Jens Lanfer

Digitalisierung der Sicherheitspolitik

1. Einleitung

Die Digitalisierung der Sicherheitspolitik kann mit einer unterschiedlichen analytischen Reichweite und Tiefenschärfe untersucht werden. Einerseits können dichte und detaillierte Struktur- und Prozessbeschreibungen der Sicherheitspolitik anleitend sein, um Bedingungen und Entwicklungen vor allem im Aufgabenbereich der Cyber-Sicherheit empirisch rekonstruieren zu können.[1] Insofern sind neben der hier relevanten Sicherheitspolitik insbesondere auch Analysen zur Gesundheits-, Verkehrs- und Verwaltungspolitik von wesentlicher Bedeutung, um quasi ›Bottom up‹ die Bedingungen und Folgen der Digitalisierung des politischen Systems in den politikwissenschaftlichen Blick zu bekommen. Andererseits sind die politischen Felder nicht unabhängig vom politischen Gesamtsystem, das etwa für die Sicherheitspolitik demokratische und rechtsstaatliche Institutionen, Strukturen und Prozesse bereithält. Vor allem die nationalstaatliche Rechtsordnung fördert oder hemmt die politische Digitalisierung, sodass hierdurch entsprechend ›Top down‹ auch die verschiedenen Politikfelder geprägt werden. Die Reichweite der Aussagen lässt sich noch steigern, wenn das politische Gesamtsystem weniger aus einer politikwissenschaftlichen, sondern aus einer gesellschaftheoretischen Perspektive untersucht wird, um die Auswirkungen gesellschaftlicher und speziell lebensweltlicher Transformationen für Politisierungspotenziale, politische Leistungsansprüche und Legitimationsanforderungen einzubeziehen. Um die Voraussetzungen für die Digitalisierung von Sicherheitspolitik beschreiben zu können, erscheinen die drei Untersuchungsperspektiven je für sich plausibel. Die folgende Untersuchung bezieht die verschiedenen Perspektiven aufeinander, um zugleich Tiefenschärfe und Verallgemeinerbarkeit zu erreichen. Auch wenn dadurch beiden analytischen Ansprüchen mehr oder weniger große Zugeständnisse gemacht werden müssen, kann aber vornehmlich auf diese Weise erfasst werden, mit welchen (grundlegenden) sicherheitspolitischen Folgen die gesellschaftliche Digitalisierung einhergeht. Die Untersuchung kann dabei eine Antwort auf die Frage geben, welche lebensweltlichen Dynamiken durch die gesellschaftliche Digitalisierung

1 Vgl. hierzu etwa Jens Lanfer, »Cyber-Sicherheit und die (Ohn-)Macht des Staates«, in: Bernhard Frevel und Michaela Wendekamm (Hg.), *Sicherheitsproduktion zwischen Staat, Markt und Zivilgesellschaft*, Wiesbaden: Springer VS 2017.

ausgelöst werden und wie sich hierdurch die sicherheitspolitischen Legitimationsbedingungen und Kapazitäten ändern.

Die Untersuchung eröffnet mit einer begrifflichen Schärfung der Werte und Wertbereiche von ›Sicherheit‹ und ›Freiheit‹ und setzt sie zueinander ins Verhältnis. Im dritten und vierten Kapitel wird dieses Verhältnis daraufhin untersucht, in welcher Weise die Digitalisierung die wertbezogenen Resonanz-, Rekombinations- und Politisierungsdynamiken in der Lebenswelt ändert. Das Kapitel fünf verdeutlicht, dass hiermit zugleich neue sicherheitspolitische Legitimationsbedingungen einhergehen, die Strukturänderungen in der Sicherheitspolitik, speziell im Aufgabenbereich der Cyber-Sicherheit, bewirken und maßgeblich prägen. Abschließend erfolgen ein Resümee und eine Verallgemeinerung der Ergebnisse für die Theorie gesellschaftlicher Digitalisierung.

2. Steigerungsverhältnis zwischen Freiheit und Sicherheit in der Lebenswelt

Sicherheit ist ein gesellschaftlicher Wert. Er ist nicht nur in sämtlichen gesellschaftlichen Teilsystemen wie Politik, Wirtschaft, Wissenschaft, Gesundheit, Religion, Massenmedien oder Recht anschlussfähig, sondern auch für unzählige und vielfältige gesellschaftliche Interaktionen und Organisationen sowie technische Anwendungen relevant. Sicherheit ist entsprechend auf sämtliche soziale Kontexte anwendbar und deshalb ein catch-all-Begriff.[2] Dabei wird mit Sicherheit nur etwas bezeichnet, was sicher erscheint, wenn auf es keine zukünftigen Nachteile zugerechnet werden.[3] Nichts lässt sich als absolut sicher bezeichnen, sodass es auch keine Sachgründe dafür geben kann, einen solchen Zustand herbeiführen zu wollen – im Gegenteil: Sicherheit ist, wie auch andere gesellschaftliche Werte, vergleichbar mit einem Leitstern, an dem sich etwa Schiffe navigierend orientieren, aber dann etwas grundlegend falsch gemacht haben, wenn sie diesen tatsächlich erreichen.[4] Sicherheit ist deshalb nur

2 Herfried Münkler, »Strategien der Sicherung: Welten der Sicherheit und Kulturen des Risikos. Theoretische Perspektiven«, in: Herfried Münkler, Matthias Bohlender und Sabine Meurer (Hg.), *Sicherheit und Risiko. Über den Umgang mit Gefahr im 21. Jahrhundert*, Bielefeld: transcript 2010, S. 22.

3 Niklas Luhmann, »Risiko und Gefahr«, in: ders. (Hg.), *Soziologische Aufklärung. Konstruktivistische Perspektiven*, 4. Auflage, Wiesbaden: VS-Verlag 2009, S. 128.

4 Christoph Gusy, »Freiheit und Sicherheit«, in: Bundeszentrale für politische Bildung, *Dossier Innere Sicherheit* 2012. Online unter http://www.bpb.de/politik/innenpolitik/innere-sicherheit/76651/freiheit-und-sicherheit [Zugriff 19.01.2019].

ein mehr oder weniger anleitendes Gefühl der Verlässlichkeit bestehender Verhältnisse vor häufig nur sehr ungenau benennbaren Gefahren.[5] Dies bedeutet auch, dass Sicherheitsansprüche immer nur dann entstehen, wenn Unsicherheiten individuell wahrgenommen oder sozial bezeichnet werden. Dabei können sich Sicherheitserwartungen entweder selbst versichern, wenn sie Gefahren und Bedrohungen gänzlich aussperren[6] und die Ungewissheit der Zukunft[7] ignorieren. Sie können aber auch Sicherheit mit intensiven emotionalen Appellen[8] vor allem vom Staat einfordern. Unabhängig davon, ob der Sicherheitswert nun objektivierbare oder subjektive Ansprüche hervorruft, ist er ein gesellschaftliches Leitbild beherrschbarer Komplexität,[9] das anleitend wirken kann, aber nicht vollständig zu erreichen ist.

Die staatliche Herstellung kollektiver Sicherheit wird von einem Glauben beherrschbarer Komplexität getragen. Sie reagiert auf Sicherheitserwartungen der Bürger*innen mit Sicherheitsversprechen, die nicht eingehalten werden können, weil sich die Kontingenzen (hyper-) moderner Dynamiken nicht beherrschen lassen. Zwar sind diese Versprechen hoch legitimationsrelevant, versuchen aber zu viel zu erreichen und werden deshalb die Adressat*innen immer enttäuschen. Mit Sicherheit geht also eine unauflösbare Paradoxie einher: Enttäuschte Sicherheitserwartungen verstärken Sicherheitsansprüche, die wiederum auf Unsicherheiten aufmerksam machen und deshalb dazu führen, dass sich staatliches Engagement zugunsten von mehr Sicherheit und die hiermit einhergehenden Sicherheitsversprechen verstärken. Dieses Paradox wird durch den mangelnden Informationswert von mitgeteilten Sicherheitsgefühlen zusätzlich verstärkt. Erst Unsicherheitsgefühle erregen Aufmerksamkeit und sorgen für weitere Unsicherheit gerade dann, wenn die Bürger*innen aneinander affizierende Anzeichen von Angst

5 Gefahr wird hier mit Münkler verstanden als drohende schwere Schädigungen. Dies gilt vergleichbar auch für die Bedrohung, »wobei diese sich von der Gefahr dadurch unterscheidet, dass ein Akteur identifizierbar ist, der durch die Erzeugung von Gefahr bestimmte Absichten verfolgt. (…) Gefahr tritt zufällig ein und hinter ihr stehen keine Absichten. Die Differenz zwischen Gefahr und Bedrohung ist eine von Kontingenz und Intention.« Herfried Münkler 2010, a. a. O., S. 11, Fn. 1. Für die Zwecke der weiteren Untersuchung wird allerdings nur der Begriff ›Gefahr‹ verwendet, weil die Unterscheidung nur für eine detaillierte Untersuchung sicherheitspolitischer Strukturen einen Mehrwert hätte.

6 Ebd., S. 12.

7 Franz-Xaver Kaufmann, »Sicherheit: Das Leitbild beherrschbarer Komplexität«, in: Stephan Lessenich (Hg.), *Wohlfahrtstaatliche Grundbegriffe. Historische und aktuelle Diskurse*, Frankfurt/M.: Campus 2003, S. 92.

8 Ebd., S. 94.

9 Ebd.

beobachten.[10] Es ist deshalb sehr unwahrscheinlich, dass sich Gruppen oder sogar die Mehrheit von Bürger*innen dauerhaft versicherheitlichen (securitization) lassen. Dies erscheint nicht erstrebenswert: Wer davon ausgeht, dass die Zukunft sicher wäre und sich selbst oder gesellschaftlichen Institutionen zu sehr vertraut, wird umso mehr enttäuscht.[11] Es besteht folglich ein Steigerungszusammenhang zwischen subjektiven Unsicherheitsempfindungen[12] und der Sicherheitsparadoxie, der sich insbesondere über unsicherheitsrelevante Ereignisse abrupt intensivieren und beschleunigen kann. Im Unterschied zu gesellschaftlichen Dynamiken erscheint zumindest die Komplexität sozialer Nahräume beherrschbar,[13] wenn die Lebenszusammenhänge und mithin die Sorgen von Individuen berücksichtigt werden, um Unsicherheitsgefühle über eine (symbolische) Verlässlichkeit zu reduzieren. Insofern lassen sich die staatlichen Sicherheitsherstellungen im Zusammenhang mit den unstillbaren Sicherheitserwartungen der Bürger*innen als *Security* und solche Sicherheitserwartungen, die aus dem Zusammenhang von individuellen Erfahrungen und unmittelbarer Lebenswelt hervorgehen, als *Safety* oder *Certainty* bezeichnen.[14]

Freiheit ist als Wert äquivalent strukturiert. Vollständige Freiheit ist unerreichbar: »Die Welt ist indeterminiert, weil sie determiniert ist, dies allerdings nicht zentral, sondern lokal.«[15] Zwei unabhängige (physische oder soziale) Systeme, die in einer interaktiven Beziehung stehen, bringen Freiheit qua Fiktion hervor, weil sie jeweils der anderen Seite Freiheiten zurechnen, aber nicht tatsächlich einen Zustand völliger Freiheit erreichen. Die andere Seite produziert für das beobachtende System Unberechenbarkeit, Intransparenz und deshalb zufällige Ereignisse, die als Freiheit bezeichnet werden. Je nach Zurechnung hat dies zur Folge, dass Freiheiten entweder als Zumutung oder als Ermöglichung aufgefasst werden. Da wo Freiheit im Verhältnis zu Freiheiten anderer erlebt

10 Vgl. Sven Opitz, »Zur Soziologie der Affekte: Resonanzen epidemischer Angst«, in: Joachim Fischer und Stephan Moebius (Hg.), *Kultursoziologie im 21. Jahrhundert*, Wiesbaden: VS Verlag 2014, S. 269–280.

11 Niklas Luhmann, *Vertrauen*, 5. Auflage, Konstanz und München: UVK Verlag 2014, S. 13, 32f.

12 Vgl. Anne Köhn und Manfred Bornewasser, *Subjektives Sicherheitsempfinden*, Working Paper Nr. 9, Verbundprojekt Kooperative Sicherheitspolitik in der Stadt (KoSiPol), Bernhard Frevel (Hg.), Münster 2012. Online unter https://d-nb.info/1140787225/34 [Zugriff 19.01.2019].

13 Franz-Xaver Kaufmann 2003, a. a. O., S. 104.

14 Zu den Unterschieden zwischen Security, Safety und Certainty vgl. Bernhard Frevel, *Innere Sicherheit. Eine Einführung*, Wiesbaden: Springer VS 2018, S. 2f.

15 Niklas Luhmann, *Einführung in die Systemtheorie*, hrsg. von Dirk Baecker, 2. Auflage, Heidelberg: Carl-Auer-System Verlag 2004, S. 178.

und erfahren wird, ist eine Optionenvielfalt vorhanden, die sich von den bestehenden Strukturen, die möglicherweise als übermäßig hemmende Normalität und Routine empfunden werden, abgrenzt. Freiheit bezeichnet also ein individuelles Gefühl der Veränderbarkeit und Gestaltbarkeit. Um den Unterschied zwischen Sicherheit und Freiheit deutlich herauszustellen, eignet sich die Unterscheidung zwischen Gefahr und Risiko.[16] Dabei setzt Freiheit Risiken voraus, um sich zu steigern. Sicherheit bezieht sich demgegenüber auf Gefahren. Das Risiko beruht auf einer freiheitlichen Entscheidung, ein Wagnis einzugehen, die das Individuum dann selbst zu verantworten hat. Risiken geht man also berechnend und kalkulierend ein, um gegenwärtig eine Chance auf zukünftig mehr Optionen gleich welcher Art zu nutzen, weil die Hoffnung besteht, dass letztlich mehr gewonnen als verloren wird. Gefahren sind von individuellen Entscheidungen unabhängig. Wirkt sich eine Gefahr schädigend aus, entzieht sich der Schaden einer zurechenbaren Intention. Er wird entsprechend als überkommend und zufällig erlebt.

Freiheit und Sicherheit sind zwei gesellschaftliche Werte, die auf ein unterschiedliches individuelles Erleben verweisen, andere Handlungsweisen motivieren und entsprechend verschiedene Ansprüche hervorbringen. Allerdings bedingen sich die beiden Werte und können nicht unabhängig voneinander gedacht werden: Immer dann, wenn Freiheit erlebt wird, muss Sicherheit vorausgesetzt werden – et vice versa. Der eine Wert setzt die Anspruchskomplexität des anderen voraus und steigert dadurch das eigene Anspruchs- als Komplexitätsniveau. Die wertbezogenen Ansprüche an Freiheit und Sicherheit bilden deshalb ein gesellschaftliches Reduktions- und Steigerungsverhältnis.[17] Sie steigern sich wechselseitig, wenn ihr Verhältnis als ausgewogen bezeichnet wird, sorgen aber für mehr oder weniger stark einseitige Ansprüche, wenn ihr Verhältnis als zu asymmetrisch bewertet wird. Dabei ist eine Gesellschaft ohne Freiheit oder Sicherheit nicht denkbar, und stabile Gesellschaftsstrukturen sind ohne ein legitimes Verhältnis zwischen beiden Werten nicht oder nur zeitweise möglich.

Für die Vermittlung von Ansprüchen an Freiheit und Sicherheit ist die *gesellschaftliche Lebenswelt* anleitend. Sie ist nach Husserl eine »wirklich anschauliche, wirklich erfahrene und erfahrbare Welt, in der sich unser ganzes Leben praktisch abspielt.«[18] Was auch oder vor allem erfahrbar und erfahren wird, ist die interaktive oder organisationale

16 Vgl. Niklas Luhmann 2009, a. a. O.

17 Vgl. ähnliche Argumentation bei Michel Foucault, *Die Geburt der Biopolitik. Geschichte der Gouvernementalität II*, 6. Auflage, Frankfurt/M.: Suhrkamp 2018, S. 100, 102.

18 Edmund Husserl, *Die Krisis der europäischen Wissenschaften und die transzendentale Phänomenologie*, Den Haag: Martinus Nijhoff 1976, S. 51.

Zurechnung auf die gesellschaftlichen Sinnreferenzen wie Politik, Wirtschaft, Wissenschaft, Gesundheit, Kunst oder Wissenschaft. Weil diese verschiedenen Sinnbezüge über gesellschaftliche Teilsysteme verarbeitet werden, sind mit den Zurechnungen zugleich auch systemische Leistungen verbunden. Dabei verspricht etwa die Politik gesellschaftliche Problemlösungen und die Wirtschaft Bedürfnisbefriedigung, auch wenn systemisch nur Macht bzw. Geld anschlussfähig wirkt. Die erwarteten Leistungen, die mit den Sinnreferenzen lebensweltlich einhergehen, beziehen sich hier auf bestehende Ansprüche und sorgen zugleich für neue. Dabei sind Menschen, Interaktionen und Organisationen nicht Elemente gesellschaftlicher Teilsysteme und gehen nicht in Sinnreferenzen auf. Im lebensweltlichen Zusammenhang können sie die Zurechnungen auf die Sinnreferenzen beliebig ändern und sie miteinander rekombinieren. Eine Mitteilung in Bezug auf etwas, also auch auf eine beliebige gesellschaftliche Sinnreferenz, kann für den Moment anleitend wirken, aber im nächsten Moment bereits die Referenz ändern oder mit einer anderen Sinnreferenz neu verbunden werden. Die Lebenswelt ist demnach eine gesellschaftliche Sphäre unüberschaubar zahlreicher und vielfältiger gesellschaftlicher Interaktionen und Organisationen, die mehr oder weniger stark über vorherige Erfahrungen und Erwartungen der Interaktionsteilnehmer*innen sowie über gesellschaftliche Semantiken aufeinander bezogen sind.[19] Weil nun die Interaktionen und Organisationen aufgrund ihrer Fähigkeiten zur Multidiversität[20] bzw. Multireferenzialität[21] operativ nicht auf Sinnreferenzen festgelegt sind, können sie sich durch eine oder mehrere Sinnreferenz(en) anleiten lassen. Dabei ist lebensweltlich immer ihre sinnbezogene Rekombinationsfähigkeit von Bedeutung, die dann sozial relevant ist, wenn das Resultat in der weiteren Kommunikation als eine plausible Begründung akzeptiert wird. Die Rekombinationen steigern oder reduzieren die Akzeptanz und Plausibilität von Begründungen für oder gegen systemische Leistungen in Bezug auf eine systemische Leistung und das hiermit verbundene Anspruchsniveau. Die Lebenswelt geht also aus den interaktiv und organisational vermittelten Dynamiken zwischen den gesellschaftlichen Sinnreferenzen hervor, bezeichnet aber einen systemisch stetig unterbrochenen und lose verbundenen Kommunikationszusammenhang, der

19 Vgl. Jens Lanfer und Tobias Vogel, »Zeitverhältnisse und die Krise der modernen Gesellschaft«, in: *Zeitschrift diskurs*, Ausgabe 3, August 2018, S. 49–52.

