gestaltet. Neben der Vielzahl verschiedener kommunaler und staatlicher Organisationen und den Verbänden, die abhängig von der Katastrophenform bei der Gefahrenabwehr beteiligt werden, sind auch je nach örtlichem Kontext die Kapazitäten privatwirtschaftlicher Infrastrukturen und bürgerschaftliches Engagement bei der Aufgabenerledigung zu berücksichtigen. Welche staatlichen, kommunalen, privatwirtschaftlichen und zivilgesellschaftlichen Akteure mit welcher Handlungsgrundlage und -kapazität einbezogen werden können, ist somit je nach Gefahr und räumlichem Kontext variabel und erfordert eine Kapazitätserhebung und strategische Koordination, die durch die zuständigen Katastrophenschutzbehörden und Krisenstäbe geleistet werden muss.

Vor diesem Hintergrund ist die typische Implementationsstruktur zudem als *stark fragmentiert* und *dekonzentriert* zu beschreiben. Im Aufgabenfeld bestehen weit weniger stabile Netzwerkstrukturen formaler und informaler Kontakte zur Aufgabenerledigung, als dies in den anderen Aufgabenfeldern im Politikfeld der Fall ist. Eine hinreichend stabile Wissens- und Handlungsgrundlage muss durch regelmäßig simulierte Gefahren- und Schadenssituationen ‚künstlich‘ erzeugt werden.

Das Implementationsarrangement zeichnet sich insgesamt durch eine typische *Politikferne* aus. Dies begründet sich einerseits darin, dass über eine längere Zeit politischen Problemperzeptionen und Problemlösungsstrukturen zu bspw. Vorsorgemaßnahmen, Risikoanalysen oder Ressourcenfragen keine oder allenfalls nur ereignisabhängig eine Bedeutung zukamen.⁵ Andererseits kommt der politischen Führung auf der jeweils zuständigen Ebene in den Krisenstäben während der Implementation durchaus eine wichtige Funktion zu. So sind die Politiker vor allem dafür zuständig, einen Katastrophenfall auszurufen und Prioritäten bei den zu schützenden Sachgütern festzulegen. Mit einer politischen Lagebeurteilung als Katastrophenfall sind erhebliche und zum Teil nicht vor auszusehende Kosten verbunden. Die Folge ist, dass die Länder und auch die Kommunen nur sehr zögerlich einen Katastrophenfall ausrufen. Die politische Abwägung bezieht sich auf die Kosten für die Mobilisierung der Katastrophenhilfe, die die Politiker rechtfertigen müssen, und die politische Verantwortlichkeit für die Schäden, die entstehen können, wenn der Katastrophenfall fälschlicherweise nicht oder nicht rechtzeitig ausgerufen wurde. Die Bedeutung der Politik reduziert sich aber insofern, als dass die politische Führung ihre

5 Diese Situation änderte sich jedoch infolge zunehmender Versicherheitlichung inkrementell und infolge von sicherheitsrelevanten Ereignissen wie Naturkatastrophen oder Terroranschläge auch abrupt. So auch Pohlmann: „Die verstärkte Wahrnehmung von Risiken durch Terroranschläge, Naturkatastrophen und Stör- und Unfälle in der Industrie sowie die gleichzeitige steigende Abhängigkeit von moderner Infrastruktur und die dadurch verursachte Vulnerabilität der heutigen modernen Gesellschaft, haben die Notwendigkeit von Vorkehrung für Schutz und Hilfe in (...) Katastrophenfällen verstärkt ins Bewusstsein gerückt.“ (Pohlmann 2013: 249)

Entscheidungen vornehmlich an fachlich-administrativen Einschätzungen – insbesondere der Feuerwehr – orientiert.

Die Folge dieser typischen Implementationsstruktur des Bevölkerungsschutzes ist eine Intransparenz über die Art und Weise der staatlichen und zivilgesellschaftlichen Leistungserbringung bei den Bürgern, die dazu führt, dass sich viele Bürger über den Katastrophenschutz nicht hinreichend informiert fühlen (European Commission 2009: 19-32).

**3 Zwischenresümee:
Aufgabenstrukturen des Politikfelds im Wandel**

Die verschiedenen Implementationsbedingungen und Programmmodi der drei Aufgabenfelder im Vergleich werden in der Tabelle 2 zusammengefasst.

Aus den Strukturen der drei Aufgabenfelder im Vergleich können im Folgenden typische Strukturbedingungen für das Politikfeld insgesamt abgeleitet werden.

Typisch für das Politikfeld der Inneren Sicherheit erscheint zunächst die *Staatszentriertheit* und *Professionalisierung* der Aufgabenwahrnehmung. In den drei Aufgabenfeldern zeigen sich vornehmlich Organisationen, die hoch professionalisiertes und/oder verbeamtetes Personal beschäftigen, die ein Wissen über die Sicherheitsherstellung im Politikfeld nahezu monopolisieren (Heinrich/Lange 2010: 78). Aufgrund der Politikferne des Implementationsarrangements bleibt die Steuerung und Kontrolle der Politik und Parlamente allgemein und ‚auf Abstand‘. Dies zeigt sich vor allem bereits daran, dass die Implementationsbedingungen

Tab. 2 Strukturmodi und Implementationsbedingungen der Aufgabenfelder im Vergleich

Aufgabenfeld/ Implement.- bedingungen	Polizei	Verfassungsschutz	Bevölkerungsschutz
typische Programm- modi	Regulativer Modus	<i>Primär:</i> Steuerungsmodus <i>Sekundär:</i> Persuasiver Modus	<i>Primär:</i> Leistungs- und Steuerungsmodus <i>Sekundär:</i> regulativer Modus Persuasiver Modus Anreizmodus
typisches Implementations- arrangement	<ul style="list-style-type: none">• stark homogen• stark geschlossen• stark politikfern• vertikal integriert• zentral/konzentriert→ staatszentriert→ verwaltungsdominant	<i>sehr stark:</i> <ul style="list-style-type: none">• homogen• geschlossen• zentral/konzentriert• politikfern→ staatszentriert,→ verwaltungsdominant→ organisationszentriert	<i>stark heterogen</i> <ul style="list-style-type: none">• offen• stark fragmentiert und de-konzentriert• politikfern→ professionsbezogen

insbesondere über exekutive Dienstanweisungen und -vorschriften anstelle von Gesetzen und Verordnungen ausgestaltet werden (Gusy 2012b: 263). Dadurch gilt im Politikfeld allgemein: Was Sicherheit ist und wie sie erreicht werden kann, obliegt vornehmlich der Deutungshoheit der Behörden mit Sicherheitsaufgaben (Polizei, Katastrophenhilfe, Verfassungsschutzämter), die sich aufgrund des fachlich-professionellen Einflusses, ihrer eigenen selbstregulativen Handlungsmuster (Schemata, Frames, Habits) (Lange 2011: 335) und nicht zuletzt aufgrund der hohen Akzeptanz in der Bevölkerung (hier nur: Polizei und Bevölkerungsschutz) bei allen Phasen (Problemperzeption, Programmformulierung, -implementation und -evaluation) der politikfeldspezifischen Prozesse auswirkt. Demnach zeigt sich eine Dominanz der Herstellung von Sicherheit (das ‚Wie‘) über politische Wertpräferenzen, die einen politischen Diskurs über das Für und Wider von Sicherheitsprogrammen (das ‚Ob‘) gewährleisten. Diese ausgeprägte Staatszentrierung muss insbesondere im Vergleich zu anderen Politikfeldern noch weiter konkretisiert werden. Demnach ist das Politikfeld nicht nur auf die exekutiven Problem- und Problemlösungskonstruktionen fixiert, sondern zusätzlich auch *verwaltungsdominiert*. Dies bedeutet, dass die politischen Prozesse stark durch die administrativen Implementationsbedingungen geprägt werden und in einem stärkeren Maße als in anderen Politikfeldern eine Selbststeuerung der Behörden und des professionalisierten Personals erfolgt und auch politisch erwartet wird (hierzu ausführlich Lanfer 2014). In einer stark pointierten Formulierung lässt sich zusammenfassen, dass Sicherheitsprogramme nicht erfolgreich sind, wenn sie von der Politik und politischen Führung gegen die Sicherheitsbehörden geplant und durchgesetzt werden. Der eigentlich für die öffentliche Verwaltung des politischen Systems typische Opportunismus (Luhmann 2007) gegenüber der politischen Führung zeigt sich im Politikfeld der Inneren Sicherheit demnach mit umgekehrten Vorzeichen: Wenn die Politik und politische Führung erfolgreich sein will, müssen sich deren Wertprämissen den Anforderungen, Erwartungen und Interessen der Sicherheitsbehörden anpassen.

Vergleichbar sind die Aufgabenfelder auch in ihrem *ambivalenten Verhältnis zwischen einer zentralen Integration und dezentralen Fragmentierung sowohl auf einer politischen Ebene als auch insgesamt im politischen Mehrebenensystem*. Die historisch gewachsene strikte institutionelle Trennung zwischen den politischen Ebenen zeigen einerseits Pfadabhängigkeiten, die eine konkurrierende Gesetzgebung nahezu ausschließen. Bei allen Verflechtungen zwischen den Sicherheitsbehörden im deutschen Mehrebenensystem bewirkt dabei die Staatszentrierung eines Bundeslandes als auch der Verweis auf kommunale Besonderheiten einmal mehr eine Beharrung auf die institutionelle Trennung der Sicherheitsherstellung. Die Aufrechterhaltung der institutionellen Trennung („dualer Föderalismus“) im Mehrebenensystem ist wahrscheinlich. Gleichzeitig nehmen aber auch die formal-institutionellen Kooperationen und Koordinationen zwischen den politischen Ebenen und netzwerkspezifische Verflechtungen zwischen den sicherheitspolitischen Organisationen unterschiedlicher politischer Ebenen zu.

Auf diese beiden grundlegenden Strukturbedingungen im Politikfeld wirken verschiedene gesellschaftliche und politische Impulse ein, mit denen entsprechend verschiedene Strukturänderungen einhergehen können: Aufgrund der stärkeren Bedeutung von Risiko-

und Sicherheitswahrnehmungen und Prozesse der ‚Versicherheitlichung‘ (Weaver: 1995) in der Gesellschaft (allgemein hierzu: Groenemeyer 2010; Singelstein/Stolle 2006; Beck 1999), lastet auf dem Politikfeld und den Aufgabenfeldern ein zunehmender Legitimationsdruck. Für die Implementationsarrangements und Programmmodi der Aufgabenfelder bedeutet dies, dass sie höheren Sicherheitserwartungen der Bürger und dadurch auch speziell privatwirtschaftlicher Unternehmen ausgesetzt sind, wobei letztere Sicherheit verstärkt als ökonomischen Wert begreifen und die Sicherheitspolitik stärker mit der Wirtschaftspolitik koppeln. Sie resultieren aus objektiven und subjektiven Unsicherheiten angesichts von Veränderungen in ihrem unmittelbaren lebensweltlichen Umfeld in (Groß-)Städten als auch angesichts steigender und neuer Gefahren und Risiken durch internationale und organisierte Kriminalität oder Klima- und Technikfolgen für kritische (Informations-) Infrastrukturen. In den drei Aufgabenfeldern führt dies zu Prozessen einer ‚neuen Sicherheit‘. *Sie ist weniger durch die bisher typische konkret-sachbezogene, objektivierbare und regulativ nach Ge- und Verboten programmierbare Sicherheitsherstellung durch eine stark professionalisierte, staatszentrierte und verwaltungsdominierte Sicherheitsherstellung einzulösen, sondern erfordert ganzheitliche Strukturen, die sich an subjektive, dynamische sowie präventionsbezogene und damit zukunftsorientierte Problemperzeptionen und Problemlösungen orientieren* (Gusy 2010: 311 f., Lanfer 2012). Auf der Ebene der Länder geht diese Entwicklung mit einer Kommunalisierung und auf der Ebene des Bundes mit einer Europäisierung und Internationalisierung der Sicherheitsgewährleistung einher. Infolge der Kommunalisierung führt dieser Trend zu einem zunehmend dezentraleren Implementationsarrangement des Aufgabenfeldes der Polizei und mithin zu einer politknäheren, heterogeneren, offeneren, dekonzentrierteren und fragmentierteren Sicherheitsgewährleistung. Gleichzeitig lässt sich durch die Europäisierung/Internationalisierung der drei Aufgabenfelder ein Trend zu zentraleren Implementationsarrangements ausmachen, der die Sicherheitsgewährleistung gleichsam politknäher, heterogener und offener, aber auch konzentrierter und integrierter ausformt. Die Strukturentwicklungen im Politikfeld der Inneren Sicherheit werden im Folgenden am Beispiel von zwei Policies verdeutlicht.

