5. Für einen queeren Sicherheitsbegriff

Die vorliegende Untersuchung hat in den vorangegangenen Kapiteln anhand wissensgeschichtlicher sowie diskursanalytischer Betrachtungen von Kryptologie und IT-Sicherheit den beiden Bereichen zugrunde liegenden negativen Sicherheitsbegriff herausgearbeitet, der im Verlauf ihrer jeweiligen Geschichte trotz technischer Neuerungen konstant geblieben ist. Anschließend an die im vorigen Kapitel durchgeführten Umdeutungen des homophoben Motivs von IT-Sicherheit anhand der *Back Orifice*-Backdoor wird allerdings eine mögliche Öffnung dieses Diskurses hin zu einem anderen Sicherheitsbegriff erkennbar. Dieses Kapitel versucht sich daher an der Möglichkeit, einen anderen Sicherheitsbegriff für die IT-Sicherheit in Stellung zu bringen. Mit Daniel Loick (2021) schlägt dieses Kapitel einen queeren Sicherheitsbegriff vor, und fragt danach, ob und wie sich dieser für die IT-Sicherheit produktiv denken lässt. Diese Frage wird im Zusammenhang mit dem *QueerOS/Queer Computation*-Diskurs bearbeitet, der sich in den letzten Jahren durch einige Publikationen, die *Computation*, also wie Computer funktionieren und wie sie genutzt werden, und Queerness zusammendenken, gebildet hat. Vor dem Einstieg in diese Diskussion werden zunächst noch mit Eve Kosofsky Sedgwicks (2003) Konzepten des *paranoid* und des *reparative reading* zwei Modi der Wissensproduktion eingeführt, die für eine solche Diskussion notwendig sind, und die Diskurse von IT-Sicherheit und Kryptologie auf ihre Zugehörigkeit zu diesen befragt.[1]

1 Teile dieses Kapitels, insbesondere die Diskussion von *paranoid* und *reparative reading* in Hinblick auf mögliche Formen von Sicherheit wurden bereits veröffentlicht (vgl. Shnayien 2022).

5.1 Paranoide und Reparative Praktiken

Die Queertheoretikerin Eve Kosofsky Sedgwick unterscheidet in ihrem Essay *Paranoid Reading and Reparative Reading, or, You're So Paranoid, You Probably Think This Essay Is About You* zwei Arten der Herstellung von Wissen: eine, die strukturelle Ähnlichkeiten zur Paranoia aufweist, und daher von ihr als *paranoid reading* bezeichnet wird, und die ihr gegenüber positionierte Form, die Sedgwick als *reparative reading* bezeichnet. Sedgwick betont die affektive Dimension der Theoriebildung und der Herstellung von Wissen über die Welt, indem sie danach fragt, was es bedeutet, und welche Konsequenzen damit einhergehen (oder auch nicht), Wissen(sproduktion) in einer spezifischen Art zu organisieren. Ihre Überlegungen leitet Sedgwick mit der kurzen Schilderung eines Gesprächs zwischen ihr selbst und der befreundeten ACT UP-Aktivistin Cindy Patton während des ersten Jahrzehnts der AIDS-Krise ein. Sedgwick schildert, wie sie Patton nach ihrer Meinung zu den »sinister rumors about the virus's origin« (ebd., 123) fragt: Wurde das HI-Virus in einem Forschungslabor hergestellt, mit dem Zweck, es als Biowaffe einzusetzen? Patton gibt eine Antwort, die Sedgwick zunächst frustriert zurücklässt:

> »›Any of the early steps in its spread could have been either accidental or deliberate,‹ she said. ›But I just have trouble getting interested in that. I mean, even suppose we were sure of every element of a conspiracy: that the lives of Africans and African Americans are worthless in the eyes of the United States; that gay men and drug users are held cheap where they aren't actively hated; that the military deliberately researches ways to kill noncombatants whom it sees as enemies; that people in power look calmly on the likelihood of catastrophic environmental and population changes. Supposing we were ever so sure of all those things —what would we know then that we don't already know?‹« (Ebd.)

Pattons Antwort ist in der Tat zunächst kontraintuitiv: Würde man nicht annehmen, dass politisches Handeln erfordert, alle Zusammenhänge und Motive, insbesondere die der Akteur_innen, gegen die man sich auflehnt, zu kennen? Würden diese nicht die Sichtweise auf die Situation, in der man sich befindet, das eigene Handeln und die eigene Strategie des Protests informieren? Sedgwick beschreibt, wie sie nach Jahren des Nachdenkens über die erhaltene Antwort feststellt, dass sie diese eben *aufgrund* der in ihr zunächst enthaltenen Trennung von historischen Zusammenhängen und den scheinbar unmittelbar aus ihnen zu folgen habenden Reaktionen als »enabling« (ebd.,

124) empfindet – als einen neuen Möglichkeitshorizont eröffnend: »Patton's comment suggests that for someone to have an unmystified, angry view of large and genuinely systemic oppressions does not intrinsically or necessarily enjoin that person to any specific train of epistemological or narrative consequences.« (Ebd.) Mit dieser Unterbrechung der ansonsten als Kontinuität wahrgenommenen Kette Wissen – Fühlen – Handeln wird die Frage danach, ob ein Verdacht wahr ist oder nicht, nicht mehr zur alles bestimmenden Frage; kann man sich von der Notwendigkeit, einen Verdacht verifizieren oder falsifizieren zu müssen, lösen, und kann, wie Sedgwick (ebd., Herv. i.O.) schreibt, stattdessen einen Ebenenwechsel hin zu den übergeordneten Fragen vollziehen: »What does knowledge *do* – the pursuit of it, the having and exposing of it, the receiving again of knowledge of what one already knows? *How*, in short, is knowledge performative, and how best does one move among its causes and effects?« Während Sedgwick die Kenntnis um die Performativität von Wissen sogleich als banal relativiert, verweist sie auf eine Verschiebung, die sich für ihr Nachdenken als spannender erwiesen habe: Die von Paul Ricoeur beschriebene *Hermeneutik des Verdachts*, und damit die ›Entzauberungsgesten‹ Marx', Nietzsches und Freuds, nach der sich stets *hinter* einem gegebenen Ding die *eigentliche Wahrheit* desselben befinde, die aufgedeckt werden müsse, hat sich in die *Critical Theory* verschoben, bis dieser Modus der Kritik synonym mit dem Üben von Kritik selbst wurde. Sedgwick (ebd., 125) folgert: »Not surprisingly, the methodological centrality of such suspicion to current critical practice has involved a concomitant privileging of the concept of paranoia.« In einer Welt voller offensichtlich zu Tage liegender systemischer Unterdrückung, so schreibt Sedgwick (ebd., 126) weiter, »to theorize out of anything *but* a paranoid critical stance has come to seem naive, pious, or complaisant.« Dabei ist es Sedgwick (ebd., 128–129) wichtig, festzuhalten, dass das Praktizieren von reparativen Formen der Wissensproduktion nicht bedeutet, die Realität zu verleugnen oder Unterdrückung nicht anerkennen zu wollen, sowie dass sich paranoide und reparative Praktiken der Wissensproduktion durchaus abwechseln oder ergänzen können. Sich gegen einen klinisch-pathologisierenden Gebrauch des Wortes Paranoia wendend, kommt es Sedgwick eher darauf an, Paranoia auf seine strukturelle Funktionsweise zu befragen, und diese nicht sofort als zu Verwerfendes oder zu Therapierendes zu markieren:

