Präzisierung

Auf Basis der konzeptionellen Überlegungen lässt sich die Zielsetzung der Arbeit nun besser präzisieren.

Ausgangspunkt ist die grundlegende, theoretisch begründete Vorentscheidung, ›die Welt‹ nicht als Versammlung von Substanzen zu begreifen, sondern als ein Effekt von Beziehungen. Aus dieser Hypothese relationaler Ontologien ergibt sich ein spezifischer Untersuchungsgegenstand – es geht um das ›Welt machen‹ im Zusammenspiel von Vorstellungen, Strategien und Techniken. Die Erwartung katastrophischer Szenarien führt zudem derzeit häufiger zum Rückgriff auf technische Prognose-Verfahren, um Sicherheit zu gewinnen. Ich möchte vor allem das rahmensetzende Moment dieser technischen Hinwendung herausarbeiten.

Meine Motivation für die Arbeit ist die Sorge vor einer Entpolitisierung durch eine solche Hinwendung zur Zukunft als Katastrophe. Gegenwärtige Bedrohungsszenarien ähneln sich zunehmend in ihrer Struktur: Das Bedrohliche ist menschengemacht. Das Gefährdende selbst bleibt allerdings unbestimmbar und es gibt einen Umschlagpunkt, von dem an es kein Zurück mehr gibt. Es gilt um jeden Preis, noch vor diesem *tipping point* zu intervenieren. Entsprechend einer solchen Strukturähnlichkeit gegenwärtiger Gefahrendiskurse ähneln sich die Bewältigungsversuche. Regelmäßig erscheint *preparedness*, also die Verbindung von Früherkennung und gezielter Intervention, als die einzig plausible bzw. überhaupt noch mögliche Umgangsweise. Eine Umgangsweise, die ein Arsenal technischer Einrichtungen notwendig macht: Sensoren zur permanenten Überwachung des Ist-Zustands;

die Speicherung möglichst aller verfügbaren Daten angesichts der unbekannten Gefahr; Datenmengen, die dann nur mit Systemen automatisierter Sichtung noch zu prozessieren sind.

Solche technischen Vorkehrungen der *preparedness* werden mit wachsender Skepsis kommentiert. Ausführliche Debatten in Sozial-, Technik-, und Medienwissenschaften beschäftigen sich mit den Veränderungen durch Überwachung und Datenspeicherung, mit den Potenzialen und Gefahren so genannter ›*Big Data*‹-Analysen und der Steuerung durch Algorithmen. Eine Kritik, die häufig direkt an den Techniken und Verfahren ansetzt. Ergänzend schlage ich einen breiteren Blickwinkel vor. Gerade das Zusammenspiel von Vorstellungen, Techniken und Praktiken des prophylaktischen Umgangs mit bedrohlicher Zukunft entwickelt eine eigene Wirkungsmacht. Zudem legitimiert das katastrophische Szenario bereits die Mittel. Die Frage, ob z.B. bestimmte Daten auf diese oder jene Weise erhoben werden sollen und welche Effekte das hat, verblasst angesichts des erwarteten Nutzens. Die Arbeit zielt daher nicht auf eine Kritik der Mittel, sondern auf eine Kritik der Wechselwirkung zwischen Mitteln und Zielen. Welche Rolle spielen Techniken bei der Etablierung einer bestimmten Hinwendung zur Zukunft? Inwiefern etablieren bestimmte Werkzeuge ihren Gegenstand mit? Wie konstituiert sich die zu bewältigende Gefahr auch aus dem Zusammenspiel von Vorstellungen und Techniken der Bewältigung?

Konzeptionelles Hilfsmittel für diese Frage ist die Suche nach Momenten der Infrastrukturierung. Gerade die Strategie der *preparedness* basiert häufig auf der Etablierung von systematisch gekoppelten Systemen. Einzelne Bestandteile dieser Umgangsweise, etwa Überwachung und Speicherung von Sensordaten oder Mustererkennung und Identifizierung von Gefahren, sollen in diesen gekoppelten Systemen möglichst automatisch ablaufen. Es werden entsprechend Sensoren und Datenspeicher verknüpft, Nutzungsrichtlinien erarbeitet und Handlungsroutinen etabliert. Der Zugang zu diesem komplexen Gefüge von Techniken und Praktiken der Bewältigung über die Betrachtung als Infrastrukturierung erlaubt es, diese Gesamtheit in den Blick zu nehmen und zugleich auf die für die Frage relevanten Momente der gegenseiti-

gen Hervorbringung und der Machtwirkungen solcher Infrastrukturen der Bewältigung zu fokussieren.

Gegenstand Syndromic Surveillance

Gegenstand der Untersuchung ist die Etablierung eines syndromischen Gesundheitsmonitoring in den USA. Über einen längeren Zeitraum und in mehreren Anläufen wurde in den USA ein technisches System zur Sammlung und Auswertung unspezifischer Gesundheitsdaten in den meisten Gesundheitsämtern installiert, Meldeabkommen mit inzwischen über 4000 Kliniken wurden abgeschlossen und eine landesweite Interessengemeinschaft aufgebaut. Im Kern steht ein zusätzliches Verfahren der gesundheitlichen Lagebeobachtung, das anders als bisherigen Verfahren, nicht auf diagnostizierten Befunden basiert, sondern laufend eintreffende, unspezifische Daten automatisch nach Auffälligkeiten durchsucht.

In den USA werden dazu vor allem die Angaben zu Beschwerden genutzt, welche die Patient:innen bei dem Erstkontakt in der Notaufnahme zu Protokoll geben. Aber auch alle möglichen weiteren gesundheitsbezogenen Daten fließen in das System ein, wie z. B. Fehlzeiten der Schulen oder Meldungen der Umweltbehörden. Alle solche Daten werden zusammengeführt und mit Hilfe automatischer Routinen geprüft. Im Kontrast zu dem üblichen Verfahren des Gesundheitsmonitoring das meist über einen turnusmäßigen Bericht bestimmter meldepflichtiger Krankheiten durch Ärztinnen und Ärzte funktioniert (so genannte *sentinel surveillance*), versprechen syndromische Verfahren insbesondere zwei Vorteile: einerseits entsteht hier kein Meldeverzug, andererseits sind solche Systeme sensibel auch für unbekannte oder neuartige Gesundheitsprobleme. Geschwindigkeit kann und soll vor allem durch die Automatisierung erreicht werden. So lassen sich Gefahren quasi im Moment des Ausbruchs registrieren und eine Reaktion einleiten. Hier entfällt – so die Erwartung und das Versprechen – der zeitliche Versatz anderer Monitorings, die auf ärztliche Diagnose, Interpretation und Meldung setzen. Ohne das Raster meldepflichtiger Krankheiten kön-

nen hier zudem auch neuartige Krankheiten mit bisher nicht beschriebenen Symptomen erkannt werden, so das Versprechen (Morse 2012).

Die Suche nach neuen technischen Lösungen für die Problemstellung des Gesundheitsmonitoring ist vor dem Hintergrund veränderter Gefahren-Diskurse erfolgt durch und durch erweiterte Möglichkeiten der Datenverarbeitung realisierbar gewesen. In einem kontroversen und von Widerständen auf unterschiedlichen Ebenen begleiteten Prozess konnte sich aus den ersten Pilotprojekten schließlich eine landesweite Strategie etablieren.