4 Strukturentwicklungen in den Aufgabenfeldern

4.1 Videoüberwachung öffentlicher Räume

Die sicherheitspolitische Policy der polizeilichen ‚Videoüberwachung öffentlichen Räume‘ (im Weiteren kurz: VÜ) steht symptomatisch für den Kommunalisierungsprozess im Aufgabenfeld der Polizei und bezieht sich in der programmatischen Ausformung auf die oben beschriebene Dynamik im Mehrebenensystem zwischen Staat und Stadt (Lanfer 2012).

Die VÜ ist ein Programm, das sich erheblich von der Videoüberwachung in privaten oder privatwirtschaftlich genutzten Räumen (wie in Kaufhäusern, Tankstellen, Personenzügen, Bahnanlagen) unterscheidet. Im Vergleich zur privaten Videoüberwachung werden VÜ

wesentlich seltener durchgeführt. Dabei darf der öffentliche Raum nur durch öffentliche Behörden mit Sicherheitsaufgaben kameraüberwacht werden. Weil das Programm mit grundrechtseinschränkenden Wirkungen der überwachten Bürger einhergeht, muss für die anordnenden Behörden eine Ermächtigungsgrundlage bestehen. Erforderlich ist somit ein Gesetz, das die durchführende Behörde auf programmbezogene Zwecke, Mittel und politisch-administrative Verfahren festlegt.

Während die Policy VÜ in Deutschland bereits seit Beginn der 1990er Jahre vor dem Hintergrund eines internationalen Trends für mehr Sicherheit im kommunalen Raum und praktischen Anwendungen von VÜ insbesondere in London politisch diskutiert wurde, erfolgten programmermöglichende Gesetzgebungsprozesse erst ab dem Jahr 2000. Die weitere Beschreibung bezieht sich exemplarisch auf die Gesetze und Programme zur VÜ in den Ländern Brandenburg, Hessen und NRW.

Am Beispiel der drei untersuchten Ländern lassen sich anhand der (1) Zweck- und Ortsbindung, (2) Zeitraum der Datenspeicherung, (3) anordnende Behörde und (4) Berichtspflichten der anordnende Behörde die Gesetze zur VÜ folgendermaßen zusammenfassen: (1) Die VÜ kann zur Abwehr von Gefahren und Straftaten in bestimmten kommunalen Räumen mit erhöhter Kriminalität (§31 Abs. 2 Bbg PolG, §14 Abs. 3 HSOG, §15a Abs. 1 PolG NRW) – den sogenannten Angsträumen – durchgeführt werden, wenn aus *Erfahrung* zu erwarten ist, dass hier auch zukünftig Straftaten begangen werden. Bei den ‚Kriminalitätsräumen‘ handelt es sich um solche öffentlichen Räume, die im Vergleich zu anderen Räumen *in der jeweiligen Kommune* als stark kriminalitätsbelastet und von der Bürgerschaft allgemein als ‚unsicher‘ bewertet werden. (2) Die Speicherung der über die VÜ aufgezeichneten Daten ist in Brandenburg bis 48 Stunden (§31 Abs. 2 BbgPolG), in Hessen bis zu zwei Monate (§14 Abs. 1 HSOG) und in NRW bis zu 14 Tage (§15a Abs. 3 PolG NRW) möglich, wenn diese nicht für die Verfolgung von Straftaten und – nur in Hessen und Brandenburg: – Ordnungswidrigkeiten benötigt werden. (3) Die Anordnungskompetenz der Maßnahme haben in Brandenburg der Innenminister auf Vorschlag des Behördenleiters (§31 Abs. 2 Bbg PolG), in Hessen die Polizeibehörden und die (kommunalen) Gefahrenabwehrbehörden (§14 Abs. 3 und 4 HSOG) und in NRW der Behördenleiter als Polizeipräsident oder Landrat (§15a Abs. 3 PolG NRW). (4) Die Voraussetzung der angeordneten Maßnahme ist zeitlich begrenzt. Um die Maßnahme fortzusetzen müssen die Voraussetzungen in Hessen nach zwei Jahren (§14 Abs. 3 HSOG), in NRW und Brandenburg nach jeweils einem Jahr überprüft werden. Eine Maßnahmenverlängerung ist in NRW aufgrund eines Nachweises der weiteren Erforderlichkeit über eine polizeiliche Dokumentation möglich (§15a Abs. 4 PolG). In Brandenburg muss der anordnende Innenminister jährlich dem parlamentarischen Innenausschuss über jede Maßnahme durch Angaben über Ort und Dauer und die hierfür jeweils zugrundeliegenden Lageerkenntnisse über die zu erwartende örtliche Kriminalitätsbelastung berichten (§31 Abs. 2 Bbg PolG).

Diese kurze Zusammenfassung der gesetzlichen Regelungen zeigt grundsätzlich vergleichbare Gesetzesinhalte in den drei Ländern, die sich nicht wesentlich hinsichtlich des Zweck- und Ortsbezugs unterscheiden: Primär ist die *Straftatenvorbeugung* in kommunalen *Kriminalitätsräumen*. Der Programmzweck bezieht sich nicht nur auf die Störer

und Straftäter, die präventiv von ihrer Tat wie insbesondere Diebstahldelikte, Raub, Körperverletzungen, Betäubungsmitteldelikte oder Sachbeschädigung abgehalten (Straftatvorbeugung) oder bei ihrer Tatausführung unterbrochen werden (Abwehr konkreter Gefahren) sollen. Er richtet sich auch auf die unverdächtigen Bürger, die sich im überwachten kommunalen Raum aufhalten, weil für die präventive Wirkung einerseits nicht zwischen den potenziellen Tätern und den unverdächtigen Bürgern unterschieden werden kann und andererseits durch die Kamerapräsenz ‚in der Fläche‘ sowohl messbare Sicherheitseffekte als auch subjektive Sicherheitsgefühle erzeugt werden sollen. Das Programm lässt sich als ein typisches Zweckprogramm bezeichnen. Der Zweck wird allgemein benannt, der konkrete Einsatz der VÜ und auch der Einsatzort sind hingegen unbestimmt und können erst durch die Implementation in Bezug auf spezifische Räume hinreichend definiert werden. Auch die konkreten Wirkungen der VÜ sind für die Erreichung des allgemeinen Zwecks unbestimmt. Hinsichtlich allgemeiner Anforderungen an hoheitliche Maßnahmen mit grundrechtseinschränkender Wirkung muss sie aber erforderlich, geeignet und verhältnismäßig sein, um das allgemeine Ziel der Straftatenvorbeugung zur Minderung der Kriminalitätsbelastung in bestimmten Kriminalitätsräumen zu erreichen.

Die Gesetze zur VÜ führen im Aufgabenfeld zu untypischen Implementationsstrukturen. Während in Brandenburg die einzelnen Behörden in Absprache mit dem Innenministerium die VÜ vorschlagen, kann sie in NRW und Hessen durch die Polizeipräsidien und speziell in Hessen auch durch die kommunalen Behörden angeordnet werden.

Die Anordnungskompetenz ist demnach relativ dezentral institutionalisiert. Der Zweckbezug des Programms verlangt mithin eine *dezentrale* Ausrichtung, weil die Ursachen und Wirkungen nicht für sämtliche Kommunen im Land allgemeinverbindlich geregelt werden können. Gleichzeitig muss das Programm *dekonzentriert* durch einzelne Behörden in Bezug auf bestimmte kommunale Räume durchgeführt werden. Dies liegt einerseits an den besonderen örtlichen Bedingungen, die für eine Programmanordnung festgestellt und für eine Programmfortsetzung über Berichte turnusgemäß geprüft werden müssen. Darüber hinaus erfordert das Programm eine enge Abstimmung mit kommunalpolitischen Akteuren, was in den drei untersuchten Ländern durch einen programmbezogenen oder auch institutionalisierten Austausch zwischen der anordnenden Behörde (in NRW etwa der Polizeipräsident) und dem Oberbürgermeister erfolgte. Die Entscheidung zur Durchführung und mithin für die Verlängerung eines Programms zeigte sich zudem abhängig von den Unsicherheitsgefühlen der Bürger in Bezug zu bestimmten ‚Angsträumen‘ und konkreten Forderungen der politischen Zivilgesellschaft, die in lokalen Medien polizeiliche oder kommunale Programme für mehr Sicherheit in der Kommune allgemein und in bestimmten kommunalen Orten einforderten. Vor diesem Hintergrund sind die Programmanordnung und -durchführung von verschiedenen kommunalpolitischen Impulsen abhängig. Die Implementation der VÜ reagiert somit auf die situations- und kontextspezifischen kommunalen Bedingungen, sodass im Verhältnis zum typischen Implementationsarrangement des Aufgabenfelds relativ offene und heterogene Implementationsbedingungen vorherrschen.

Die Implementationsprozesse der VÜ lassen sich als Konglomerat von Interessen kommunaler und staatlicher Akteure beschreiben. Die Kommunalpolitik hat ein zunehmendes Sicherheitsinteresse, weil die Unsicherheitsgefühle der Bürgerschaft in Bezug zu bestimmten kommunalen Orten zunehmen und die Gefahr besteht, dass die Attraktivität der Stadt für kaufkräftige Bürger und Investoren gerade durch kriminalitätsbelastete kommunale Räume des Transits wie publikumsintensive Orte, Bahnhofsvorplätze oder Parks (Wehrheim 2012) abnimmt. Die (Ober-)Bürgermeister können sich entsprechend über Sicherheitsthemen und -programme profilieren. Während die Kommunen durchgängig eine Ausweitung von polizeilicher VÜ begrüßen, zeigen sich die politischen Interessen im Land weit weniger homogen. Die Untersuchung der Policy-Prozesse in den drei Ländern zeigt einen Policy-Konflikt zwischen Policy-Befürwortern und -Gegnern, der sich an dem oben beschriebenen Wertdual einer ‚kollektiven Sicherheit‘ und ‚individueller Freiheit‘ orientiert (Lanfer 2012, 2014). Die zentralen Argumente der beiden Policy-Koalitionen beziehen sich auf die Verhältnismäßigkeit in Verbindung mit den Effekten der VÜ. Die Gegner kritisieren, dass die geringen Programmeffekte die kontinuierlichen und weitgehenden Grundrechtseinschränkungen der Bürger nicht aufwiegen. Die Befürworter betonen hingegen, dass durch die Kameraüberwachung zahlreiche und vielfältige Effekte zur Straftatenvorbeugung, Steigerung des allgemeinen Sicherheitsgefühls der Bürger und für eine verbesserte Straftatenverfolgung erreicht werden können. Zudem werden vom Polizeipersonal einzelfallbezogen positive Effekte für die polizeiliche Aufgabenwahrnehmung angeführt.

Die Programmformulierungen waren ein Resultat der konfliktintensiven Policy-Prozesse. Sie haben konkrete Bedeutung für die Implementationsprozesse, weil die polizeilichen und ministerialen (Evaluations-)Berichte über die Programmeffekte politische Kontroversen auslösen (können). Dadurch bestehen hohe administrative Anforderungen für die Plausibilisierung einer Anordnung und Verlängerung des Programms. Diese hohen Anforderungen wurden von den Policy-Gegnern während den Gesetzgebungsprozesse wo immer möglich durchgesetzt, um eine ‚flächendeckende‘ VÜ bereits im Ansatz zu verhindern.