> »I myself have no wish to return to the use of ›paranoid‹ as a pathologizing diagnosis, but it seems to me a great loss when paranoid inquiry comes to seem entirely coextensive with critical theoretical inquiry rather than being

> viewed as one kind of cognitive/affective theoretical practice among other, alternative kinds.« (Ebd., 126)

Diese Sichtweise erlaubt Sedgwick eine Analyse der Verschiebung von Paranoia als Wissensobjekt anti-homophober Theoriebildung, wie etwa bei Hocquenghem, hin zu Paranoia als Methode. Diese Verschiebung sieht sie in der Funktionsweise von Paranoia begründet: Paranoia sei ansteckend, würde symmetrische Epistemologien hervorbringen (vgl. ebd.), Verdacht gegen (Hinter-)List ins Feld führen und umgekehrt, frei nach dem Motto: »it takes one to know one« (ebd., 127). Das Wissen darum, in einer Welt zu leben, in der systemische Unterdrückung an der Tagesordnung ist, führe dennoch, wie Sedgwick betont, nicht automatisch dazu, Ereignisse paranoid strukturiert narrativieren zu müssen, und ziehe auch nicht zwangsläufig eine bestimmte Haltung oder bestimmte Handlungsoptionen nach sich (vgl. ebd.), kurzum: das Wissen um systemische Unterdrückung habe keine deterministischen Auswirkungen auf zukünftiges Handeln. Paranoia als Methode zu hinterfragen, erlaubt es Sedgwick, Paranoia als Standardmethode der *Critical Theory* vom Thron zu stoßen und als eine mögliche Herangehensweise unter vielen zu markieren: »[P]aranoid practices«, schreibt sie, »represent *a* way, among other ways, of seeking, finding, and organizing knowledge. Paranoia knows some things well and others poorly.« (Ebd., 130, Herv. i.O.) Angesichts der AIDS-Krise, zu deren Zeit sich auch das den Text eröffnende Gespräch mit der befreundeten Aktivistin Patton zugetragen hat, und die Sedgwicks Theoriebildung hier zugrunde liegt, lässt sich die von ihr vorgenommene Unterscheidung von paranoiden und reparativen Praktiken als eine Strategie verstehen. Eine Strategie, die »enabling« (ebd., 124) ist, da ihr Einsatz darauf basiert, in dieser Welt nicht bloß zu überleben, sondern *gut* zu leben,[2] ohne im Spiel des paranoid-reaktiven Antizipierens des Schlimmstmöglichen gefangen zu sein, ohne immer schon von der Welt in eine scheinbar ausweglose Epistemologie des Sterben-Lassens und Umgebracht-Werdens verstrickt worden zu sein.[3] Dabei geht es Sedgwick nicht darum, der reparativen Position mehr Wahrheit

2 Die gewählte Formulierung, *gut* zu leben, bezieht sich an dieser Stelle explizit nicht auf die Fantasie des *guten Lebens*, die Lauren Berlant (2011) in *Cruel Optimism* bespricht.

3 Hannah McCann und Whitney Monaghan (2019, 146) weisen darauf hin, dass Sedgwick außerdem bemerkt, dass ihre eigene Kritik, die sie in ihren vorherigen Werken geübt hat, radikaler hätte sein können, wenn sie reparativ geübt worden wäre.

zuzusprechen als der paranoiden, sondern eher um die verschiedenen Konsequenzen, die sich aus den unterschiedlichen Positionierungen ergeben können. Eine Form der Wissensproduktion zu wählen, die nicht paranoid, sondern reparativ ist, zieht andere Kreise, entwirft andere Narrative, und damit verändern sich auch die wahrgenommenen Möglichkeiten für das eigene Handeln, auch, wenn diese, wie bereits angedeutet, nicht deterministisch sind. Es lässt sich ein Bewusstsein dafür entwickeln, dass auch eine paranoid strukturierte Wissensproduktion nicht bedeutet, an diese Form der Wissensproduktion gebunden zu bleiben: Die Position kann gewechselt werden.

5.1.1 Paranoide Praktiken in IT-Sicherheit und Kryptologie

Bisher ist nicht genauer ausgeführt worden, was Paranoia als Methode der Wissensproduktion eigentlich kennzeichnet. Sedgwick macht in ihrem Aufsatz fünf Kriterien aus, anhand derer sie im Verlauf ihres Texts diskutiert, was paranoide Praktiken sind, aber auch, wo in der *Critical Theory* oder der psychoanalytischen Theoriebildung sie diese beobachtet. Dieser Struktur folgt auch das vorliegende Unterkapitel, wenn auch anhand eines anderen Korpus: Basierend auf Sedgwicks Definition paranoider Praktiken als Form der Wissensproduktion wird hier anhand verschiedener Fallbeispiele aufgezeigt, dass Kryptologie und IT-Sicherheit als wissenschaftliche Disziplinen sowohl was die Forschungsdesiderate als auch Techniken, Rhetoriken und Veröffentlichungen angeht, mittels paranoider Praktiken Wissen generieren. Die folgenden Abschnitte orientieren sich daher an den von Sedgwick definierten Merkmalen paranoider Praktiken der Wissensproduktion[4] und diskutieren diese anhand ausgewählter Beispiele aus IT-Sicherheit und Kryptologie, von denen manche ausführlicher behandelt werden, und bei manchen nur kurz auf bereits erfolgte Ausführungen verwiesen wird, was noch einmal als ein kurzer Überblick über die bisherigen Teile dieser Untersuchung dient. Auf reparative Praktiken der Wissensproduktion wird im Anschluss genauer eingegangen.

4 Sedgwick unterteilt ihre Ausführungen zu paranoiden Praktiken in fünf Abschnitte. Die folgenden Ausführungen ziehen zwei dieser Punkte zusammen, daher erfolgt die Diskussion hier in vier Unterkapiteln.

»Paranoia is anticipatory«

»*There must be no bad surprises,*« schreibt Sedgwick (2003, 130, Herv. i.O.), sei der vorderste Imperativ paranoid strukturierter Wissensproduktion. Das Verhindern jeglicher Überraschungen, guter oder schlechter (aber vor allem schlechter) Natur, sei die Grundlage des intimen Verhältnisses von paranoiden Praktiken und Wissen im allgemeinen, und kreiere eine komplexe zeitliche Relation des Wissens zum wissenden Subjekt, in der die unbedingte Ausrichtung auf die Zukunft von der um ihrer Willen zu vermeidenden möglichen Vergangenheit informiert ist: Da es keine bösen Überraschungen geben dürfe, und da bereits die Möglichkeit einer bösen Überraschung eine solche sei, müsse Paranoia auch die schlechten Nachrichten immer schon gewusst haben (vgl. ebd., 130). Die Bewegung nach vorne, um von dort einen Blick zurückzuwerfen, gilt auch für die Relation von Kryptographie und Kryptanalyse, den beiden Teilgebieten der Kryptologie. Befasst sich Kryptographie mit der Verschlüsselung von Nachrichten, so kümmert sich Kryptanalyse um das Brechen von Verschlüsselung auf einem unvorhergesehenen Weg. Nun ließe sich einwenden, dass es keine Kryptanalyse geben könne ohne Kryptographie, denn was würde diese denn entschlüsseln wollen? »But in the real world«, bemerkt David Kahn (1967, 753),