Das Fallbeispiel eignet sich exemplarisch für das hier verfolgte Erkenntnisinteresse. Syndromisches Monitoring stellt ein konkretes Werkzeug des Umgangs mit (katastrophischer) Zukunft dar. *Syndromic Surveillance* ein einschlägiges Beispiel für die derzeit insgesamt typische Konzeption von Gefahren (als emergent, unkalkulierbar, katastrophisch) und für einen derzeit typischen Versuch deren technischer Bewältigung (Echtzeit-Monitoring, automatisierte Mustererkennung). Zugleich ist der Gegenstand *Syndromic Surveillance* selbst bisher wenig in den Fokus kritischer Sicherheitsforschung geraten. Womöglich auch, weil es sich um ein Beispiel im Seuchenschutz handelt, also außerhalb der üblichen Sphäre kritischer Sicherheitsforschung. Entsprechend ist der Fall noch nicht überlagert von kritischen Diskursen und den Reaktionen darauf. Schließlich ist der Gegenstand sehr gut geeignet, um ihn als Infrastrukturierung zu betrachten und zu befragen. Das Fallbeispiel der Etablierung eines neuen Gesundheitsmonitorings in den USA ist vor allem auch daher spannend, weil es dabei nicht bloß um ein Konzept oder eine technische Möglichkeit geht, sondern eine schließlich auch realisierte veränderte Praxis in den Gesundheitsbehörden der einzelnen Counties, auf Ebene der Bundesstaaten und an den *Centers for Disease Control*. Der Fall ist auch ein Beispiel für die teils konflikthafte Etablierung einer veränderten Praxis, für die Aushandlung der Befugnisse von Bundesbehörden, für das Ringen um die Souveränität von Daten und die aktive Beteiligung der Epidemiolog:innen vor Ort.

Syndromic Surveillance in den USA lässt sich auch betrachten als eine jahrelange Aushandlung der Notwendigkeit dieser Methode, der best-

möglichen dinglichen Form (Größe und Standorte von Eingabeterminals und Datenspeichern, Software-Protokolle und Standards) und der erforderlichen Aufgaben und Pflichten der beteiligten Akteure. Aus diesem Prozess sind letztlich eine Reihe konkreter technischer Einrichtungen und Systeme hervorgegangen – landesweit etwa das System *BioSense* 2.0. Nach wie vor sind daneben auf der Ebene der Bundesstaaten unterschiedliche technische Realisierungen eines syndromischen Monitorings mit dem identischen Funktionsprinzip im Einsatz (Buehler u.a. 2008). Die Perspektive der Infrastrukturierung ist gut geeignet, um diesen komplexen Vorgang der Etablierung von *Syndromic Surveillance* in den USA in Form von mehreren in Bezug stehenden sozio-technischen Einrichtungen zu fassen. Diese Infrastrukturierung ist vor allem auch eine explizite Form der Reaktion auf veränderte Gefahrenszenarien im Bereich *Public Health*.

Syndromic Surveillance verstehe ich somit als Klammer für einen vielfältigen Vermittlungs- und Aushandlungsprozess technischer Möglichkeiten, politischer Ziele und geteilter Überzeugungen. Als Infrastrukturierung kommen Bestandteile dieses Prozesses aus einem anderen Blickwinkel, nämlich im Hinblick auf das Rahmensetzende des Technischen in der Bearbeitung unerwünschter Zukunft in den Blick. Als Infrastruktur werden die verschiedenen Bestandteile einerseits sichtbar und zugleich der Fokus auf die Wechselwirkungen gerichtet. Technische Systeme, aber auch veränderte Routinen in den Gesundheitsbehörden und neue Erwartungen an die Epidemiolog:innen werden als ein wechselseitiges Gefüge greifbar. Eine Perspektive, für die auch Praktiker:innen im Feld argumentieren. So wirbt beispielsweise Henry Rolka von den Centers for Disease Control in einem frühen Aufsatz, in dem er für hinderliche und förderliche Faktoren bei der Etablierung von *Syndromic Surveillance* sensibilisieren will, für die Berücksichtigung des Infrastrukturellen in einem ähnlich breiten Sinn:

> »The professional relationships and established roles among public health levels (local, state, and federal) must be considered carefully as the context in which public health surveillance activity and system maturity take place. To ignore this extant infrastructure in advancing

> surveillance methodology involves the risk of developing irrelevant ideas because they may not be feasible to implement.« (Rolka 2006, 102)

Um die gegenseitige Hervorbringung von Vorstellungen und Vorkehrungen im Zuge der »Reifung« von *Syndromic Surveillance* geht es im Folgenden. Dabei untersuche ich die Herausbildung des *National Syndromic Surveillance Program* als ein Fallbeispiel für eine ›Politik der Katastrophe‹ – eine Infrastrukturierung zur Bewältigung aktueller Gefahrendiskurse.

Vor allem behaupte ich, dass sich gerade dieses Beispiel in gewisser Weise paradigmatisch lesen lässt. Das Beispiel ist einerseits ein marginaler Sonderfall, andererseits exemplarisch für ein derzeit in vielen Bereichen prägendes Zusammenspiel von Bewältigungsweisen, Techniken und hergestellter Zukunft.

Einerseits ist *Syndromic Surveillance* eine sehr spezifische Antwort im US-amerikanischen Gesundheitssystem geblieben. Die bestimmte technische Anwendung selbst beschränkt sich bisher auf die USA.[1] Auch für die praktische Arbeit in Infektionskontrolle und Seuchenschutz spielt das System auf der Ebene der lokalen Gesundheitsbehörden nur eine begrenzte Rolle.

Andererseits ist *Syndromic Surveillance* greifbarer Ausdruck einer generellen Verschiebung der Herangehensweise an die Überwachung von

1 Auf EU-Ebene wurde Syndromic Surveillance zuletzt zur Erfassung von Gesundheitsproblemen in Unterkünften für Geflüchtete vorgeschlagen (European Centre for Disease Prevention and Control 2016). Eine Umsetzung hat das Robert-Koch-Institut bereitgestellt (Koch-Institut 2020). Vor allem auf der Ebene eines globalen Monitorings sind unterschiedliche Systeme ausprobiert (und teils wieder fallen gelassen) worden. Prominent das Google Projekt *FluNet* zum syndromischen Monitoring von grippeähnlichen Infekten mittels Suchanfrage-Daten (Ginsberg u.a. 2009). Syndromisches Gesundheitsmonotoring spielt innerhalb der NATO Streitkräfte eine Rolle. Seit 2010 kommt bei NATO-Missionen das französische *Near Realtime Surveillance System* ASTER (»Alert et Surveillance en Temps Reel«) zum Einsatz. Hintergrund ist die wachsende Sorge vor nonbattle injuries (DNBI) und einem krankheitsbedingten Ausfall von Soldat:innen in zunehmend asymmetrischen Konflikten (Holtherm 2012).

Krankheiten in der Bevölkerung. Auch in anderen Kontexten wird verstärkt der Ausbau von Kapazitäten einer so genannten *Epidemic Intelligence* gefordert, um die bestehenden Monitoring-Verfahren zu ergänzen (Paquet u.a. 2006). Zunehmend wird dabei nach Wegen gesucht, die Fokussierung auf das Pathogen und dessen Registrierung bei der Überwachung des Infektionsgeschehens durch den Einbezug weiterer Faktoren zu ergänzen. Sozioökonomische Faktoren wie der Zugang zu Wasser oder zu medizinischer Versorgung beeinflussen das Krankheitsgeschehen ebenso wie gesellschaftliche Rahmenbedingungen, politische Konflikte oder Umweltveränderungen.