Zur Konkretisierung der Programmziele lässt sich aus den leitfadengestützten Befragungen mit dem Personal der anordnenden Behörden in den drei untersuchten Ländern die folgende *Effekthierarchie* (Primär-, Neben- und Sekundäreffekt) rekonstruieren: Für die Anordnung und Durchführung des Programms primär anleitend sind die Abschreckungseffekte. Die VÜ muss gefahrenabwehrend/straftatenverhütend wirken, weil sie dadurch die Entdeckungswahrscheinlichkeit der Täter erhöht. Mit diesem Primäreffekt kann das Programm eine im Verhältnis zum Sicherheitsbedarf der Bürger zu geringe Polizeipräsenz in den Kriminalitätsräumen kompensieren. Als Nebeneffekt soll das Unsicherheitsgefühl der Bürger reduziert werden, damit sie sich in den videoüberwachten Kriminalitätsräumen angstfrei bewegen können. Als sekundärer Effekt soll schließlich eine verbesserte Straftatenverfolgung erreicht werden, wenn von Straftätern bei der Tatausführung Bilder aufgezeichnet werden, die für das Strafverfahren als Beweismittel verwendet werden können. Diese Effekthierarchie ist dem Anspruch nach normbezogen und somit zweck- und rechtmäßig. Als Präventionsprogramm mit stark grundrechtseinschränkenden Wirkungen

sind aber die tatsächlichen Programmeffekte von grundlegender politischer Bedeutung. Die zu erwartenden Effekte für die Programmimplementation müssen relativ ausführlich begründet und die Programmwirkungen infolge der Implementation durch die gesetzlich geforderten Berichte nachgewiesen werden, wenn die Maßnahme verlängert werden soll.

Bei der VÜ als Präventionsprogramm ist die Feststellung einer hohen Kriminalitätsbelastung und einer gefahrendabwehrenden/straftatenvorbeugenden Wirkung schwierig und mithin nur durch methodisch plausible und damit aufwändige wissenschaftliche Evaluationsstudien zu belegen (Bornewasser/Classen/Stolpe 2008, Bornewasser 2005, Bücking 2004). In den drei untersuchten Ländern erfolgten die Dokumentationen über die Programmwirkung im Rahmen der turnusmäßigen Berichte ausschließlich durch die zuständigen Behörden und zeigten Veränderungen der räumlichen Kriminalitätsbelastung anhand der polizeilichen Kriminalstatistik im Verhältnis zur kommunalen Gesamtkriminalität und einem Vergleichsraum. Signifikante Änderungen ließen sich dabei häufig nicht feststellen und wenn doch, konnten die Effekte nicht eindeutig auf das Programm zurückgeführt werden. Die Fortsetzung des Programms erfolgte somit in der Regel nicht durch sachbezogene Informationen über Effekte, die immer auch anders ausgelegt werden können, sondern aufgrund einer politisch-administrativen Überzeugung über die Wirkung der VÜ. Diese Probleme stehen in Verbindung mit den Begründungsschwierigkeiten bei der Auswahl der Kriminalitätsräume, weil eine Anordnung aus denselben Gründen nicht ‚objektiv‘ begründet werden kann. Der Zweck der VÜ ist somit hinsichtlich der Anordnung als auch Fortsetzung stark abhängig von Einschätzungen und Interpretationen der Behörden und bezieht sich nicht zuletzt auf die – zumindest durch die Behörden – nicht quantifizierbaren Unsicherheitsgefühle der Bürger.

Die Effekte der VÜ werden vor allem durch ihre politischen Gegner bezweifelt. Kritisiert werden vor allem die Verdrängungseffekte (Straftäter suchen nicht überwachte Orte auf), Vermeidungseffekte (Straftäter schützen sich vor Identifizierung) und die fehlende präventive Wirkung bei Gewaltdelikten, die häufig im Affekt begangen werden. Auch wird das Programm im Verhältnis zu anderen Sicherheitsprogrammen bewertet. Die Befragung des Polizeipersonals zeigt, dass neben den politischen Policy-Gegnern nicht zuletzt die Polizei eine mögliche Ausweitung des Programms kritisiert, weil dieselben Effekte durch eine Erhöhung der Polizeipräsenz zu erreichen wären und die finanziellen und personellen Ressourcen entsprechend falsch investiert seien. Aus diesen Gründen wird sowohl die Geeignetheit und Verhältnismäßigkeit als auch die Erforderlichkeit des Programms kritisiert.

Insgesamt lässt sich die VÜ als ein zweckbezogenes und zukunftsoffenes Zweckprogramm bezeichnen, das allgemeine raumbezogene Ziele verfolgt, um Straftaten in einem öffentlichen Raum über verdachtsunabhängige Überwachung vorzubeugen und diesen dadurch insgesamt effektiv oder symbolisch sicherer zu machen. Die bereits oben ausgeführte Implementationsbedingung der VÜ zeigt eine deutliche Abweichung vom typischen Implementationsarrangements des Aufgabenfelds. Als vornehmlich staatliches Instrument der Gefahrenabwehr mit stark grundrechtseinschränkender Wirkung ist es untypisch unbestimmt hinsichtlich seiner operativen Elemente. Als Zweckprogramm ermöglicht es eine kontext- und situationsspezifische Auswahl, Schwerpunktsetzung

und Kombination nahezu sämtlicher Operationsmodi. Dabei wirkt der *Steuerungsmodus* anleitend, der mit einem *regulativen Modus* verbunden wird: Die VÜ ist ein Instrument, das sich durch unklare Problemstrukturen (Ursachen) und Problemlösungen (Wirkungen) auszeichnet. Ob die VÜ eingesetzt wird, hängt von kommunalen Kontexten und Situationen ab, die eine Begründung mehr oder weniger plausibel erscheinen lassen. Vor allem in Brandenburg und NRW müssen die VÜ in ein kommunales Sicherheitskonzept eingebunden werden, sodass einerseits eine intensive Abstimmung zwischen dem Polizeipersonal und kommunalen Akteuren mit Sicherheitsinteressen erforderlich ist und andererseits die Isolierung eines Effekts der VÜ zusätzlich erschwert wird. Darüber hinaus zeigt sich, dass mit dem Programm bestimmte Kontextsteuerungen verbunden sind, die weit mehr als die Installation von Kameras umfassen. Beispielsweise besteht nach Angaben eines Polizeipräsidenten ein wesentliches Problem darin, dass nach einer Einstellung der VÜ die hierfür verantwortliche Behörde (in der Regel die Polizeipräsidenten) gerade für schwere Straftaten im vorher überwachten Raum politisch verantwortlich gemacht werden. Insofern sind es nicht zuletzt verschiedene Deutungsstrukturen zwischen den verschiedenen kommunalen und staatlichen Akteuren, die auf den Bedarf und die Art und Weise einer unsicherheitsreduzierenden Wirkung des Programms Einfluss nehmen. Zu unterscheiden sind dabei gänzlich unbestimmte Wirkungen auf die Unsicherheitsgefühle und nur unzureichend bestimmbar präventive Wirkungen. Gleichzeitig wirkt mit dem Steuerungsmodus ein regulativer Modus: Neben den vielfältigen Verfahrensvorschriften (Datenschutz, Berichtspflichten) darf die VÜ auch nur dann durchgeführt werden, wenn eine *konkrete* Gefahr im überwachten Raum zeitnah abgewehrt werden kann. Dies setzt voraus, dass sie nur in unmittelbarer Nähe zu einer Polizeibehörde durchgeführt werden kann, die zudem Polizeipersonal für die kontinuierliche Inaugenscheinnahme der Monitore ‚abstellen‘ muss. Daneben umfasst die VÜ ein *Anreiz- und Überzeugungsmodus*: Die Bürger und mithin die potenziellen Täter sollen davon überzeugt werden, dass im überwachten Raum Straftaten entdeckt werden. Gleichzeitig werden Anreize gesetzt, den Raum als sicher zu bewerten, unabhängig davon, ob dieser – vor allem durch die polizeiliche Kriminalitätsstatistik – ‚objektivierbar‘ als unsicher bezeichnet werden konnte oder durch die VÜ infolge einer Reduktion von Kriminalität faktisch sicherer gemacht wurde. Aus der Perspektive der Kommunen erscheint die VÜ auch deshalb positiv, weil sie sich auch auf die Reduktion von Ordnungsverstößen auswirken kann.

Die VÜ kann als Instrument nicht auf einen bestimmten operativen Modus reduziert werden. Es wirkt vielmehr ein anderer/neuer Modus, der so wie einige andere kommunale Sicherheitskonzepte als *raumbezogener* Modus charakterisiert werden kann.

Das Programm der VÜ im Aufgabenfeld der Polizei zeigt sich als eine spezifische Problemlösung für die Anforderungen einer ‚neue Sicherheit‘ zwischen Staat und Stadt. Die Programmeffekte sind ganzheitlich ausgelegt, präventiv resp. zukunftsorientiert und (auch) auf die subjektiven Unsicherheitsgefühle der Bürger bezogen. Dabei fokussieren sie eindeutig eine kollektive Sicherheit, die nur schwer mit individuellen Freiheiten einzelner Bürger im Einklang gebracht werden können. Das Programm umfasst operative und instrumentelle Elemente, die als untypisch bezeichnet werden können, um auf die gleichsam untypischen

Implementationsbedingungen reagieren zu können. Im Aufgabenfeld steht das Programm symptomatisch für eine neue Rolle der Polizei, die für die (kommunale) Sicherheitsgewährleistung nicht mehr alleine zuständig ist, sondern hierbei nur noch ein, wenngleich weiterhin wesentlicher, Akteur unter vielen ist. Im Sinne des anleitenden Steuerungsmodus zeigt sich, dass die Polizei als Interdependenzmanager (Mayntz 1997: 273) fungiert und bei ihrer Aufgabenwahrnehmung heterogene Interessen in einer offenen, dialogischen Form kontext- und situationsspezifisch (dezentral, dekonzentriert) einbeziehen muss. Die Polizei bewegt sich dabei zwischen einer ‚alten‘ und einer ‚neuen Sicherheit‘. Eine Vermischung beider Sicherheitsparadigmen und verschiedener Implementationsarrangements wirkt für einen Programmerfolg nicht förderlich, weil die VÜ bereits am Output scheiterte. Im Untersuchungszeitraum macht nur das Land Hessen – vermutlich aufgrund der erweiterten Anordnungs Kompetenzen für die Kommunen – über Einzelfälle hinaus vom Programm Gebrauch macht. Aussagen über die Output-, Impact oder sogar Outcome-Effekte sind dabei abhängig von den spezifischen kommunalen Implementationskontexten und -situationen. Effekte werden dabei in der Regel nicht nach methodischen Standards oder Gütekriterien evaluiert, sondern nur durch die anordnenden Behörden in Verbindung mit den Innenministerien geschätzt.

4.2 Cyber-Sicherheit

Die Policy Cyber-Sicherheit bezeichnet ein sicherheitspolitisches Thema, das sich auf Gefährdungen und Risiken der öffentlichen Sicherheit durch zunehmende gesellschaftliche Nutzung von Informations- und Kommunikationstechnologien bezieht. Die Policy ist quasi ein ‚Querschnittsthema‘ und koppelt zunehmend nicht nur innerhalb des Politikfelds die Aufgabenfelder und -bereiche, sondern konzentriert und zentralisiert die sicherheitspolitischen Strukturen auf Bundesebene, um effektivere Governance-Netzwerke zwischen staatlichen und privatwirtschaftlichen Sicherheitsakteuren auf europäischer und internationaler Ebene zu etablieren. Entsprechend bringt die Policy den gegenwärtigen Politikfeldwandel besonders gut zum Ausdruck.

Die Policy bezieht sich zunächst auf Gefahren und Risiken für die öffentliche Sicherheit, die durch die computergesteuerte Datenverarbeitung und digitale Kommunikation vor allem im Internet erkannt werden. Sie führen entsprechend zu Computerkriminalität, die *in einem weiten Sinne* sämtliche Straftaten umfasst, „bei deren Begehung auch der Computer als Tatmittel Verwendung findet“ (wie Kapitalanlagebetrug, Rauschgifthandeln, illegaler Waffenhandeln, Geldwäsche, Beleidigung, Vorbereitung terroristischer Handlungen, Urheberrechtsverletzungen) und sich in einem engeren Sinne auf die Straftaten bezieht, die „das Vorhandensein der EDV voraussetzen“ (Groll 2006a: 48) (wie Computerbetrug, -sabotage, -spionage, Softwarepiraterie, Datenschutzdelikte). Dabei versteht das Bundesministerium des Innern (2011) unter ‚Cyber-Raum‘ einen öffentlichen zugänglichen virtuellen Raum „aller auf Datenebene vernetzten IT-Systeme im globalen Maßstab“. Die Europäische Kommission definiert ‚Cyber-Crime‘ als „criminal acts that are committed

online by using electronic communications networks and information systems.“ (European Commission) Die auf Cyber-Crime im Cyber-Raum gerichtete erweiterte *Cybersicherheit* lässt sich nach dem Bundesamt für Sicherheit in der Informationstechnik beschreiben als

„das Aktionsfeld der klassischen IT-Sicherheit auf den gesamten Cyber-Raum. Dies umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein. Damit wird praktisch die gesamte moderne Informations- und Kommunikationstechnik zu einem Teil des Cyber-Raums.“

Aufgrund gering ausgeprägter sozialer Kontrolle, teilweise fehlender und nicht auf die neue Qualität der Kommunikation bezogenen rechtlichen Regelungen in den Staaten, der geringen Entdeckungswahrscheinlichkeiten von Cybercrime (vgl. Tabelle 1) aufgrund eines hohen Ausmaßes an (technisch gesicherter) Anonymität sowie raumentbundener resp. staatsübergreifender Interaktionen bei gleichzeitig geringen Handlungskapazitäten der (noch) dominant staatsbezogenen Sicherheitsbehörden zeigt sich der ‚Cyber-Raum‘ als ein im hohen Ausmaß staatlich unkontrolliertes oder auch unkontrollierbares ‚globales Dorf‘.