> »the cryptanalyst – or more accurately the potential cryptanalyst – comes first. What need for cryptography if no one would eavesdrop? Why build forts if no one would attack? Thus the assumption that someone will attempt a cryptanalysis, no matter how tentatively or incompetently, engenders cryptography.«

Kryptographie ist also schon immer auf ihren angenommenen Angriff hin ausgerichtet – laut Kahn existiert sie, um einen möglichen Angriff auf sie zu verhindern. Diese stets auf die möglichen Zukünfte gerichtete Zeitlichkeit findet sich auch im Essay *Why Cryptography Is Harder Than It Looks* von Bruce Schneier. Erstmals 1997 im Journal *Information Security Bulletin* erschienen, ist der Beitrag heute auf Schneiers Blog nachzulesen, und wirkt, abgesehen von einigen einleitenden Bemerkungen, wie ein tagesaktueller Essay.[5] Schneier erläutert, warum gute Kryptographie den Kern eines jeden sicheren IT-Systems bil-

5 Man würde zwar vermuten, dass ein Beitrag aus der IT-Sicherheit eine – gemessen an dem Tempo technischer Innovation und dem daher schnelllebigen Feld – eher geringe Halbwertszeit haben sollte, doch da der Beitrag sich auf die Prinzipien der Kryptographie bezieht und weniger auf konkrete Verfahren, erscheint er vergleichsweise zeitlos.

det, und zählt anhand verschiedener Faktoren auf, warum es schwerer sei als es aussehe, ein sicheres System herzustellen. Er führt aus, dass mögliche Sicherheitslücken eines digitalen Systems nicht bloß kryptographischer Natur sein können, sondern auch die softwareseitige Implementierung guter kryptographischer Verfahren betreffen können, die Usability eines Systems (und dadurch den korrekten Einsatz der Sicherheitsmechanismen[6]) oder die Modellbildung selbst. Im Schlussplädoyer schreibt Schneier (1997, Herv. MS):

> »History has taught us: never underestimate the amount of money, time, and effort someone will expend to thwart a security system. *It's always better to assume the worst*. Assume your adversaries are better than they are. Assume science and technology will soon be able to do things they cannot yet. Give yourself a margin for error. Give yourself more security than you need today. When the unexpected happens, you'll be glad you did.«

Stets vom schlechtestmöglichen Szenario auszugehen, sollte also der Modellbildung zugrunde liegen, nach der ein Verfahren zur Herstellung von Sicherheit auf seine Leistung beurteilt wird. Die Sicherheitsleistung, und damit das Verhältnis von Verschlüsselung zu Entschlüsselung, sei schon immer von Zeit als alles bestimmendem Faktor geprägt gewesen, wie David Kahn (1967, 753) ausführt, »because all practical matters involving mortal men connect eventually with that one inexorable, irreversible, irretrievable factor.« Der Wettlauf um die Zeit verändert sich jedoch mit den Medien, in denen er ausgetragen wird, und den Zeitlichkeiten, in denen diese operieren und die sie herstellen. Kryptologie entwickelte sich Kahn (ebd., 72) zufolge in den ersten 3000 Jahren ihrer Existenz kaum, und wenn, dann nicht linear. Bestehendes Wissen ging mit den Zivilisationen, die es hervorgebracht hatten, unter, anderes wiederum wurde in Schriften erhalten, von wo aus es weiterentwickelt werden konnte. Doch erst mit der Renaissance westlicher Gesellschaften, so führt Kahn (ebd., 72–73) etwas pathetisch aus, habe die Entwicklung der Kryptologie Fahrt aufgenommen, und sei zu größerer Wichtigkeit gekommen: »The story of cryptology during these years is, in other words, exactly the story of mankind.« An dieser Stelle lässt sich spezifizieren: Sie ist die Geschichte westlicher Gesellschaften und ihrer (schneller werdenden) Medien. Mit der Mechanisierung des Schreibens und dem kommerziellen Erfolg der Schreibmaschine Ende des

6 Ein klassisches Beispiel wäre die Verwendung von »1234« oder einem ähnlich leichten Passwort, da die User_innen mit der Fülle an Passwörtern, die sie sich merken müssen, überfordert sind.

19. Jahrhunderts konnte auch die Verschlüsselung in Form von Chiffriermaschinen automatisiert werden (vgl. Landwehr 2008, 42). Dies war vor allem für militärische Zwecke interessant, denn die ersten Chiffriermaschinen automatisierten Additions- oder Substitutionschiffren und beschleunigten diese um ein Vielfaches, da das Nachschauen in einer Tabelle oder einem im Kreis notierten Alphabet damit entfiel (vgl. ebd.). Die Mechanisierung der Ver- und Entschlüsselung erreichte mit dem Brechen der Enigma während des Zweiten Weltkriegs ihr wohl bekanntestes Diskursereignis, das maßgeblich dazu beitrug, dass heute die Sicherheit eines kryptographischen Systems im Hinblick auf ihre Beweisbarkeit in zwei Kategorien beurteilt wird, die beide in Abhängigkeit zur ihrer Berechenbarkeit durch Computer stehen (vgl. Maurer 2016, 57). Die erste Kategorie heißt *information-theoretically secure*,[7] was bedeutet, dass die Verschlüsselung niemals durch Berechnungen mit einer deterministischen Rechenmaschine gebrochen werden kann. Die zweite, und verbreitetere Kategorie trägt den Namen *computationally secure* und meint, dass die Verschlüsselung zwar theoretisch mittels mathematischer Verfahren berechnet und so gebrochen werden kann, aber diese Berechnung unter den gegebenen Umständen nicht praktikabel ist (vgl. ebd.). Dies bedeutet konkret, dass die gewählte Verschlüsselung zu Brechen ein mathematisches Problem darstellt, das sich nicht in Polynomialzeit auf einer universellen Turingmaschine lösen lässt. Maurer (ebd., 58) weist darauf hin, dass die Informatik mathematische Aussagen über *Computation* treffen möchte, und zu diesem Zweck ein mathematisches Modell von *Computation* notwendig wurde, was durch Alan Turing realisiert wurde. Doch schuf Alan Turing ein mathematisches Modell von *Computation*, wie es Maurer schreibt, oder mechanisierte er die Mathematik, wie es Bettina Heintz (1993) darlegt? Mit Turings Aufsatz *On Computable Numbers, With an application to the Entscheidungsproblem* fielen, wie Heintz (ebd., 71) ausführt, auf theoretischer Ebene erstmals ein formalistisches Verständnis von Mathematik und Mechanizität in eins. Die formalistische Auffassung der Mathematik, die gekennzeichnet ist von einem »radikale[n] Verzicht auf Repräsentation« (ebd., 16), wurde erstmals von David Hilbert im 20. Jahrhundert formuliert, obgleich erste Ansätze des Formalismus bis in die zweite Hälfte des 19. Jahrhunderts zurückreichen (vgl. ebd., 17). »In der formalistischen Mathematik«, fasst Heintz (ebd., 16) zusammen,

7 Der Ausdruck *perfectly secure* kann synonym verwendet werden (vgl. Katz/Lindell 2008, 47), wobei der Begriff *information-theoretically secure* selbsterklärender ist.