> »Researchers are now exploring the multifactorial causes of emergence. No longer is the question ›What causes Ebola?‹ but rather, ›Why does an Ebola outbreak occur at a particular time or location?‹« (Olson u.a. 2015, 1285)

Entsprechend diesem veränderten Interesse wird zunehmend nach Wegen gesucht, indikator-basierte Monitoring Systeme, die sich meist eng an Diagnosen von Pathogenen orientieren, zu ergänzen. Ein Vorschlag ist die Ergänzung mit einer ereignis-orientierten Überwachung. Dabei sollen vor allem informelle, nicht-medizinische und nicht primär für den Zweck des Monitoring erstellte Daten einbezogen werden, beispielsweise Kurznachrichten in sozialen Medien (Brownstein, Freifeld und Madoff 2009). Eine *Epidemic Intelligence* auf Basis von digitalen Werkzeugen und einem ereignis-basierten Monitoring spielt inzwischen auch für die Arbeit der europäischen Gesundheitsbehörde eine wichtige Rolle (Bengtsson, Borg und Rhinard 2019).

Erst 2021 hat die WHO eine eigene Dependance in Berlin eröffnet, in der weltweite Daten zusammenlaufen sollen und so die Basis für eine datenbasierte »outbreak science« geschaffen werden soll (Engelmann 2021).

Syndromic Surveillance ist ein konkretes Beispiel für diese übergreifende Verschiebung. Insofern ist die Struktur des mit *Syndromic Surveillance* zu bewältigenden Problems und die in Dingen, Praktiken und Verfahrensweisen wirklich gemachte Problemlösung in vielen Aspekten typisch.

Syndromic Surveillance ist zugleich eine symptomatische Antwort auf die zunehmend anders gefassten Herausforderungen. Das Beispiel selbst mag ein Sonderfall sein, nicht aber der Zusammenhang zwischen Sicherheitsdiskursen, politischen Strategien und den zum Einsatz gebrachten Techniken, der sich an diesem Beispiel zeigt.

National Syndromic Surveillance Program

Für die Darstellung der syndromischen Gesundheitsüberwachung als eine Infrastrukturierung, um die es mir zentral geht, ist zuvor ein grundlegendes Verständnis des Beispiels, der Hintergründe und Eckpunkte der Entwicklung in den letzten Jahren hilfreich. In diesem Kapitel möchte ich diesen Rahmen kurz skizzieren.

Entscheidender Ausgangspunkt für die Entwicklung, die ich nachfolgend als Infrastrukturierung syndromischer Gesundheitsüberwachung in den USA beschreiben möchte, sind die Terroranschläge am 11. September 2001. Schon seit Mitte der 1990er Jahre existieren Bemühungen und Initiativen, die neuen Möglichkeiten der Datenverarbeitung auch für den Zweck des Gesundheitsmonitoring zum Einsatz zu bringen. Die Anfänge des Internet weckten zunehmend Erwartungen an die Nutzung von nahe-Echtzeit-Informationen auch für Aufgaben der *Public Health*. Eine Arbeitsgruppe an den CDC regt bereits 1995 die Entwicklung eines elektronischen Systems zum Gesundheitsmonitoring an. In der Folge wurde ein Datenstandard entwickelt und im Jahr 2000 stellte der US-Senat erstmals Fördermittel zur Verfügung, um die Bundesstaaten mit technischen Systemen zur Nutzung dieses Datenstandards auszustatten (National Electronic Disease Surveillance System Working Group 2001). Dadurch war das *National Electronic Disease Surveillance Systems* (NEDSS) etabliert, vorrangig um einen Datenaustausch zwischen Laboren, Kliniken und Gesundheitsämtern effizienter zu machen. Das System bildet nach wie vor eine Grundlage für diese Art des Datenaustausch (Rolka und O'Connor 2010, 5).

Im Zuge solcher Initiativen für einen möglichst zeitnahen Datenaustausch zwischen Gesundheitsämtern und Kliniken wurden auch

erste Versuche mit der Sammlung von unspezifischen Gesundheitsdaten unternommen.

Die Anfänge sind verzweigt. Frühe Versuche Aussagen über das Gesundheitsgeschehens systematisch auf Basis von nicht-diagnostizierten Daten zu treffen, werden zum Beispiel in New York unternommen. 1995 begann die Gesundheitsbehörde der Stadt – zunächst spezifisch im Hinblick auf Durchfallerkrankungen –, die Angaben aus Pflegeheimen, Labordaten und Verkaufszahlen von Apotheken im Zusammenhang zu betrachten (Heffernan u.a. 2004). Seit 2001 wurde die Datenbasis um Meldungen der Notrufzentralen und Angaben aus den Notaufnahmen der Kliniken erweitert. Die Auswertung der Daten erfolgt hier noch wenig automatisiert. »Each day an analyst with master's- or doctoral-level training in public health and statistical software programming experience dedicates 2-3 hours to collect, process, and analyze data and disseminate results.« (Heffernan u.a. 2004, 26) Ein ähnliches frühes System RODS kommt in Pennsylvania, Utah, Ohio und New Jersey zum Einsatz (Wagner u.a. 2004).

Parallel entwickeln einzelne Gesundheitsämter ereignisbezogene Verfahren des syndromischen Monitorings. Hier werden für den begrenzten Zeitraum der Veranstaltung zusätzliche Mitarbeiter:innen eingesetzt, um gesundheitsbezogene Daten in einer Meldestelle zusammen zu führen und zu überwachen. Die Übermittelung der Daten erfolgt in diesen Fällen noch per Telefax und die Daten müssen per Hand in den Rechner übertragen werden (Davies-Cole 2012). Die so genannte ›*Drop-in syndromic surveillance*‹ kam erstmals bei dem Treffen der Welthandelsorganisation 1999 in Seattle zum Einsatz und später bei weiteren Großereignissen wie der Amtseinführung des US-Präsidenten 2001 (Henning und Hamburg 2003).

Bereits Ende der 1990er Jahre erscheint die US-Hauptstadt als besonders wahrscheinliches Ziel für einen bioterroristischen Anschlag. Vor diesem Hintergrund entwickelt eine Gruppe des *Walter Reed Army Institute for Research* (WRAIR) ein System, um frühzeitig gesundheitliche Auffälligkeiten innerhalb der in der *National Capital Region* (Maryland, Virginia, Washington DC) stationierten Soldat:innen zu erkennen (Lewis u.a. 2002). Schon seit 1997 werden die Beschwerden, mit denen sich

Soldat:innen, Angehörige oder Veteran:innen an ein medizinisches Behandlungszentrum des Militärs wenden, gemäß der ICD-9 Codes (Internationale Klassifikation der Krankheiten, 9. Revision) klassifiziert. Der nächste Schritt, die elektronische Übermittlung, Speicherung und statistische Auswertung dieser Daten, war dadurch in diesem Fall relativ einfach umzusetzen (Broome u.a. 2002). Dieses System wurde als *Electronic Surveillance System for the Early Notification of Community-Based Epidemics* (ESSENCE) bezeichnet und sammelte im Dezember 1999 erstmals Daten (Lewis u.a. 2002). 2001 wird das ESSENCE genannte System in den US-Militärkliniken weltweit eingeführt (Office of Preparedness & Response 2012).

Ein Zusammenschluss der *Johns Hopkins University* in Baltimore und der Gesundheitsämter von Maryland, Virginia und Washington, DC überträgt dieses System im gleichen Jahr in den zivilen Bereich. Das anfangs unter dem Namen ESSENCE II laufende System integriert Daten aus den Notaufnahmen des Militärs, von zivilen Kliniken, Angaben zu Fehlzeiten in den Schulen, Verkaufsstatistiken von Drogeriemärkten, Meldungen von Tierärzten und die amtliche Grippestatistik (Lombardo u.a. 2003; Lombardo, Burkom und Pavlin 2004). Erste Daten werden seit 1999 über das System registriert und seit den Anfängen in einzelnen Bezirken Marylands werden zunehmend mehr Datenquellen in das System einbezogen.