Die Zunahme der Cyberkriminalität steigern die Gefahren und Risiken für die öffentliche Sicherheit insbesondere in den folgenden Bereichen:

- Verunsicherungen der Bürger bei der Nutzung des Internets und die hiermit verbundene Beeinträchtigung der Geschäftsvorgänge
- Verbreitung verfassungsfeindlicher Positionen
- Wirtschaftsspionage
- Cyber-Angriffe auf öffentliche Einrichtungen und Infrastrukturen durch Hacker und Terroristen.

Während zunächst Anfang der 1990er Jahre der Problemfokus auf das „unerwünschte Eindringen in fremde Rechnersysteme, Computersabotage, Softwarepiraterie und Scheckkartenfälschung“ (Lange/Mittendorf 2001: 278) und das Ausforschen von Datenbanken durch gegnerische Nachrichtendienste (Böttcher 2015: 53) lag, entwickelt sich ab Mitte der 1990er Jahre ein zusätzlicher Fokus, indem sich das BKA und die LKÄ auf die Verbreitung verbotenen Materials wie Kinderpornografie und den Vorbereitungen von Verbrechen zuwendeten (Lange/Mittendorf 2001: 278). Seit Beginn des 21. Jahrhunderts intensiviert sich die Problemperspektive insbesondere hinsichtlich der Gefährdungen der wirtschaftlichen Nutzung des Internets.

Neben den Aufgabenfeldern der Polizei und des Verfassungsschutzes zeigen sich auch für den Bevölkerungsschutz neue Problemperspektiven wie insbesondere durch terroristische und extremistische Angriffe auf die öffentlichen Infrastrukturen im In- und Ausland.

Das Politikfeld der Inneren Sicherheit ist somit in sämtlichen Aufgabenfeldern mit neuen Sicherheitsgefahren und -risiken konfrontiert: „Die Gefahr kann von (fast) überall kommen, sie kann (fast) überall zuschlagen und sie kann (fast) alles lahm legen.“ (Groll

2006a: 50) Die Cyber-Sicherheit ist dabei ein sicherheitspolitisches Problem, das sich vor allem technikabhängig zeigt und einen beschleunigten und teilweise auch abrupten Wandel der Problemperzeption und Problemlösungsorientierung hervorruft. Hiermit verbunden ist ein stetiger Informationsbedarf der staatlichen Sicherheitsbehörden, die häufig nicht die ausreichenden administrativen Kapazitäten (wie finanzielle Ressourcen, Bereitstellung und Ausbildung des Personals) entwickeln (können), um handlungsfähig zu bleiben. Um dieses Problem zu lösen erfolgt zunehmend eine Kooperation und auch stärkere Aufgabenteilung zwischen den Organisationen staatlicher und privater Sicherheitsproduzenten (Lange/Mittendorf 2001: 288-290).

Diese sicherheitspolitische Strategie wird auch vom Bundesministerium des Innern (2016b) betont. Nach Böttcher (2015: 98f.) führe die potenziell grenzenlose Cyberwelt entsprechend auch zu einer grenzenlosen Kooperation der einzelnen Sicherheitsakteure. In diesem Sinne verstärkt die Policy den staatlichen Bedarf an koordinierter Sicherheitsherstellung einerseits zwischen den Aufgabenfeldern und -bereichen. Die Policy fungiert somit gegenwärtig als Schnittstelle der drei Aufgabenfelder ‚Polizei‘, ‚Verfassungsschutz‘ und ‚Bevölkerungsschutz‘ und verzahnt deren Problem- und Problemlösungsstrukturen zunehmend miteinander. Andererseits verzahnt die Policy auch verschiedene Politikfelder (vor allem die Innere und äußerer Sicherheit), Staaten und sämtliche nachgeordneten politischen Ebenen miteinander.

Die aus der Policy mit starker Querschnittswirkung („Meta-Policy“) hervorgehenden Sicherheitsprogramme beziehen sich dann auch auf das gesamte Spektrum staatlicher Handlungsformen. *Regulative Programme* lassen sich vornehmlich unter eine ‚Internetüberwachung‘ subsumieren. Hierunter fallen alle staatlichen Handlungsweisen, „welche auf die Sammlung und Auswertung von im Internet vorhandenen oder beim Zugang zum Internet anfallenden Daten abzielen.“ (Groll 2006b: 140) Bei der Überwachung der Internetdaten ist zu unterscheiden zwischen der teilweise auch infolge von automatisierter und systematischer Suchsoftware unterstützen Recherche nach verbotenen Text- und Bildinhalten, dem keine Eingriffsqualität von Seiten der Sicherheitsbehörden zukommt, und den Informationserhebungen und -verarbeitungen über die Provider, was rechtlich mit einer Telekommunikationsüberwachung gleichgestellt wird (ebd.) und besondere Ermächtigungsgrundlagen erfordert. Diese sind mit den Artikeln 1-3 des Terrorismusbekämpfungsgesetzes geschaffen worden. Die privatwirtschaftlichen Unternehmen (Provider) haben demnach gegenüber dem Bundesverfassungsschutz, MAD und BND umfangreiche Auskunftspflichten. Nach der am 24. Oktober 2001 beschlossenen Telekommunikationsüberwachungsverordnung wurden die Voraussetzungen geschaffen, „über die Installation fester Schnittstellen bei den Providern die Direktüberwachung der Inhalts-, Verbindungs- und Nutzungsdaten (...) ohne Zeitverzug und auf Kosten der Anbieter zu ermöglichen.“ (Groll 2006b: 142) Hierdurch erhalten die Sicherheitsbehörden Auskünfte von den Providern hinsichtlich bereits erfolgter und zukünftiger Nutzung des Netzes (ebd.).

Daneben sind die vornehmlich präventiv orientierten *Steuerungs- und Überzeugungsprogramme* hervorzuheben: Die Überzeugungsprogramme sollen bei den Bürgern und der Privatwirtschaft sicherheitssensible Verhaltensweisen im Umgang mit dem Computer und

Internet erzeugen und Unsicherheiten reduzieren. Dadurch soll zum Selbstschutz angeregt werden. Die Steuerungsprogramme sind darauf ausgelegt, Governance-Netze zwischen staatlichen und privatwirtschaftlichen ‚Wissensträgern‘ zu begründen, durch die Informationen über Gefährdungslagen und mögliche Problemlösungen erzeugt werden sollen. Sie tragen dazu bei, dass sich die Policy zu einem neuen Aufgabenbereich institutionalisiert und eine eigene Implementationsstruktur ausbildet. Diese spezifischen Governance-Netze und Steuerungsprogramme werden im Weiteren beschrieben:

Zunächst ist als Kooperationsforum das am 23. Februar 2011 gegründete Nationale Cyber-Abwehrzentrum (Cyber-AZ) hervorzuheben. Es wird zwar vom Bundesamt für Sicherheit in der Informationstechnik (BSI) federführend geleitet, bietet aber einen institutionellen Austausch vornehmlich zwischen dem BSI, BfV und BBK. Weitere Mitglieder sind das BKA, die BPol, das Zollkriminalamt (ZKA), der BND und die Bundeswehr. Insofern werden über die drei zentralen Aufgabenfelder im Politikfeld der Inneren Sicherheit hinaus auch Aufgabenfelder des Politikfelds der äußeren Sicherheit miteinander verzahnt. Von der Zusammenarbeit der Sicherheitsbehörden geht eine Gefahr für die rechtstaatliche Ordnung aus und erfordert eine besondere Sensibilität. Entsprechend betont das BMI, dass alle Informationen der teilnehmenden Behörden unter strikter Bewahrung ihrer jeweiligen gesetzlichen Aufgaben und Befugnisse über tägliche Lagebesprechungen eruiert, zusammengeführt und bewertet werden (Bundesministerium des Innern 2016a). Dabei bewerte

„das BSI einen Cyber-Angriff aus technischer Sicht, das BfV befasst sich mit der Frage, ob der Angriff möglicherweise von einem ausländischen Nachrichtendienst ausgegangen ist und das BBK bewertet die Auswirkungen von möglichen Angriffen auf Infrastrukturen. Die darüber hinaus mitwirkenden Behörden fügen ihre Erkenntnisse über neue Angriffswege und Angriffswerkzeuge ein, dadurch liegt innerhalb kürzester Zeit ein aktuelles, umfassendes Lagebild vor.“ (ebd.)

Über eine verstärkte Zusammenarbeit zwischen den Sicherheitsbehörden hinaus, widmet sich der *Cyber-Sicherheitsrat (Cyber-SR)* vor allem den Beziehungen zwischen den staatlichen Sicherheitsbehörden und der Wirtschaft. Nach dem BMI bilde der Cyber-SR eine politisch-strategische Ebene zwischen Staat und Wirtschaft und entwickle präventive Instrumente und übergreifende Politikansätze für Cyber-Sicherheit. In diesem Rahmen erfolgte die bisherige Schwerpunktsetzung auf den Schutz kritischer Infrastrukturen und die Cyber-Außenpolitik Deutschlands. Der Cyber-SR tagt dreimal jährlich. Die teilnehmenden Organisationen sind insbesondere das Bundeskanzleramt, die Ressorts ‚Auswärtiges Amt‘ und die Bundesministerien der Verteidigung, für Wirtschaft und Technologie, für Justiz, für Finanzen und für Bildung und Forschung sowie Vertreter der Länder Baden-Württemberg und Hessen. Aus der Wirtschaft sind „vier hochrangige Wirtschaftsvertreter“ vom Bundesverband der Deutschen Industrie e. V., der BITKOM als Verband der digitalen Wirtschaft, der Deutsche Industrie- und Handelskammertag und der Übertragungsnetzbetreiber Amprion als assoziierte Mitglieder vertreten (Bundesministerium des Innern 2016b). Als weiteres Koordinationsgremium ist das Gemeinsame Internetzentrum (GIZ) anzuführen, an dem das BfV geschäftsführend und das BKA, der BND, MAD und Generalbundes-

anwalt beteiligt sind. Darüber hinaus bestehen Kooperationen zwischen dem BMI, BSI, BBK und verschiedener Unternehmen zum Schutz kritischer Infrastrukturen (KRITIS) als gemeinsame Initiative, wobei die Telekommunikation und Informationstechnik hier u. a. als ein schutzbedürftiger ‚Sektor‘ relevant ist.

Auf der europäischen Ebene verfolgt die European Union Agency for Network and Information Security (ENISA) das Ziel, einzelstaatliche Behörden und EU-Institutionen zu beraten und andererseits den Austausch von sicherheitsrelevanten Verfahrensweisen durch Kooperation zwischen EU-Institutionen, den staatlichen Behörden der Mitgliedstaaten und den Unternehmen zu erleichtern. Die Organisation verfolgt demnach sowohl Überzeugungs- und Informationsprogramme als auch Steuerungsprogramme. Letzteres kommt insbesondere durch die Computer Emergency Response Teams (CERTs) zum Ausdruck. Deren Ziel ist es, dezentral Instrumente in den Mitgliedstaaten (in Deutschland vor allem die Verwaltungen der Länder) hervorzubringen, die zum Aufbau von Kapazitäten für einen effektiven und effizienten Schutz kritischer Informationsinfrastrukturen sorgen, indem sie insbesondere IT-Sicherheitsvorfälle sammeln, auswerten und hierüber (standardisiert) berichten.