20 Peter Fuchs, »Autopoiesis, Mikrodiversität, Interaktion«, in: Marie-Cristin Fuchs (Hg.), *Theorie als Lehrgedicht. Systemtheoretische Essays I*, Bielefeld: transcript 2004, S. 93.

21 Thomas Drepper, *Organisationen der Gesellschaft. Gesellschaft und Organisationen in der Systemtheorie Niklas Luhmanns*, Wiesbaden: VS Verlag 2003, S. 200.

über Wiederaufnahmen von plausiblen Begründungen für vergleichbare Themen, Erwartungen, Strukturen oder Leistungen kontinuiert wird.

Für die Ausformung von gesellschaftlichen Werten und Wertverhältnissen ist die Lebenswelt anleitend, weil sie wertbezogene Ansprüche sowohl an subjektive Erfahrungen bindet als auch mit plausiblen Begründungen versorgt. Dies bedeutet zugleich, dass sich Ansprüche an Freiheit und Sicherheit mit je unterschiedlichen Sinnreferenzen lebensweltlich zu begründen versuchen. Die gesellschaftliche Wertbedeutung ist damit abhängig von den gesellschaftlichen Sinnreferenzen, die über Interaktionen und Organisationen in unterschiedlicher Anzahl und Intensität auf Werte zugerechnet werden. Seit Beginn der Moderne, die als Prozesse der Ausdifferenzierung voneinander operativ unabhängiger gesellschaftlicher Teilsysteme beobachtet werden kann, erhält der Freiheitswert lebensweltlich die größere Resonanz. Freiheit wurde zum Leitwert der Moderne, weil lebensweltlich viele Sinnreferenzen intensiv auf die individuellen Freiheitsansprüche zugerechnet wurden. Gegenüber einer geschichteten (stratifikatorischen) Gesellschaft versprachen sie mehr individuelle Entfaltungsmöglichkeiten und Optionen. Das Verhältnis zwischen Freiheit und Sicherheit formte sich entsprechend so aus, dass möglichkeitsschaffende Kontingenzen auf Freiheit und bestandsbewahrende Notwendigkeiten auf Sicherheit zugerechnet werden. In der Moderne ist demnach der Freiheitswert mit vielen Sinnreferenzen verbunden, weil die sinnverarbeitenden gesellschaftlichen Teilsysteme hierdurch ihre Komplexität steigern und mehr individuell nutzbare Möglichkeiten erzeugen können. Der Sicherheitswert verweist hingegen vornehmlich auf die politische Sinnreferenz, um sicherheitspolitische Leistungen zu beanspruchen, die erforderlich erscheinen, um Sicherheit für die erreichte (inter-)nationale öffentliche Ordnung zu gewährleisten[22]. Das Ausmaß an Sicherheit im Verhältnis zur Freiheit ist grundlegend abhängig von der Resonanzverteilung der gesellschaftlichen Sinnreferenzen und damit auch von den

22 Seit Thomas Hobbes verkörpert insbesondere der Staat die Quelle gesellschaftlicher Sicherheit und rechtfertigt als Leviathan eine absolute Herrschaft: »Der alleineige Weg zur Errichtung einer solchen allgemeinen Gewalt, die in der Lage ist, die Menschen vor dem Angriff Fremder und vor gegenseitigen Übergriffen zu schützen und ihnen dadurch eine solche Sicherheit zu verschaffen […], liegt in der Übertragung ihrer gesamten Macht und Stärke auf einen Menschen oder eine Versammlung von Menschen, die ihre Einzelwillen und Stimmenmehrheit auf einen Willen reduzieren können. […] Ist dies geschehen, so nennt man diese zu einer Person vereinte Menge *Staat*, auf lateinisch *civitas*. Dies ist die Erzeugung jenes großen *Leviathan*«. Thomas Hobbes, *Leviathan – oder Stoff, Form und Gewalt eines kirchlichen und bürgerlichen Staates*, Iring Fetscher (Hg.), Neuwied/Berlin: Hermann Luchterhand Verlag 1966, S. 134. Aufgrund der starken Bedeutung

resonanzabhängigen Zurechnungspotenzialen auf die Werte. Wenn allerdings ein bestimmtes Wertverhältnis in der Lebenswelt nicht mehr akzeptiert wird, weil das Ausmaß entweder von Freiheit oder Sicherheit als eine zu große Zumutung empfunden wird, politisiert sich das Werteverhältnis. Dadurch verstärken sich die Forderungen nach einer kollektiv bindenden Entscheidung des politischen Systems, um die Werteniveaus anzupassen. Durch die *Politisierung wird das lebensweltliche Steigerungsverhältnis der beiden Werte ›Freiheit‹ und ›Sicherheit‹ zu einem politischen Konkurrenzverhältnis umgeformt*.

Das Konkurrenzverhältnis wird im politischen Gesamtsystem durch den antagonistischen Gegensatz zwischen individueller Freiheit und kollektiver Sicherheit ausgeformt. Der Gegensatz ist zwar nicht auflösbar, aber kann und soll in ein legitimes politisches Gleichgewicht gebracht werden. Auch für demokratische Verfassungsstaaten wirkt der Freiheitswert typisch resonanzstärker als der Sicherheitswert. Er ist vor allem über bürgerliche Abwehrrechte gegenüber staatlichen Handlungsformen, hier vor allem dem staatlichen Gewaltmonopol, institutionell zahlreich und vielfältig verankert. Anleitend ist Freiheit insbesondere als eine (sicherheits-)politische Stopp-Regel gegen staatliches Überengagement (in kollektiver Sicherheit) oder schlicht symbolisch-ideell. Hingegen konzentrierte sich der Sicherheitswert lange Zeit vornehmlich auf die Sicherheitspolitik, hat dabei allerdings als staatliche Legitimationsquelle eine maßgebliche, operativ-materielle Bedeutung. Insofern führt die Politisierung zwischen Freiheit und Sicherheit vor allem zu einem speziell sicherheitspolitischen Konkurrenzverhältnis, das dann als *Sicherheit vor dem Staat und durch den Staat* ausgeformt wird.

Die lebensweltliche Resonanzverteilung der Sinnreferenzen auf die beiden Werte ist grundsätzlich dynamisch, wird aber über Phasen anhaltender Gleichgewichtszustände stabilisiert. Aufgrund einer wachsenden gesellschaftlichen Unübersichtlichkeit infolge von sozialen Umbrüchen und der gefühlten und faktischen Verletzlichkeit der zunehmend komplexeren (hyper-)modernen Gesellschaft vergrößert sich die lebensweltliche Kluft zwischen Freiheit und Sicherheit.[23] Freiheit versorgt die Gesellschaft zunehmend mit dramatischer Kontingenz, die aber keine Absicherung mehr findet. Sicherheit wird deshalb mehr als jemals zuvor in der Moderne über emotionale Appelle eingefordert. Sie wird der dramatischen Kontingenz mit einer dramatischen Notwendigkeit

von freiheitlichen Ansprüchen infolge der funktionalen Ausdifferenzierung und der Institutionalisierung von Nationalstaaten als demokratische Verfassungsstaaten wirkt die absolute Herrschaft weltweit nicht mehr als eine bessere Alternative anleitend.

23 Bernhard Frevel 2018, a. a. O., S. 1.

gegenübergestellt.[24] Dies hat zur Folge, dass die Lebenswelt nicht mehr für eine ausreichende Stabilität menschlicher Erfahrungen sorgt. Sie bietet also weniger Orientierung, weil gesellschaftliche Strukturen nicht nur weniger verlässlich erscheinen, sondern Verlässlichkeit durch das gesellschaftliche Faible für Innovationen[25] geradezu antiquiert erscheint.[26] Wenn vor diesem Hintergrund ›Sicherheit‹ als gesellschaftliche Leitvokabel des 21. Jahrhunderts bezeichnet werden kann,[27] dann resultiert dies also aus dem zunehmenden Resonanzungleichgewicht der gesellschaftlichen Sinnreferenzen in der Lebenswelt, die jeweils unterschiedlich auf die Werte ›Freiheit‹ und ›Sicherheit‹ zugerechnet werden: Die Sinnreferenzen der sich beschleunigenden und entgrenzenden Teilsysteme wie Wirtschaft, Wissenschaft, Massenmedien oder Kunst beziehen sich auf den Freiheitswert, und der Sicherheitswert bezieht sich vornehmlich auf die politische Sinnreferenz, die über ein politisches System verarbeitet wird, das weiterhin durch Nationalstaaten begrenzt ist.

Freiheit und Sicherheit lassen sich jeweils in negative und positive Wertebereiche als *›Freiheit von‹* und *›Freiheit zu‹*[28] sowie *›Sicherheit vor‹* und *›Sicherheit über‹* analytisch unterteilen. Die ›Freiheit von‹ lässt sich im weitesten Sinne als Abwesenheit von Zwang und Repressionen verstehen, die das Individuum allgemein daran hindern, ein Ziel zu erreichen.[29] Aufgrund des Schutzes von Freiheitsansprüchen der Schwächeren gegenüber denen der Stärkeren setzte sich die negative Freiheit als ein Mindestmaß an persönlichem Freiraum durch, der unter keinen Umständen verletzt werden darf.[30] Hingegen stellt sich mit der ›Freiheit zu‹ nicht die Frage danach, ob und inwieweit das Individuum von Zwängen befreit ist, sondern wie es etwa über Bildung und sozialer Inklusionssicherung zur Freiheit angeleitet werden kann, um sie gebrauchen zu können.[31] Während die negative Freiheit eine abwehrende Tendenz hat, charakterisiert sich die positive Freiheit als Gestaltungsfreiheit. Die

24 Zum hypermodernen Verhältnis zwischen dramatischer Kontingenz und dramatischer Notwendigkeit vgl. Günther Ortmann 2009.

25 Jens Aderhold, *Form und Funktion sozialer Netzwerke in Wirtschaft und Gesellschaft. Beziehungsgeflechte als Vermittler zwischen Erreichbarkeit und Zugänglichkeit*, Wiesbaden: VS Verlag 2004, S. 54.

26 Vgl. Jens Lanfer, *Innovationen in Politik und Gesellschaft*, Wiesbaden: Springer VS 2018, S. 23–31.

27 Christopher Daase, Philipp Offermann und Valentin Rauer, »Einleitung«, in: dies. (Hg.), *Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr*. Frankfurt/M.: Campus 2012, S. 7.

28 Vgl. Isaiah Berlin, *Freiheit. Vier Versuche*, Frankfurt/M.: S. Fischer Verlag 1995, S. 197–256.

29 Ebd., S. 202.

30 Ebd., S. 203.

31 Ebd., S. 203.

freiheitsbezogenen Wertbereiche bilden im Verhältnis zueinander Waagschalen, um einerseits die Autonomie des Einzelnen insbesondere vor staatlichen Eingriffen zu schützen sowie andererseits das Mitgestalten am Gleichgewicht der Werte über das Durchsetzen von Ansprüchen (auch gegen den Sicherheitswert) zur Teilhabe an und für die Ausübung von Macht zu ermöglichen.[32]

Äquivalent dazu lässt sich auch der Sicherheitswert analytisch in einen negativen und positiven Wertbereich unterteilen. Es bilden sich der negative Anspruch an eine Sicherheit vor Gefahren und der positive Anspruch an eine Sicherheit über soziale Verhältnisse. Weil der Sicherheitswert vornehmlich auf die politische Sinnreferenz verweist, beziehen sich beide Seiten auf die Leistungen des politischen Systems und prägen damit das nationalstaatliche Legitimationsniveau. Die Wertansprüche an eine ›Sicherheit vor‹ werden vor allem über die Sicherheitspolitik entlang der beiden Politikfelder der inneren und äußeren Sicherheit verarbeitet. Für das Bereithalten von Kapazitäten für die Gewährleistung der (inter-) nationalen öffentlichen Sicherheit sind insbesondere die Verteidigung des Staatsgebiets und von Bündnispartnern vor äußeren Feinden sowie die polizeiliche Abwehr von Gefahren für die öffentliche Sicherheit anleitend. Hiermit geht ein kollektiver Sicherheitsanspruch einher, der immer mit Eingriffsermächtigungen der Sicherheitsbehörden in individuelle Freiheiten der Bürger*innen verbunden ist. Auf der anderen Seite war zunächst die Sicherheit über soziale Verhältnisse vornehmlich sozialpolitisch und für das (selektive) Bereithalten von sozialen Hilfen über die Sozialarbeit etwa in den Bereichen der sozialen Fürsorge oder der Sozialplanung relevant. Über das Leitbild einer ›erweiterten Sicherheit‹[33] ist dieser Wertbereich nun auch sicherheitspolitisch anleitend. Sicherheit soll nicht nur über eine objektivierbare Gefahrenabwehr (Security), sondern auch über stabile soziale Verhältnisse (Safety, Certainty) hergestellt werden, indem sowohl staatlich und gemeinschaftlich als auch politikfeld- und systemübergreifend etwa kommunale Räume oder Wohn- und Geschäftsviertel über verschiedene Praktiken, Programme oder Techniken versicherheitlicht werden sollen, um Unsicherheitsgefühle von Bürger*innen zu reduzieren oder gänzlich zu vermeiden. Vor allem gemeinschaftliche Formationen – verstanden als intermediäre Ebene zwischen Individuum und

32 Burkhardt Kiegeland, »Die Freiheit von & Freiheit zu«, in: *Zeitpunkt*, 109, September/Oktober 2010, S. 10. Online unter http://www.zeitpunkt.ch/fileadmin/download/ZP_109/ZP_109_Freiheit_von___Freiheit_zu.pdf [Zugriff 19.01.2019].

33 Vgl. Stephan Heinrich und Hans-Jürgen Lange, »Erweiterung des Sicherheitsbegriffs«, in: Hans-Jürgen Lange, H. Peter Ohly und Jo Reichertz (Hg.), *Auf der Suche nach neuer Sicherheit. Fakten, Theorien und Folgen*, 2. Auflage, Wiesbaden: VS Verlag 2009, S. 253–268.

Gesellschaft[34] – sorgen für eine Ausweitung von Kooperationen zwischen Akteuren mit unterschiedlichen Sicherheitsinteressen. Dies wird über eine community of practice gefördert, die sich auf gemeinsame Expertisen, konkrete Fertigkeiten, materielle und soziale Ressourcen, geteilte Erwartungen und Handlungsprämissen gründet.[35] Hierin sind mehr oder weniger stark auch ökonomische Erwartungen, Ressourcen und Interessen eingewoben. Lebensweltlich erweitert sich der Sicherheitsanspruch von der reinen negativen Sicherheit in Bezug auf die politische Sinnreferenz und, als Ausdruck einer regulierbaren Sicherheit vor Gefahren, durch eine Sicherheit über (die politische, ökonomische und gemeinschaftliche Gestaltung) soziale(r) Verhältnisse.

Die beiden negativen Wertbereiche ›Freiheit von‹ und ›Sicherheit vor‹ sind lebensweltlich relativ stark auf die politische Sinnreferenz fixiert. Bilden sie ein illegitimes Wertverhältnis aus, werden sie politisiert und in ein (sicherheits-)politisches Konkurrenzverhältnis überführt. Demgegenüber gehen mit den beiden positiven Werten ›Freiheit zu‹ und ›Sicherheit über‹ keine vergleichbar konkreten Ansprüche an bestimmte Sinnreferenzen einher. Weil sie weniger nach Sinnreferenzen differenzieren, sie vielmehr über gemeinschaftliche Formationen rekombinieren, entwickeln sie nur ein geringes Politisierungspotenzial. Damit verbleiben sie quasi in der Lebenswelt. Bei umfassenden Transformationsprozessen wie der gesellschaftlichen Digitalisierung wirken die positiven Wertbereiche entsprechend offener und anpassungsfähiger.

3. Das Wertverhältnis zwischen Freiheit und Sicherheit infolge der gesellschaftlichen Digitalisierung

Die gesellschaftliche Digitalisierung ist ein Transformationsprozess, der in seiner Wirkung wahrscheinlich die Strukturen und Strukturbedingungen sowohl der Lebenswelt als auch sämtlicher Teilsysteme ändert. Über technische Innovationen wie vor allem des Computers und Internets bildete sich ein digitales Universum an Daten in einem bisher nicht vorstellbaren Ausmaß. Dies steigert die lebensweltlichen und systemischen Rekombinationspotenziale immens. Dies bedeutet auch, dass Freiheiten und mithin Möglichkeiten als Optionen, Chancen und Kontingenzen weiter zunehmen. Von diesen technischen Neuerungen und Potenzialen ›profitieren‹ gerade die Teilsysteme, die neue Möglichkeiten schneller und radikaler nutzen und verarbeiten können. Sie erreichen neue Komplexitätsschübe, produzieren für andere Teilsysteme verstärkt

34 Vgl. Amitai Etzioni, *Der dritte Weg zu einer guten Gesellschaft: Auf der Suche nach der neuen Mitte*, Hamburg: Miko-Edition 2001.

35 Vgl. Felix Stalder, *Kultur der Digitalität*, Berlin: Suhrkamp 2016, S. 131–161.

Irritationen und steigern dadurch zugleich die lebensweltliche Resonanz für den gesellschaftlichen Sinn, den sie systemisch verarbeiten. Die Folge ist, dass sich durch die gesellschaftliche Digitalisierung die Wertdiskrepanz von Freiheit und Sicherheit weiter verschärft.