Die koordinierten Anschläge auf das *World Trade Center* und das Pentagon in New York und Washington am 11. September 2001 sind dann ein entscheidender Einschnitt und Antrieb für die weitere Etablierung solcher Systeme. Die Anschläge bedeuten auch einen sicherheitspolitischen Paradigmenwechsel mit weitreichenden Folgen (Hooker und Ali 2009). Eine dieser Folgen betrifft die veränderte Betrachtung von *Public Health* als einen Schauplatz von Landesverteidigung und entsprechend eine neue Aufmerksamkeit für Gesundheitsmonitoring an sich, und für das Bemühen um neue technische Lösungen in diesem Bereich.

Die manifest gewordene Tatsache einer latenten Bedrohung durch terroristische Anschläge im eigenen Land lässt die bisherige Politik der Abschreckung durch Drohung mit harten Vergeltungsmaßnahmen ungenügend erscheinen. Stattdessen erklärt die Bush Administration

erstmals explizit ein präemptives Vorgehen zu einer offiziellen Maßgabe. So erstmals ausdrücklich und explizit in der *National Security Strategy* von 2002:

> »The greater the threat, the greater is the risk of inaction – and the more compelling the case for taking anticipatory action to defend ourselves, even if uncertainty remains as to the time and place of the enemy's attack. To forestall or prevent such hostile acts by our adversaries, the United States will, if necessary, act preemptively.« (NSC 2002)

Dieser Wechsel der Strategie von Abschreckung hin zu proaktivem Eingreifen wird begleitet von einer Erweiterung der für nationale Sicherheit relevant gemachten Gegenstandsbereiche. Mit den Anschlägen wird auch deutlich, dass sich nationale Sicherheit nicht mehr allein mit außenpolitischen Mitteln erreichen lässt. In dem 2002 formulierten *Homeland Security Act* wird eine neue Strategie umfassender Vorsicht formuliert und mit dem *Department of Homeland Security* institutionalisiert. Das *Department* erhält die Aufgabe, alle möglichen intentionalen und nicht-intentionalen Bedrohungen nationaler Sicherheit im Inneren und Äußeren zu erkennen und darauf vorbereitet zu sein. Dazu werden in dieser neu geschaffenen Behörde unterschiedliche innenpolitische Handlungsfelder wie Katastrophenschutz, Transport und Versorgung gebündelt. Wie es George W. Bush in einer erklärenden Handreichung zu dem Gesetz formuliert:

> »The Department of Homeland Security would make Americans safer because our nation would have: One department whose primary mission is to protect the American homeland; One department to secure our borders, transportation sector, ports, and critical infrastructure […].« (Bush 2002, 2)

Das Politikfeld *Public Health* – und hier insbesondere der Tätigkeitsbereich Infektionskontrolle – bekommt mit dem *Homeland Security Act* zudem eine neue Relevanz und begriffliche Fassung. Biologische Bedrohungen werden in der neuen Strategie in einer Reihe mit nuklearen Waffen, chemischen und radioaktiven Stoffen als mögliche Mittel ter-

roristischer Angriffe adressiert. Das *Department* soll auch die Verteidigung gegen Angriffe mittels Infektionskrankheiten systematisch bündeln. »The Department would unify our defenses against human, animal, and plant diseases that could be used as terrorist weapons.« (Bush 2002, 12)

Kurz nach den Anschlägen vom 11. September, im Oktober 2001, werden eine Reihe von Briefen an Personen des öffentlichen Lebens in den USA versandt, die Sporen des Milzbrandbakteriums (B. anthracis) enthalten. Fünf Menschen sterben und 17 erkranken teils schwer (Hester 2020). Der ›Amerithrax‹ Vorfall liefert einen sichtbaren Beleg für das bioterroristische Szenario. In direkter Folge zum 11. September verankerte dieser Vorfall die Gefahr eines bioterroristischen Anschlags in der öffentlichen Wahrnehmung. Auch später liefert der Verweis auf Bioterrorismus immer wieder eine Begründung für die Notwendigkeit eines detaillierten Monitorings. Die permanente Überwachung der gesundheitlichen Lage der Bevölkerung sei insbesondere im Hinblick auf die Früherkennung von solchen Anschlägen geboten.

Als ›Biosicherheit‹ gefasst wird Infektionsschutz damit von nun an zu einem Schauplatz nationaler Sicherheit. Die konkrete Forderung ist vor allem die Einrichtung eines landesweiten *Biosurveillance*-Systems (Morse 2012). Die Forderung wird in folgenden Direktiven mehrfach wiederholt und präzisiert (*Biodefense for the 21st Century*, 2004; *National Strategy for Pandemic Influenza* 2005; *Homeland Security Presidential Directive 21*, 2007). Schließlich bleibt es nicht nur bei Forderungen. Für den Ausbau von *Biosurveillance* in den Bundesstaaten und an den *Centers for Disease Control* werden zwischen 2001 und 2007 allein 32 Milliarden US$ aus Bundesmitteln investiert (Office of Inspector General 2007, 2). Generell erfährt die Idee eines Monitorings unspezifischer – z.B. auch bioterroristischer Bedrohungen – nach dem 11. September landesweit Zuspruch, und die Bereitschaft für die Installation entsprechender Systeme wächst.

Für die Entwicklung und Institutionalisierung syndromischer Gesundheitsüberwachung bedeutet die neue Angst vor Bioterrorismus und die sicherheitspolitische Thematisierung des öffentlichen Gesundheitsgeschehens somit einen massiven Schub (Rolka und O'Connor

2010). Vor allem die Fördertöpfe zur nationalen *Preparedness* im Nachgang des 11. September sind ein wichtiger Anreiz bei der Einrichtung solcher Systeme auf Ebene der Bezirke und der Bundesstaaten (Purtle u.a. 2018, 2). Nach einer Schätzung des CDC ergänzen 2003 bereits etwa 100 Gesundheitsämter ihre Gesundheitsbeobachtung um eine Komponente zur Speicherung und Auswertung unspezifischer Daten (Buehler u.a. 2003). Die Verbreitung solcher Systeme gewinnt in dieser Zeit rasch an Fahrt und bis 2007 ist in 83 % der US-Bundesstaaten ein System syndromischer Überwachung im Einsatz. Teils entwickeln die Bundesstaaten eigene technische Lösungen, in der Mehrzahl kommt das so genannte ESSENCE-System zum Einsatz (*Electronic Surveillance System for the Early Notification of Community-based Epidemics*), das wie skizziert aus der Kooperation der *Johns Hopkins University*, des *Walter Reed Army Institute for Research* (WRAIR) und Gesundheitsämtern in der *National Capital Region* hervor gegangen ist (Chen, Zeng und Yan 2010a).

Neben der Bereitstellung von Finanzmitteln bekommen die ersten Systeme nach dem 11. September auch einen erheblichen Entwicklungsschub. Verfahren zum Gesundheitsmonitoring werden in den Jahren nach 2001 mit unter dem Dach des Verteidigungsministeriums entwickelt. Als Reaktion auf den 11. September erarbeitet die *Defense Advanced Research Projects Agency* (DARPA) des Verteidigungsministeriums ein im Nachgang umstrittenes, sehr weitreichendes Überwachungsprojekt. Das so genannte *Total Information Awareness* (TIA) Projekt sollte zum Zweck der Terrorismusbekämpfung ein möglichst umfassendes System zur Sammlung und Nachverfolgung personenbezogener Daten ermöglichen (Electronic Privacy Information Center 2004). Ein Teil dieses tatsächlich möglichst total geplanten Systems sollte auch eine Komponente sein, die vor allem in Richtung Infektionskrankheiten und waffenfähiger Biokampfstoffe orientiert ist. Diese *Bio-event Advanced Leading Indicator Recognition Technology* (Bio-ALIRT) nahm die mit ESSENCE in den Militärkrankenhäusern bereits unternommenen Bemühungen auf und half insbesondere, die automatischen Verfahren der Mustererkennung zu verbessern.