Die CERTs ermöglichen eine vertikale und horizontale Koordination im europäischen Mehrebenensystem des Politikfelds der Inneren Sicherheit, sodass durch sie eine hoch anspruchsvolle diagonale Implementationsstruktur verfolgt wird. Weitere Handlungsformen von ENISA sind die Vermittlung von good practices, die Initiierung von Übungen wie z. B. Cyber Europe 2016 (Enisa 2016b), Cyber Atlantic 2011 (Enisa 2016a) sowie Trainingseinheiten und Seminare (Enisa (2016c). Zudem soll durch das Programm European Public Private Partnership for Resilience (EP3R) der Austausch zwischen staatlichem und privatem Sektor gefördert werden (Enisa 2016d).

Ein weiterer zentraler Akteur der Cyber-Sicherheit auf der europäischen Ebene ist das *Europol*, das insbesondere die polizeiliche Zusammenarbeit der Polizeibehörden aus den Mitgliedstaaten koordiniert. Das hier angesiedelte European Cybercrime Centre – EC3) bildet den Schwerpunkt bei der Bekämpfung von Cyber-Kriminalität in der EU, indem es die Mitgliedstaaten und die EU bei der Bewertung und Ermittlung unterstützt und Kooperationen mit internationalen Akteuren unterhält (EC3 Europol (2016b)).

Einige für die Policy bedeutende Organisationen auf der internationalen Ebene sind die der UN zugehörigen International Telecommunication Union (ITU) mit dem Arbeitsbereich ‚Cybersecurity‘, die OECD, OSZE und NATO. Sie entwickeln verschiedene Strategien zur Gewährleistung von Cyber-Sicherheit, indem sie Einfluss auf das internationale Staatensystem nehmen und verschiedene Standards, Übereinkommen, Empfehlungen und Interessen für eine Erweiterung der Sicherheitsherstellung und/oder einer Gewährleistung des Datenschutzes in die politische Diskussion einbringen.

Die Strukturverflechtungen im Aufgabenbereich der Cyber-Sicherheit sind zahlreich und vielfältig. Jedes Aufgabenfeld des Politikfelds wird einbezogen und institutionell miteinander verzahnt. Innerhalb der Aufgabenfelder und Aufgabenbereiche erfolgen komplexe diagonale Kooperationen zwischen den spezifischen Sicherheitsbehörden im politischen Mehrebenensystem (international, europäisch, gesamt- bzw. bundesstaatlich und länder-

bzw. regionenbezogen). Dabei sind bereits die formalen Strukturgeflechte innerhalb der Aufgabenfelder und gerade auch zwischen den Aufgabenfeldern im Mehrebenensystem unübersichtlich. Die folgende Abbildung 2 gibt eine Übersicht über die Strukturen der Cyber-Sicherheit, die sich auf die policy-spezifischen Kooperationen der *zentralen* Akteure und Institutionen bezieht.

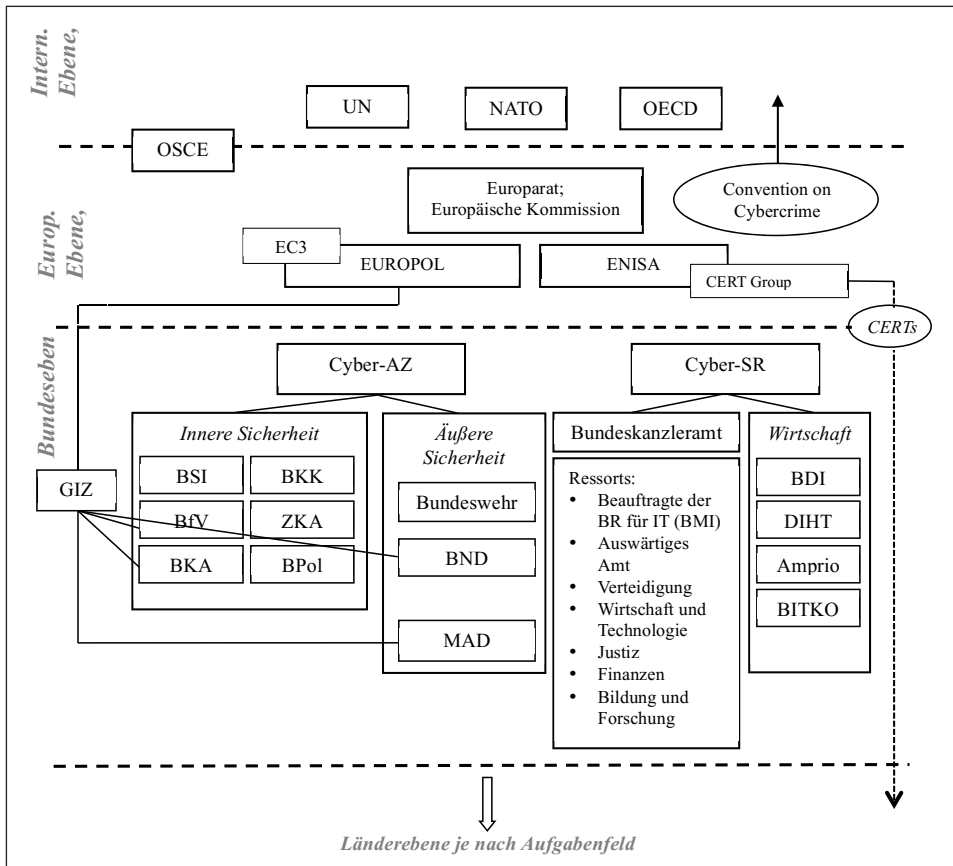


Abb. 2 (Aufgabenfeldübergreifende) Strukturen von Cyber-Sicherheit im Politikfeld der Inneren Sicherheit

Quelle: Lanfer (2017: 61).

Deutlich wird an den Policy-Strukturen, dass die vormalig im Politikfeld eher untypischen Verflechtungen zwischen den Politikfeldern der äußeren und Inneren Sicherheit, zwischen den Aufgabenfeldern der Inneren Sicherheit, der Europäisierung/Internationalisierung als auch der Ökonomisierung/Privatisierung durch die Beteiligung privatwirtschaftlicher Organisationen bei der politischen Problem- und Problemlösungsfindung zunehmen.

Die Policy Cyber-Sicherheit hat dabei sicherlich eine Sonderstellung im Politikfeld, weil der Problem- und Problemlösungsbezug staats-, politik- und aufgabenfeldübergreifende Handlungslogiken hervorbringt. Hieraus ergeben sich sowohl Kapazitäten zur Steigerung der leistungsbezogenen Output-Legitimität als auch Gefahren für die demokratiebezogene Input-Legitimität, weil die Politik- und Aufgabenfelder zur Machtbegrenzung weiterhin mehr oder weniger stark voneinander formal-institutionell getrennt sind.

Die fortschreitende Institutionalisierung des neuen Aufgabenfelds ist stark abhängig von den staatlichen Problemperceptionen und Problemlösungen, beschränkt sich aber nicht hierauf. Während durch das (zwischen-)staatliche Behördennetzwerk die kollektive Sicherheit betont wird, betonen Bürgerrechtsorganisationen den Wert der individuellen Freiheit. Dabei wird die Gewährleistung von Bürgerrechten als Abwehrrechte der Bürger vor staatlichen Sicherheitsprogrammen kontinuierlich eingefordert. Die Aufrechterhaltung von Anonymität im Internet, Betonung von Selbstschutz der Bürger gegen IT-Angriffe, Freiheit von Überwachung und Kontrolle im Netz leiten die Gegenpositionen an. Ein sicheres Internet meint entsprechend auch den Schutz individueller Freiheiten, des Rechtes auf informationelle Selbstbestimmung und allgemein demokratischer Strukturen (Bendieck 2012: 5). So sehen die Datenschützer und die Wirtschaftslobby die Verschlüsselungstechnik im elektronischen Datenverkehr als erforderlich, um die informationelle Selbstbestimmung zu sichern und den Selbstschutz jedes Einzelnen zu fördern. Durch anonyme Netzzugänge soll somit letztlich ein allgemeines Vertrauen bei den Bürgern bzw. potenziellen Konsumenten für die Nutzung von IT und elektronischer Geschäftsvorgänge gewährleistet und erhöht werden. Diese Interessen stehen jedoch im Konflikt zu sicherheitsorientierten politischen Programmen in der Cyber-Sicherheit. Stellvertretend für diesen Konflikt ist die Diskussion um Verschlüsselungstechniken („Hacker Tools“), die einen anonymen Netzzugang fördern und dadurch gleichzeitig die staatlichen Überwachungsmöglichkeiten reduzieren und deren Verbot beispielsweise der Europarat gegen die Interessen von Datensicherungsexperten einforderte (Groll 2006a: 51). So sorgte die Telekommunikationsüberwachung lange Zeit für Widerstand bei den privatwirtschaftlichen Unternehmen und IT-Verbänden, weil sie die Provider dazu verpflichtete, Inhalts-, Verbindungs- und Nutzungsdaten zur Verfügung zu stellen (Groll 2006b: 141-142). Von Befürwortern einer kollektiven Sicherheit in den USA und der EU bestehen darüber hinaus Forderungen, private Unternehmen darauf zu verpflichten, Cyberangriffe an die zuständigen Stellen zu melden. Nach Bendieck (2012: 25) steht dem die Freiheit über die Informationsverfügung des Einzelnen oder des einzelnen Unternehmens entgegen:

„Hier handelt es sich um eine schwierige, kontroverse Abwägung hoher politischer Güter. Sie führt vor Augen, wie notwendig es ist, Fragen der Internetregulierung nicht nur in technischen Expertengremien zu besprechen, sondern in einem möglichst partizipativen Kontext unter Einschluss parlamentarischer Gremien.“

Insgesamt gehe die Europäische Kommission zwar ausführlich auf die sicherheitspolitischen Herausforderungen und Zielsetzungen sowie auf notwendige Maßnahmen ein, „sagt jedoch nichts darüber, dass parallel ein umfassendes Regelwerk geschaffen werden müsste, das die informationellen Grundrechte der Bürger gegenüber expansiven staatlichen Eingriffen schützt.“ Dabei sei auch bemerkenswert, „dass sich die Dynamik der europäischen Sicherheitspolitik immer mehr auf administrative Akteure konzentriert.“ (Bendieck 2012: 21)

Festzuhalten bleibt, dass die Policy Cyber-Sicherheit stärker die kollektive Sicherheit betont und zunehmend quasi nachholende sicherheitspolitische Entwicklungen zu beobachten sind, die dazu führen, dass individuelle Freiheitsrechte im Cyber-Raum verstärkt eingefordert werden. Neben dem überraschenden politischen Erfolg der Partei ‚Die Piraten‘ ist hierfür auch der internationale Protest nach Veröffentlichung der geheimen NSA-Dokumente durch Edward Snowden bezeichnend. Die bürgerrechtlichen Diskurse erstrecken sich von der Utopie eines entstaatlichen und herrschaftsfreien ‚Cyber-Raums‘ bis hin zur Dystopie eines omnipräsenten Überwachungsstaates im Sinne der Orwellschen Beschreibung. Beide Seiten sind empirisch nicht haltbar: Einerseits ist der Staat aufgrund des ‚big data‘-Problems und den mangelnden Ressourcen gegenwärtig nicht in der Lage, den Cyber-Raum gänzlich zu überwachen und Straftaten wie Spionage und Terrorismus verlässlich zu verhindern oder zu verfolgen (Groll 2006a: 51-52). Andererseits steht dem geforderten herrschaftsfreien Cyber-Raum nicht allein ein staatliches Engagement entgegen. Privatwirtschaftliche Unternehmen waren und sind hier durch ihre bei weitem umfangreicheren Überwachungsstrukturen wesentlich engagierter.⁶

Bei der politikfeldspezifischen Ambivalenz zwischen den Forderungen, die sich auf die Sicherheit *vor* und *durch* den Staat beziehen, wird zunächst letzteres stärker betont. Nach einer Umfrage vom Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM 2016: 49) stimmten 87 Prozent der Befragten voll und ganz (48 Prozent) und eher (38 Prozent) zu, dass sie vor der staatlichen Überwachung und insbesondere der Polizei nichts zu verbergen hätten. 78 Prozent sprachen sich für stärkere staatliche Eingriffe ins Internet für eine vorbeugende Gefahrenabwehr (z. B. Terrorismusabwehr) aus und 74 Prozent vertraten die Meinung, „dass der Staat viel stärker oder stärker zur Aufklärung von Verbrechen und Verfolgung von Straftaten ins Internet eingreifen sollte.“ Speziell bei staatlichen Eingriffen in den Datenschutz zeigt sich hingegen die politikfeldtypische Ambivalenz einer Sicherheit durch und vor dem Staat sehr deutlich: 51 Prozent der Befragten forderten ein stärkeres oder viel stärkeres Intervenieren des Staates in den Datenschutz, 43 Prozent hingegen einen weniger starken oder gar keinen staatlichen Eingriff (ebd.: 47).