Der digitale Raum erweitert die umfassende Lebenswelt um die *digitale Lebenswelt*. Diese geht aus den digitalen Interaktionen der User mit der Technik und untereinander auf der Grundlage elektronisch produzierter Daten hervor. Im Unterschied zur physischen (analogen) Lebenswelt können sich die User über vorherige Interaktionen detailliert informieren und hieran (potenziell) ohne Daten- und Sinnverlust anschließen. Während sich also die physische Lebenswelt auf immer subjektive Erfahrungen und Erwartungen der Interaktionsteilnehmern*innen gründet, sorgen die digitalen Daten für ein Gesetz der Fortsetzung von Interaktionszusammenhängen. Hierfür müssen die Daten allerdings gespeichert, verarbeitet und abrufbar gehalten werden. Es ist also eine digitale Infrastruktur erforderlich, die als ›informationstechnische Nervenstränge‹ digitale Datenimpulse auf eine bestimmte (selektive) Weise ermöglichen. Für die interaktionsermöglichende Darstellung und Verarbeitung der großen Datenmengen (›big data‹) sind etwa Websites und Hyperlinks mitsamt ihren Inhalten sowie mustererkennende Algorithmen(systeme) anleitend, die abhängig von der Programmierung bzw. deren Prämissen, die für die User in der Regel intransparent sind, bestimmte Daten automatisch erkennen und zu Informationen aufbereiten.

Im digitalen Raum sind also digitale Infrastrukturen erforderlich, die von Betreiber*innen mit unterschiedlichen Sinnreferenzen bereitgestellt werden. Dominant wirken aber Unternehmen, die unterschiedliche Dienstleistungen anbieten, um die Interaktionen der User im digitalen Raum zu ermöglichen und – etwa für eine höhere Benutzerfreundlichkeit – zu optimieren. Die infrastrukturellen Grundlagen der digitalen Lebenswelt setzen die wirtschaftliche Sinnreferenz zunehmend voraus. Die wirtschaftliche Sinnreferenz erreicht dadurch nicht so wie in der sonstigen Lebenswelt eine resonanzstarke, sondern eine resonanzdominante Bedeutung. Nach Zuboff entwickelt sich entsprechend durch den digitalen Raum und die digitale Lebenswelt der Überwachungskapitalismus als eine neue Wirtschaftsform, mit der ein neues Zeitalter einhergeht.[36] Die Autorin bezeichnet das hierfür anleitende Prinzip als die Erzeugung von

> »proprietärem Verhaltensüberschuss, aus dem man mithilfe fortgeschrittener Fabrikationsprozesse, die wir unter der Bezeichnung ›Maschinen- oder künstliche Intelligenz‹ zusammenfassen, Vorhersageprodukte fertigt, die erahnen, was sie jetzt, in Kürze oder irgendwann tun. Und schließlich werden diese Vorhersageprodukte auf einer neuen Art

36 Vgl. Shoshana Zuboff, *Das Zeitalter des Überwachungskapitalismus*, Frankfurt/M.: Campus 2018.

von Marktplatz für Verhaltensvorhersagen gehandelt, den ich als Verhaltensterminkontraktmarkt bezeichne.«[37]

Die Freiheit von Überwachung im digitalen Raum richtete sich in den Anfängen des Internets zunächst gegen die politische Sinnreferenz oder konkret gegen staatliche Herrschaftsansprüche. Mit dem Internet gingen Ansprüche auf einen herrschaftsfreien Raum einher. Die Freiheiten von politischen Repressionen und Zwängen bestehen aber nun wesentlich stärker als die vor wirtschaftlicher Überwachung – mit Folgen für die informationelle Selbstbestimmung der User. Dabei ist der politisch regulierte Datenschutz in der gegenwärtigen Ausformung wenig wirksam, weil die User den Unternehmen vertraglich die Daten im Tausch gegen den unentgeltlichen Gebrauch der digitalen Infrastruktur zur Verfügung stellen. Neben den großen Unternehmen im digitalen Raum Apple, Alphabet, Amazon, Microsoft und Facebook, die unterschiedliche digitale Infrastrukturen der Informationsbereitstellung, des Online-Handels oder der Social Media bereithalten, etablieren sich nur wenige Konkurrenzunternehmen. Ausgeprägte ›Lock-in‹-Effekte bei den Usern sorgen dafür, dass die digitalen Interaktionen unter gewohnten infrastrukturellen Bedingungen, die zudem Interaktionsgeschichten verfügbar halten, fortgeführt werden. Die ›big five‹ erreichen dadurch ein weltweites Oligopol. Die Optionen für die User, der wirtschaftlichen Überwachung zu entgehen, sind aufgrund des mangelnden Angebots an Alternativen und aufgrund von Bequemlichkeiten (Lesen des privatrechtlichen Vertrags, Suche nach Alternativen) entsprechend gering. Zugleich entwickelt sich nur eine geringe Bereitschaft zur Verteidigung der Individualdaten, *weil die Unternehmen nicht nur restriktiv die individuellen Freiheiten einschränken, sondern zugleich eine Freiheit zum selbstbestimmten Handeln über digitale Interaktionen mit der Technik und mit anderen Usern ermöglichen*. Deshalb wird der Verlust an negativen Freiheiten durch deutliche Zugewinne an positiven Freiheiten kompensiert. Weil zudem Freiheiten in der Hypermoderne vornehmlich auf die wirtschaftliche Sinnreferenz zugerechnet werden, entwickelt sich ein geringeres Protestpotenzial. Aufgrund dieser Prozesse steigt zwar die Diskrepanz zwischen Freiheit und Sicherheit, die Politisierung ist aber vergleichsweise gering. Was Sicherheit für die persönlichen Daten im digitalen Raum bedeutet und wie sie hergestellt werden sollte, unterliegt damit weitaus weniger der Deutungsmacht des Staates, der ansonsten zunehmend hinsichtlich der Sicherheit vor Gefahren adressiert wird, sondern fällt auf den Einzelnen zurück. Im digitalen Raum scheint gegenwärtig nicht die negative, sondern die positive Sicherheit anleitend zu sein, die das Individuum selbst verpflichtet, seine Individualinteressen vor Gefahren zu schützen. Auf diese Weise wirkt die Versicherheitlichung über die digitale community anleitend, über die das Individuum

37 Ebd., S. 22.

zum Selbstschutz verpflichtet und angeleitet wird. Das Individuum muss darüber entscheiden, inwieweit und unter welchen Bedingungen es im digitalen Raum interagiert und an der digitalen Lebenswelt partizipiert. Zwar unterscheidet sich dies zunächst nicht von der sonstigen (physischen, analogen) Lebenswelt, aber eine Vermeidung von Überwachung bedeutet für das Individuum häufig zugleich, dass es nicht mehr an der digitalen Lebenswelt teilnehmen kann und die Exit-Option wählen muss. Weil sich die digitale Lebenswelt auf immer mehr Bereiche der umfassenden Lebenswelt ausweitet, ist dies zunehmend keine realistische Option mehr.

Dass nun eine weitergehende politische Regulation die wirtschaftliche Überwachung nicht deutlich begrenzt und die Freiheit vor wirtschaftlicher Überwachung mittels Datenschutz nicht durchsetzt, hat viele Ursachen: Das Bedürfnis nach einer Freiheit von Überwachung im digitalen Raum ist im Verhältnis zu den Zugewinnen an Freiheiten zur Interaktion in der digitalen Lebenswelt gering, dem staatlichen Handeln speziell im digitalen Raum wird nicht vertraut oder keine ausreichende Wirkung (Impact) zugeschrieben, die (sicherheits-)politischen Machtkapazitäten sind aufgrund weiterhin vornehmlich nationalstaatlicher Bindung im Verhältnis zur Gegenmacht der weltweit agierenden Online-Unternehmen nicht ausreichend oder die politischen Wirkungen einer Regulation (Outcome) für andere Politikfelder (insbesondere Wirtschafts- und Technologiepolitik) erscheinen ungewiss und deshalb zu riskant.

Die lebensweltlichen Verhältnisse zwischen den Werten und Wertbereichen von Freiheit und Sicherheit können in Bezug auf die Bereitschaft zur Verteidigung persönlicher Daten über eine Wertematrix zusammenfassend dargestellt werden (Abbildung 1). Mit der digitalen Lebenswelt geht ein geringes Politisierungspotenzial einher, um das stark asymmetrische Verhältnis zwischen Freiheit und Sicherheit auszugleichen. Die Macht zur Gestaltung der digitalen Verhältnisse im Sinne der Freiheit zur Selbstbestimmung wird über wirtschaftliche Möglichkeiten gefördert, sodass hierdurch Freiheitseinschränkungen durch die wirtschaftliche Überwachung kompensiert werden. Die sich verstärkenden lebensweltlichen Ansprüche an eine staatliche Sicherheit vor Gefahren beziehen sich überwiegend auf die physische Lebenswelt und werden über die digitale Öffentlichkeit des Internets[38] gesteigert, ohne dass die Gefahren für die persönlichen Daten im digitalen Raum mit vergleichbar hohen Sicherheitsansprüchen thematisiert werden. Insofern lässt sich eine nur geringe Politisierung des Verhältnisses zwischen Freiheit und Sicherheit beobachten, die zur Folge hat, dass dem Individuum eine Selbstschutzverpflichtung zur Versicherheitlichung auferlegt wird. Demgegenüber könnte eine Politisierung sowohl die Freiheit von wirtschaftlicher Überwachung und die Sicherheit vor Gefahren im

38 Vgl. Mercedes Bunz, *Die stille Revolution*, Suhrkamp: Berlin 2012, S. 113–133.

digitalen Raum verstärken. Aber wie kann dies geschehen? Für die Freiheit könnte eine weitergehende Transparenz von Verträgen und Datenverwendungen politisch eingefordert sowie die Datenverwendung für andere Zwecke als die Optimierung von Online-Angeboten mehr oder weniger stark einschränkt werden. Für mehr Sicherheit vor Gefahren kann von den Online-Unternehmen – insbesondere von denen, die Social Network Sites anbieten – eine über die bisherigen Verpflichtungen (Netzwerkdurchsetzungsgesetz) hinausgehende Sicherheitsherstellung politisch eingefordert werden, indem die Unternehmen dazu aufgefordert werden, rechtswidrige Inhalte schneller als bisher zu erkennen, zu löschen und die Täter*innen etwa über die Sperrung von Online-Accounts zu sanktionieren. Dagegen kann aber zugleich eingewendet werden, dass einerseits die Effekte weitergehender Regulationen für eine Freiheit von wirtschaftlicher Überwachung gering ausfallen, weil die Algorithmen der Unternehmen für die User und Sicherheitsbehörden weiterhin intransparent sind, und dass andererseits eine verstärkte Sicherheit über Online-Unternehmen bzw. eine Privatisierung von Sicherheit mit negativen Folgen für die bürgerlichen Freiheiten einhergeht, weil dann die öffentlichen Diskurse in der digitalen Lebenswelt durch demokratisch nicht legitimierte und kontrollierbare Unternehmensentscheidungen beschränkt werden. Es lässt sich zusammenfassen, dass die Politisierungspotenziale für eine Freiheit vor (wirtschaftlichen) Restriktionen und eine Sicherheit vor wirtschaftlichen Überwachungen gering sind. Das stark asymmetrische Steigerungsverhältnis von Freiheit und Sicherheit im digitalen Raum wird demnach weit weniger als in der sonstigen Lebenswelt in eine politische Logik und entsprechend in ein Konkurrenzverhältnis überführt. Mit der gesellschaftlichen Digitalisierung der Gegenwart gehen demnach nur geringe Politisierungspotenziale und eine zunehmende Bedeutung der positiven Wertbereiche von Freiheit und Sicherheit einher.

Wertvermittlung zwischen Freiheit und Sicherheit in der digitalen Lebenswelt	Ansprüche an die ›Freiheit von‹ Zwang und Restriktionen	Ansprüche an die ›Freiheit zur‹ Selbstbestimmung
Ansprüche an die ›Sicherheit vor‹ Gefahren	*Die Bereitschaft zur Verteidigung von Individualdaten ist hoch.* → *Hohes Politisierungspotenzial*	*Die Bereitschaft zur Verteidigung von Individualdaten ist moderat.* → *Moderates Politisierungspotenzial*
Ansprüche an die ›Sicherheit über‹ soziale Verhältnisse	*Die Bereitschaft zur Verteidigung von Individualdaten ist moderat.* → *Moderates Politisierungspotenzial*	Die Bereitschaft zur Verteidigung von Individualdaten ist gering. → Geringes Politisierungspotenzial

Abb. 1: Lebensweltliche Wertvermittlung zwischen Freiheit und Sicherheit (eigene Darstellung)

4. Zwischen (digitaler) Lebenswelt und Sicherheitspolitik

Vor dem Hintergrund dieser Entwicklungen in der (digitalen) Lebenswelt soll im Weiteren vor allem der *sicherheitspolitischen Bedeutung des positiven im Verhältnis zum negativen Sicherheitswert* für die Gewährleistung (inter-)nationaler öffentlicher Sicherheit nachgegangen werden.

Als lebensweltliche Folge einer relativ eindeutigen und übersichtlichen Zurechnung der negativen Wertbereiche auf die politische Sinnreferenz konzentriert sich die deutsche Sicherheitspolitik bis heute auf die Abwehr vor Gefahren für die (inter-)nationale öffentliche Sicherheit – also auf den negativen Wertbereich von Sicherheit. Was Sicherheit ist und wie sie hergestellt werden soll, folgt also gegenwärtig weiterhin der Deutungsmacht staatlicher Sicherheitsbehörden,[39] wenngleich die oben beschriebenen lebensweltlichen Entwicklungen die Sicherheitsansprüche deutlich ausweiteten und sich die Sicherheit über soziale Verhältnisse als Alternative etabliert. Aufgrund dieser klaren Ausrichtung kann durch die sicherheitspolitische Wertkonkurrenz zwischen einer Sicherheit vor dem und durch den Staat ein politisches Gegengewicht gebildet werden, um einem staatlichen Überengagement über formal-institutionelle Stopp-Regeln ebenso wirksam entgegenzuwirken. Über diese Prozesse formte die Sicherheitsgewährleistung über die Zeit typische Strukturbedingungen, die sowohl eine effektive staatliche Sicherheitsherstellung als auch eine effektive politische Regulation und Kontrolle zulassen. Dies sind zugleich die Voraussetzungen dafür, dass die deutsche Sicherheitspolitik – hier speziell die Polizei als das legitimationsrelevanteste Aufgabenfeld – gegenwärtig ein hohes Legitimationsniveau erreicht: Kontrolle und Regulation steigert die Input-Legitimation; effektive staatliche Sicherheitsherstellungen steigern die Output-Legitimation; transparente und plausible Zurechnungen und intendierte Bewirkungen von Kontrolle, Regulation und Effekten steigern die Throughput-Legitimation.[40] Die steigende Bedeutung

39 Vgl. Jens Lanfer, »Die Dominanz der Verwaltung im Politikfeld Innere Sicherheit – Sicherheitskulturelle Untersuchung am Beispiel der Videoüberwachung öffentlicher Räume in NRW«, in: Hans-Jürgen Lange und Michaela Wendekamm (Hg.), *Dimensionen der Sicherheitskultur*, Wiesbaden: Springer VS 2014, S. 197–234.

40 Vgl. Fritz W. Scharpf, »Legitimationskonzepte jenseits des Nationalstaats«, in: Gunnar Folke Schuppert, Ingolf Pernice und Ulrich Haltern (Hg.), *Europawissenschaft*, Baden-Baden: Nomos 2005, S. 705–741 und vgl. Dieter Grunow, »Verbindlichkeit in einer komplexen Umwelt. Die Kommunalisierung sozialer Hilfen als Gegenstand politik- und verwaltungswissenschaftlicher Forschung«, in: ders. et al. (Hg.), *Vereinbarte Verbindlichkeit im administrativen Mehrebenensystem. Kommunalisierung im Sozialsektor*, Wiesbaden: VS Verlag 2011, S. 20f.

einer Sicherheit über soziale Verhältnisse verändert nun die typischen Strukturbedingungen der Sicherheitspolitik gerade dann, wenn sich der Staat vor dem Hintergrund knapper Ressourcen hierauf einlässt, um auf die ansteigenden Sicherheitsansprüche der Bürger*innen nicht nur mit Versprechungen auf künftige Sicherheiten zu reagieren. So entwickelte sich etwa seit den 1990er Jahren eine *neue Sicherheitsorientierung auch für den Staat*, die – entlang der Sach-, Sozial- und Zeitdimension – als *erweiterte*, *vernetzte* und *präventive Sicherheit* bezeichnet werden kann:

Die erweiterte Sicherheit bezieht sich auf eine Ausweitung der Sicherheitsherstellung auf andere Teilsysteme der Gesellschaft, übergreifende gesellschaftliche Bereiche und andere Politikfelder jenseits der inneren und äußeren Sicherheit. So ist Sicherheit etwa in der Wirtschaft, Medizin, Bildung oder im Sport sowie für die öffentliche Infrastruktur, Stadtplanung, den öffentlichen Verkehr oder in den verschiedenen Politikfeldern der Wirtschafts-, Gesundheits-, Sozial-, Verbraucher-, Ordnungs- oder Energiepolitik von zunehmender Bedeutung. Diese Ausweitung ist eine Reaktion auf ein neues Bedürfnis nach Kontrolle. Wirksame Kontrollierbarkeiten und Kontrollfähigkeiten müssen den Bürger*innen zumindest suggeriert, aber auch stärker über Zertifikate, Prüfsiegel und Gütezeichen nachgewiesen werden. Die neue Sicherheitskultur, die Praktiken für die neue Sicherheitsorientierung hervorbringt, ist auf eine Steigerung der Versicherheitlichung über Kontrolle und Vorsorge ausgelegt, entzieht sich dem Freiheitswert als gesellschaftlichem Leitwert und verrechnet[41] die Freiheit mit Gefahren, die mit ihr einhergehen (könnten). Allerdings gehen damit ungleiche und exklusive Chancen auf Versicherheitlichungen einher, weil nicht gesellschaftliche, sondern vor allem gemeinschaftliche Verhältnisse versicherheitlicht werden können, die insbesondere anhand von vergleichbaren sozioökonomischen Strukturen identifiziert werden. Sie sollen entsprechend auch vor schlechter gestellten sozialen Gemeinschaften schützen. Die Devise ›Gleiche Sicherheit für alle, die es sich leisten können‹[42] für Freiheiten, die über Ausgrenzung des Gefährlichen und Bedrohlichen abgesichert werden, bringt auch neue Bedarfe an Bevölkerungskontrolle hervor, um Formen der Aus- und Abgrenzung bis hin zur Separation zu ermöglichen.