> »gibt es keinen Verweis mehr auf irgend etwas außerhalb des mathematischen Systems, heiße das nun Anschauung, Evidenz, sinnliche Erfahrung oder Intuition. Die Mathematik erzeugt die Objekte, mit denen sie operiert, und die Regeln, nach denen sie vorgeht, selbst und findet sie nicht irgendwo vor […].«

Formalistische Mathematik begreift Mathematik also als ein in sich geschlossenes, logisches System ohne Bezug auf ein Außen. Innerhalb des Systems lassen sich Behauptungen über das Verhältnis von Elementen zueinander aufstellen, verifizieren oder falsifizieren, kurz: für diese Mathematik stehen eher die Beziehungen zwischen ihren Gegenständen als die Gegenstände selbst im Vordergrund (vgl. ebd., 20). Hilbert war angetreten, den Ansatz von Alfred North Whiteheads und Bertrand Russels *Principia Mathematica* (erschienen zwischen 1910–1913) konsequent weiterzudenken. *Principia Mathematica* sollte die Mathematik von dem befreien, was Douglas Hofstadter (2007, 24) als »Seltsame Schleifen« bezeichnet: Den kleinen Widersprüchen der Selbstbezüglichkeit, die sich in die Mathematik über die Mengenlehre oder die Zahlentheorie eingeschlichen hatten. So versuchten Whitehead und Russel, »die gesamte Mathematik, wohlgemerkt ohne Kontradiktionen (!), aus der Logik abzuleiten« (ebd., 26), was bedeutet, die Mathematik auf solide axiomatische Annahmen zu stellen, und alle getätigten Aussagen aus diesen Axiomen logisch herleiten zu können. Den Beweis der Widerspruchsfreiheit dieser umfassenden Unternehmung blieben sie jedoch schuldig (vgl. ebd.), und an dieser Stelle kommt Hilbert ins Spiel. Hilbert wollte genau diesen Beweis liefern, »daß jeder wahre Satz der Zahlentheorie sich innerhalb des von P.M. [*Principia Mathematica*, MS] abgesteckten Rahmens ableiten läßt« – ein Unterfangen, das Hofstadter (ebd.) ebenfalls als eine Seltsame Schleife bezeichnet, denn »[w]ie kann man seine Beweismethoden auf der Grundlage eben dieser Beweismethoden rechtfertigen? Es ist, als wollte man sich an den eigenen Haaren aus dem Sumpf ziehen.« Hilbert hatte seine Theorie an drei Grunderwartungen ausgerichtet: Er veranschlagte, dass die formalistische Mathematik widerspruchsfrei, vollständig und entscheidbar sei – allerdings ebenfalls, ohne dies bewiesen zu haben (vgl. Heintz 1993, 63). Diese Erwartungen wurden der Reihe nach gedämpft: Zunächst durch Kurt Gödel, der 1931 mit dem sogenannten *Unvollständigkeitsbeweis* darlegte, dass inhaltlich wahre Sätze innerhalb eines gegebenen Systems existieren, die nicht aus diesem ableitbar sind, und dass die Widerspruchsfreiheit eines gegebenen Systems niemals aus diesem selbst heraus bewiesen werden kann, sondern nur mittels

eines übergeordneten Systems (vgl. ebd., 64–65). Gödels *Unvollständigkeitsbeweis* falsifizierte damit auch die Grundannahmen von Whiteheads und Russels *Principia Mathematica* (vgl. Hofstadter 2007, 27). Die Widerlegung des Hilbert'schen Programms wurde von der mathematischen Community mit Erleichterung aufgenommen, denn hätte Hilbert Recht behalten, so wäre die Mathematik grundsätzlich mechanisierbar gewesen und die mathematische Beweisführung damit gänzlich automatisierbar, was in letzter Konsequenz Mathematiker_innen obsolet gemacht hätte (vgl. Heintz 1993, 63–64). Alan Turings 1936 erschienener Aufsatz *On Computable Numbers, With an application to the Entscheidungsproblem* bewies nicht die grundsätzliche Mechanisierbarkeit der Mathematik,[8] wohl aber die grundsätzliche Mechanisierbarkeit eines in sich geschlossenen mathematischen Systems (vgl. ebd., 64). Mit der Turingmaschine, fasst Heintz (ebd.) pointiert zusammen, werden »Formalisierung und Mechanisierung […] bedeutungsäquivalente Begriffe.« Die Turingmaschine entspricht also einem Algorithmus, und für jede im Turing'schen Sinne berechenbare Funktion gibt es eine Turingmaschine. In seinem Aufsatz führt Turing noch eine weitere Maschine ein, die er als *universelle Maschine* bezeichnet. Diese kann jede beliebige Turingmaschine in sich aufnehmen und berechnen. »Mit seiner Arbeit«, so folgert Heintz (ebd., 10), »hat Turing die formalistische Auffassung der Mathematik zu Ende gedacht und sie gleichzeitig radikalisiert: Jede Operation im Rahmen eines formalen Systems läßt sich im Prinzip auch von einer Turingmaschine ausführen.« Die Turingmaschine ist also eine symbolische Maschine, die, ganz nach der Leitidee der formalistischen Mathematik, mit den Relationen ihrer Gegenstände zueinander befasst ist – genau wie das Verhältnis von Kryptographie und Kryptanalyse, von Ciphertext und Plaintext. Ihre erste physische Realisierung erfuhr sie, als Turing und sein Team in Bletchley Park erste Vorläufer unserer heutigen Computer bauten, um die Verschlüsselung der Enigma zu brechen. So ist die Geschichte der Kryptologie untrennbar mit der Geschichte der Informatik verbunden:

8 Turing (1987, 19) weist in der Einleitung zu *On Computable Numbers, With an application to the Entscheidungsproblem* (dt. Übersetzung: *Über Berechenbare Zahlen mit einer Anwendung auf das Entscheidungsproblem*) explizit darauf hin, dass die von ihm konstruierte Maschine nur mit bestimmten Zahlen operieren kann: »In den Abschnitten 9 und 10 liefere ich einige Argumente mit der Absicht zu zeigen, daß die berechenbaren Zahlen alle Zahlen einschließen, die natürlicherweise als berechenbar angesehen werden könnten. Insbesondere zeige ich, daß bestimmte große Zahlenklassen berechenbar sind. […] Die berechenbaren Zahlen umfassen jedoch nicht alle definierbaren Zahlen, wofür das Beispiel einer definierbaren Zahl, die nicht berechenbar ist, gegeben wird.«