6 Im Anschluss an die Surveillance-Studies, die verschiedene Überwachungs- und Kontrollstrukturen in einer Gesellschaft analysieren, kann speziell zur elektronischen Datenverarbeitung die dataveillance (Clarke 1994) empirisch untersucht werden. Dataveillance meint dabei „the proactive surveillance of what effectively become suspect populations, using new technologies to identify ‚risky groups‘“. (Levi/Wall 2004: 200)

5 Fazit

Das Politikfeld der Inneren Sicherheit strukturiert sich grundlegend durch die drei Aufgabenfelder Polizei, Verfassungsschutz und Bevölkerungsschutz. Bei allen strukturellen Unterschieden sollen hier vor allem die Gemeinsamkeiten der Aufgabenfelder zusammengefasst werden. Dies sind vor allem der Trennföderalismus und die hiermit verbundene formal-institutionelle Aufgabenwahrnehmung durch die Bundesländer, eine ausgeprägte Dominanz des Staates resp. der Verwaltung (im weitesten Sinne) und eine hohe Professionalisierung der politisch-administrativen und – nur im Aufgabenfeld des Bevölkerungsschutzes – verbandlich organisierten Akteure. Auch im Strukturwandel ähneln sich die Aufgabenfelder. Von großer Bedeutung sind hierbei zunächst die Zentralisierungsprozesse im politischen Mehrebenensystem, durch die die, in ihrer Bedeutung vormals eher marginalisierte, Bundesebene in sämtlichen Aufgabenfeldern zunehmend sicherheitspolitische Kompetenzen erhält. Dies steht in Verbindung mit den Europäisierungs- und Internationalisierungsprozessen, mit denen ein horizontaler und vertikaler Kooperations- und Koordinationsbedarf zwischen den verschiedenen politischen Ebenen einhergeht und auch aufgrund neuer sicherheitspolitischer Anforderungen nicht mehr oder zumindest nicht hinreichend durch die Länder gedeckt werden kann. Die grundlegende Darstellung der Policy Cyber-Sicherheit verdeutlicht diese Zentralisierung anhand der komplexen Strukturgeflechte zwischen den politischen Akteuren der verschiedenen Aufgabenfelder. Sie folgen dem Bedarf für eine größere Reichweite der politischen Programme, indem sie sich zunehmend weniger auf die kontext- und situationsbezogene Abwehr konkreter Gefahren beziehen und sich vorbeugend, ganzheitlich und dynamisch auf Gefahren und Risiken einstellen, um eine Antwort auf die sich verstärkenden (Un-) Sicherheitsempfindungen der Bürger zu geben. Vor allem über Präventionsprogramme mit straftatenvorbeugenden Wirkungen oder der Informationserhebung an Unverdächtigen als potenziellen Gefährdern soll für Sicherheit ‚in der Fläche‘ gesorgt werden. Gleichsam werden dadurch allerdings die Freiheiten sämtlicher Bürger eingeschränkt. Für den im politischen Konsens unzugänglichen Politikfeldkonflikt werden Sicherheiten vor dem Staat durch die steigenden Anforderungen von Sicherheiten durch den Staat begrenzt oder über die Sicherheitspolitik semantisch etwa über die Losung ‚Freiheit durch Sicherheit‘ oder durch die Forderung nach Sicherheit als Grundrecht überlagert. Die Prozesse sind Ursache und zugleich Folge einer ‚Versicherheitlichung‘ der Gesellschaft, die den Wert Sicherheit zunehmend schätzt, gerade weil die Ausfallwahrscheinlichkeit von dem, was vormals als sicher galt, steigt – auch wenn sich dies nur in einem geringen Maß durch die Polizeiliche Kriminalstatistik objektivieren lässt. Im Politikfeld der Inneren Sicherheit bezieht sich dies vornehmlich auf die Ausweitung und Intensivierung von Gefahren und Risikopotenzialen infolge höherer Kriminalitätszahlen und neuer Kriminalitätsformen. Während das Paradigma der ‚alten Sicherheit‘ auf bekannte Gefahren und Risiken ausgerichtet war, bezieht sich die neue Sicherheit verstärkt auf das *Unbekannte*.

So werden die Zentralisierungsprozesse im Politikfeld etwa durch Gefahren und Risiken von Terrorismus verstärkt. Terroristische Anschläge können zu jeder Zeit und an

jedem Ort mit erheblichen Schäden für bedeutende Rechtsgüter der Bürger einhergehen. Ob, wann und mit welcher Intensität dies geschieht, ist unbekannt. Äquivalent zur Verschiebung des Sicherheitswertes von der individuellen Freiheit zur kollektiven Sicherheit zeigt sich auch am Terrorismus, dass er seit langem nicht mehr die Form einer staatlichen Terrorherrschaft annimmt, die im 19./20. Jahrhundert Ängste bei den Bürgern schürte und gegen die individuelle Freiheitsrechte institutionalisiert wurden, sondern seinen Ausdruck in individualisierten Terror gegen Staaten findet, deren legitimierende Fähigkeiten zur Sicherheitsgewährleistung dadurch demonstrativ auf die Probe gestellt werden. Die Ausweitung kollektiver Sicherheit kann als eine Reaktion der Sicherheitspolitik verstanden werden, auf die unbekannten Erscheinungsformen einer quasi omnipräsenten Terrorgefahr zu reagieren. An den bundespolitischen Sicherheitsstrukturen wird auch die Politikfeldverzahnung zwischen der weiterhin formal-institutionell getrennten Inneren und äußeren Sicherheit deutlich. Beide Politikfelder verfolgen vergleichbare Problemperzeptionen und Problemlösungen, sodass sie politisch zunehmend aufeinander bezogen werden, weil die Sicherheitsbedrohungen keine räumlich begründete Trennung mehr rechtfertigen. Die Abwehr von Terrorismus erfolgt somit nicht nur im Inneren mit mehr oder weniger weitreichenden und symbolischen Sicherheitsprogrammen gegen das Unbekannte. Auch in der äußeren Sicherheit fehlt es an Adressabilitäten: wo vorher Staaten zu Rechenschaft gezogen werden konnten, sind es jetzt Gruppierungen, deren interne Struktur wesentlich diffuser ist und die sich transnational formieren. Die Programmformen einer neuen äußeren Sicherheit zeigen sich an neuen Formen der Kriegsführung (Münkler 2004), unter anderem zur Abwehr von Terrorismus, dessen Schäden sich aber vornehmlich im Inneren zeigen.

Manifestiert sich das Unbekannte hingegen an Fremdheit, werden die Dezentralisierungsprozesse des Politikfelds relevant. Die Beschreibung der Policy VÜ verdeutlicht, dass die Kriminalität und stärker noch die Unsicherheitsempfindungen der Bürger in den Großstädten zunehmen und zu neuen Formen kommunaler Sicherheitsgewährleistung unter staatlicher Regie führen. Es wächst der Bedarf an neuen Sicherheitsprogrammen, die aufgrund mangelnder Ressourcen (insbesondere für Polizeipersonal) sowohl bei den Ländern als auch bei den Kommunen gleichsam Sicherheit ‚in der Fläche‘ – insbesondere ganzer kommunaler Räume – versprechen. Etwa in Verbindung mit dem gegenwärtigen migrationspolitischen und teilweise fremdenfeindlichen politischen Diskurs verstärken sich die ohnehin zunehmenden Unsicherheitsgefühle kommunaler Bürgerschaften. Eine VÜ ist für die kommunale Sicherheitspolitik zunehmend nicht nur ein Symbol für Sicherheit in einem bestimmten Raum, sondern gleichsam eine Möglichkeit, die Sicherheitsgefühle der gesamten Bürgerschaft durch die Demonstration staatlicher und kommunaler Handlungsfähigkeit insgesamt zu steigern.

Die beschriebenen Prozesse der Zentralisierung und Dezentralisierung von Sicherheitsgewährleistungen im Politikfeld und das Paradigma einer ‚neuen Sicherheit‘ werden zunehmen. Offen bleibt hingegen die Frage, wie die Justierung zwischen individueller Freiheit und kollektiver Sicherheit als Sicherheit vor dem und durch den Staat bei steigendem Sicherheitsbedarf gelingen kann, wenn sich die Sicherheitsforderungen sowohl für als auch gegen eine Ausweitung des staatlichen Engagements richten. Zu erwarten sind

stärkere Konflikte in der Sicherheitspolitik, die nur dadurch staatlich kompensiert werden können, wenn Sicherheit nicht mehr umfassend, sondern partieller für die hergestellt wird, die mit einem hohen Einfluss Sicherheit einfordern. Hiermit verbunden sind dann in einem stärkeren Maße ökonomische Interessen, wie sie bei der Policy Cyber-Sicherheit und den verschiedenen Policies zur Sicherheit speziell im kommunalem Raum (u. a. die polizeiliche Videoüberwachung öffentlicher Räume) deutlich werden. Die zukünftige Gewährleistung von Innerer Sicherheit kann somit insgesamt als eine große Herausforderung für die demokratischen Prozesse und der hiermit verbundenen (input- und Output-)legitimen Anforderungen einer gerechten Sicherheitsherstellung beobachtet werden.

Zur vertiefenden Lektüre empfohlen:

- Lange, Hans-Jürgen/Gusy, Christoph (Hg.): Kooperation im Katastrophen- und Bevölkerungsschutz. Wiesbaden 2015.
- Lange, Hans-Jürgen/Lanfer, Jens (Hg.): Verfassungsschutz. Reformperspektiven zwischen administrativer Effektivität und demokratischer Transparenz. Wiesbaden 2016.
- Lange, Hans-Jürgen/Ohly, Peter H./Reichert, Jo (Hg.): Auf der Suche nach neuer Sicherheit. Fakten, Theorien und Folgen. Wiesbaden 2008.

Literatur

- Baier, Maximilian: Die parlamentarische Kontrolle der Nachrichtendienste und deren Reform. Hamburg 2009.
- Bäuerle, Michael: Polizeirecht in Deutschland. In: Aus Politik und Zeitgeschichte: Polizei. 48/2008: 15-20.
- Baumann, Fritz-Achim: Polizei und Nachrichtendienste. In: Innenministerium des Landes Nordrhein-Westfalen (Hg.): Rechtsgrundlage des Verfassungsschutzes in NRW. Düsseldorf 1997: 4-25.
- Beck, Ulrich: Weltrisikogesellschaft, ökologische Krise und Technologiepolitik. In: Beck, Ulrich/Jaher, Maarten A./Kesselring, Sven (Hg.): Der Unschärfe Ort der Politik. Empirische Fallstudien zur Theorie der reflexiven Modernisierung. Opladen 1999: 307-334.
- Bendieck, Annegret: Europäische Cybersicherheitspolitik. Berlin 2012.
- Bitkom: Datenschutz im Internet. Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht. <https://www.bitkom.org/Publikationen/2011/Studie/Studie-Datenschutz-im-Internet/BITKOM-Publikation-Datenschutz-im-Internet.pdf>, Stand 30.03.2016.
- Blum, Sonja/Schubert, Klaus: Politikfeldanalyse. Wiesbaden 2009.
- Bornwasser, Manfred/Classen, Dieter/Stolpe, Ilona (Hg.): Videoüberwachung öffentlicher Straßen und Plätze. Ergebnisse eines Pilotprojekts im Land Brandenburg. Frankfurt a.M. 2008.
- Bornwasser, Manfred: Evaluation der Videoüberwachung. In: Hempel, Leon/Metelmann, Jörg (Hg.): Bild-Raum-Kontrolle. Frankfurt a.M. 2005: 235-254.
- Böttcher, Astrid: Die Strukturlandschaft der Inneren Sicherheit der Bundesrepublik Deutschland. In: Böttcher, Astrid/ Lange, Hans-Jürgen (Hg.): Cyber-Sicherheit. Wiesbaden 2015: 69-102.