Auch wenn das TIA-Vorhaben nach drei Jahren eingestellt wurde, bildeten die Entwicklungen im Rahmen von Bio-ALIRT einen entschei-

denden Fortschritt für die technischen Lösungen (Rolka und O'Connor 2010, 6f). In der Entwicklungsabteilung des Verteidigungsministeriums wurden – als Nebeneffekt eines umfassenden Überwachungssytems – die existierenden Ansätze zum syndromischen Gesundheitsmonitoring zusammengeführt und entscheidend weiterentwickelt (DARPAO A 2003).

Allerdings gibt es gegen Einführung solcher Systeme auch einige Widerstände. Neben der Einrichtung eines Terminals bei den lokalen Gesundheitsämtern und dem Aufsetzen eines Servers mit der Datenbank ist vor allem die Beteiligung der Kliniken für das Funktionieren zentral. Die tägliche Zusammenstellung und Übermittlung der Daten bedeutet innerhalb der Klinik immerhin einen Zeitaufwand von etwa einer Stunde (Dugas 2012). In der Phase nach dem 11. September war diese Bereitschaft zur Meldung von Daten auf privatwirtschaftlicher Seite häufig gegeben, lässt aber immer mehr nach (Russell 2012). Viele Krankenhäuser verweigern die Teilnahme an dem System, häufig mit dem Argument einer unklaren Rechtslage und dem Schutz der Privatsphäre der Patient:innen. In einer Umfrage 2007 benennen 54 % der Krankenhäuser dieses Problem als Hinderungsgrund (Purtle u.a. 2018).

Erneut liefert eine äußere Rahmenbedingung hier einen entscheidenden Schub für die weitere Etablierung solcher Systeme. 2007 beschließt der US-Senat ein Gesetz zur Förderung der elektronischen Patientenakte (*Electronic Health Records*). Das so genannte *Health Information Technology for Economic and Clinical Health* (HITECH) Programm verspricht den Krankenhäusern eine substanzielle Fördersumme, sofern sie ihre Verwaltung auf digital gespeicherte Daten umstellen. 2010 konnte eine einzelne für das Programm qualifizierte Klinik mit Fördermitteln zwischen zwei Millionen bis zu 6,4 Millionen US$ pro Jahr rechnen (Purtle u.a. 2018). Bedingung für die Gelder war neben der bloßen Einführung auch der Nachweis einer substanziellen Verwendung (*meaningful use*) der elektronischen Patientenakten. Das Einspeisen der Daten in ein System syndromischer Gesundheitsüberwachung war eine der drei Möglichkeiten, diese substanzielle Verwendung nachzuweisen. Der HITECH-Act bildete dadurch häufig den noch fehlenden Anstoß für ein Krankenhaus, sich zur täglichen

Meldung der Daten an solche Monitoring-Systeme zu verpflichten. Im Jahr 2019 gehen Daten von 4000 Krankenhäusern (NSSP 2019), das sind 68 % aller Notaufnahmen in den USA (Purtle u.a. 2018), in solch ein Monitoring ein.

Parallel zu der Entwicklung auf Ebene einzelner Bundesstaaten begann mit dem Paradigmenwechsel durch den 11. September auch auf der Ebene der *Centers for Disease Control* (CDC) in Atlanta – der nationalen Gesundheitsbehörde – das Bemühen um ein besseres und vor allem zeitlich unverzügliches Monitoring des Gesundheitsgeschehens. Eine konkrete Forderung aus dem *Public Health Security and Bioterrorism Preparedness and Response Act,* mit dem der US-Senat 2002 auf die Vorfälle am 11. September 2001 antwortet, ist – wie bereits skizziert – die Einrichtung von verbesserter Methoden der Biosurveillance. An den CDC mündete dieser Auftrag in der Entwicklung einer neuen Komponente im System des gesundheitlichen Monitorings. Gesucht wird nun explizit ein System gesundheitlicher Früherkennung und Lagebeobachtung und für das Erkennen möglicher bioterroristischer Anschläge (Gould, Walker und Yoon 2017). Ein entsprechendes System wurde an den CDC dann 2003 unter dem Namen *BioSense* eingeführt. Das System entsprach weitgehend dem in der *National Capital Region* und für die US-Militärkliniken entwickelten ESSENCE-System. Grundlage sollte auch hier Angaben über Beschwerden sein, die bei den Kliniken im Erstkontakt mit den Patient:innen registriert und dann zeitnah gemeldet werden. Die drei zentralen technischen Komponenten sind auch hier eine Struktur zur Datenübertragung und Speicherung, Skripte zum automatisierten Prozessieren der Daten und eine Benutzeroberfläche zur Interaktion mit dem System.

Allerdings verlief die Etablierung des landesweiten *BioSense*-Systems anfangs schleppend. Nach dem Start mit etwa 300 Gesundheitsämtern begannen die CDC ab 2005, direkte Kooperationsvereinbarungen mit den Krankenhäusern abzuschließen. Ziel war es, innerhalb von drei Jahren landesweit alle Krankenhäuser als Datenlieferanten für das *BioSense* System verpflichten zu können. Bis 2007 konnten jedoch nur 10 % verpflichtet werden. 2008 lieferten 333 Militärkrankenhäuser, 770 Versorgungseinrichtungen für Veteranen und 532 privatwirtschaft-

liche Krankenhäuser Daten an das nationale *BioSense*-System (Gould, Walker und Yoon 2017).

Vor allem provozierte die CDC mit diesem Bemühen um direkte Kooperationen mit den Kliniken vielfach Widerstand und Skepsis bei den Gesundheitsbehörden der Einzelstaaten, die sich durch diese direkten Vereinbarungen umgangen sahen (Purtle u.a. 2018, 2). Verstärkt wurde diese skeptische Haltung durch eine Welle kritischer Einschätzungen zur Sinnhaftigkeit dieser neuen Methode des Gesundheitsmonitorings an sich. Einzelne Epidemiolog:innen zogen die Qualität, Validität und den Nutzen dieser neuen syndromischen Überwachung in Frage (Barlas 2007). Aus dem US-Kongress wurde die Zahl der falschen Alarmmeldungen betont und unter Verweis auf Kosten-Nutzen-Kalkulationen in Frage gestellt (US Department of Homeland Security 2005).

Als Konsequenz aus dieser Kritik und der schleppenden Etablierung entschlossen sich die CDC 2008 zu einer Neukonzeption des Systems. Im Jahr 2012 wurde das neu aufgesetzte System *BioSense 2.0* online gestellt. Im Unterschied zur ersten Version laufen die Daten hier von den Kliniken zunächst an die lokalen Behörden und werden dann erst weiter nach Atlanta zu den CDC geschickt. Die lokalen Stellen sind nun aktiver einbezogen (Gould, Walker und Yoon 2017).