Computer entstanden mit der Mechanisierung von Kryptographie und Kryptanalyse. Turing war es also gelungen, eine Schnittstelle zu schaffen, an der sich die Mechanisierung der Mathematik und ein mathematisches Modell computergestützter Rechenvorgänge trafen. An dieser Intersektion wird auch die erste Konsequenz der neuen Medialität von Kryptologie deutlich: Die Symbiose von Mathematik und Maschine generiert das Spannungsfeld *Zeit(/Geld) vs. Rechenleistung*, in der sich die Kryptologie von da an befindet. So ist Schneiers Appell, man solle stets davon ausgehen, dass Wissenschaft und Technik bald zu Dingen in der Lage sein werden, die zu einem gegebenen Zeitpunkt noch unmöglich seien, vor allem in digital-medialen Kontexten relevant: Die stetige Weiterentwicklung der Technik sowie der Rechenleistung erzeugt eine andauernde Beschleunigung. Und tatsächlich erscheint es möglich, diese schlechtestmögliche Zukunft nicht nur nebulös zu erahnen, sondern sie zu berechnen. Christof Paar und Jan Pelzl (2016, 13–14) führen in *Kryptografie Verständlich* aus, dass eine vollständige Einschätzung technologischen Fortschritts (neue Erfindungen eingeschlossen) zwar unmöglich sei, aber sehr wohl anhand des *Mooreschen Gesetzes* die Beschleunigung bereits existierender Systeme in Relation zu monetären und zeitlichen Ressourcen geschätzt werden könne. Dieses Gesetz beschreibt das exponentielle Wachstum von Rechenleistung: Es besagt, dass sich die Rechenleistung von Computern bei konstant bleibenden Kosten alle 18 Monate verdoppelt.[9] Der Verweis auf das Mooresche Gesetz bringt zum ersten Mal auch explizit monetäre Ressourcen in die Evaluation von Sicherheit mit ein, die sich mit zeitlichen Ressourcen abwechseln müssen. Angelehnt an Paars und Pelzls (ebd., 14) Beispiel lässt sich das Mooresche Gesetz anhand einer fiktiven Akteurin folgendermaßen veranschaulichen: In diesem Augenblick müsste sie Computer im Wert von einer Million Euro besitzen, um eine Verschlüsselung in einem Monat zu brechen. In 18 Monaten müsste sie nur eine halbe Million investieren, da die Computer doppelt so schnell rechnen können. In drei Jahren nur noch eine Viertelmillion, in 15 Jahren nur noch 1000€. Alternativ könnte die fiktive Akteurin in 15 Jahren eine Million Euro aufwenden und die Verschlüsselung in 45 Minuten brechen. Diese Überlegungen sind relevant für die Länge der verwendeten Schlüssel bei Verschlüsselungsverfahren, die nach dem *Kerckhoffs'schen Prinzip*

9 Während sich bereits erste Abweichungen von den Vorhersagen des Mooreschen Gesetzes in den letzten Jahren gezeigt haben, ist unklar, ob, und wann genau es seine Gültigkeit verlieren könnte (vgl. Rotman 2020).

funktionieren. Hier gilt: je länger der verwendete Schlüssel, desto exponentiell länger dauert ein *Brute-Force*-Angriff,[10] mit dem der Schlüssel geknackt werden soll. Cloudanbieter und Bankensysteme verwenden in der Regel 256 Bit lange Schlüssel, was einen Brute-Force-Angriff einige Dekaden kostet, selbst für den Fall, dass Quantencomputer eingesetzt würden (vgl. ebd., 13). Einen solchen antizipierenden Blick beschreibt auch Sedgwick (2003, 131) als Modalität paranoider Praktiken der Wissensproduktion: »No time could be too early for one's having-already-known, for its having-already-been-inevitable, that something bad would happen. And no loss could be too far in the future to need to be preemptively discounted.«

»Paranoia is reflexive and mimetic«

Eingangs wurde bereits kurz erwähnt, dass Sedgwick Paranoia als ansteckend betrachtet, und in der Ansteckung die Herstellung symmetrischer Epistemologien erkennt. Diese Ansteckungen, und vor allem die symmetrischen Epistemologien werden, Sedgwick (2003, 131) zufolge, durch die Eigenschaft von Paranoia, sich reflexiv und mimetisch zu verhalten, hergestellt: »Paranoia seems to require being imitated to be understood, and it, in turn, seems to understand only by imitation.« In Anschluss daran formuliert Sedgwick (ebd., Herv. i.O.) eine Art Motto der paranoiden Form der Wissensproduktion: »Paranoia proposes both *Anything you can do (to me) I can do worse*, and *Anything you can do (to me) I can do first* – to myself.« Bezogen auf Kryptographie und IT-Sicherheit lassen sich in den Bereichen der Modellbildung und bei sogenannten Penetrationstests für diese Aussage konkrete Beispiele finden. In Kapitel 2 wurde bereits ausführlich auf die kryptographische Modellbildung der *Beweisbaren Sicherheit* eingegangen, deren Aufgabe es Jonathan Katz und Yehuda Lindell (2008, 23–24) zufolge sei, die Gegebenheiten der Welt in ein mathematisches Modell derselben zu übersetzen, was schlussendlich dazu führt, ein mathematisches Modell der Welt zu entwerfen – ein Ansatz, der innerhalb der *Beweisbaren Sicherheit* durchaus kritisiert wird (vgl. Koblitz 2007). Kryptographische Modellbildung versucht, Sicherheit *vor* etwas herzustellen, und definiert mittels Reduktionen zu diesem Zweck genau, wovor es sichern soll und kann. Die verwendete Methode des_der antizipierten Angreifer_in bleibt, dem »arbitrary

10 Bei einem Brute-Force-Angriff (dt. etwa: Angriff mit roher Gewalt) werden nacheinander sämtliche Möglichkeiten eines Schlüssels durchprobiert, bis der richtige gefunden wurde. Je nach Komplexität des jeweiligen Passworts kann dies sehr schnell gehen, oder aber mehrere Jahrtausende in Anspruch nehmen.

adversary principle« (Katz/Lindell 2008, 22) folgend, strategisch unbestimmt. Die Modellbildung in der IT-Sicherheit geht, wie Schneier (1997) darlegt, etwas anders vor, da sie mehr Aspekte in die Herstellung von Sicherheit einbeziehen muss als die Kryptographie, wie beispielsweise das User Interface, oder die betrieblichen Abläufe, in die ein Kryptosystem eingebunden werden soll. Schneier (1997) beschreibt die Vorgehensweise kompakt:

> »A good design starts with a threat model: what the system is designed to protect, from whom, and for how long. The threat model must take the entire system into account – not just the data to be protected, but the people who will use the system and how they will use it. What motivates the attackers? Must attacks be prevented, or can they just be detected? If the worst happens and one of the fundamental security assumptions of a system is broken, what kind of disaster recovery is possible? The answers to these questions can't be standardized; they're different for every system.«

Die Vorgehensweise von *Threat Modeling* orientiert sich nicht nur an der von Sedgwick beschriebenen antizipierenden Haltung von Kryptographie und IT-Sicherheit, sondern auch an der Notwendigkeit, durch Imitation zu verstehen: Beim Threat Modeling wird aus der Perspektive der Angreifer_innen gedacht, um auf diese Weise möglicherweise auszunutzende Sicherheitslücken innerhalb des eigenen Systems zu identifizieren (vgl. Shostack 2014). Sind diese Sicherheitslücken einmal identifiziert, können sie präventiv angegangen werden: In seinem Handbuch *Threat Modeling. Designing for Security* weist Adam Shostack (ebd., 12–13) darauf hin, dass als Reaktion auf ein identifiziertes Problem vier Möglichkeiten in Frage kommen: 1.) das Ausnutzen einer Sicherheitslücke könne durch zusätzliche Sicherheitsmaßnahmen erschwert werden, 2.) eine Sicherheitslücke könne komplett geschlossen werden, 3.) das identifizierte Problem könne auf eine andere Entität ausgelagert werden, bspw. auf eine Firma, die entsprechende Dienstleistungen anbietet (es könnte dabei z.B. um die DSGVO-konforme Verwaltung von Kund_innendaten gehen), 4.) das Risiko könne akzeptiert werden. Auf diese Weise erzeugt Threat Modeling symmetrische Wissensbestände und Wissensgeschichten: Designer_innen von (sicheren) Systemen orientieren sich an den von ihnen erwarteten Verhaltensweisen von Hacker_innen, um ihre Systeme genau gegen diese abzusichern. Hacker_innen wiederum orientieren sich an dem von ihnen erwarteten Verhalten von Designer_innen, und versuchen dort anzugreifen, wo sie eine Sicherheitslücke vermuten. Dies ist die Symmetrie, die Sedgwick (2003, 131) beschreibt, wenn sie formuliert: »Paranoia seems to

require being imitated to be understood, and it, in turn, seems to understand only by imitation.«