- Bücking, Hans J./Kubera, Thomas: Eine digitale Streifenfahrt ... Evaluation einer Videoüberwachung beim Polizeipräsidium Bielefeld. Bielefeld 2004.
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: BBK-Glossar. Ausgewählte zentrale Begriffe des Bevölkerungsschutze: Band 8. Bonn 2011. http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/Praxis_Bevoelkerungsschutz/Band_8_Praxis_BS_BBK_Glossar.pdf?__blob=publicationFile, Stand 07.10.2016
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: Bevölkerungsschutz in Deutschland. Informationen für Betreiber Kritischer Infrastrukturen. https://www.google.de/url?sa=t&rc=t&q=&src=s&source=web&cd=2&ved=0ahUKEwiA4ZPck-jLAhVCz3IKHQ7VCd4QFggq-MAE&url=http%3A%2F%2Fwww.bbk.bund.de%2FSharedDocs%2FDownloads%2FBBK%2F-DE%2FPublikationen%2FBroschueren_Flyer%2FFaltblatt_bevoelkerungsschutz-management.pdf%3F__blob%3DpublicationFile&usg=AFQjCNHlC0HwPpSlhHQgPqPlp74VVD20rw&cad=rja, Stand 07.10.2016.
- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe: Kritische Infrastrukturen. http://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html;jsessionid=C-599113CFFA617B5DD3F109BE1368BF6.1_cid345, Stand 07.10.2016.
- Bundesamt für Sicherheit in der Informationstechnik: CERTs als zentrales Element nationaler Cyber-Sicherheit. 20. Jahrgang. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/KES/kes0612_pdf.pdf?__blob=publicationFile&v=1, Stand 07.10.2016.
- Bundesamt für Sicherheit in der Informationstechnik: Cyber-Sicherheit. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html, Stand: 07.10.2016.
- Bundesamt für Sicherheit in der Informationstechnik: National response plans: IT-Crisis Response in Germany. 4th ENISA Workshop am 29.05.2008. https://www.enisa.europa.eu/activities/cert/events/file/ENISA_german_national_response_plan_Vorbach.pdf, Stand 07.10.2016.
- Bundeskriminalamt: Cybercrime. Bundeslagebild 2013. Wiesbaden 2013. http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2013,templateId=raw,property=publicationFile.pdf/cybercrime-Bundeslagebild2013.pdf, Stand 07.10.2016.
- Bundeskriminalamt: Cybercrime. Bundeslagebild 2014. Wiesbaden 2014. http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2014,templateId=raw,property=publicationFile.pdf/cybercrime-Bundeslagebild2014.pdf, Stand 07.10.2016.
- Bundesministerium des Inneren (Hg.): Cyber-Sicherheitsstrategie für Deutschland. Berlin 2011a.
- Bundesministerium des Inneren: IT und Netzpolitik. Berlin 2016b. http://www.bmi.bund.de/DE/Themen/IT-Netzpolitik/it-netzpolitik_node.html, Stand 10.07.2016.
- Bundesministerium des Inneren: Nationales Cyber-Abwehrzentrum. Berlin 2016a. <http://www.bmi.bund.de/DE/Themen/Sicherheit/IT-Cybersicherheit/Cyberabwehrzentrum/cyberabwehrzentrum.html>, Stand 10.07.2016.
- Bundesministerium des Innern (Hg.): Nationale Strategie zum Schutz kritischer Infrastrukturen. Berlin 2009. http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf?__blob=publicationFile, Stand 07.10.2016.
- Bundesministerium des Innern (Hg.): Polizeiliche Kriminalstatistik 2009. Berlin 2010.
- Bundesministerium des Innern (Hg.): Polizeiliche Kriminalstatistik 2010. Berlin 2011b.
- Bundesministerium des Innern (Hg.): Polizeiliche Kriminalstatistik 2011. Berlin 2012.
- Bundesministerium des Innern (Hg.): Polizeiliche Kriminalstatistik 2012. Berlin 2013.
- Bundesministerium des Innern (Hg.): Polizeiliche Kriminalstatistik 2013. Berlin 2014.
- Bundesministerium des Innern (Hg.): Polizeiliche Kriminalstatistik 2014. Berlin 2015.
- Clarke, Roger: Dataveillance: Delivering '1984'. In: Green, Lelia/Guinery, Roger (Hg.): Framing Technology. Society, Choice and Change. London 1994: 117-130.

- Collin, Peter: Die Videoüberwachung von Kriminalitätsschwerpunkten. Juristische Schulung. München 2006: 494-497.
- Daase, Christopher: Der erweiterte Sicherheitsbegriff. Working Paper 1/2010, Projekt Sicherheitskultur im Wandel. Goethe-Universität, Frankfurt 2010. <http://www.sicherheitskultur.org/WorkingPapers/01-Daase.pdf>, Stand 30.03.2016.
- Daun, Anna: Die deutschen Nachrichtendienste. In: Jäger, Thomas/Daun, Anna (Hg.): Geheimdienste in Europa. Transformation, Kooperation und Kontrolle. Wiesbaden 2009: 56-77.
- Dolata, Ulrich: Risse im Netz- Macht, Konkurrenz und Kooperation in der Technikentwicklung und -regulierung. In: Simonis, Georg/Martinsen, Renate/Saretzki, Thomas (Hg.): Politik und Technik. Analysen zum Verhältnis von technologischem, politischem und staatlichem Wandel am Anfang des 21. Jahrhunderts. Opladen 2001: 37-54.
- EC3 Europol: Combating Cybercrime in a Digital Age. 2016b. <https://www.europol.europa.eu/ec3>, Stand 10.07.2016.
- EC3 Europol: EC3 Programme Board. 2016a. <https://www.europol.europa.eu/ec/ec3-board>, Stand 10.07.2016.
- ENISA: Cyber Atlantic 2011. 2016a. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-atlantic/cyber-atlantic-2011>, Stand 10.07.2016.
- ENISA: Cyber Europe 2016: Are you ready for the next cyber crisis? 2016b. <https://www.enisa.europa.eu/media/multimedia/cyber-europe-2016-are-you-ready-for-the-next-cyber-crisis> Stand, 10.07.2016.
- ENISA: European Public Private Partnership for Resilience (EP3R). 2016d. <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r>, Stand 10.07.2016.
- ENISA: Sichert Europas Informationsgesellschaft. 2016c. <https://www.enisa.europa.eu/media/enisa-auf-deutsch>, Stand 10.07.2016.
- European Commission: Civil protection. Special Eurobarometer 328. Wave 72.2 – TNS Opinion & Social. November 2009. http://ec.europa.eu/public_opinion/archives/ebs/ebs_328_en.pdf, Stand 10.07.2016.
- European Commission: Migration and Home Affairs: Cybercrime. http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm, Stand 10.07.2016.
- Europol: European Cybercrime Centre to be established at Europol. <https://www.europol.europa.eu/content/press/european-cybercrime-centre-be-established-europol-1417>, Stand 10.07.2016.
- Eurostat: Statistiken zur Kriminalität. Daten vom Januar 2014. ec.europa.eu/eurostat/statistics-explained/index.php/Crime_statistics/de#Weitere_Informationen_von_Eurostat, Stand 10.07.2016.
- Feltes, Thomas: „Community Policing“ – ein polizeipolitisches Modell für Europa. In: Fehevary, Janos/Stangl, Wolfgang (Hg.): Polizei zwischen Europa und den Regionen. Analysen disparater Entwicklungen. Wien 2001: 119-132.
- Frankfurter Allgemeine: Erpressung im Internet nimmt zu. www.faz.net/aktuell/wirtschaft/netz-wirtschaft/bka-zu-cyberkriminalitaet-internet-erpressung-nimmt-zu-13120596.html, Stand 10.07.2016.
- Füth, Dorothée: Erfahrungen mit Evaluierungsprozessen in Nordrhein-Westfalen am Beispiel der präventivpolizeilichen Videoüberwachung. In: Albers, Marion/Weinzierl, Ruth (Hg.): Menschrechtliche Standards in der Sicherheitspolitik. Baden-Baden 2010: 55-63.
- Groenemeyer, Axel: Wege der Sicherheitsgesellschaft. Gesellschaftliche Transformationen der Konstruktion und Regulierung innerer Unsicherheiten. In: Groenemeyer, Axel (Hg.): Wege der Sicherheitsgesellschaft – Transformation der Konstruktion und Regulierung innerer Unsicherheiten. Wiesbaden 2010: 9-22.

- Groenemeyer, Axel (Hg.): Wege der Sicherheitsgesellschaft. Gesellschaftliche Transformation der Konstruktion und Regulierung innerer Unsicherheiten. Wiesbaden 2010.
- Groll, Kurt H. G.: Computerkriminalität. In: Lange, Hans-Jürgen (Hg.): Wörterbuch zur Inneren Sicherheit. Wiesbaden 2006a: 48-52.
- Groll, Kurt H.G.: Internetüberwachung. In: Lange, Hans-Jürgen (Hg.): Wörterbuch zur Inneren Sicherheit. Wiesbaden 2006b: 140-144.
- Groß, Hermann: Deutsche Länderpolizeien. In: Aus Politik und Zeitgeschichte: Polizei. 48/2008: 20-26.
- Grumke, Thomas: Das Innenmysterium. Prozesse und Strukturen der Verfassungsschutzämter nach dem NSU. In: Lange, Hans-Jürgen/Lanfer, Jens (Hg.): Verfassungsschutz. Reformperspektiven zwischen administrativer Effektivität und demokratischer Transparenz. Wiesbaden 2016: 153-169.
- Grunow, Dieter: Bürokratieforschung. In: Kaina, Viktoria/Römmle, Andrea (Hg.): Politische Soziologie. Ein Studienbuch. Wiesbaden 2009: 353-384.
- Gusy, Christoph: Katastrophenschutzrecht – Zur Situation eines Rechtsgebietes im Wandel. In: Lange, Hans-Jürgen/Endreß, Christian/Wendekamm, Michaela (Hg.): Versicherheitlichung des Bevölkerungsschutzes. Wiesbaden 2013: 207-220.
- Gusy, Christoph: Parlamentarische Kontrolle der Nachrichtendienste im demokratischen Rechtsstaat. In: Zeitschrift für Rechtspolitik. Heft 02/2008: 36-40.
- Gusy, Christoph: Reform der Sicherheitsbehörden. In: Zeitschrift für Rechtspolitik. 2012a. Heft 08/2012: 230-234.
- Gusy, Christoph: Sicherheitsgesetzgebung. In: KritV. 2012b. Jg. 95, 3/2012: 247-269.
- Gusy, Christoph: Vom neuen Sicherheitsbegriff zur neuen Sicherheitsarchitektur. Verwaltungsarchiv. 3/2010: 309-333.
- Heinrich, Stephan/Lange, Hans-Jürgen: Kriminalpolitik, politische Steuerung und wissenschaftliche Politikberatung. In: Dahme, Heinz-Jürgen/Wohlfahrt, Norbert (Hg.): Systemanalyse als politische Reformstrategie. Wiesbaden 2010: 74-89.
- Hobbes, Thomas: Leviathan. Frankfurt a.M. 2006.
- Infratest dimap: ARD-DeutschlandTREND Januar 2016. Eine Studie im Auftrag der tagessthemen. http://www.infratest-dimap.de/fileadmin/user_upload/dt1601_bericht.pdf, Stand 10.07.2016.
- Kelling, George L./Wilson, James Q.: Broken Windows: The police and neighbourhood Safety. In: The Atlantic Monthly. March 1982: 29-38.
- Knelangen, Wilhelm: Europäisierung und Globalisierung der Polizei. In: Aus Politik und Zeitgeschichte: Polizei. 48/2008: 33-38.
- Kohl, Andreas: Videoüberwachung. In: Lange, Hans-Jürgen (Hg.): Wörterbuch zur Inneren Sicherheit. Wiesbaden 2006: 356-360.
- Kohlstruck, Michael: Bürgernähe und Bürgerkontrolle schließen sich aus – Der Verfassungsschutz überspannt den Bogen. In: Heinrich Böll Stiftung Sachsen (Hg.): Wer schützt die Verfassung? Kritik zu den Verfassungsschutzbehörden und Perspektive jenseits der Ämter, Dresden 2013: 117-128. http://www.weiterdenken.de/sites/default/files/verfassungsschutz_2013_download_m.pdf, Stand 30.03.2016.
- Kutscha, Martin: Trennungsgebot. In: Lange, Hans-Jürgen (Hg.): Wörterbuch zur Inneren Sicherheit. Wiesbaden 2006: 337-340.
- Kury, Helmut: Präventionskonzepte. In: Lange, Hans-Jürgen/Ohly, Peter H./Reichert, Jo (Hg.): Auf der Suche nach neuer Sicherheit. Wiesbaden 2008: 21-48.
- Landesamt für Datenschutz Bremen: Opportunitätsprinzip/Legalitätsprinzip. http://www.verfassungsschutz.bremen.de/sixcms/detail.php?gsid=bremen77.c.2076.de&template=20_glossar_d&begriff=O, Stand 30.03.2016.
- Landesbetrieb Information und Technik NRW: CERT. <https://www.it.nrw.de/informationstechnik/Services/CERT/Index.html>, Stand 30.03.2016.