Zudem werden nun für die lokalen Gesundheitsämter auch monetäre Anreize geschaffen, sich an dem *BioSense 2.0* System zu beteiligen. Die CDC erhalten mit der Neuauflage des Programms nun auch die Möglichkeit, Partner mit einer Auszeichnung für gelungene Kooperation zu honorieren. In der ersten Runde 2012 wurden 34 dieser Auszeichnungen vergeben (Gould, Walker und Yoon 2017). Die Auszeichnung ist jeweils mit 250.000 US$ dotiert und in der Situation knapper Budgets vor allem im Sozial- und Gesundheitsbereich sind solche Preise eine der raren Möglichkeiten für die lokalen Gesundheitsbehörden, finanzielle Spielräume zu erweitern. (Purtle u.a. 2018)

Auf der technischen Ebene zielte die Neuauflage von *BioSense* vor allem darauf, das System für die Endnutzer zugänglicher zu machen und die Präzision und Geschwindigkeit zu erhöhen. Im Zuge dessen wurde die ursprüngliche webbasierte Oberfläche ersetzt und an Stelle dessen eine neue Plattform eingerichtet, auf der die Software SAS

und R-Studio für die Datenanalyse laufen. Für die Abfrage der Gesundheitsdaten und die Kategorisierung von Syndromen kommt nun auch auf der landesweiten Ebene das ESSENCE-System zum Einsatz (Gould, Walker und Yoon 2017).

Schließlich weitet sich mit der Neukonzeption des Instruments *BioSense* 2.0 auch die Zielsetzung. Den CDC geht es nun nicht mehr ausschließlich um die Einrichtung eines Datenerhebungs- und Auswertungsinstruments. Erhebliche Aufmerksamkeit bekommt nun der Aspekt von Schulung und Interaktion mit den beteiligten Akteuren. Ab 2004 finden jährliche Tagungen auf regionaler Ebene statt, um die Erwartungen an syndromisches Gesundheitsmonitoring allgemein und an das System *BioSense* 2.0 im Besonderen mit Vertreter*innen lokaler und bundesstaatlicher Gesundheitsbehörden abzustimmen. Die Ergebnisse dieser Tagungen werden regelmäßig veröffentlicht (zunächst als *Public Health Information Network Preparedness Early Event Detection Guidelines*, später als *NSSP Update*). Weitere Maßnahmen wie Webinars, monatliche Konferenzschaltungen oder *BioSense* 2.0-Nutzertreffen während großer landesweiter *Public Health* Tagungen zielen auf den aktiven Einbezug der Nutzer:innen. Es geht nun auch um die Etablierung einer *Syndromic Surveillance Community*.

»BioSense has evolved from focusing on systems and technology to a community of practice with shared tools, methods, and expertise« (Gould, Walker und Yoon 2017). Um diese Verschiebung deutlich zu machen, erfolgen die Anstrengungen der CDC für eine nationale syndromische Gesundheitsüberwachung seit 2014 unter dem neuen Namen *National Syndromic Surveillance Program*. Die technische Plattform *BioSense* 2.0 selbst rückt mit dieser Bezeichnung in den Hintergrund. Stattdessen wird mit dem neuen Namen vor allem der Aspekt eines landesweiten Zusammenschlusses betont.

Dem Konzept einer ›Community of Practice‹ entsprechend gibt es keine formalen Hürden für die Mitgliedschaft in der NSSP. Jede Person oder Organisation, die sich für die Stärkung syndromischer Gesundheitsüberwachung einsetzen möchte, kann Mitglied werden. Im November 2018 waren das 541 Personen, davon 183 (34 %) Vertreter:innen einer bundesstaatlichen Gesundheitsbehörde, 100 (18 %) Vertreter:in-

nen einer kommunalen Gesundheitsbehörde und 82 (15 %) Einzelpersonen mit Interesse oder Verantwortung für syndromische Überwachung (Gould u.a. 2019).

Das an den CDC angesiedelte landesweite System syndromischer Gesundheitsüberwachung ist durch die Neuauflage als *BioSense* 2.0 in Verbindung mit der Etablierung einer *Community of Practice* nach einem langen Prozess mit einer Reihe von Widerständen nun relativ etabliert. Derzeit melden 4000 Kliniken Daten an die *BioSense*-Plattform, damit werden etwas mehr als die Hälfte der Notaufnahme-Patient:innen in den USA durch das System erfasst (NSSP 2019). Daneben sind nach wie vor eine Vielzahl von Systemen syndromischer Überwachung im Betrieb, auf lokaler, sowie auf bundestaatlicher Ebene (Chen, Zeng und Yan 2010a).

Über einen Zeitraum von knapp zwei Jahrzehnten konnte sich in den USA ein neuartiges Verfahren des Gesundheitsmonitoring etablieren und in der Mehrzahl der Gesundheitsbehörden in den Bezirken, auf Ebene der Bundesstaaten und US-weit an den CDC zu einem Bestandteil der epidemiologischen Praxis werden.

> »During the past 15 years, syndromic surveillance has evolved from a set of ad hoc methods used mostly in postdisaster settings to a mature technology that runs continuously to detect and monitor a range of health issues.« (Hopkins u.a. 2017)

In der chronologischen Skizze konnten einzelne Einschnitte deutlich werden. Vor allem die Anschläge vom 11. September haben diese Etablierung in mehrerer Hinsicht entscheidend gefördert – finanziell, durch ein günstiges Agenda-Setting und durch Beteiligung militärischer Expertise. Durch die Anschläge vom 11. September, und kurz darauf durch den Vorfall von per Post versendeter Briefe mit Sporen von Milzbrandbakterien (*B. anthracis*) in den USA, wurde das Gefahrenszenario bioterroristischer Anschläge greifbarer und handlungsleitend. Auch dadurch wurde die Suche nach neuen – möglichst unverzüglichen – Formen der Infektionskontrolle intensiviert (Henning und Hamburg 2003; Morse 2012).

Parallel zu den Einzellösungen der Bundesstaaten wuchs auch national der wahrgenommene Handlungsdruck und 2003 begann an den *Centers for Disease Control* (CDC) in Atlanta mit dem System *BioSense* der Versuch, eine landesweit übergreifende Lösung zu etablieren (Bradley u.a. 2005). Über einen Zeitraum von gut zehn Jahren und mehrere Iterationen ist dieses Ziel schließlich 2015 erreicht. *BioSense* bildet nun das zentrale technische System in der seitdem als *National Syndromic Surveillance Program* explizit formulierten Strategie eines syndromischen Gesundheitsmonitoring (Gould, Walker und Yoon 2017).

Die chronologische Entwicklung zeigt auch eine zunehmende Systematisierung von syndromischer Gesundheitsüberwachung in den USA, d.h. deren allmähliche Annahme eines systematischen Charakters. Techniksoziologisch gesprochen formiert sich syndromisches Gesundheitsmonitoring immer mehr zu einer sozio-technischen Konstellation, einer losen Kopplung von trainierten Routinen der Epidemiolog:innen bei der Eingabe von Abfragen, mechanisierte Abläufe der an die *BioSense* Plattform angebundenen Geräte und eine algorithmisierte Musterkennung der eintreffenden Daten (Rammert und Schubert 2006).

Die anfänglich noch isoliert in einzelnen Gesundheitsämtern getesteten Prototypen konnten allmählich auf einen gemeinsamen Datenstandard verpflichtet und integriert werden. Die zunächst konkurrierenden Entwicklungen auf der Ebene einzelner Bundesstaaten und an den *Centers for Disease Control* konnten schließlich zumindest zu großen Teilen in eine funktionsfähige Struktur des kontrollierten Datenaustausch gebracht werden. Die *BioSense* 2.0-Plattform ist neben einer Reihe von weiterhin existierenden Lösungen auf der Ebene der Bundesstaaten zu einem breit genutzten System geworden (Gould, Walker und Yoon 2017).

Parallel ist durch die aktive Förderung des Praxis- und Wissenstransfers etwa auf Konferenzen und durch die Bereitstellung von Handreichungen und *best-practice*-Beispielen eine Gemeinschaft der Anwender:innen entstanden. Nicht zuletzt unter Einfluss einer Reihe von Förderprogrammen hat sich eine *community of practice* etabliert. Die von den CDC propagierte Bezeichnung *National Syndromic Surveillance Program*

(NSSP) verweist auf diesen inzwischen mehrfach integrierten Charakter syndromischer Gesundheitsüberwachung.