Die *vernetzte* Sicherheit befördert die Versicherheitlichung über Akteure mit Sicherheitsinteressen unterschiedlicher Art, die in Kooperation, Koordination oder nur in sicherheitsproduzierender Koexistenz

41 Dirk Baecker, *Was ist Kultur? Und einige Anschlussüberlegungen zum Kulturmanagement, zur Kulturpolitik und zur Evaluation von Kulturprojekten*, Witten 2015. Online unter https://catjects.files.wordpress.com/2015/11/was_ist_kultur1.pdf [Zugriff 19.01.2019].

42 Trutz von Trotha, »Vom Wandel des Gewaltmonopols oder der Aufstieg der präventiven Sicherheitsordnung«, in: *Kriminologisches Journal*, 42, H. 3 2010, S. 231.

dort aktiv werden, wo sich Unsicherheitsgefühle verstärken. Insofern bilden sie Sicherheitsregime mit einer heterarchische Ordnung als solche, »in denen die Autonomie der konkurrierenden Herrschaftszentren immer durch einen zentralisierten Herrschaftsapparat begrenzt ist«,[43] aber mit diesem konkurrieren. Sie versicherheitlichen bestimmte Räume, Kontexte und Situationen, indem verschiedene Sinnreferenzen und Bereichslogiken aufeinander bezogen werden, um Unsicherheitsgefühle zu reduzieren oder ihnen vorzubeugen. Es etablieren sich etwa in den Kommunen (Shopping Malls, Fußgängerzonen, Geschäftsviertel), aber auch in Räumen des Transits (Bahnhöfe, Flughäfen)[44] Sicherheitsregime, die Überwachung und Kontrolle über eine Sicherheitsgovernance[45] unter Beteiligung privater und privatwirtschaftlicher Akteure mit Sicherheitsinteressen, kommunaler und staatlicher Behörden mit Sicherheitsauftrag sowie über den Einsatz von Sicherheitstechniken möglichst sichtbar machen und durchsetzen. Die Versicherheitlichung über kontextabhängige Gemeinschaften mit gemeinschaftlichen Praktiken bezieht die Sicherheitsbehörden mehr oder weniger stark mit ein. Insbesondere für das polizeiliche Handeln setzt dies voraus, dass neue polizeiliche Management- und Handlungsformen als Steuerungs- und Raumprogramme entwickelt werden müssen, die es ermöglichen, die *Sicherheitsregime* in polizeiliche Strategien einzubinden, um eine öffentliche Sicherheit vor Gefahren negativer Regimewirkungen zu erreichen.[46]

Die *präventive* Sicherheit bezieht sich auf Maßnahmen, Programme und Praktiken einer Versicherheitlichung sozialer Verhältnisse, um zu verhindern, dass Gefahren konkret und damit sichtbar werden. Wenn Gefahren nicht akut und entsprechend nicht erlebt und erfahren werden, so die Hoffnung, entfallen konkrete Abwehrmaßnahmen und es entwickeln sich weniger Unsicherheitsgefühle, die sich eigendynamisch verstärken. Die Vorsorge vor Gefahren wie Epidemien, Ausfällen technischer

43 Trutz von Trotha, »Die präventive Sicherheitsordnung. Weitere Skizzen über die Konturen einer ›Ordnungsform der Gewalt‹«, in: *Kriminologisches Journal*, 42, H. 1 2010, S. 25.

44 Vgl. Jan Wehrheim, *Die überwachte Stadt. Sicherheit, Segregation und Ausgrenzung*, 3. Auflage, Opladen: Verlag Barbara Budrich 2012.

45 Vgl. Hubert Beste, »Zur Privatisierung verloren geglaubter Sicherheit in der Kontrollgesellschaft«, in: Hans-Jürgen Lange, H. Peter Ohly und Jo Reichertz (Hg.), *Auf der Suche nach neuer Sicherheit*,Wiesbaden: VS Verlag 2008, S. 183–202 und vgl. Jens Lanfer, »Sicherheitsgewährleistung zwischen Staat und Stadt«, in: Matthias Lemke (Hg.), *Die gerechte Stadt. Politische Gestaltbarkeit verdichteter Räume*, Stuttgart: Franz Steiner Verlag 2012, S. 148–159.

46 Vgl. Jens Lanfer, »Sicherheitsherstellung unter polizeipolitischen Bedingungen der Kontextbezogenheit«, in: Hans-Jürgen Lange und Michaela Wendekamm (Hg.), *Die Verwaltung der Sicherheit. Theorie und Praxis der Öffentlichen Sicherheitsverwaltung*, Wiesbaden: Springer VS 2018, S. 35–68.

Einrichtungen, Naturkatastrophen, Straftaten oder Ordnungsverstößen lassen sich zeitlich in eine primäre, sekundäre und tertiäre (Kriminal-)Prävention unterteilen.[47] Die primäre Prävention bezieht sich auf die Allgemeinheit und ist umfassend. Sie will bereits das Entstehen von Gefahrenquellen verhindern. Sekundäre Prävention ist adressatenspezifischer und bezieht sich auf eine Präventionsarbeit mit solchen Personen, die als Gefährder oder Opfer in Betracht kommen können. Die tertiäre Prävention konzentriert sich auf die Evaluation bestimmter konkreter Gefahren und Schädigungen, um einem erneuten Auftreten vorzubeugen. Damit ist die erweiterte und vernetzte Sicherheit entsprechend auch darauf ausgelegt, Daten und Informationen über mögliche Gefahren zu erheben und zu verarbeiten, um die Prävention über eine erweiterte Kontrolle sowie netzwerkförmige Koordination und Kooperation optimieren zu können.

Diese neue Sicherheitsorientierung ändert die politische Sicherheitsgewährleistung, die sich auf den Wertbereich einer Sicherheit über soziale Verhältnisse einstellt. Sie umfasst Gewährleistungsformen, die nicht nur die politische Sinnreferenz, sondern viele gesellschaftliche Sinnreferenzen einbeziehen. Dies bedeutet zugleich, dass die lebensweltlich erfahrbare und erfahrene Sicherheit aus einer Rekombination verschiedener Sinnreferenzen hervorgeht, die versicherheitlichende Sinnüberschüsse erzeugt und nutzt.

Auch oder insbesondere in der digitalen Lebenswelt sind diese Sinnüberschüsse für eine Versicherheitlichung sozialer Verhältnisse anleitend. Über das Verhalten der User können mittels Algorithmen Daten generiert und zu sicherheitsrelevanten Informationen verarbeitet werden. Dabei sind Algorithmen keine neue technische Entwicklung. Sie kommen als Handlungsvorschriften für die digitale Kommunikation und Funktionsweise moderner Kommunikationsinfrastrukturen bereits seit längerem zum Einsatz, um bestimmte Probleme über definierte Einzelschritte (maschinell) zu lösen.[48] Sie gewinnen aber desto größere Relevanz, je dringender das sinnabhängige Selektionsproblem im Umgang mit großen Datenmengen wird. Ein Algorithmus, der in der Regel als Element in ein komplexeres digitales algorithmisches System eingebunden ist (etwa in einem SAP-Softwaresystem), wird bislang vornehmlich deterministisch darauf programmiert, große Datenmengen zu durchsuchen, um Muster zwischen verschiedenen Merkmalen zu erkennen und diese mit bekannten Mustern zu vergleichen. Daneben entwickeln sich Möglichkeiten für dynamische, selbstlernende Algorithmen (›Machine Learning‹,

47 Helmut Kury, »Präventionskonzepte«, in: Hans-Jürgen Lange, H. Peter Ohly und Jo Reichertz (Hg.), *Auf der Suche nach neuer Sicherheit*, Wiesbaden: VS Verlag 2008, S. 27f.

48 Wolfgang Hoffmann-Riem, Wolfang, »Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht«, in: *Archiv des öffentlichen Rechts*, 142 2017, S. 2f.

›Deep Learning‹), die sich für eine Sinnreferenz und angeleitet von bestimmten Programmprämissen unabhängig von menschlichen (Detail-) Programmierungen selbstständig weiterentwickeln können und sollen.[49] Im digitalen Raum sind Algorithmen omnipräsent. Mit mehr oder weniger großen Lernfähigkeiten werden sie sowohl von Internetsuchmaschinen als auch für individuelle Produktofferten im Online-Handel oder für Filter-Routinen von E-Mail-Diensten verwendet. In Bezug zu den Verhaltensüberschüssen, die von den Usern in Interaktion mit der Technik oder in der digitalen Lebenswelt erzeugt werden, sind Algorithmen für eine Datenerhebung und -auswertung (in Echtzeit) gegenwärtig zwar vor allem ökonomisch relevant, ihre Bedeutung steigt aber auch für die Leistungen anderer Systeme wie auch für die Auswertung von Daten für sicherheitsrelevante Informationen. Die Folge ist, dass das, was je gegenwärtig in der digitalen Lebenswelt erfahren wird, mehr oder weniger stark über Algorithmen gefiltert ist und dass Daten und Informationen für die lebensweltliche Inanspruchnahme von Sinnreferenzen sowie für die Legitimation systemischer Leistungen zunehmend stärker über Algorithmen aus der digitalen Lebenswelt erzeugt bzw. aufbereitet werden.

Für die hier relevante Sphäre zwischen der digitalen Lebenswelt und der Sicherheitspolitik ist zu betonen, dass sich eine Kultur von Algorithmen, die sich mit Stalder als Algorithmizität[50] bezeichnen lässt, auch für versicherheitlichende Praktiken von Sicherheitsregimen eignet, weil sie über die Daten im digitalen Raum staatliche Sicherheitsherstellungen und gesellschaftliche Versicherheitlichungen ermöglichen. Die Algorithmizität kann als das Gesamtpotenzial von Algorithmen bezeichnet werden, in deren Zusammenhang ein einzelner sinn- und zweckbezogener Algorithmus als Mechanismus zur Reduktion sozialer Komplexität mit hohem Technologiepotenzial (Bewirkung sozialer Wirkungen) in Erscheinung tritt, um soziale Verhältnisse – etwa mit Sicherheitsanspruch – kontrollieren und steuern zu können. Vergleichbar mit der neuen Sicherheitsorientierung werden vormals funktional oder institutionell unabhängige Systeme, Bereiche, Ebenen, Kontexte und Situationen aufeinander bezogen. Die Sinnreferenzen erhalten ein neues Rekombinationspotenzial, das viele neue Möglichkeiten hervorbringt und damit auch Ansprüche zur Nutzung nach sich zieht. Demnach kommen Algorithmen auch in der Sicherheitspolitik zur Anwendung; im Verhältnis zur Wirtschaft aber bei weitem nicht so umfangreich und intensiv. Die Potenziale der Algorithmizität für eine erweiterte, vernetzte und präventive Sicherheit und mithin für eine Versicherheitlichung der Lebenswelt über den digitalen Raum sind allerdings groß.

Insbesondere aufgrund der Aussagen des Whistleblowers Edward Snowden erhielt die algorithmische Verarbeitung von sicherheitsrelevanten

49 Vgl. Felix Stalder 2016, a. a. O, S. 177–181.
50 Ebd., S. 164–202.

Daten aus dem digitalen Raum durch die britischen und US-amerikanischen Geheimdienste große öffentliche Aufmerksamkeit. Über (oder in Kooperation mit?) großen Online-Unternehmen konnten digitale Daten (in Echtzeit) auswertetet werden, um sicherheitsrelevante Informationen für die staatliche Sicherheitsherstellung vor terroristischen Gefahren zu erzeugen. Die Datenerhebung und -auswertung hatte dabei nicht nur die Qualität einer anlasslosen Totalüberwachung der Bürger*innen im In- und Ausland ohne richterliche Anordnung, sondern bezog sich auch auf die Überwachung anderer Regierungen und internationaler und supranationaler Organisationen wie den Vereinten Nationen und der Europäische Union sowie von Wirtschaftsunternehmen.[51] Um dies zu ermöglichen, scheinen die Geheimdienste Verschlüsselungscodes von Telekommunikationsanbietern zu nutzen, um über Smartphones weitere Datenwelten einzubeziehen.[52] Neben den Geheimdiensten hat auch die Polizei ein Interesse an der algorithmischen Verarbeitung digitaler Daten. Hierfür ist das ›Predictive Policing‹ anleitend. Dieses Vorhaben umfasst die verschiedenen Facetten der neuen Sicherheitsorientierung in Anwendung auf den digitalen Raum, weil über algorithmische Mustererkennungen aus den immensen Datenmengen, die über das vergangene menschliche Verhalten im digitalen Raum erzeugt werden, Vorhersagen über das künftige Verhalten abgeleitet werden sollen. Entsprechend ist Predictive Policing »der Versuch, dieses Versprechen für die staatliche Gefahrenabwehr einzulösen.«[53] Der Datenumfang, der für eine solche präventive Sicherheitsorientierung (potenziell) einbezogen werden kann, verdeutlicht den gleichzeitigen Anspruch an die erweiterte und vernetzte Sicherheit: Artikel, Blogs und Social Media in der digitalen Lebenswelt, intelligente Videoüberwachung[54]

51 Alexander Dix, »Notwendigkeit und Chancen eines modernen europäischen Rechtsrahmens angesichts von ›PRISM‹ und ›TEMPORA‹«, in: Udo Bub und Klaus-Dieter Wolfenstetter (Hg.), *Beherrschbarkeit von Cyber Security, Big Data und Cloud Computing. Tagungsband zur dritten EIT ICT Labs-Konferenz zur IT-Sicherheit*, Wiesbaden: Springer Vieweg 2014, S. 9–12.

52 Jeremy Scahill und Josh Begley, »How Spies Stole the Keys to the Encryption Castle«, in: The Intercept, 19. Februar 2015. Online unter https://theintercept.com/2015/02/19/great-sim-heist/ [Zugriff 19.01.2019].

53 Timo Rademacher (2017), »Predictive Policing im deutschen Polizeirecht«, in: Archiv des öffentlichen Rechts, 142 2017, S. 367.

54 Die ›intelligente Videoüberwachung‹ integriert die Mensch-Maschine-Interaktion, die Interaktion zwischen Datenverarbeitungssystemen und menschlichen Beobachtern, und kann von der Norm abweichendes Verhalten als ein ungewöhnliches Ereignis oder auffälliges Bewegungsmuster in überwachten Räumen feststellen und das Sicherheitspersonal hierauf aufmerksam machen. Zudem geht mit der ›intelligenten‹ Videoüberwachung das Potenzial einher, biometrische Muster zu erkennen und verschiedene observierende oder eingriffsbezogene Maßnahmen gegen Gefährder*innen und zur Strafverfolgung auslösen.

auch mittels Drohnen und Satelliten, optische Geräte in Verbindung mit der sich weiterentwickelnden ›Augmented reality‹-Technik (als Nachfolgerin der gescheiterten ›Google Glass‹-Anwendung). Zwar können solche Daten für die Sicherheitspolitik demokratischer Verfassungsstaaten gegenwärtig weder erzeugt und aufbereitet noch für eine Sicherheit vor Gefahren oder eine Versicherheitlichung sozialer Verhältnisse verwendet werden, weil hierfür die rechtlichen Möglichkeiten nicht bestehen und die Technik (teilweise) noch nicht ausgereift ist. Allerdings zeigt die Überwachungsoffensive in der VR China, dass jenseits rechtsstaatlicher Beschränkungen und bereits durch die gegenwärtig verfügbare Technik politische Visionen einer gesellschaftlichen Gesamtsteuerung mit mehr oder weniger großer Wirkung programmatisch auf den Weg gebracht werden. Dafür ist ein ›Sozialkreditsystem‹ als Herrschaftsinstrument anleitend, das die Bürger*innen über Indikatoren wie Zahlungsmoral, Strafregister, Einkaufsgewohnheiten, ökologisches oder soziales Verhalten, Besuch von Angehörigen oder Staatskritik bewertet. Positives Verhalten wird mit Sozialpunkten belohnt und negatives Verhalten mit Punkteabzug bestraft. Ein geringes Punktekonto führt zu Restriktionen bei der Nutzung des öffentlichen Verkehrs, der Schul- und Berufswahl oder bei Buchung von Hotels.[55] Deutlich ist, dass die Freiheiten von Repressionen und Zwängen weitgehend ausgeschaltet werden, um Privilegien für Freiheiten zum selbstbestimmten Handeln politisch – also über einen umfassenden Machtanspruch – verteilen zu können. Freiheiten werden zuerkannt und wirken als Luxus in einer versicherheitlichten Gemeinschaft. In demokratischen Verfassungsstaaten herrschen zwar völlig andere Bedingungen, aber die sicherheitskulturelle Verrechnung zwischen Freiheit und Sicherheit über die diskursiv ›offenen‹ positiven Wertbereiche insbesondere in der digitalen Lebenswelt deutet bereits darauf hin, dass Freiheiten im Verhältnis zur neuen Sicherheitsorientierung als variabel und abhängig behandelt werden und nicht als solche, die über relativ fixierte Sinnreferenzen vorausgesetzt werden müssen.

Die demokratische Macht der Bürger*innen zum selbstbestimmten Handeln und zur Gestaltung der vormals vor allem sicherheitspolitischen Ordnung konzentriert sich unter dem Vorzeichen einer Versicherheitlichung der digitalen Lebenswelt stark auf die Gewährleistung von Gestaltungsmacht über die Teilnahme an der digitalen Lebenswelt. Dies verspricht zwar eine Fülle von neuen Möglichkeiten, hiermit werden aber zugleich Freiheiten von (insbesondere wirtschaftlichen) Repressionen aufgegeben. Die Resonanzverschiebungen und die hieraus resultierenden

Vgl. Monika Desoi, Intelligente Videoüberwachung. Rechtliche Bewertung und rechtsgemäße Gestaltung, Wiesbaden: Springer Vieweg 2018, S. 17–21.