- Lanfer, Jens: Cyber-Sicherheit und die (Ohn-)Macht des Staates. In: Frevel, Bernhard/Wendekamm, Michaela (Hg.): Sicherheitskooperationen zwischen Staat, Markt und Zivilgesellschaft. Wiesbaden 2017: 47-72.
- Lanfer, Jens: Die Dominanz der Verwaltung im Politikfeld Innere Sicherheit – Sicherheitskulturelle Untersuchung am Beispiel der Videoüberwachung öffentlicher Räume in NRW. In: Lange, Hans-Jürgen/Endreß, Christian/Wendekamm, Michaela (Hg.): Dimensionen der Sicherheitskultur. Wiesbaden 2014: 197-235.
- Lanfer, Jens: Gewährleistung von Innerer Sicherheit zwischen Staat und Stadt. Politische Gestaltbarkeit verdichteter Räume. In: Lemke, Matthias (Hg.): Die gerechte Stadt. Stuttgart 2012: 139-166.
- Lanfer, Jens/Lange, Hans-Jürgen: Der Verfassungsschutz im Politikfeld der Inneren Sicherheit zwischen politischen und administrativen Legitimationsanforderungen. In: Lange, Hans-Jürgen/Lanfer, Jens (Hg.): Verfassungsschutz. Reformperspektiven zwischen administrativer Effektivität und demokratischer Transparenz. Wiesbaden 2015: 121-150.
- Lanfer, Jens: Politische Evaluationsprozesse in Gesetzgebungsverfahren zur Videoüberwachung öffentlicher Räume. Darstellung anhand des empirischen Vergleichs von Brandenburg, Hessen und Nordrhein-Westfalen. In: Gusy, Christoph (Hg.): Evaluation von Sicherheitsgesetzen. Wiesbaden 2015: 85-126.
- Lange, Hans-Jürgen: Das Politikfeld Innere Sicherheit. In: Grunow, Dieter (Hg.): Verwaltungshandeln in Politikfeldern. Opladen 2003: 225-272.
- Lange, Hans-Jürgen/Endreß, Christian: Bevölkerungsschutz als integraler Bestandteil der Sicherheitsarchitektur. In: Lange, Hans-Jürgen/Endreß, Christian/Wendekamm, Michaela (Hg.): Versicherheitlichung des Bevölkerungsschutzes. Wiesbaden 2013: 9-26.
- Lange, Hans-Jürgen/Endreß, Christian/Wendekamm, Michaela/Matzke, Malte: Akteure, Perspektiven und Wechselbeziehungen der Naturgefahrenabwehr. Schriftenreihe Forschungsforum Öffentliche Sicherheit. Berlin 2012.
- Lange, Hans-Jürgen/Frevel, Bernhard: Innere Sicherheit im Bund, in den Ländern und in den Kommunen. In: Lange, Hans-Jürgen/Ohly, H. Peter/Reichert, Jo (Hg.): Auf der Suche nach neuer Sicherheit. Wiesbaden 2008: 115-148.
- Lange, Hans-Jürgen/Heinrich, Stephan: Erweiterung des Sicherheitsbegriffs. In: Lange, Hans-Jürgen/Ohly, H. Peter/Reichert, Jo (Hg.): Auf der Suche nach neuer Sicherheit. Wiesbaden 2008: 253-267.
- Lange, Hans-Jürgen: Innere Sicherheit und der Wandel von Staatlichkeit. In: Schmidt, Manfred G./Zohlnhöfer, Reimut (Hg.): Regieren in der Bundesrepublik Deutschland. Innen- und Außenpolitik seit 1949. Wiesbaden 2006: 87-112.
- Lange, Hans-Jürgen/Mittendorf, Volker: Innere Sicherheit und Technik – Die Bedeutung technologischer Adaptionen im Hinblick auf Spezialisierung und Aufgabenwandel der Polizei, in: Simonis, Georg/Martinsen, Renate/Saretzki, Thomas (Hrsg.): Politik und Technik. Analyse zum Verhältnis von technologischem, politischem und sozialem Wandel am Anfang des 21. Jahrhunderts, Wiesbaden 2001: 268-292.
- Lange, Hans-Jürgen: Zum Wandel der Institutionen und Steuerungsformen des staatlichen Sicherheitssystems. In: Zoche, Peter/Kaufmann, Stefan/Haverkamp, Rita (Hg.): Zivile Sicherheit. Gesellschaftliche Dimensionen gegenwärtiger Sicherheitspolitiken. Bielefeld 2011: 319-340.
- Leggewie, Claus/Meier, Horst: Nach dem Verfassungsschutz. Plädoyer für eine neue Sicherheitsarchitektur der Berliner Republik. Berlin 2012.
- Legnaro, Aldo: Konturen der Sicherheitsgesellschaft. Eine polemisch-futurologische Skizze. *Leviathan* 25/2, 1997: 271-284.
- Levi, Mike/Wall, David: Technologies, Security, and Privacy in the Post-9/11 European Information Society. *Journal of Law and Society*. Jg. 31, 2/2004: 194-220.
- Lisken, Hans/Lange, Hans-Jürgen: Die Polizeien des Bundes. In: Lange, Hans-Jürgen (Hg.): Staat, Demokratie und Innere Sicherheit in Deutschland. Opladen 2000: 151-166.

- Luhmann, Niklas: Opportunismus und Programmatik in der öffentlichen Verwaltung. In: Luhmann, Niklas.: Politische Planung. Aufsätze zur Soziologie von Politik und Verwaltung. 5. Auflage, Wiesbaden 2007: 165-180.
- Mayntz, Renate: Soziale Dynamik und politische Steuerung. Theoretische und methodologische Überlegungen. Schriften des Max-Planck-Instituts für Gesellschaftsforschung Köln. Band 29, Frankfurt a.M. 1997.
- Mintzberg, Henry: The Structuring of Organizations. Englewood Cliffs 1979.
- Möllers, Martin H.W./Ooyen, Robert Chr. van: Bundeskriminalamt, Bundespolizei und „neue“ Sicherheit. In: Aus Politik und Zeitgeschichte: Polizei. 48/2008: 26-32.
- Murck, Manfred: Die Rolle der Landesbehörden für Verfassungsschutz bei der Zusammenarbeit der Nachrichtendienste in Europa. In: Jäger, Thomas/Daun, Anna (Hg.): Geheimdienste in Europa. Transformation, Kooperation und Kontrolle. Wiesbaden 2009: 182-203.
- NATO: Cyber security. http://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=uk, Stand 10.07.2016.
- OECD: Cybersecurity Policy Making at a Turning Point. Paris 2012: <https://www.oecd.org/sti/ieconomy/cybersecurity-policy-making.pdf> Stand 10.07.2016.
- OSCE: Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attack: Focusing on Threats Emanating from Cyberspace. Wien 2013. <http://www.osce.org/atu/103500?download=true>, Stand 10.07.2016.
- Ostendorf, Heribert: Mehr Prävention und weniger Strafe, weniger Prävention und mehr Strafe oder mehr Prävention und mehr Strafe. In: Bewährungshilfe. Soziales, Strafrecht, Kriminalpolitik. Jg. 52, 1/2005: 57-66.
- Pohlmann, Kristine: Bundeskompetenzen im Bevölkerungsschutz, Wiesbaden 2013.
- Reuband, Karl-Heinz: Kriminalitätsfurcht. Erscheinungsformen, Trends und soziale Determinanten. In: Hans-Jürgen Lange/H. Peter Ohly/Jo Reichertz (Hg.): Auf der Suche nach neuer Sicherheit. Wiesbaden 2008: 233-251.
- Sabatier, Paul A./Weible, Christopher M.: The Advocacy Coalition Framework. In: Sabatier, Paul A.: Theories of the Policy Process. Boulder 2007: 189-222.
- Sack, Detlef: Regieren und Governance in der BRD. Ein Studienbuch. München 2013.
- Schenck, Jean-Claude: Bundespolizei/Bundesgrenzschutz. In: Lange, Hans-Jürgen (Hg.): Wörterbuch zur Inneren Sicherheit. Wiesbaden 2006: 36-39.
- Schütte, Matthias: Bundesamt für Verfassungsschutz. In: Lange, Hans-Jürgen (Hg.): Wörterbuch zur Inneren Sicherheit. Wiesbaden 2006: 22-26.
- Siebel, Walter/Wehrheim, Jan: Sicherheit und urbane Öffentlichkeit. Deutsche Zeitschrift für Kommunalwissenschaft. Jg. 42, 1/2003: 11-30.
- Singelstein, Tobias/Stolle, Peer (Hg.): Die Sicherheitsgesellschaft. Sozial Kontrolle im 21. Jahrhundert, 2. Auflage. Wiesbaden 2006.
- Singer, Jens Peter: Nachrichtendienste zwischen innerer und äußerer Sicherheit. In: Jäger, Thomas/Daun, Anna (Hg.): Geheimdienste in Europa. Transformation, Kooperation und Kontrolle. Wiesbaden 2009: 265-292.
- Stegmaier, Peter/Feltes, Thomas: Vernetzung als neuer Effektivitätsmythos für innere Sicherheit. Aus Politik und Zeitgeschichte: Innere Sicherheit im Wandel. 12/2007: 18-25.
- Striegel, Sebastian: Parlamentarische Kontrolle des Verfassungsschutzes. In: Heinrich Böll Stiftung Sachsen (Hg.): Wer schützt die Verfassung? Kritik zu den Verfassungsschutzbehörden und Perspektive jenseits der Ämter, Dresden 2013: 81-93. http://www.weiterdenken.de/sites/default/files/verfassungsschutz_2013_download_m.pdf, Stand 10.07.2016.
- Sturm, Gabriele/Meyer, Katrin: Alterung in deutschen Großstädten – internationalisiert. In: Marzetzke, Steffen (Hg.): Städte im demographischen Wandel. Wesentliche Strukturen und Trends

- des demografischen Wandels in den Städten Deutschlands. Bundesinstitut für Bevölkerungsforschung, Heft 125. Wiesbaden 2008: 51-64.
- Voelcker, Ina: Die altersgerechte Stadt. Eine gerontologische Perspektive. In: Lemke, Matthias (Hg.): Die gerechte Stadt. Stuttgart 2012: 117-138.
- Weaver, Ole: Securitization and Desecuritization. In: Lipschutz, Ronnie D. (Hg.): On Security. New York 1995: 46-86.
- Wehrheim, Jan: Die überwachte Stadt. Sicherheit, Segregation und Ausgrenzung. 3. Auflage, Opladen 2012.
- Wendekamm, Michaela/Matzke, Malte: Das Ehrenamt im Katastrophen- und Bevölkerungsschutz. In: Lange, Hans-Jürgen/Gusy, Christoph (Hg.): Kooperation im Katastrophen- und Bevölkerungsschutz. Wiesbaden 2015: 289-304.
- Wiedemann, Gregor: Verfassungsschutz durch Aufklärung? In: Heinrich Böll Stiftung Sachsen (Hg.): Wer schützt die Verfassung? Kritik zu den Verfassungsschutzbehörden und Perspektive jenseits der Ämter. Dresden 2013: 131-144. http://www.weiterdenken.de/sites/default/files/verfassungsschutz_2013_download_m.pdf, Stand 10.07.2016.
- YouGov: Großes Vertrauen in Karlsruhe, wenig in die Regierung. 10. Juli 2012. <https://yougov.de/news/2012/07/10/grosses-vertrauen-karlsruhe-wenig-die-regierung/>, Stand 10.07.2016.
- Zeit Online: Großes Vertrauen in Karlsruhe, wenig in die Regierung. 9. Juli 2012. <http://www.zeit.de/politik/deutschland/2012-07/umfrage-institutionen-karlsruhe>, Stand 10.07.2016.

Implementation in Politikfeldern

Eine Anleitung zum verwaltungsbezogenen Vergleich

Grunow, D. (Hrsg.)

2017, IX, 430 S. 50 Abb., 23 Abb. in Farbe., Softcover

ISBN: 978-3-531-17790-8