Auf die Spitze getrieben wird dieses Wissensverhältnis zwischen Hersteller_in und Angreifer_in, bei dem stets zu vermuten ist, dass man sich nicht gründlich genug in die andere Partei hineinversetzt habe, beim sogenannten *Penetrationstest*. Bei diesem Verfahren wird ein_e Dienstleister_in damit beauftragt, die Sicherheit eines Unternehmens durch einen Angriff zu testen, nur für den Fall, dass die bisher hergestellte epistemologische Symmetrie noch nicht symmetrisch genug ist. Das auszuschließende *störende Dritte* soll bei diesem Verfahren ein System wortwörtlich penetrieren: Es soll einen Eingang finden. In einem Praxisleitfaden des Bundesamtes für Sicherheit in der Informationstechnik (BSI 2016) heißt es dazu, der Penetrationstest sei ein

> »erprobtes und geeignetes Vorgehen, um das Angriffspotenzial auf ein IT-Netz, ein einzelnes IT-System oder eine (Web-)Anwendung festzustellen. Hierzu werden die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System eingeschätzt und daraus notwendige ergänzende Sicherheitsmaßnahmen abgeleitet beziehungsweise die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen überprüft.«

Es werden zwei Arten von Penetrationstests unterschieden: Blackbox-Tests und Whitebox-Tests.[11] Bei Blackbox-Tests stehen den für den Angriff nur Name und Webadresse des zu prüfenden Unternehmens zur Verfügung, bei Whitebox-Tests steht ebenfalls der zu überprüfende Code zur Verfügung, sowie unter Umständen umfangreichere Informationen zur Organisationsstruktur des zu prüfenden Unternehmens (vgl. ebd., 5). Das BSI (ebd., 5–6) empfiehlt die Durchführung von Whitebox-Tests, da bei Blackbox-Tests sowohl der Aufwand für die Prüfer_innen, als auch die Möglichkeit, unbeabsichtigt Schaden anzurichten, höher sei, sowie unter Umständen Angriffspunkte übersehen werden können: »Es besteht die Gefahr, dass im Rahmen eines Blackbox-Tests Szenarien wie der Angriff eines informierten Innentäters nicht berücksichtigt werden.« Penetrationstests lassen sich damit als das von Sedgwick (2003, 131) zusammengefasste Motto der paranoiden Form der Wissensproduktion verstehen: »*Anything you can do (to me) I can do worse*, and *Anything you can do (to me) I can do first* – to myself.« Auf diese Art tragen Penetrationstests, analog zu Sybille Krämers (2008, 149) Bemerkung,

11 Shostack (2014, 192) differenziert zwischen »black box«- und »glass box«-Tests.

Computerwürmer würden zur *Immunisierung* eines Betriebssystems anregen, zur Immunisierung eines gegebenen Systems bei, nur um dieses weiter in Richtung der von Loick (2021, 271) benannten »Fortifizierungslogik« eines negativen Sicherheitsbegriffs zu führen. Die symmetrische Epistemologie, die mit paranoiden Praktiken der Wissensproduktion einhergeht, führt damit zu einer Verhärtung des Wissens und der Praktiken von Designer_innen und Angreifer_innen, die sich in der bereits dargelegten Steigerungslogik zueinander verhalten. So bleibt immer ein generelles Misstrauen bezüglich der Überprüfbarkeit von Sicherheit, ein Restrisiko, das niemals eingeholt werden kann, wie auch Schneier (1997) bemerkt: »No amount of general beta testing will reveal a security flaw, and there's no test possible that can prove the absence of flaws.« Paranoia findet also stets das heraus, was sie schon weiß (vgl. Sedgwick 2003, 135): Dass ein System unsicher ist. So empfiehlt es sich, weiterhin vom Schlimmsten auszugehen, denn »[i]n a paranoid view, it is much more dangerous […] to be unanticipated than often to be unchallenged.« (Ebd., 133)

»Paranoia is a strong theory of negative affects«

Sedgwick (2003, 136) bestimmt Paranoia weitergehend als eine »strong theory of negative affects«. Um sich diesem Punkt zu nähern, definiert sie zunächst eine *strong theory* mit dem Psychoanalytiker Silvan Tomkins (in ebd., 134) als »capable of accounting for a wide spectrum of phenomena which appear to be very remote, one from the other, and from a common source.« Die zentrale Leistung einer solchen Theorie sei es also, ungenau genug zu sein, um ein großes Feld zu organisieren, was sowohl Vor- als auch Nachteile mit sich brächte. Als Gegenteil der *strong theory* bestimmt Tomkins (in ebd.) die »weak theory«, die »little better than a description of the phenomena which it purports to explain« auf Phänomene begrenzt sei, die bereits als nah beieinander erscheinen. Tomkins (in ebd.) trifft die Unterscheidung von *weak* und *strong theory* im Hinblick auf die von ihm vorgelegte Affekttheorie, zu der er schreibt:

> »A humiliation theory is strong to the extent to which it enables more and more experiences to be accounted for as instances of humiliating experiences on the one hand, or to the extent to which it enables more and more anticipation of such contingencies before they actually happen.«

Eine Affekttheorie ist, so formuliert Sedgwick (ebd., 135, Herv. i.O.), »among other things, a mode of *selective* scanning and amplification«, also eine Art, Ereignisse für sich zu sortieren und zu bewerten. Als »humiliation theory«

kann dementsprechend eine Organisationsform begriffen werden, die auf die Vermeidung von Demütigung/Erniedrigung des Selbst ausgelegt ist. Sedgwick (ebd., 134) folgert aus Tomkins Ausführungen, dass eine solche Theorie paradoxer Weise nicht etwa durch das Vermeiden oder Abmildern von Demütigung oder Erniedrigung an Stärke gewinne, sondern vielmehr dadurch, dass sie ihr Versprechen nicht einlöse. Dies bedeutet, um ein Beispiel aus dem Alltag anzuführen, dass man sich so sehr man möchte auf eine Situation vorbereiten, so viele Eventualitäten mitbedenken, immer vom Schlimmsten ausgehen und sich auf dieses vorbereiten kann – schlussendlich wird doch etwas anderes passieren als das, mit dem man gerechnet hat. Die paranoiden Praktiken, mit denen man versucht, negative Überraschungen zu vermeiden, haben sich als ineffektiv herausgestellt, und die Demütigung verdoppelt sich: Nicht nur ist eine (negative) Überraschung eingetreten, sie ist auch *trotz* der eigenen Vorbereitung eingetreten. Das paradoxe Moment besteht Tomkins und Sedgwick zufolge darin, dass die »humiliation theory« nicht für ihre Ineffektivität verworfen werde, sondern dass sie im Gegenteil ihre Stärke aus dem Scheitern ziehe: Man hätte sich eben noch besser vorbereiten müssen. Diese Logik ist in weiten Teilen der Struktur von IT-Sicherheit, aber auch der Kryptographie erkennbar, beispielsweise in der Steigerungslogik, dem Wettrennen zwischen Sicherheitslücken und Sicherheitsupdates, Computerviren und Antivirensoftware etc.: Ständig werden IT-Sicherheitsmaßnahmen am potenziell schlimmstmöglichen zu vermeidenden Szenario ausgerichtet, um dann in letzter Konsequenz doch nicht zuverlässig zu schützen. Die angebotene Lösung entspricht jedoch nicht einer Veränderung des Sicherheitsbegriffs, sondern einer Verstärkung der Sicherheitsmechanismen, einem Sicherheitspatch, einem Update. Dasselbe gilt für die Modellbildung innerhalb der *Beweisbaren Sicherheit*, die vorzugsweise verbessert wird, anstatt ihre Limitationen anzuerkennen (vgl. Katz/Lindell 2008, 23).