55 Vgl. Tagesschau.de, Auf dem Weg zur totalen Überwachung, 20.05.2018. Online unter https://www.tagesschau.de/ausland/ueberwachung-china-101.html [Zugriff 19.01.2019]

neuen Strukturbedingungen führen also zu Wertverschiebungen und zu einer mangelnden Politisierung von Freiheit und Sicherheit. Die positiven Wertbereiche auf beiden Seiten der Wertverhältnisse treten in den Vordergrund und fallen quasi zusammen, weil sie miteinander verrechnet werden, ohne als Konkurrenzverhältnis in einen politischen Konflikt zu geraten. Als Gründe für diese Verschiebungen können die neue Komplexität und Unübersichtlichkeit angeführt werden, die bestehende gesellschaftliche und lebensweltliche Strukturbedingungen in Frage stellen, um neue Formen der Komplexitätsverarbeitung zuzulassen. Was vorher mit einem relativ strikten Bezug auf die negativen Wertbereiche politisiert werden konnte, verliert sich zugleich im Kausalitätsnebel des sachlich, sozial und zeitlich entgrenzten digitalen Raums. Die alten Wertunterscheidungen einer ›Freiheit von‹ und ›Sicherheit vor‹ erscheinen gegenüber den innovativen Versprechungen für bisher unbekannte Freiheiten und Sicherheiten antiquiert, weil sie unter den neuen digitalen Bedingungen mit Einschränkungen und mangelnder Wirksamkeit in Verbindung gebracht werden. Argumente für Freiheiten zur Selbstbestimmung (unter wirtschaftlichen Vorzeichen) mit einem Versprechen auf eine zugleich wirksamere Sicherheit (über wenig zu kontrollierende Sicherheitsregime) wirken für viele gerade deshalb plausibel, weil Gefahren für die persönlichen Daten und durch die neue Sicherheit nicht ausreichend deutlich bezeichnet werden können. Die Folge ist eine politische Passivität, die sich mit den Folgen der ohnehin unüberschaubaren Dynamiken abfindet. Wertansprüche verebben aufgrund einer zunehmend unbequemeren Selbstbestimmung (Lesen vertraglicher Teilnahmebedingungen eines ›Social Media‹-Angebots, Suche nach Alternativen) oder weil Begründungen für kurzfristige individuelle Vorteile von Kontrolle und Vorsorge (Einsparung bei Versicherungen, unternehmensgeleitete Selbstoptimierung) plausibler wirken.[56] Deutlich wird auch, dass das Politische weniger vital ist, weil im lebensweltlichen Diskurs (antagonistische) politische Gegensätze an Orientierungskraft verlieren. Die folgende Abbildung versucht abschließend am Beispiel exemplarischer Positionierungen das Spektrum möglicher Sicherheitsansprüche der Bürger*innen und die hiermit verbundenen Machtverhältnisse (power to/power over[57]) darzustellen.

56 Über informationelle Mü(n)digkeit und unbequeme Selbstbestimmung und der hiermit einhergehenden Gefahr einer unzureichenden Politisierung vgl. Stefan Ullrich, »Informationelle Mü(n)digkeit. Über die unbequeme Selbstbestimmung«, in: *Datenschutz und Datensicherheit*, Ausgabe 10 2014, S. 696–700. Online unter http://gewissensbits.gi.de/wp-content/uploads/2015/12/Informationelle-M%C3%BCndigkeit-Stefan-Ullrich.pdf [Zugriff 19.01.2019].

57 Vgl. Peter Imbusch, »Macht und Herrschaft in der wissenschaftlichen Kontroverse«, in: ders. (Hg.), *Macht und Herrschaft. Sozialwissenschaftliche Theorien und Konzeptionen*, 2. Auflage, Wiesbaden: Springer VS 2012,

Wertvermittlung zwischen Freiheit und Sicherheit in der digitalen Lebenswelt	Ansprüche an die ›Freiheit von‹ Zwang und Restriktionen	Ansprüche an die ›Freiheit zur‹ Selbstbestimmung
Ansprüche an die ›Sicherheit vor‹ Gefahren	*Exemplarische Positionierung:* ›Solange nicht für einen wirksamen Datenschutz gesorgt wird, verzichte ich auf eine Teilnahme an sozialen Netzwerken.‹ → Ansprüche an die Kontrolle von Staat und Unternehmen (›power to‹) im digitalen Raum über das politische System (›power over‹) und Sorgen über ein vitales politisches Konkurrenzverhältnis zwischen Freiheit und Sicherheit.	*Exemplarische Positionierung:* ›Ich bin mir den Gefahren bewusst und stelle mich auf diese ein. Die weitere Teilnahme an sozialen Netzwerken ist mir jedoch wichtiger.‹ → Ansprüche an die Kontrolle von Staat und Unternehmen (›power to‹) im digitalen Raum werden mit neuen Möglichkeiten verrechnet (›power over‹) und reduzieren das politische Konkurrenzverhältnis zwischen Freiheit und Sicherheit.
Ansprüche an die ›Sicherheit über‹ soziale Verhältnisse	*Exemplarische Positionierung:* ›Zwar müssen die Bedingungen zur Teilnahme an sozialen Netzwerken im digitalen Raum geändert werden, jeder Einzelnen muss sich aber selbst schützen.‹ → (Enttäuschte) Ansprüche an Kontrolle von Staat und Unternehmen (›power to‹) führen zu gemeinschaftlichen Erwartungen und Praktiken eines individuellen Selbstschutzes (›power over‹) und reduzieren das politische Konkurrenzverhältnis zwischen Freiheit und Sicherheit.	*Exemplarische Positionierung:* ›Ich möchte an den sozialen Netzwerken auch unter den gegenwärtigen Bedingungen teilnehmen, weil ich keine Gefahren für mich sehe – ich habe ja schließlich nichts zu verbergen.‹ → Ansprüche an einen wirksameren Schutz durch den Staat und Unternehmen (›power to‹) über Sicherheitsregime (›power over‹) ignorieren das politische Konkurrenzverhältnis zwischen Freiheit und Sicherheit.

Abb. 2: Das Spektrum an Sicherheitsansprüchen vor und durch Staat und Wirtschaft (eigene Darstellung).

S. 9–36 und Marvin E. Olson und Martin N. Marger, *Power in Modern Societies*, 2. Auflage, Boulder: Westview Press 1993.

5. Die Digitalisierung der Sicherheitspolitik

Vor dem Hintergrund gesellschaftlicher und mithin (sicherheits-)politischer Digitalisierungsprozesse und den sich ändernden Strukturbedingungen sucht die politische Gewährleistung (inter-)nationaler öffentlicher Sicherheit nach Möglichkeiten, die Sicherheit vor Staat *und* – wie dargelegt – nunmehr auch Wirtschaft als auch durch Staat und Wirtschaft miteinander so zu vereinbaren, dass die sicherheitspolitische Kapazität für eine Sicherheit vor Gefahren (im digitalen Raum) weiterhin gewährleistet werden kann. Im Weiteren werden zunächst die sicherheitspolitischen Kapazitäten und Strukturbedingungen unter den Bedingungen von Cyber-Sicherheit beschrieben, um zu verdeutlich, welche politischen Unsicherheitszonen mit der Digitalisierung der Sicherheitspolitik einhergehen und wie diese durch neuen Strukturbedingungen absorbiert werden.[58] Darüber hinaus werden den Algorithmen speziell für die Gewährleistung von Cyber-Sicherheit Leistungskapazitäten zugeschrieben, sodass deren Machtpotenzial für die Sicherheit vor und durch Staat und Wirtschaft untersucht werden muss.

5.1. Sicherheitspolitische Kapazitäten und Strukturen unter den Bedingungen von Cyber-Sicherheit

Die sicherheitspolitische Gesamtkapazität für die Gewährleistung (inter-)national öffentlicher Sicherheit setzt sich zusammen aus den verschiedenen Kapazitäten sicherheitspolitischer Politik- und Aufgabenfelder: Bundeswehr und Nachrichtendienst in der äußeren Sicherheit; Polizei, Verfassungsschutz und Bevölkerungsschutz in der inneren Sicherheit. Die Kapazitäten der Aufgabenfelder sind abhängig von dem oben beschriebenen Zusammenhang zwischen der Input-, Throughput- und Output-Legitimation.

Gewöhnlich leitet das Konkurrenzverhältnis zwischen Freiheit und Sicherheit die sicherheitspolitischen Prozesse an, indem die Sicherheit vor dem und die Sicherheit durch den Staat als zwei entgegengesetzte politische Wertpräferenzen ausgeformt werden. Die sicherheitspolitischen Programme bilden dann einen spezifischen Konsens zwischen den beiden Werten. Welcher von beiden dann stärker berücksichtigt wird, ist vor allem abhängig von den lebensweltlichen Trends, die entweder den Freiheits- oder den Sicherheitswert betonen. Wie oben beschrieben ist gegenwärtig der Sicherheitswert resonanzstark. Der Staat erhält neue

58 Vgl. auch Jens Lanfer, »Strukturprinzipien des Politikfelds der Inneren Sicherheit im Wandel«, in: Stephan Barton, Ralf Kölbel und Michael Lindemann (Hg.), *Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens*, Baden-Baden: Nomos 2015, S. 335–338.

Eingriffsbefugnisse insbesondere in den Bereichen der Telekommunikationsüberwachung, Videoüberwachung und biometrischen Kontrollsysteme, um auf veränderte Problemlagen wie neuartige Konfliktformen und Kriege im internationalen Raum,[59] transnationale Formen von organisierter Kriminalität und Terrorismus,[60] zunehmende Straßenkriminalität bei gleichzeitig geringen Aufklärungsquoten[61] sowie ansteigende Unsicherheitsgefühle[62] reagieren zu können. Von besonderer Bedeutung sind dabei vor allem die Sicherheitsprogramme auch in Verbindung mit Sicherheitstechniken, die ›in der Fläche‹ und präventiv wirken. Sie leisten dann zugleich eine Reduktion von Unsicherheitsgefühlen, weil der Staat den Bürger*innen zumindest symbolisch demonstriert, dass etwas getan wird. Dabei werden auch die unverdächtigen Bürger*innen *gemeinschaftlich* in die Sicherheitsherstellung einbezogen, weil sie die staatliche Überwachung erdulden müssen. Je nach Sicherheitsanspruch werden die Bürger*innen hiervon nicht zwingend abgeschreckt, sondern auch versicherheitlicht, zumal das hiermit verbundene Versprechen einer straftatenvorbeugenden Wirkung plausibilisierend wirkt. Die gegenwärtig unterliegende Wertpräferenz der Sicherheit vor dem Staat kann eine Ausweitung der staatlichen Sicherheit aufgrund einer ›großen Koalition für Sicherheit‹ zwar nicht verhindern, sucht aber parallel dazu – vor allem über Vetos und Auflagen des Bundesverfassungsgerichts – nach neuen rechtlichen Begrenzungen und Formen zur effektiven Steuerung und Kontrolle der Sicherheitsbehörden. Insofern ist diese staatliche Ausformung der erweiterten, vernetzten und präventiven Sicherheitsorientierung eine Herausforderung für die Sicherheit vor dem Staat, weil stark einseitig die Output-Legitimation gesteigert werden soll, aber die Throughput- und Input-Legitimation deutlich reduziert wird.

Zugleich formen sich die Implementationsstrukturen um. Über gleichzeitige Prozesse der Zentralisierung und Dezentralisierung der vormals wesentlich stärker von den Bundesländern dominierten Sicherheitsgewährleistung erhalten die politischen Ebenen des Bundes und der Kommunen eine größere Bedeutung. Gefördert werden Kooperationen und Koordinationen einerseits zwischen Sicherheitsbehörden

59 Vgl. Mary Kaldor, *New and Old Wars. Organized Violence in a Global Era*, Cambridge: Polity Press 1999 und vgl. Herfried Münkler, *Die neuen Kriege*, 5. Auflage, Reinbek: Rowohlt 2014.

60 Vgl. Arndt Sinn, *Organisierte Kriminalität* 3.0, Berlin, Heidelberg: Springer Verlag 2016 und Wolfgang Benedek et al. (Hg.), *Transnational Terrorism, Organized Crime and Peace-Building. Human Security in the Western Balkans*, New York: Palgrave 2010.

61 Jens Lanfer, »Das Politikfeld Innere Sicherheit«, in: Dieter Grunow (Hg.), *Implementation in Politikfeldern. Eine Anleitung zum verwaltungsbezogenen Vergleich*, 2. Auflage, Wiesbaden: Springer VS 2017, S. 61.

62 Vgl. Bernhard Frevel 2018, a. a. O., S. 55–66.

unterschiedlicher Politik- und Aufgabenfelder und anderer Nationalstaaten gegen inter- und transnationale Sicherheitsprobleme auf der Bundesebene sowie andererseits zwischen kommunalen und staatlichen sowie privaten und privatwirtschaftlichen Akteuren gegen Verunsicherungen der Bürger*innen im sozialen Nahraum auf der kommunalen Ebene. Insofern intensivieren sich entlang des politischen Mehrebenensystems der Sicherheitspolitik horizontale, vertikale und diagonale Vernetzungen zwischen unterschiedlichen Akteuren.

Diese Programm- und Strukturentwicklungen für die staatliche Sicherheitsherstellung in der physischen Welt bilden zugleich die Grundlage für die Gewährleistung von Cyber-Sicherheit. Der Strukturwandel ist ähnlich, aber wesentlich weitreichender. Für den Aufgabenbereich der Cyber-Sicherheit sind die Akteursnetzwerke nicht Randerscheinungen einer ansonsten institutionell typisch strikt nach politischen Ebenen gegliederten Sicherheitsgewährleistung, sondern die typischen Implementationsarrangements. Weil Cyber-Gefahren die Raumstrukturen transzendieren, sind die institutionellen Ebenen in diesem Aufgabenbereich nicht anleitend. Cyber-Angriffe und -Spionage können von überall auf der Welt zu jeder Zeit erfolgen, wenn hierfür die erforderlichen Kenntnisse und (Computer-)Techniken vorhanden sind. Neben der Raumdimension ist auch die Referenz- und Gefahrendimension der Sicherheitsgewährleistung weit weniger deutlich, als in der physischen Welt, weil unklar ist, mit welcher Intensität und Reichweite ein potenzieller Cyber-Angriff einhergehen kann. Dabei kann die Cyber-Kriminalität einzelne oder tausende Individuen, können Cyber-Attacken kritische Informationsinfrastrukturen nur einzelner Unternehmen und Behörden oder (teil-)öffentliche Informationsinfrastrukturen mit weitreichenden Folgen für ganze Regionen oder gesellschaftliche Teilsysteme (wie Währungssysteme, Telekommunikations- oder Energienetzwerke, technische Großanlagen) treffen. Für die Abwehr von Cyber-Kriminalität und -Attacken müssen dann verschiedene Gefährdungsgrade hinsichtlich der Intensität, Reichweite und zeitliche Nähe zum (potenziellen) Schadenseintritt (nationale Verwundbarkeit, Gefahren, Risiken, Bedrohungen) unterschieden werden. Aufgrund der neuen Unübersichtlichkeit und Verwobenheit von vormals relativ klar getrennten Bereichen lässt sich im Aufgabenbereich der Cyber-Sicherheit eine Vernetzung zwischen den Aufgabenfeldern als anleitender Koordinationstyp beobachten. Demnach ›spiegeln‹ die staatlichen Problemlösungsdimensionen die Problemdimensionen des Regelungsfelds. Die Gewährleistung von Cyber-Sicherheit kann also als eine sicherheitspolitische Meta-Policy bezeichnet werden. Sie transzendiert die Raum-, Sach-, Referenz- und Gefahrendimension der inneren und äußeren Sicherheit.[63]

63 Vgl. Christopher Daase: *Der erweiterte Sicherheitsbegriff*, Working Paper 1, Sicherheitskultur im Wandel, Frankfurt 2010. Online unter http://www.

Weil sich jedes Aufgabenfeld gemäß der formal-institutionellen Ausformung nur spezifisch auf die Cyber-Sicherheit beziehen kann, bilden sich entsprechend auch feldspezifische *Unsicherheitszonen* für die staatliche Herstellung von Cyber-Sicherheit:

Das *Aufgabenfeld der Polizei* umfasst die Bereiche der Gefahrenabwehr und Strafverfolgung. Es konzentriert sich im digitalen Raum vornehmlich auf die Verfolgung von Straftaten, weil die Abwehr konkreter Gefahren aufgrund mangelnder virtueller Präsenz der Polizei im digitalen Raum, unzureichender technischer Ausstattung und rechtlicher Befugnisse kaum möglich ist. Die erste Unsicherheitszone besteht entsprechend darin, dass die Polizei ihrer originären Zuständigkeit gegenwärtig und unter vergleichbaren Bedingungen auch zukünftig nicht nachkommen kann. Sie konzentriert sich hingegen auf die Verfolgung von Cyber-Kriminalität als eine spezifische Form der Computerkriminalität, die das Vorhandensein von EDV-Techniken voraussetzt, aber nur solche Straftaten umfasst, die sich auf die Daten in informationstechnischen Systemen beziehen.[64] Aufgrund der aktuellen und potenziellen Datenströme im digitalen Raum steigt die Intensität gefährdeter individueller und kollektiver Rechtsgüter, die Reichweite potenzieller Angriffsziele auf private und öffentliche Informationsinfrastrukturen, die Tatgelegenheiten und der Nutzen für die Täter*innen. Symptomatisch hierfür steht der Trend zum Internet der Dinge und zur Industrie 4.0, mit dem sämtliche dieser Entwicklungen verbunden sind. Zudem sorgt der grenzenlose digitale Raum für geringe Aufklärungsquoten und Entdeckungswahrscheinlichkeiten,[65] die potenzielle (Wiederholungs-)Täter*innen zu Straftaten motivieren. Beide Unsicherheiten gehen mit den unzureichenden Möglichkeiten grenzüberschreitender Ermittlungen und

sicherheitskultur.org/fileadmin/files/WorkingPapers/01-Daase.pdf [Zugriff 19.01.2019] und Jens Lanfer 2017, a. a. O.