Im Folgenden helfen mir die zuvor entwickelten Überlegungen für eine machtsensible Auseinandersetzung mit diesem Fallbeispiel. Indem eine sozio-technische Konstellation, wie die hier skizzierte Herausbildung eines syndromischen Gesundheitsmonitoring, als eine Infrastrukturierung aufgefasst wird, treten die verbundenen Voreinstellungen und die bestimmte Gerichtetheit schärfer hervor.

Syndromic Surveillance als Infrastrukturierung

Wie oben ausgeführt (siehe Kapitel »Infrastrukturierung«), hilft mir Infrastruktur als Perspektive dabei, die relationale Beschaffenheit eines Phänomens ernst- und wahrnehmen zu können und zugleich die Machtwirkungen, d.h. dessen Anteil im Ermöglichen bzw. Verunmöglichen bestimmter Situationen herauszustellen. Infrastrukturierung richtet den Fokus auf die Kopplung von unterschiedlichen Bestandteilen in sozio-technischen Konstellationen. Die Frage, ob eine Infrastruktur vorliegt, ist eine kurze Fassung der Frage, inwiefern die Routinen der Nutzer:innen, die zu benutzenden Geräte und relevante Wissensbestände systematisch aufeinander abgestimmt sind und inwiefern diese Interaktion auf Dauer gestellt wird. Das Phänomen wird so explizit auf die Beziehungen hin befragt, aus denen es überhaupt erst erwächst. Die Vermittlung, das in-Bezug-setzende, die Verbindung von Elementen sozio-technischer Konstellationen rückt damit in den Vordergrund (siehe Kapitel »Politik der Ontologien«).

Übertragen auf die folgende Analyse ist der Ansatzpunkt damit nicht das Phänomen *Syndromic Surveillance* an sich. Die Heuristik der Infrastrukturierung zielt explizit darauf ab, die ›*black box*‹ des etablierten Phänomens zu öffnen und die Kopplungen, Verbindungen und Anordnungen von Elementen in den Vordergrund zu stellen, aus denen sich das Phänomen konstituiert. Ein dezidiert sozio-technisches Phänomen wie *Syndromic Surveillance* lässt sich besonders einfach aus dieser Perspektive betrachten. Nicht als ein ›fertiges Objekt‹, sondern

als ein Effekt von Beziehungen, die allmählich den Gegenstand in bestimmter Weise hervorgebracht haben. Infrastrukturierung verweist auf den Prozess der allmählichen Formation des Phänomens aus verknüpften Elementen, von deren versuchsweisen Anordnung in den ersten Prototypen, über das gegenseitige Vertrauen auf routinisierte und formalisierte Praktiken, bis hin zu einem in vielerlei Hinsicht etablierten und adressierbaren *National Syndromic Surveillance Program*.

Mit der Betrachtung als Infrastrukturierung wird neben dem Relationalen vor allem auch das Machtvolle betont, das von der Kopplung und Verstetigung von Elementen ausgeht. Im Unterschied zu einer offenen Frage etwa nach *Assemblages* fällt mit der Auffassung des Phänomens als eine Infrastrukturierung besonderes Augenmerk auf den Zweck, mit dem hier Elemente in einen dauerhaften Bezug gebracht werden.

Überwiegend umfasst *Syndromic Surveillance* die Einrichtung eines technischen Systems zur Datenerhebung, Speicherung und Auswertung. Bei der Frage nach Machtwirkungen dieser Infrastrukturierung ist die Rolle von Technik sinnigerweise besonders zu betonen. Häufig legt eine solche Fokussierung auf die Macht der Technik allerdings entweder eine deterministische oder eine instrumentelle Lesart nahe.

Auf der einen Seite steht die Gefahr, Machtwirkungen mit den Möglichkeiten eines technischen Werkzeugs gleichzusetzen. Letztlich kommt es dadurch aber zu einer Überbewertung der sozialen Gestaltungs- und Prägekraft des Technischen. Entgegen einer zu einfachen Idee von gesellschaftsprägender Kraft bestimmter Techniken, sind auch die bedingenden Kontexte, legitimierenden Vorstellungen und Entscheidungen miteinzubeziehen. »The sociological tendency to see society as shaped by technology needs to be countered by critical scrutiny of the profoundly political character of technological innovation and deployment« (Zedner 2009, 259). Auf der anderen Seite steht eine instrumentelle Lesart, die Machtwirkungen ausschließlich jenseits des Technischen verortet. Akteure haben demnach bestimmte Interessen, Ziele. Techniken sind dann nur passive Werkzeuge zur Erfüllung dieser Zwecke.

Mit der Heuristik Infrastrukturierung ist auch das Versprechen verbunden, einen dritten Weg aus diesem Dilemma zu finden. Das Gerund ›Strukturierung‹ betont die prozesshafte Vorstellung und unterstreicht die Bedeutung der Nutzungsweisen. Der offene Begriff der Kopplungen ist nicht per se auf technische Bestandteile und deren Funktionsweisen festgelegt. Alle möglichen auf Dauer gestellte und relevant gemachte Anordnungen sind in die Analyse eines Phänomens als Infrastrukturierung einzubeziehen.

Die doppelte Bedeutung von Relevanz ist in diesem Zusammenhang eine hilfreiche Richtschnur für einen anderen Blick auf Machtwirkungen technischer Systeme. Zum einen verweist Relevanz darauf, dass mit der Infrastrukturierung bestimmte Möglichkeiten nahegelegt werden. Das Kontingent denkbarer möglicher und letztlich gewählter Nutzungen ist nach einer erfolgten Infrastrukturierung verändert – bestimmte Nutzungen sind relevanter gemacht, anderes erscheint abwegiger.

Zum anderen liegen die Machtwirkungen einer Infrastrukturierung in der Etablierung eines solchen Möglichkeitsfeldes an sich. Die Elemente einer Infrastruktur entstehen aus den Verbindungen, d.h. das Relevant-Machen meint nicht nur die Re-Strukturierung im Kontingent der bestehenden Möglichkeiten, sondern die Etablierung dieser Gegenstände selbst. Im Folgenden schlüssele ich diese beiden Momente des Relevant-Machens mit den Begriffen Voreinstellung und Gerichtetheit auf.

Der erste Aspekt des Relevant-Machens als Ausdruck der Machtwirkungen einer Infrastrukturierung lässt sich mit einem Gedanken von N. Katherine Hayles verdeutlichen. In ihrer Auseinandersetzung mit der Technogenese, also der wechselseitigen Beeinflussung von technischen Werkzeugen und sozialen Formen, unterstreicht Hayles in ganz ähnlicher Weise das Relevant-Machen als Auswahl aus der Kontingenz des sozio-technischer Zusammenwirkens. Werkzeuge und technische Ensembles werden entscheidend durch Aufmerksamkeit mit konstituiert, so ihre These (Hayles 2011, 201f). Zur Begründung führt Hayles die Unterscheidung von Materialität und Physikalität technischer Ensembles ein. Physische Attribute von Werkzeugen sind notwendig für ihre Rolle in sozio-technischen Arrangements. Allerdings erklärt sich

diese Rolle nicht aus dieser Physikalität. Erst durch Aufmerksamkeit bekommen bestimmte physische Attribute Relevanz für das Verhältnis von Technik und sozialen Formen. Hayles spricht von einer bestimmten Materialität solcher Techniken, die durch Aufmerksamkeit aus der potentiell unbestimmbaren Menge physikalischer Eigenschaften heraus mit Bedeutung versehen werden. »Materialität, so möchte ich behaupten, entsteht, wenn Aufmerksamkeit sich mit Physikalität verbindet, um ganz bestimmte relevante Attribute zu identifizieren und zu isolieren.« (Hayles 2011, 201f)

Dieser Gedanke soll klären helfen, was ich im Folgenden als Voreinstellung einer Infrastrukturierung untersuchen will. Es geht dabei um bestimmte Einspurungen und nahe gelegte Nutzungen, die mit der dauerhaften Anordnung von Elementen verbunden sind. Die Infrastrukturierung syndromischen Monitorings ist nicht nur ein epistemisch-diskursives Ereignis sondern auch als ein technisches Ensemble wirkungsvoll. Aber – dem Gedanken Hayles folgend – nicht durch die bloße Physikalität der Elemente wie Formulare, Datenspeicher, Web-Interfaces und Prozessoren –, sondern in einer bestimmten Materialität, die durch Aufmerksamkeit relevant gemacht worden ist. Die Implikationen syndromischen Monitorings kommen zum einen also in einer bestimmten materiell unterlegten Strukturierung des Feldes möglichen Handelns zum Ausdruck. Aspekte dieser Machtwirkung einer Infrastrukturierung beschreibe ich im Folgenden unter der Klammer Voreinstellung.

Für die Analyse der Machtwirkungen ist zum anderen ein zweiter Aspekt des Relevant-Machens entscheidend. Infrastrukturierung soll nicht nur als eine Anordnung bestehender Elemente verstanden werden. Mit der Anordnung und dem in-Beziehung-Setzen werden neue Tatsachen geschaffen. Aus der sozio-technischen Verschränkung gehen nicht allein veränderte Auffassungen über Bestehendes hervor. Entsprechend der Annahme relationaler Ontologien liegt das Augenmerk gerade auf der Hervorbringung der Sachverhalte an und für sich.

Diesen zweiten Aspekt des Relevant-machens als Hervorbringung ist in der Technikphilosophie von Martin Heidegger grundgelegt. Ausgehend von dem üblichen instrumentellen Verständnis von Technik als

eine Mittel-Zweck-Beziehung entfaltet Heidegger in dem Aufsatz »Die Technik und die Kehre« eine grundsätzlichere Bedeutungsebene des Technischen. Werkstoffe und Werkzeuge werden aus einer bestimmten Veranlassung heraus in Beziehung gebracht. Dabei kommt es vor allem auch zu einem »Her-vor-bringen« (Heidegger 1962, 6). Wohlgemerkt spricht Heidegger nicht von einer Herstellung, sondern von einer Überführung von etwas zuvor Verborgenen in eine Unverborgenheit. »Das Entscheidende der *techne* liegt somit keineswegs im Machen und Hantieren, nicht im Verwenden von Mitteln, sondern in dem […] Entbergen.« (Heidegger 1962, 6) In diesem Begriff des ›Entbergens‹ bleibt das Spannungsfeld zwischen einer Determination durch Technik und einer völligen Verfügung über die Technik als Mittel erhalten. Die Vorstellung des ›aus dem Verborgenen holen‹ verweist auf Beschränkungen und Kontingenzen. Es ist eben kein beliebiges Herstellen möglich. Zugleich wird das grundlegend konstitutive Moment von Technik in der Hervorbringung des Realen unterstrichen.

Diese philosophische Bestimmung soll die zweite Annahme zu den Machtwirkungen einer Infrastrukturierung verdeutlichen. Erst über die Verschränkung von Elementen im Zuge einer Infrastrukturierung wird eine ansonsten nicht vorhandene (verborgene) Realität in bestimmter Weise hervorgebracht. In der folgenden Auseinandersetzung mit syndromischen Monitoring fasse ich diesen Aspekt von Machtwirkungen als Gerichtetheit.

Diese Unterscheidung von Voreinstellungen und Gerichtetheit hilft mir bei der Strukturierung der Analyse. Wie in den folgenden Kapiteln jeweils ausgeführt wird, sind unter dem Label *National Syndromic Surveillance Program* inzwischen eine Reihe von Elementen gekoppelt, um auffällige Änderungen des Gesundheitsgeschehens zu Erfassen (siehe Kapitel »Erfassen«), das Gesundheitsgeschehen zweitens besser zu Verstehen (siehe Kapitel »Verstehen«) und drittens um zukünftige Entwicklungen Voraussehen (siehe Kapitel »Voraussehen«) zu können.

Indem sich *Syndromic Surveillance* entsprechend diesen Vorstellungen immer mehr etabliert und aus weitreichenderen Beziehungen konstituiert wird, ändert sich teilweise die Wirkung. Die Zwecke, auf die eine Infrastruktur ausgerichtet sind, geben nur eine grobe Ahnung von

den Machtwirkungen der etablierten Infrastruktur. Die neu ausgerichtete, systematisierte und auf Dauer gestellte sozio-technische Konstellation entfaltet auch eine bestimmte Gerichtetheit, die nicht deckungsgleich mit den eingangs identifizierten Zwecken sein muss. In der folgenden Analyse interessiert mich besonders dieser machtvolle Überschuss des Infrastrukturellen. Der Gewinn der Analyse liegt besonders im Aufzeigen dieser Implikationen der Einrichtung von syndromischer Gesundheitsüberwachung. Jeweils machtvolle Voreinstellungen und eine Gerichtetheit, die unabhängig von den Intentionen, welche die Akteure mit diesem Werkzeug verfolgen, eine bestimmte Auffassung von Gesundheit und den Grenzen und Möglichkeiten von Gesundheitspolitik nahelegt.

Im Folgenden wende ich somit diese Perspektive einer Infrastrukturierung auf das *National Syndromic Surveillance Program* an. Material sind zum einen die vielfältigen Texte, die in Bezug auf diese Systeme entstanden sind. Wie bereits skizziert, sind Idee und Praxis syndromischer Gesundheitsüberwachung in den USA über einen langen Zeitraum gereift. Idee, Nutzen und Praxis mussten teils gegen Widerstände begründet und durchgesetzt werden. Entsprechend ist der Prozess begleitet von einer umfangreichen wissenschaftlichen Beobachtung die in Aufsätzen, grauer Literatur und Konferenzbeiträgen dokumentiert ist.

Neben diesem Textmaterial konnte ich durch Feldforschung in der *National Capital Region* im Sommer 2012 Einblicke in die Praxis der epidemiologischen Arbeit mit dem ESSENCE-System bekommen und Gespräche mit Nutzer:innen in den bezirklichen und bundesstaatlichen Gesundheitsbehörden führen. Als Teil der offenen *community of practice* hatte ich zudem Zugriff auf Schulungsmaterial, Webinars und Präsentationen. Die Gesprächspartner haben mir schließlich Folien und Skripte eigener Präsentationen zur Verfügung gestellt, die ebenfalls in den Materialkorpus eingegangen sind.

Aus dieser Auseinandersetzung mit den wissenschaftlichen Debatten, den politischen Begründungen, den kritischen Kommentaren und den praktischen Erfahrungen der beteiligten Akteure ergibt sich eine Perspektive auf den Fall, die ich im Folgenden darstellen möchte.

Ausgangs- und Anknüpfungspunkt sind dabei gemäß der Heuristik Infrastrukturierung bestimmte Kopplungen, die ich für jeweils symptomatisch halte. Das Spezifische des syndromischen Gesundheitsmonitoring zeigt sich auch in den Verbindungen, die zwischen zuvor nicht in Beziehung stehenden Elementen hergestellt werden. Ausgehend von solchen Kopplungen geht es dann jeweils um die Plausibilisierung dieser Kopplung (Vorstellungen), um die avisierten Ziele (Voreinstellung) und schließlich um die Implikationen und Wirkungen (Gerichtetheit).