64 Unter die Delikte von Cyber-Kriminalität fallen Computerbetrug, Betrug mit Zugangsberechtigung zu Kommunikationsdiensten, Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitungen, Datenveränderung/Computersabotage sowie das Ausspähen und Abfangen von Daten. Vgl. Bundeskriminalamt (2014), Bundeslagebild Cybercrime 2014, Wiesbaden, S. 3, Fn. 1. Online unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2014.html [Zugriff 19.01.2019].

65 Landeskriminalamt NRW, *Cybercrime in Nordrhein-Westfalen. Lagebild 2013*, Düsseldorf 2013. Online unter https://polizei.nrw/sites/default/files/2016-11/Lagebild_Cybercrime_NRW_2013.pdf [Zugriff 19.01.2019] und Landeskriminalamt NRW, *Cybercrime in Nordrhein-Westfalen. Lagebild 2014*, Düsseldorf 2014. Online unter https://polizei.nrw/sites/default/files/2016-11/Cybercrime_2014.pdf [Zugriff 19.01.2019].

Rechtsdurchsetzungen einher.[66] Die Frage, welche Ausmaße diese beiden Unsicherheitszonen für das Aufgabenfeld der Polizei annehmen, bezeichnet zugleich eine weitere Unsicherheitszone.[67]

Die Unsicherheitszonen für die polizeiliche Abwehr und Verfolgung von Cyber-Kriminalität entstehen weniger durch eine hohe Deliktsintensität, dafür aber stärker durch eine potenziell hohe Reichweite geschädigter Personen. Der gegenwärtige Fall eines relativ groß angelegten Diebstahls persönlicher Daten von mehr als 50 Personen des öffentlichen Lebens in Verbindung mit deren Veröffentlichung ist geeignet, das Unsicherheitsgefühl der Bürger*innen zu verstärken, sodass künftig der politische Druck zur weitergehenden Regulation des privatwirtschaftlichen Angebots von Online-Plattformen, z. B. E-Mail-Dienste, steigen wird, damit unter anderem die E-Mail-Dienste die persönlichen Accounts wirksamer vor Datendiebstahl schützen. Hier steigen die Positionierungen für eine Sicherheit vor Gefahren, indem Unternehmen in die Pflicht genommen werden und nicht nur auf den individuellen Selbstschutz als eine Sicherheit über soziale Verhältnisse der Online-Community und auf privatwirtschaftliche Schutzsoftware abgestellt wird. Darüber hinaus wird die polizeiliche Leistungsfähigkeit kritisiert, so auch in dem aktuellen Fall des Doxing. So betont beispielsweise *Zeit-Online*, dass die Sicherheitsbehörden die Doxing-Opfer, die bereits vor dem öffentlichkeitswirksamen Fall Anzeige erstatteten, wie Einzelfälle behandelten, den Zusammenhang zwischen den Straftaten nicht sahen und das Ausmaß nicht realisiert haben. Zudem brachten die Ermittlungen keine Ergebnisse, sondern sorgten nur dafür, dass der betroffene Account für den User bis zum Abschluss der (erwartbar) ergebnislosen Ermittlung nicht verfügbar war.[68] Auch wenn dieser aktuelle Fall nur einer unter vielen ähnlich gelagerten Fällen ist, zeigt er doch exemplarisch, dass der Druck auf die Sicherheitspolitik und -verwaltung zunimmt, zugleich aber relativ wenige polizeiliche Ressourcen, Strategien und Strukturen sowie rechtliche und praktische Möglichkeiten für eine Abwehr solcher Gefahren bestehen. Neben dieser hohen Problemreichweite steigert sich aber zugleich die Problemintensität von Cyber-Kriminalität, wenn Daten von Wirtschaftsunternehmen gestohlen werden. Der Diebstahl von

66 Vgl. Dominik Brodowski, »Cybersicherheit durch Cyber-Strafrecht? Über die strafrechtliche Regulierung des Internets, in: Hans-Jürgen Lange und Astrid Bötticher (Hg.), Cyber-Sicherheit, Wiesbaden: Springer VS, S. 265f.

67 Bundeskriminalamt, *Bundeslagebild Cybercrime 2013*, Wiesbaden 2013. Online unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2013.html [Zugriff 19.01.2019].

68 Vgl. Kai Biermann et al., »Die lange unerkannte Serientat«, in: *Zeit-online*, 7.01.2019. Online unter https://www.zeit.de/digital/datenschutz/2019-01/datenklau-hackerangriff-orbit-doxing-ermittlungen [Zugriff 19.01.2019]

Kund*innendaten etwa im Online-Handel hat zwar zunächst lediglich eine geringe Reichweite. Er zieht aber intensive Imageschäden der Unternehmen nach sich. Auch der Diebstahl von Betriebsgeheimnissen wie Informationen über zukünftige Projekte hat nur eine geringe Reichweite, entwickelt aber eine vergleichsweise hohe Intensität. Die Folgen von Cyber-Kriminalität können also insgesamt auch die Attraktivität eines nationalen Wirtschaftsstandorts beeinträchtigen.[69]

In den *Aufgabenfeldern der Bundeswehr und des Nachrichtendienstes für die äußere Sicherheit sowie des Verfassungs- und Bevölkerungsschutzes für die innere Sicherheit* bilden sich Unsicherheitszonen vor allem hinsichtlich der Problemintensität von Cyber-Sicherheit. Zu sagen, ob, inwieweit und mit welchen Folgen ausländische Regierungen, politische Gruppierungen oder Organisationen aus einem ausländischem Staatsgebiet Cyber-Attacken auf das Bundesgebiet vor allem in Form von Cyber-Sabotage planen oder bereits durchführen, erfordert Informationen über und aus dem digitalen Raum, die durch die Sicherheitsbehörden der vier Aufgabenfelder eingeholt und ausgewertet werden müssen. Zwar wirkt auch hier eine große Problemreichweite, weil weltweit für entsprechend viele Akteure neue Möglichkeiten bestehen, unterhalb der Schwelle militärischer Aktionen einen anderen Staat effektiv und effizient anzugreifen. Wesentlicher erscheinen aber der Schutz vor einzelnen feindlichen oder terroristischen Cyber-Sabotagen, die jeweils geeignet sind, die kritischen *Informations*infrastrukturen einzelner oder mehrerer Staaten zu manipulieren oder außer Kraft zu setzen. Die informationstechnische Infrastruktur eines Nationalstaats ist ein hochkomplexes Datennetzwerk, das viele Angriffspunkte mit großem Schadenspotenzial aufweist. Störungen solcher Informationsinfrastrukturen können sich entsprechend über Kaskadeneffekte auf die physische nationale Infrastruktur und aufgrund raumentbundener Funktionssysteme einer funktional differenzierten Gesellschaft zunehmend auch auf andere OECD-Staaten auswirken.[70] Die Gewährleistung von Cyber-Sicherheit in diesen Aufgabenfeldern bezieht sich auch oder insbesondere auf präventive Analysen, um Schwachstellen und Angriffspunkte zu identifizieren und zu sichern oder infolge einer erfolgreichen Attacke weitere Bedrohungen und Folgeschäden für andere Anlagen und Datennetze mit öffentlicher Bedeutung zu verhindern. Daneben konzentrieren sich der Nachrichtendienst und Verfassungsschutz auf die Identifizierung und

69 Vgl. Kurt H. G. Groll, »Computerkriminalität«, in: Hans-Jürgen Lange (Hg.): *Wörterbuch zur Inneren Sicherheit*, Wiesbaden: Springer Verlag 2006, S. 51.

70 Anja Dalgaard-Nielsen, »Homeland Security: American and European Responses to September 11«, in: Thomas Jäger, Alexander Höse und Kai Oppermann (Hg.), *Transatlantische Beziehungen. Sicherheit – Wirtschaft – Öffentlichkeit*, Wiesbaden: Springer VS 2005, S. 263.

Prävention vor Cyber-Spionage von ausländischen Regierungen und Unternehmen, die nicht nur staatliche Institutionen betreffen kann, sondern gegenwärtig insbesondere auch als eine Form der Wirtschaftskriminalität betrieben wird.

Für die verschiedenen Unsicherheitszonen und die mit ihnen verbundene Problemintensität und Problemreichweite lässt sich nun zusammenfassen, dass im Schadensfall beide Dimensionen die Unsicherheitsgefühle der Bürger*innen steigern und entsprechenden Druck auf die politisch-administrativen Strukturen insbesondere dann auslösen, wenn über die Zeit eine sich verstärkende Dynamik sowohl intensive als auch weitreichende Schäden nach sich ziehen. Während bei einer hohen Problemreichweite der politische Druck vor allem durch öffentlichkeitswirksame Ereignisse steigt, kann bei einer hohen Problemintensität nicht auf Schädigungen vor allem von kritischen Informationsinfrastrukturen ›gewartet‹ werden, um hierüber zu lernen (tertiäre Prävention), sondern es werden mittels fiktiver Szenarien präventiv Daten und Informationen über potenzielle Verwundbarkeiten informationstechnischer Systeme aufbereitet und analysiert (primäre und sekundäre Prävention).

Gemäß der Logik einer erweiterten, vernetzten und präventiven Sicherheitsorientierung durchzieht der Aufgabenbereich ›Cyber-Sicherheit‹ die verschiedenen Aufgabenfelder der inneren und äußeren Sicherheit und stellt die bisher stark ausgeprägte institutionelle Trennung zur Machtbegrenzung der Sicherheitsbehörden nicht nur in Frage, sondern formt sie stark abweichend aus. Im Aufgabenbereich der Cyber-Sicherheit bildet sich ein Implementationsfeld, das sich von den sonstigen Strukturbedingungen der Sicherheitspolitik deutlich unterscheidet, um hoch dynamisch neue Programmformen, Implementationsstrukturen und Governance-Modi annehmen zu können.[71] Die Implementationsbedingungen für Cyber-Sicherheit sind stark dezentralisiert, dekonzentriert, fragmentiert, für die Zivilgesellschaft offener und aufgrund der unterschiedlichen Akteure wesentlich heterogener sowie von außen schwer regulierbar, kontrollierbar und deshalb relativ politikfern und konsensorientiert. Im deutlichen Gegensatz hierzu lassen sich die typischen Implementationsbedingungen als stark zentralisiert, konzentriert, vertikal-integriert, relativ geschlossen und homogen sowie als (zumindest ereignisabhängig) politiknah und deshalb situativ konfliktorientiert bezeichnen.[72] Auch wenn über die erweiterte, vernetzte und präventive Sicherheitsorientierung auch die anderen Aufgabenfelder mittlerweile mehr oder weniger stark von den typischen Strukturbedingungen abweichen, sind die Strukturänderungen über die Cyber-Sicherheit nicht

71 Jens Lanfer 2017, Cyber-Sicherheit, a. a. O., S. 61.

72 Jens Lanfer 2017, Das Politikfeld, a. a. O. und Jens Lanfer 2018, a. a. O., S. 339–362.

vergleichbar aufgabenfeldspezifisch, partiell und inkrementell, sondern aufgabenfeldübergreifend, umfassend und abrupt. Es lässt sich damit zusammenfassen, dass sich verstärkt auf der Bundesebene netzartige ›Informationsdrehscheiben‹, aber auch auf der kommunalen Ebene auffällig variable Implementationsmuster bilden, die auch als Schablone für die stark pfadabhängigen feldspezifischen Implementationsstrukturen von Cyber-Sicherheit auf Landesebene anleitend wirken könnten. Insgesamt lassen sich die Implementationsarrangements im Aufgabenbereich der Cyber-Sicherheit auf Bundesebene als *hoch flexibel und dynamisch netzwerkorientiert und deshalb problembezogen ›amöbenartig‹* – also der Typik eines Gestaltwandlers entsprechend[73] – beschreiben.

Weil sich die stark abweichenden Strukturbedingungen der Cyber-Sicherheit auf die Steigerung der Leistungskapazitäten und damit auf die Output-Legitimation der Sicherheitspolitik ausrichten, stellt sich zugleich die Frage, in welcher Weise auch die Input- und Throughput-Legitimation gesichert werden kann, um für die Gewährleistung von Cyber-Sicherheit die sicherheitspolitische Gesamtkapazität zu erhöhen. Hier zeigen sich deutliche Legitimationsdefizite. Die typischen Strukturbedingungen der Sicherheitspolitik nehmen gerade deshalb eine im Vergleich zu anderen Politikfeldern (wie der Sozial-, Gesundheits- oder Wirtschaftspolitik) auffällig klar gegliederte Form an, weil sie sowohl auf die staatliche Leistungsfähigkeit (Sicherheit durch den Staat) als auch auf die politische Regulierbarkeit und Kontrollierbarkeit (Sicherheit vor dem Staat) ausgerichtet sind. Die einseitige Steigerung speziell der Leistungskapazität, wie bei der Herstellung von Cyber-Sicherheit, führt zu Verlusten bei der Steuerungs- und Kontrollkapazität des administrativen Handelns über die Parlamente und Gerichte. Um diese Defizite zu verringern, müssen geeignete Eingriffsermächtigungen und Verwaltungsverfahren für die netzwerk- und amöbenartigen Implementationsstrukturen entwickelt werden, die auf die besonderen Bedingungen angepasst sind, um eine Input- und Throughput-Legitimation zu sichern. So zeigt sich gegenwärtig insbesondere im Aufgabenfeld der Polizei eine hohe Gesamtkapazität, weil es sich sowohl über eine hohe Leistungskapazität als auch Regulierungs- und Kontrollkapazität stabilisiert. Ein viel beachteter Indikator hierfür ist das hohe polizeiliche Institutionenvertrauen. Allerding zehrt eine einseitige Steigerung der Leitungskapazität wegen der administrativen Intransparenz und insgesamt undurchsichtigen Strukturarrangements von dieser Vertrauensreserve als riskante Vorleistung der Bürger*innen und Politik. Wer dabei kontrolliert und wer die Kontrolleure kontrolliert, wirft neue institutionelle

73 Dieter Grunow, »Der Ansatz der politikfeldbezogenen Verwaltungsanalyse«, in: ders. (Hg.), *Verwaltungshandeln in Politikfeldern*, Opladen: Leske+Budrich 2003, S. 22.

Fragen auf. Die zunehmend intransparenten Strukturen und Prozesse bergen die Gefahr, dass sie – sicherheitspolitisch typisch ereignisabhängig etwa über künftige Skandale – in legitimationsgefährdendes Misstrauen umschlagen können, wenn nicht für ausgleichende Dynamiken zwischen einer Sicherheit vor dem Staat und durch den Staat gesorgt wird. Der Vertrauensvorschuss erhöht sich infolge der nachholenden Versicherheitlichung und der hiermit verbundenen stärkeren Bedeutung einer Sicherheit durch den Staat im Konkurrenzverhältnis zur Sicherheit vor dem Staat. Sicherheitspolitisch typisch ereignisabhängig, vor allem infolge politischer Skandale, kann diese politisch-administrative Intransparenz aber abrupt in generalisiertes Misstrauen umschlagen, mit der die Throughput-Legitimation (und mithin auch die Input- und Output-Legitimation) drastisch fällt und Proteste gegen ein staatliches Überengagement auslöst. Der Geheimdienstskandal in den USA und Großbritannien verdeutlichen diese Situation, wobei die Inlands- und Auslandsgeheimdienste ohnehin legitimationsschwach sind und die sicherheitspolitischen Auswirkungen nicht vergleichbar hoch wären wie im polizeilichen Aufgabenfeld.[74]

Mit diesen (potenziellen) Legitimationsproblemen ist schließlich die Frage verbunden, ob die untypischen Strukturen im Aufgabenbereich der Cyber-Sicherheit eine *vorübergehende* Anpassung an neue sicherheitspolitische Leistungsanforderungen im Zuge der gesellschaftlichen Digitalisierung darstellen oder ob sie *nur* auf diese Weise eine ausreichende Leistungskapazität zur Herstellung von Cyber-Sicherheit bereithalten können. Nach Baecker führt die digitale Transformation der Gesellschaft dazu, dass die Strukturbedingungen der gesellschaftlichen Teilsysteme – entsprechend auch die des (sicherheits-)politischen Systems – und mithin der funktional differenzierten Gesellschaft insgesamt auf eine Netzwerklogik umstellen.[75] Das bedeutet einen fundamentalen politischen Wandel, der jedoch in dieser Form bereits gegenwärtig am Aufgabenbereich der Cyber-Sicherheit beobachtet werden kann. Es ist also eine offene Frage, ob die stark abweichenden Strukturentwicklungen im Aufgabenbereich über die Zeit von den typischen Strukturbedingungen der Sicherheitspolitik wieder eingefangen werden oder ob die kontinuierlichen gesellschaftlichen Transformationsprozesse diese neuen Strukturformen stabilisieren, sie darüber hinaus in der gesamten Sicherheitspolitik, in anderen Politikfeldern und mithin im politischen Gesamtsystem

74 Jens Lanfer und Hans-Jürgen Lange, »Der Verfassungsschutz im Politikfeld der Inneren Sicherheit zwischen politischen und administrativen Legitimationsanforderungen«, in: dies. (Hg.), *Verfassungsschutz. Reformperspektiven zwischen administrativer Effektivität und demokratischer Transparenz*, Wiesbaden: Springer VS 2016, S. 147.

75 Dirk Baecker, *4.0 oder Die Lücke die der Rechner lässt*, Leipzig: Merve Verlag 2018.

durchsetzen. Dagegen sprechen jedoch die voranschreitenden Prozesse der Institutionalisierung und mithin Zentralisierung in der Cyber-Sicherheit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder das Cyber Information Hub der Bundeswehr verdeutlichen diesen Trend und lassen sich als Vorboten für weitergehende Institutionalisierungen zur Steigerung der Throughput- und Input-Legitimation bezeichnen. Sie können letztlich dazu führen, dass sich der bisher politik-/aufgabenfeldübergreifende und über lose gekoppelte Sicherheitsbehörden koordinierte Aufgabenbereich über weitergehendes Cyber-Sicherheitsrecht, Verfahrensregelungen und spezifische Cyber-Sicherheitsbehörden zu einem autonomen Aufgabenfeld institutionalisiert. Dem stehen allerdings vielfältige administrative und rechtliche Schwierigkeiten entgehen. Vor allem das verfassungsmäßig geforderte Trennungsgebot sowohl der äußeren von der inneren Sicherheit als auch der Polizei vom Verfassungsschutz erfordern neue (input- und outputbezogene) Lösungen, wie Kompetenzen recht- und zweckmäßig zugeordnet und auch hierarchisiert werden können.

5.2 Die Macht der Algorithmen und die Algorithmen der Macht

Die gegenwärtig ›amöben- und netzwerkartigen‹ Strukturarrangements zur Herstellung von Cyber-Sicherheit sind auf die Erzeugung und Verarbeitung sicherheitsrelevanter Daten für übergreifende und sich schnell verändernde Problembereiche und -intensitäten ausgerichtet. Mit dem Design von Implementationsstrukturen für eine höhere sicherheitspolitische Gesamtkapazität werden die sicherheitsrelevanten Akteure im Aufgabenbereich der Cyber-Sicherheit (intendiert oder nur vorläufig?) in einem bestimmt unbestimmten Verhältnis belassen. Diese Situation scheint auch für die politisch-administrativen Programme als Richtigkeitsbedingungen für das Verwaltungshandeln der Sicherheitsbehörden zuzutreffen. Insbesondere auf Bundesebene wirkt für die Kooperation und Koordination der Behörden aus den unterschiedlichen Aufgabenfeldern das Zweckprogramm anleitend, weil strikt regulierende Konditionalprogramme nicht geeignet sind, um einen hoch dynamischen Bereich, der auf die Erzeugung sicherheitsrelevanter Informationen ausgelegt ist, zu regeln. Je nach Aufgabenfeld weichen hiervon die Behörden auf Landesebene mehr oder weniger stark ab, weil weiterhin die typischen sicherheitspolitischen Strukturbedingungen anleitend sind. Insofern steigt die Bedeutung der Bundesebene stark. Sie ist im Aufgabenbereich der Cyber-Sicherheit eine ›Informationsdrehscheibe‹ für die Länder und prägt die Auslösebedingungen für die Sicherheitsprogramme, auf die sich dann die stark länderdominierten Implementationsstrukturen einstellen können. Auf Bundesebene sind also vornehmlich rahmende

politisch-administrative Programme anleitend, die zwar eine große Offenheit zulassen, aber vor allem die administrative Erhebung und Verarbeitung von Daten aus dem digitalen Raum je nach Aufgabenfeld unterschiedlich regulieren. Die Datenbanken sind formal-institutionell auf die Zuständigkeiten und Kompetenzen der Behörden angepasst, die sich entsprechend mit einer unterschiedlichen Tiefe und Breite über die gespeicherten persönlichen Daten der Bürger*innen informieren können.

Für die zahlreichen und vielfältigen Unsicherheitszonen der Aufgabenfelder erscheinen allerdings Algorithmen vielversprechend, weil sie Daten aus dem digitalen Raum für sicherheitspolitische Informationen erheben und fallbezogen auswerten können. Abhängig von den staatlichen Eingriffsermächtigungen je nach nationalstaatlicher Rechtsordnung, Aufgabenfeld und Aufgabenbereich können diese Algorithmen mehr oder weniger anleitend sein. Dabei ist vor allem von großer Bedeutung, ob und inwieweit die Sicherheitsorganisationen auf die privatwirtschaftlich erhobenen Daten zugreifen können und in welcher Weise sie untereinander (diese oder eigene) Daten austauschen dürfen. Nach Stevens erscheint es ein besonderes Interesse der Sicherheitsbehörden zu sein, die Daten aus dem digitalen Raum zu nutzen, um Cyber-Sicherheit effektiv und effizient herzustellen:

> »On the one hand, cyber security is the antidote to state-sponsored ›cyber attacks‹ on critical information infrastructures and to the actions of ›cyber terrorists‹ and ›cyber criminals‹. On the other, cyber security creates a more conducive environment for business and affords government opportunities for the exploitation of cyberspace as a means to achieve, inter alia, a potentially more effective and affordable way of achieving our national security objectives.«[76]

Zwar werden den Sicherheitsbehörden in Deutschland zunehmend mehr Ermächtigungsgrundlagen eingeräumt, im Vergleich zu anderen Staaten wie Australien, Großbritannien oder den USA sind ihre Möglichkeiten aber (noch) sehr begrenzt. Relativ umfangreich ist die zur Terrorabwehr einrichtete Antiterrordatei, die sich aus unterschiedlichen Datenbanken der ca. 40 Sicherheitsbehörden speist und über die sich die Sicherheitsbehörden im Kooperationsverbund Gemeinschaftliches Terrorabwehrzentrum (GTAZ) informieren können. Welche Daten für die jeweiligen Datenbanken der Sicherheitsorganisationen erhoben und unter welchen Bedingungen sie gespeichert und anderen Sicherheitsbehörden zur Verfügung gestellt werden können, ist gesetzlich geregelt, um übermäßige und anlasslose Erhebungen und Speicherungen zu verhindern. Eine automatische Auswertung über einen Algorithmus erfolgt hier bisher anscheinend (noch) nicht. Dies ist jedoch bei der gemeinsamen Nutzung

76 Timm Stevens, *Cyber Security and the Politics of Time*, Cambridge: Cambridge University Press 2016.

von Datenbanken im internationalen Raum weniger der Fall. So hatten (und haben noch?) der Bundesnachrichtendienst und der Bundesverfassungsschutz Zugriff auf die amerikanische Spionagesoftware XKeyscore, die weltweit Kommunikationen im digitalen Raum speichert und auswertet. Weil Informationen durch die Geheimdienste erhoben und gespeichert und Informationen über das GTAZ zwischen den Sicherheitsbehörden weitergeben werden, müssen das Parlament und die Bürger*innen schlicht darauf vertrauen, dass Informationen zwischen den Behörden nicht unrechtmäßig weitergegeben werden, auch wenn zur Terrorabwehr in Verbindung mit oder zur Herstellung von Cyber-Sicherheit eine Vielzahl informeller Abstimmungen zwischen den Behörden verschiedener Aufgabenfelder auf Bundesebene erfolgen. Politische Kontrollen und Regelungen sind bereits unter diesen Bedingungen prekär. Auch im Aufgabenfeld der Polizei sind die oben beschriebenen Entwicklungen zur einem ›Predictive Policing‹ abhängig von Algorithmen, die die sicherheitspolitischen Leistungskapazitäten steigern, wenn sie funktionieren. Die Potenziale von Algorithmen beziehen sich hier möglicherweise nicht nur auf die Sicherheit durch den Staat, sondern auch auf die Sicherheit vor dem Staat. Nach Rademacher kann der Einsatz von Algorithmen polizeiliche Diskriminierungen (wie Racial Profiling) ausschließen, die bei menschlichen Selektionen – bewusst oder unbewusst – mehr oder weniger stark anleitend sind.[77] Aber auch hier ist entscheidend, wer durch welche Programmvorgaben und mit welcher Wirkung etwa gegen Diskriminierung programmiert, den Algorithmus kontrolliert und wer welchen (administrativen) Kontrolleur mit welchen Möglichkeiten (politisch) kontrolliert. Diese Intransparenz reduziert die demokratischen und rechtlichen Kontroll- und Regulierungskapazitäten stark.

Vor allem weil sich die Unsicherheitszonen für die Herstellung von Cyber-Sicherheit hinsichtlich der Problemintensität und/oder Problemreichweite ausweiten werden, ist künftig eine verstärkte staatliche Nutzung von Algorithmen zu erwarten, die das Kontroll- und Steuerungsdefizit weiter verschärfen werden. Weil sich die automatische Verarbeitung der Daten von Online-Unternehmen und anderer Aufgabenfelder ausweiten wird, stellt sich umso dringender die Frage, welches Verhältnis die Sicherheit vor und durch Staat und Wirtschaft annehmen wird. Hierbei sind verschiedene Governance-Formen zu unterscheiden: greift der Staat einseitig hoheitlich auf bestimmte Daten der Unternehmen zu, sorgen die Unternehmen in Eigenregie für digitale Sicherheit oder bilden sich Sicherheitsregime mit einer heterarchischen Ordnung. Aufgrund der lebensweltlichen Orientierung an einer Sicherheit über soziale Verhältnisse, um weitere Freiheiten zur Datenerzeugung

77 Timo Rademacher, a. a. O., S. 375.

zuzulassen, ist zu erwarten, dass eine einseitige staatliche Sicherheitsherstellung im hierarchischen Modus nicht mehr anleitend sein wird. Gerade im Hinblick auf die hohe Bedeutung von Algorithmen spricht vieles dafür, dass sich der gemeinschaftliche Modus intensiviert. Für die Gesamtkapazität der Sicherheitsgewährleistung hat dies allerdings Folgen: Wie (in-)transparent sind Sicherheitsregime bei der politökonomischen Verarbeitung von Daten der Bürger*innen zur Herstellung von Sicherheit über den digitalen Raum und in welchem Ausmaß tritt die privatisierte Sicherheitsherstellung über diese heterarchische Ordnung in Konkurrenz zur weiterhin hierarchisch zentralisierten Sicherheitsordnung des Staates? Die Macht der Algorithmen zur Sicherheitsherstellung liegt bei den Unternehmen, weil diese die informationstechnischen, finanziellen und wissensintensiven Ressourcen bereithalten, um die Algorithmen zu programmieren und weiterzuentwickeln, um aus den unüberschaubaren Datenmengen der User, die ohnehin nur ihnen verfügbar sind, sicherheitsrelevante Informationen zu erzeugen. Wenn aber Algorithmen (selbst-)lernend die Sicherheitsregime selbst anleiten, weil sie in ihren Programmbedingungen für die Akteure intransparent werden, stellt sich die Frage nach dem gesellschaftlichen Koordinationsmechanismus neu. Hierbei erscheint dann nicht mehr die von den Akteuren nutzbare Macht der Algorithmen anleitend, damit sie ihren Einfluss auf die Sicherheitsherstellung vergrößern können, sondern der Algorithmus erhält die Deutungshoheit darüber, was Sicherheit ist und wie sie hergestellt werden sollte. Als automatisch-reflexives Programm zur Sicherheitsherstellung fällt er auf sich selbst zurück. Er schafft und strukturiert Koordinationsbedarfe und dirigiert als Steuerungsprogramm nachgeordnete regulative Programme der Sicherheitsbehörden und Unternehmen. Die Macht der Algorithmen transformiert sich in eine Algorithmizität der Macht. Für die Sicherheitspolitik bedeutet dies, dass das, was Cyber-Sicherheit ist und wie sie hergestellt werden soll, zukünftig möglicherweise weit weniger deutungsmächtig durch die Sicherheitsbehörden beantwortet wird, sondern von Algorithmen, die eingebettet in Sicherheitsregimen entlang der Problem- und Problemlösungsdimensionen sicherheitspolitische Selektionen vornehmen. Insofern läge die Deutungsmacht der staatlichen Herstellung von Cyber-Sicherheit bei den gemeinschaftlichen Algorithmen, die die Unsicherheitszonen zu absorbieren und die sicherheitspolitische Leistungskapazität zu steigern versprechen. Dabei ist aber schließlich zu berücksichtigen, dass die sicherheitspolitische Bedeutung von Algorithmen dann nicht allzu groß ausfallen kann, wenn weiterhin eine hohe sicherheitspolitische Dynamik in der Cyber-Sicherheit vorherrschend ist. Die Algorithmen erkennen zwar Abweichungen, aber keine Zufälle und mithin innovative Technikentwicklungen, mit denen neue Gefährdungen einhergehen. Weil ein unterbrochenes Gleichgewicht zwischen

pfadabhängigen Technikanwendungen und pfadkreativen Technikentwicklungen weiterhin die Sicherheitsdynamiken im digitalen Raum bestimmt, müssen Informationen zur Absorption dieser grundlegenden Unsicherheitszone auch über die Sicherheitsbehörden oder das Sicherheitsregime analog ausgewertet werden. Sollen Algorithmen verstärkt für eine Steigerung der sicherheitspolitischen Leistungskapazitäten genutzt werden, müssen nicht nur einseitig zur Steigerung von Kontroll- und Regulierungskapazitäten, sondern auch zur Steigerung von Leistungskapazitäten regulative Mittel und Wege gefunden werden, die gesellschaftliche und politische Macht von Algorithmen zu begrenzen, um sie zu nutzen.

6. Resümee und Ausblick

Es lässt sich zusammenfassen, dass die lebensweltliche Bedeutung des Sicherheitswerts deutlich zunimmt. Die staatliche Herstellung von Sicherheit vor Gefahren reicht nicht mehr aus, um den Sicherheitsansprüchen gerecht zu werden. Als Alternative wird der positive Wertbereich von Sicherheit gestärkt. Hiermit geht eine gemeinschaftliche Sicherheitsherstellung einher, die auch den Staat als ein Akteur unter vielen in den neuen Sicherheitsregimen einbezieht. Der Staat entwickelt zugleich eine neue Sicherheitsorientierung. Anleitend wirkt hierfür weniger eine klar regulierbare und kontrollierbare, sondern eine erweiterte, vernetzte und präventive Sicherheitslogik. Dies passt zum Zeitgeist der Digitalisierung und insbesondere zur aufkommenden Kultur der Algorithmizität, die die vormals voneinander unabhängigen und getrennten gesellschaftlichen Teilsysteme und Institutionen entgrenzend aufeinander bezieht. Aber diese veränderten Strukturbedingungen lassen sich nicht nur in der Lebenswelt, sondern auch an den Strukturentwicklungen in der Sicherheitspolitik beobachten. Für die Gewährleistung von Cyber-Sicherheit formen sich die typischen Strukturbedingungen und nehmen eine netzwerk- und amöbenartige Form an. Sie werden agil,[78] um die zahlreichen sicherheitspolitischen Unsicherheitszonen absorbieren zu können, die infolge der gesellschaftlichen Digitalisierungsprozesse entstehen. Die Algorithmen entwickeln nun ein sicherheitspolitisches Potenzial, um gemäß der neuen Sicherheitsorientierung verloren geglaubte staatliche Leistungskapazitäten im Bereich der Cyber-Sicherheit und darüber hinaus über die Kooperation mit Unternehmen und sonstigen Akteuren der Sicherheitsregime im digitalen Raum zurückzugewinnen. Aufgrund der Intransparenz algorithmischer Systeme sind hierdurch deutliche Verluste

78 Zum Phänomen der Agilität in Arbeitszusammenhängen vgl. Dirk Baecker 2018, a. a. O., S. 167–177.

für die Kontroll- und Regulationskapazität zu erwarten. Es entwickelt sich eine zunehmende Diskrepanz zwischen der Sicherheit vor und durch Staat und Wirtschaft. Die hohe lebensweltliche Bedeutung von Sicherheit reduziert aber die Politisierungspotenziale mit der Folge, dass die Wertverhältnisse zwischen Freiheit und Sicherheit weniger politisiert werden und Freiheitsansprüche gegenüber staatlichen und wirtschaftlichen Zwängen und Repressionen im lebensweltlichen Diskurs weniger plausibel wirken. Sicherheitspolitisch wird demnach das wertbezogene Steigerungsverhältnis weit weniger in ein Konkurrenzverhältnis zwischen einer Sicherheit vor dem und durch den Staat überführt, um vornehmlich die staatliche Sicherheitsherstellung zu steigern. Aber nur über die Sicherheitspolitik kann das asymmetrische Verhältnis zwischen Freiheit und Sicherheit in der Lebenswelt nicht kompensiert werden. Die Sicherheit vor Gefahren wird ergänzt durch eine Sicherheit über soziale Verhältnisse. Für eine erweiterte, vernetzte und präventive Sicherheitsorientierung wird der Staat zunehmend eingebunden in gefahren-, raum-, kontext- und situationsbezogene Sicherheitsregime unterschiedlicher zivilgesellschaftlicher Akteure, die jeweils ein spezifisches Interesse an eine Versicherheitlichung haben.

Nach Baecker bewirkt die gesellschaftliche Digitalisierung eine Abkehr von der funktional differenzierten Gesellschaft, für die der Kritiküberschuss und die Kulturform des Gleichgewichts zentral waren.[79] Für die nächste Gesellschaft sei hingegen ein Kontrollüberschuss wesentlich, der aus der anleitenden Strukturform des Netzwerks und der Kulturform der Komplexität hervorgehe. Diese Prognose kann über die exemplarische Untersuchung einer Digitalisierung der Sicherheitspolitik bestätigt werden. Das Gleichgewicht zwischen der lebensweltlichen Freiheit und Sicherheit und der politischen Sicherheit vor dem und durch den Staat wird durch die neue gesellschaftliche und politische Komplexität im Umgang mit der gesellschaftlichen Digitalisierung unterbrochen. Es bilden sich entgrenzende Netzwerke, die die vormals institutionell getrennten Räume und funktional begrenzten Teilsysteme transzendieren. Die Komplexitätsschübe verringern die sicherheitspolitischen Leistungskapazitäten, die infolge einer neuen Sicherheitsorientierung über sachliche, soziale und zeitliche Vernetzungen gesteigert werden sollen. Dies führt zugleich dazu, dass die politischen Kontroll- und Regulierungskapazitäten stark abnehmen. Dies gilt insbesondere für die aufziehende Kultur der Algorithmizität, durch die die Algorithmen der Macht eigendynamisch und deutungsmächtig Ursache- und Wirkungszusammenhänge identifizieren und bestimmte (sicherheitspolitische) Problemlösungen plausibilieren. Wer dann die Algorithmen in welcher Weise programmiert

79 Vgl. Baecker, Dirk (2018), *4.0 oder Die Lücke die der Rechner lässt*, Leipzig: Merve Verlag 2018, S. 61–75.

und dabei welche (sicherheitsbezogenen) Interessen verfolgt, wird nicht mehr deutlich zurechenbar, sodass rechtsstaatliche Selbstbegrenzungen der Politik über kollektiv bindendes Entscheiden an der neuen Komplexität von Kontrolle, Regulation und Leistung zunehmend weniger wirksam werden (sollen).

Die gegenwärtigen Strukturbedingungen können allerdings auch starke Beharrungskräfte entwickeln. Speziell für den Bereich der Cyber-Sicherheit bilden sich neben den Netzwerken neue Organisationen für Cyber-Sicherheit, die dazu führen können, dass sich ein neues Aufgabenfeld ›Cyber-Sicherheit‹ für die innere und/oder äußere Sicherheit ausbildet. Nach einer Phase der Umstrukturierung könnten sich die alten sicherheitspolitischen Strukturbedingungen für eine Sicherheit vor dem *und* durch den Staat reformieren. Die Struktur- und Institutionenentwicklung in der Cyber-Sicherheit ist eine offene Frage, die weitere sicherheitspolitische Forschungen erforderlich werden lässt. Hierfür anleitend sind dann nicht nur die digitalen Innovationen zur Steigerung sicherheitspolitischer Leistungskapazitäten, sondern auch politische Innovationen zur Steigerung von demokratischen und rechtsstaatlichen Kontroll- und Regulationskapazitäten, die vor dem Hintergrund gegenwärtiger Legitimationsbedingungen nur in enger Verbindung mit den Leistungskapazitäten eine politische sicherheitspolitische Gesamtkapazität hervorbringen. Insofern können die funktionale Differenzierung gesellschaftlicher Teilsysteme, die vitalen Resonanzverschiebungen zwischen den gesellschaftlichen Sinnreferenzen und mithin zwischen den gesellschaftlichen Werten Freiheit und Sicherheit, die binnenfunktionale und institutionelle Differenzierung politischer Bereichslogiken, die legitimationsrelevante Differenzierung zwischen den konkurrierenden sicherheitspolitischen Wertansprüchen an eine Sicherheit vor dem und durch den Staat sowie die Machtdifferenzierung zwischen der staatlichen Sicherheitsherstellung und einflussorientierten, aber nicht vergleichbar legitimierten Sicherheitsregimen nur aufrechterhalten werden, wenn neue politisch-administrative Institutionen und neue Formen des Datenschutzes geschaffen werden, »um funktionsbereichsübergreifende Datenströme unmöglich zu machen«[80] oder sie zumindest politisch regulieren und kontrollieren zu können.

80 Gesa Lindemann, »Die Verschränkung von Leib und Nexistenz«, in: Florian Süssenguth (Hg.), *Die Gesellschaft der Daten. Über die digitale Transformation der sozialen Ordnung*, Bielefeld: transcript 2015, S. 63.

Literatur

Aderhold, Jens (2004): *Form und Funktion sozialer Netzwerke in Wirtschaft und Gesellschaft. Beziehungsgeflechte als Vermittler zwischen Erreichbarkeit und Zugänglichkeit*, Wiesbaden: VS Verlag. S. 54.

Baecker, Dirk (2015): *Was ist Kultur? Und einige Anschlussüberlegungen zum Kulturmanagement, zur Kulturpolitik und zur Evaluation von Kulturprojekten*, Witten. Online unter https://catjects.files.wordpress.com/2015/11/was_ist_kultur1.pdf [Zugriff 19.01.2019].

Baecker, Dirk (2018): *4.0 oder Die Lücke die der Rechner lässt*, Leipzig: Merve Verlag.

Benedek, Wolfgang et al. (Hg.) (2010), *Transnational Terrorism, Organized Crime and Peace-Building. Human Security in the Western Balkans*, New York: Palgrave.

Berlin, Isaiah (1995): *Freiheit. Vier Versuche*, Frankfurt/M.: S. Fischer Verlag, S. 197–256.

Beste, Hubert (2008): »Zur Privatisierung verloren geglaubter Sicherheit in der Kontrollgesellschaft«, in: Hans-Jürgen Lange, H. Peter Ohly und Jo Reichertz (Hg.), *Auf der Suche nach neuer Sicherheit*, Wiesbaden: VS Verlag, S. 183–202.

Biermann, Kai et al. (2019): »Die lange unerkannte Serientat«, in: *Zeit-online*, 7.01.2019. Online unter https://www.zeit.de/digital/datenschutz/2019-01/datenklau-hackerangriff-orbit-doxing-ermittlungen [Zugriff 19.01.2019].

Brodowski, Dominik, »Cybersicherheit durch Cyber-Strafrecht? Über die strafrechtliche Regulierung des Internets, in: Hans-Jürgen Lange und Astrid Bötticher (Hg.), *Cyber-Sicherheit*, Wiesbaden: Springer VS, S. 249–275.

Bundeskriminalamt (2013): *Bundeslagebild Cybercrime 2013*, Wiesbaden. Online unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2013.html [Zugriff 19.01.2019].

Bundeskriminalamt (2014): Bundeslagebild Cybercrime 2014, Wiesbaden. Online unter https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2014.html [Zugriff 19.01.2019].

Dix, Alexander (2014): »Notwendigkeit und Chancen eines modernen europäischen Rechtsrahmens angesichts von ›PRISM‹ und ›TEMPORA‹«, in: Bub, Udo und, Klaus-Dieter Wolfenstetter (Hg.), *Beherrschbarkeit von Cyber Security, Big Data und Cloud Computing. Tagungsband zur dritten EIT ICT Labs-Konferenz zur IT-Sicherheit*, Wiesbaden: Springer Vieweg, S. 9–12.

Bunz, Mercedes (2012): *Die stille Revolution*, Suhrkamp: Berlin.

Daase, Christopher (2010): *Der erweiterte Sicherheitsbegriff*, Working Paper 1, Sicherheitskultur im Wandel, Frankfurt/M. Online unter http://www.sicherheitskultur.org/fileadmin/files/WorkingPapers/01-Daase.pdf [Zugriff 19.01.2019].

Dalgaard-Nielsen, Anja (2005): »Homeland Security: American and European Responses to September 11«, in: Thomas Jäger, Alexander Höse und Kai Oppermann (Hg.), *Transatlantische Beziehungen. Sicherheit – Wirtschaft – Öffentlichkeit*, Wiesbaden: Springer VS, S. 255–266.

Desoi, Monika (2018): *Intelligente Videoüberwachung. Rechtliche Bewertung und rechtsgemäße Gestaltung*, Wiesbaden: Springer Vieweg.

Drepper, Thomas (2003): *Organisationen der Gesellschaft. Gesellschaft und Organisationen inder Systemtheorie Niklas Luhmanns*, Wiesbaden: VS Verlag.

Daase, Christopher, Philipp Offermann und Valentin Rauer (2012): »Einleitung«, in: dies. (Hg.), *Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr*. Frankfurt/M.: Campus, S. 7–19.

Etzioni, Amitai (2001): *Der dritte Weg zu einer guten Gesellschaft: Auf der Suche nach der neuen Mitte*, Hamburg: Miko-Edition.

Frevel, Bernhard (2018): *Innere Sicherheit. Eine Einführung*, Wiesbaden: Springer VS.

Foucault, Michel (2018): *Die Geburt der Biopolitik. Geschichte der Gouvernementalität II*, 6. Auflage, Frankfurt/M.: Suhrkamp.

Fuchs, Peter (2004): »Autopoiesis, Mikrodiversität, Interaktion«, in: Marie-Cristin Fuchs (Hg.), *Theorie als Lehrgedicht. Systemtheoretische Essays I*, Bielefeld: transcript, S. 73–94.

Groll, Kurt H. G. (2006): »Computerkriminalität«, in: Hans-Jürgen Lange (Hg.): *Wörterbuch zur Inneren Sicherheit*, Wiesbaden: Springer Verlag, S. 48–52.

Grunow, Dieter (2003): »Der Ansatz der politikfeldbezogenen Verwaltungsanalyse«, in: ders. (Hg.), *Verwaltungshandeln in Politikfeldern*, Opladen: Leske+Budrich, S. 15–59.

Grunow, Dieter (2011): »Verbindlichkeit in einer komplexen Umwelt. Die Kommunalisierung sozialer Hilfen als Gegenstand politik- und verwaltungswissenschaftlicher Forschung«, in: ders. et al. (Hg.), *Vereinbarte Verbindlichkeit im administrativen Mehrebenensystem. Kommunalisierung im Sozialsektor*, Wiesbaden: VS Verlag, S. 16–22.

Gusy, Christoph (2012): »Freiheit und Sicherheit«, in: Bundeszentrale für politische Bildung, *Dossier Innere Sicherheit*, 14.06.2012. Online unter http://www.bpb.de/politik/innenpolitik/innere-sicherheit/76651/freiheit-und-sicherheit [Zugriff 19.01.2019]

Heinrich, Stephan und Hans-Jürgen Lange (2009): »Erweiterung des Sicherheitsbegriffs«, in: Hans-Jürgen Lange, H. Peter Ohly und Jo Reichertz (Hg.), *Auf der Suche nach neuer Sicherheit. Fakten, Theorien und Folgen*, 2. Auflage, Wiesbaden: VS Verlag, S. 253–268.

Hobbes, Thomas (1966): *Leviathan – oder Stoff, Form und Gewalt eines kirchlichen und bürgerlichen Staates*, Iring Fetscher (Hg.), Neuwied/Berlin: Hermann Luchterhand Verlag.

Hoffmann-Riem, Wolfgang (2017): »Verhaltenssteuerung durch Algorithmen – Eine Herausforderung für das Recht«, in: *Archiv des öffentlichen Rechts*, 142, S. 1–42.

Husserl, Edmund (1976): *Die Krisis der europäischen Wissenschaften und die transzendentale Phänomenologie*, Den Haag: Martinus Nijhoff.

Imbusch, Peter (2012): »Macht und Herrschaft in der wissenschaftlichen Kontroverse«, in: ders. (Hg.), *Macht und Herrschaft. Sozialwissenschaftliche Theorien und Konzeptionen*, 2. Auflage, Wiesbaden: Springer VS, S. 9–36.

Kaldor, Mary (1999): *New and Old Wars. Organized Violence in a Global Era*, Cambridge: Polity Press.

Kaufmann, Franz-Xaver (2003): »Sicherheit: Das Leitbild beherrschbarer Komplexität«, in: Stephan Lessenich (Hg.), *Wohlfahrtstaatliche Grundbegriffe. Historische und aktuelle Diskurse*, Frankfurt/M.: Campus, S. 73–104.

Kiegeland, Burkhardt (2010): »Die Freiheit von & Freiheit zu«, in: *Zeitpunkt*, 109, September/Oktober, S. 9–11. Online unter http://www.zeitpunkt.ch/fileadmin/download/ZP_109/ZP_109_Freiheit_von___Freiheit_zu.pdf [Zugriff 19.01.2019].

Köhn, Anne und Manfred Bornewasser (2012): *Subjektives Sicherheitsempfinden*, Working Paper Nr. 9, Verbundprojekt Kooperative Sicherheitspolitik in der Stadt (KoSiPol), Bernhard Frevel (Hg.), Münster. Online unter https://d-nb.info/1140787225/34 [Zugriff 19.01.2019].

Kury, Helmut (2008): »Präventionskonzepte«, in: Hans-Jürgen Lange, H. Peter Ohly und Jo Reichertz (Hg.), *Auf der Suche nach neuer Sicherheit*, Wiesbaden: VS Verlag, S. 21–48.

Landeskriminalamt NRW (2013): *Cybercrime in Nordrhein-Westfalen. Lagebild 2013*, Düsseldorf. Online unter https://polizei.nrw/sites/default/files/2016-11/Lagebild_Cybercrime_NRW_2013.pdf [Zugriff 19.01.2019].

Landeskriminalamt NRW (2014): *Cybercrime in Nordrhein-Westfalen. Lagebild 2014*, Düsseldorf. Online unter https://polizei.nrw/sites/default/files/2016-11/Cybercrime_2014.pdf [Zugriff 19.01.2019].

Lanfer, Jens (2012): »Sicherheitsgewährleistung zwischen Staat und Stadt«, in: Matthias Lemke (Hg.), *Die gerechte Stadt. Politische Gestaltbarkeit verdichteter Räume*, Stuttgart: Franz Steiner Verlag, S. 139–166.

Lanfer, Jens (2014): »Die Dominanz der Verwaltung im Politikfeld Innere Sicherheit – Sicherheitskulturelle Untersuchung am Beispiel der Videoüberwachung öffentlicher Räume in NRW«, in: Hans-Jürgen Lange und Michaela Wendekamm (Hg.), *Dimensionen der Sicherheitskultur*, Wiesbaden: Springer VS, S. 197–234.

Lanfer, Jens (2015): »Strukturprinzipien des Politikfelds der Inneren Sicherheit im Wandel«, in: Stephan Barton, Ralf Kölbel und Michael Lindemann (Hg.), *Wider die wildwüchsige Entwicklung des Ermittlungsverfahrens*, Baden-Baden: Nomos, S. 317–346.

Lanfer, Jens und Hans-Jürgen Lange (2016): »Der Verfassungsschutz im Politikfeld der Inneren Sicherheit zwischen politischen und administrativen Legitimationsanforderungen«, in: dies. (Hg.), *Verfassungsschutz. Reformperspektiven zwischen administrativer Effektivität und demokratischer Transparenz*, Wiesbaden: Springer VS, S. 121–150.

Lanfer, Jens (2017):»Cyber-Sicherheit und die (Ohn-)Macht des Staates«, in: Bernhard Frevel und Michaela Wendekamm (Hg.), *Sicherheitsproduktion zwischen Staat, Markt und Zivilgesellschaft*, Wiesbaden: Springer VS, S. 47–72.

Lanfer, Jens (2017):»Das Politikfeld Innere Sicherheit«, in: Dieter Grunow (Hg.), *Implementation in Politikfeldern. Eine Anleitung zum verwaltungsbezogenen Vergleich*, 2. Auflage, Wiesbaden: Springer VS, S. 55–99.

Lanfer, Jens (2018): *Innovationen in Politik und Gesellschaft*, Wiesbaden: Springer VS.

Lanfer, Jens (2018):»Sicherheitsherstellung unter polizeipolitischen Bedingungen der Kontextbezogenheit«, in: Hans-Jürgen Lanfer und Michaela Wendekamm (Hg.), *Die Verwaltung der Sicherheit. Theorie und Praxis der Öffentlichen Sicherheitsverwaltung*, Wiesbaden: Springer VS, S. 35–68.

Lanfer, Jens und Tobias Vogel (2018): »Zeitverhältnisse und die Krise der modernen Gesellschaft«, in: *Zeitschrift diskurs*, Ausgabe 3, August, S. 45–67.

Lindemann, Gesa (2015): »Die Verschränkung von Leib und Nexistenz«, in: Florian Süssenguth (Hg.), *Die Gesellschaft der Daten. Über die digitale Transformation der sozialen Ordnung*, Bielefeld: transcript, S. 41–66.

Luhmann, Niklas (2004): *Einführung in die Systemtheorie*, hrsg. von Dirk Baecker, 2. Auflage, Heidelberg: Carl-Auer-System Verlag.

Luhmann, Niklas (2009): »Risiko und Gefahr«, in: ders. (Hg.), *Soziologische Aufklärung. Konstruktivistische Perspektiven*, 4. Auflage, Wiesbaden: VS-Verlag, S. 126–162.

Luhmann, Niklas (2014): *Vertrauen*, 5. Auflage, Konstanz und München: UVK Verlag.

Münkler, Herfried (2010): »Strategien der Sicherung: Welten der Sicherheit und Kulturen des Risikos. Theoretische Perspektiven«, in: Herfried Münkler, Matthias Bohlender und Sabine Meurer (Hg.), *Sicherheit und Risiko. Über den Umgang mit Gefahr im 21. Jahrhundert*, Bielefeld: transcript, S. 11–34.

Herfried Münkler (2014): *Die neuen Kriege*, 5. Auflage, Reinbek: Rowohlt.

Olson, Marvin E. und Martin N. Marger (1993): *Power in Modern Societies*, 2. Auflage, Boulder: Westview Press.

Opitz, Sven (2014): »Zur Soziologie der Affekte: Resonanzen epidemischer Angst«, in: Joachim Fischer und Stephan Moebius (Hg.), *Kultursoziologie im 21. Jahrhundert*, Wiesbaden: VS Verlag, S. 269–280.

Ortmann, Günther (2009): *Management der Hypermoderne. Kontingenz und Entscheidung*, Wiesbaden: VS Verlag für Sozialwissenschaften.

Rademacher, Timo (2017): »Predictive Policing im deutschen Polizeirecht«, in: *Archiv des öffentlichen Rechts*, 142, S. 366–416.

Scahill, Jeremy und Josh Begley (2015): »How Spies Stole the Keys to the Encryption Castle«, in: *The Intercept*, 19. Februar. Online unter: https://theintercept.com/2015/02/19/great-sim-heist/ [Zugriff 19.01.2019].

Scharpf, Fritz W. (2005): »Legitimationskonzepte jenseits des Nationalstaats«, in: Gunnar Folke Schuppert, Ingolf Pernice und Ulrich Haltern (Hg.), *Europawissenschaft*, Baden-Baden: Nomos, S. 705–741.

Sinn, Arndt (2016): *Organisierte Kriminalität 3.0*, Berlin, Heidelberg: Springer Verlag.
Stalder, Felix (2016): *Kultur der Digitalität*, Berlin: Suhrkamp.
Stevens, Tim (2016): *Cyber Security and the Politics of Time*, Cambridge: Cambridge University Press.
Tagesschau.de (2018): *Auf dem Weg zur totalen Überwachung*, 20.05.2018. Online unter https://www.tagesschau.de/ausland/ueberwachung-china-101.html [Zugriff 19.01.2019].
Trotha, Trutz von (2010): »Die präventive Sicherheitsordnung. Weitere Skizzen über die Konturen einer ›Ordnungsform der Gewalt‹«, in: *Kriminologisches Journal*, 42, H. 1, S. 24–40.
Trotha, Trutz von (2010): »Vom Wandel des Gewaltmonopols oder der Aufstieg der präventiven Sicherheitsordnung«, in: *Kriminologisches Journal*, 42, H. 3, S. 218–234.
Ullrich, Stefan (2014): »Informationelle Mü(n)digkeit. Über die unbequeme Selbstbestimmung«, in: *Datenschutz und Datensicherheit*, Ausgabe 10, S. 696–700, Online unter http://gewissensbits.gi.de/wp-content/uploads/2015/12/Informationelle-M%C3%BCndigkeit-Stefan-Ullrich.pdf [Zugriff 19.01.2019].
Wehrheim, Jan (2012): *Die überwachte Stadt. Sicherheit, Segregation und Ausgrenzung*, 3. Auflage, Opladen: Verlag Barbara Budrich.
Zuboff, Shoshana (2018): *Das Zeitalter des Überwachungskapitalismus*, Frankfurt/M.: Campus.