Ein weiterer erwähnenswerter Aspekt von Paranoia als »strong theory of negative affects« ist, dass »only paranoid knowledge […] has so thorough a practice of disavowing its affective motive and force and masquerading as the very stuff of truth.« (Sedgwick 2003, 138) Paranoide Wissensproduktion tarne also ihre Affekte als rationale Wahrheitssuche. Sedgwick führt diesen Punkt anhand der Werke Marcel Prousts aus, hier soll dies anhand eines Aufsatzes aus dem Feld der Kryptographie getan werden. In ihrem Aufsatz *A Riddle Wrapped in an Enigma* gehen die Kryptographen Neal Koblitz und Alfred Menezes (2016) genauer auf ein öffentliches Statement der NSA ein, die sich im August 2015 für die Notwendigkeit der Entwicklung von Post-Quanten-

Kryptographie[12] aussprach. Die NSA war nicht die einzige Institution, die sich ungefähr 20 Jahre nach der Entstehung dieses Forschungsgebietes für eine stärkere Förderung desselben aussprach, und so war zunächst nichts an diesem Statement aufsehenerregend. »However, one passage was puzzling and *unexpected*« (ebd., 34, Herv. MS), bemerken Koblitz und Menezes: Organisationen oder Verkäufer_innen, die noch nicht von RSA-Verschlüsselung auf ECC-Verschlüsselung[13] umgestellt hatten, bräuchten dies nicht zu tun, sondern sollten stattdessen ihr Geld für das Update auf Post-Quanten-Protokolle sparen (vgl. ebd., 35). Aus dieser Aussage erwuchs der Verdacht innerhalb der kryptographischen Community, dass die NSA sich von ECC distanziere (vgl. ebd., 35), was zu weiteren Spekulationen führte. Kurz nach Veröffentlichung des NSA-Statements erschien ein Artikel in der *New York Times*, in dem, basierend auf den Snowden-Enthüllungen, die kleptographische Backdoor in DUAL_EC_DRBG öffentlich gemacht wurde (vgl. ebd., 36), was die Diskussion weiter anheizte. Koblitz und Menezes gehen in ihrem Artikel den innerhalb der kryptographischen Community besprochenen einzelnen Verdachtsmomenten, sowie den Diskussionen über die möglichen Motive der NSA nach, die von der angenommenen Fähigkeit der NSA, RSA, ECC oder sogar Post-Quanten-Kryptographie zu brechen, bis hin zu der Idee reichen, die Distanzierung von ECC sei ein gegen Russland und China gerichtetes Täuschungsmanöver. Die Autoren machen sich über keine dieser Theorien lustig, sondern wägen sorgfältig Für und Wider ab, kommen jedoch am Ende ihres Artikels zu keinem Ergebnis: »We cannot offer a definitive conclusion; the reason for the NSA's pulling back from ECC remains an enigma. Readers are invited to choose from the possible explanations we've given, or come up with their own theories.« (Ebd., 42) Koblitz' und Menezes' Artikel ist insofern bemerkenswert, als er in einem renommierten Journal erschienen ist, und dennoch nichts außer Spekulationen beinhaltet, und sogar zu eigenen, weiteren aufruft – so wird der Versuch der Vermeidung negativer Überraschungen durch antizipierende, reflexive, mimetische Strategien als Wahrheitssuche gekleidet.

12 Unter der Bezeichnung Post-Quanten-Kryptographie werden kryptographische Verfahren zusammengefasst, die Angriffen mit einem Quantencomputer standhalten.

13 Das Akronym ECC steht für *elliptic curve cryptography*, also für kryptographische Verfahren, die auf elliptischen Kurven rechnen.

»Paranoia places faith in exposure«

Die letzte Eigenschaft paranoider Praktiken der Wissensproduktion, die Sedgwick bespricht, ist der paranoide Glaube an die Performativität von Wissen. Dazu bemerkt sie:

> »Whatever account it may give of its own motivation, paranoia is characterized by placing, in practice, an extraordinary stress on the efficacy of knowledge per se – knowledge in the form of exposure. […] That a fully initiated listener could still remain indifferent or inimical, or might have no help to offer, is hardly treated as a possibility.« (Sedgwick 2003, 138)

In diesem kurzen Ausschnitt lassen sich zwei Momente festhalten. Der erste ist die Form des Wissens als Aufdeckung, Enthüllung, oder Entlarvung. In all diesen möglichen deutschen Übersetzungen des Wortes *exposure* schwingt nicht nur die Geste der Hermeneutik des Verdachts mit, sondern leise auch die Möglichkeit einer Demütigung. Dieser Zusammenhang ist es, der ein bestimmtes Wissen an eine Handlung bindet, respektive die Möglichkeit eines Indifferent-Bleibens angesichts des erworbenen Wissens für unwahrscheinlich erachtet. Sedgwick (ebd.) bemerkt außerdem: »Maybe that's why paranoid knowing is so inescapably narrative.« Diese Struktur mitsamt ihrem Hang zum Erzählen von Geschichten lässt sich vor allem anhand von Whistleblowing beobachten. So sagte beispielsweise der NSA-Whistleblower Edward Snowden über seine Beweggründe, die Öffentlichkeit über die Praktiken der NSA zu unterrichten: »My sole motive is to inform the public as to that which is done in their name and that which is done against them.« (Greenwald et al. 2013) In dieser Motivation schwingt allerdings auch Snowdens Glaube an die Wirksamkeit von Wissen in Form einer Enthüllung mit. Dies erklärt sich im Zusammenhang mit Snowdens Statement aus einem Videointerview mit Laura Poitras und Glenn Greenwald, das später Teil des Dokumentarfilmes Citizenfour (USA/GER, R: Laura Poitras) wurde: »The greatest fear that I have regarding the outcome for America of these disclosures is that nothing will change« (Poitras/Greenwald 2013, TC 10:47-10:58). Die Enthüllung ist also unmittelbar an eine zukünftige Handlung gebunden, oder stellt mindestens bereits eine Handlungsaufforderung dar. Ähnlich, wie Sedgwick (2003, 145) paranoide Praktiken der Wissensproduktion auch bei sich selbst erkennt und diese in ihrem Aufsatz adressiert, möchte ich dies an dieser Stelle auch tun. Meinen Artikel *Der rosafarbene Elefant im Raum. Überlegungen zur fehlenden Wut über die NSA-Affäre*, der ein Jahr nach den Snowden-Enthüllungen erschien, und darüber hinaus von dem Ansteckungspotential der paranoiden Position zeugt, empfinde ich heute als

nahezu lehrbuchhaft von paranoiden Praktiken der Wissensproduktion getragen:

> »Zieht man derzeit Bilanz über die NSA-Affäre, die dazugehörige Berichterstattung und die Reaktionen von Politik und Bevölkerung, so muss man feststellen, dass […] die Reaktionen auf die Enthüllungen zu wünschen übrig lassen. […] Dabei sollte man meinen, eine solche Einsicht in Geheimdienstpraktiken und die damit verbundene Erkenntnis, flächendeckend überwacht zu werden, würde größere Empörung hervorrufen. Stattdessen lassen sich Gleichmut, ja sogar Resignation ob der ganzen Angelegenheit beobachten.« (Shnayien 2014, 1)

Diese Textstelle folgt der Bemerkung Sedgwicks (2003, 138), dass die Vorstellung, »a fully initiated listener could still remain indifferent or inimical« so weit entfernt erscheint, dass sie nicht einmal als Möglichkeit in Betracht gezogen wurde – die damit einhergehenden negativen Affekte machten sich umso stärker bemerkbar.

5.1.2 Reparative Praktiken

Die bisherigen Kapitel dieses Buchs haben gezeigt, dass sowohl Kryptologie als auch IT-Sicherheit als Disziplinen ein negativer Sicherheitsbegriff zugrunde liegt. Mit Sedgwicks fünf Eigenschaften paranoider Praktiken der Wissensproduktion wurde anhand von Beispielen aus den beiden Disziplinen verdeutlicht, dass diese ihr Wissen mit paranoiden Praktiken generieren: Im Zentrum beider Disziplinen steht der Wunsch nach einer Vermeidung oder Abmilderung negativer Affekte, die mit dem Hack, dem Knacken von Verschlüsselung, mit dem Einbruch des *störenden Dritten* in das als geschlossen und sauber imaginierte System verbunden sind. Vor diesem Hintergrund lässt sich auch der negative Sicherheitsbegriff, der Sicherheit *vor* etwas herstellt, das er antizipieren, verstehen, und basierend auf diesem Verstehen präventiv verhindern muss, als von paranoiden Praktiken der Wissensproduktion gekennzeichnet lesen. Doch Paranoia gründet in IT-Sicherheit und Kryptologie auch auf der Nicht-Einholbarkeit der Welt durch das Modell: Medien und Menschen verhalten sich nicht so, wie die kryptographische Modellbildung oder das *threat modeling* der Informatik es antizipieren. In der stets ineffektiven Vermeidung der negativen Affekte erweist sich der paranoid strukturierte Diskurs als eine (Ab-)Sicherungsstrategie: Ein Hack konnte zwar nicht verhindert werden, dafür war aber wenigstens niemand überrascht. Paranoide Praktiken erweisen

sich damit einerseits über den negativen Sicherheitsbegriff als Strategien der Herstellung von Sicherheit, sowie innerhalb des Diskurses durch ihr Wesen einer »strong theory of negative affects« als Sicherungsstrategien des Diskurses selbst.

An diese Erkenntnisse anschließend stellen sich die Fragen, wie man sich mit reparativen Praktiken und Lesarten der Kryptologie und der IT-Sicherheit nähern kann, ob reparative Praktiken der Wissensproduktion eine Rolle für Kryptologie und IT-Sicherheit spielen könnten, und wenn ja, welche. Dazu muss zuerst bestimmt werden, was reparative Praktiken sind oder sein können. Sedgwick geht in ihrem Aufsatz erstaunlich kurz auf diese ein, und spezifiziert sie nicht in derselben Ausführlichkeit, wie sie paranoide Praktiken behandelt. Heather Love (2010, 237, Herv. i.O.), eine ehemalige Schülerin Sedgwicks, schreibt in ihrem Artikel *Truth and Consequences: On Paranoid Reading and Reparative Reading*, in dem sie ihre Beziehung zu Sedgwick, sowie zu deren Aufsatz reflektiert: »Reparation in the essay is on the side of *multiplicity, surprise, rich divergence, consolation, creativity,* and *love*.« Eine reparative Position, soviel verrät auch Sedgwick (2003, 146), sei offen für Überraschungen, oder empfinde es als realistisch, überrascht zu werden. Reparative Praktiken sind, oder vielmehr die Einnahme einer reparativen Position bei Sedgwick sei, wie Anja Michaelsen (2018, 98) in ihrem Aufsatz *Sedgwick, Butler, Mulvey: Paranoide und reparative Perspektiven in Queer Studies und medienwissenschaftlicher Geschlechterforschung* ausführt, als ein »politisch notwendiger Perspektivwechsel formuliert«, der im Zeichen eines »besseren Verständnisses für die lebensermöglichenden Strategien unterdrückter und marginalisierter Gruppen« stehe. Dies lässt sich vor allem anhand der Sätze erkennen, mit denen Sedgwick (2003, 150–151) ihren Aufsatz schließt:

> »No less acute than a paranoid position, no less realistic, no less attached to a project of survival, and neither less nor more delusional or fantasmatic, the reparative reading position undertakes a different range of affects, ambitions, and risks. What we can best learn from such practices are, perhaps, the many ways selves and communities succeed in extracting sustenance from the objects of a culture – even of a culture whose avowed desire has often been not to sustain them.«

Bezugnehmend auf diese Textstelle weist Michaelsen (2018, 98) darauf hin, dass eine reparative Position durch die Verschiebung des Erkenntnisinteresses von der Funktionsweise struktureller, systemischer Gewalt hin zu den Elementen und Modi, »die eine Existenz unterdrückter und marginalisierter

Subjekte ermöglichen – nicht erst nach Überwindung der bestehenden Gegebenheiten, sondern innerhalb dieser« weder beabsichtige, »die Bedeutung systemischer und systematischer Gewalt zu relativieren noch Identitäten zu re-essenzialisieren.« Dennoch könnte eine paranoide Position ihr ebendies vorwerfen, denn das Einnehmen einer reparativen Position ist, wie Sedgwick formuliert, nicht leicht: Die paranoiden Praktiken leisten Widerstand gegen andere Formen der Wissensproduktion. Paranoides Wissen »systematically disallows any explicit recourse to reparative motives«, was auch dazu führe, dass reparative Vorgehensweisen von einer paranoiden Position aus als unzulässige Formen der Wissensproduktion erscheinen, »both because they are about pleasure (›merely aesthetic‹) and because they are frankly ameliorative (›merely reformist‹).« (Sedgwick 2003, 144) Mit anderen Worten: Die explizit politische Ausrichtung der Wissensproduktion zeichne sich innerhalb eines dominant-paranoiden Diskurses deutlich ab, und werde sogleich als zu politisch (»merely reformist«), zu unaussagekräftig oder irrelevant (»merely aesthetic«) verworfen. Diese Abwehrmechanismen der paranoiden Position gegenüber der reparativen werfen auch die Fragen auf, welche Geste Sedgwicks Aufsatz vollzieht, und wie er gelesen wird: paranoid oder reparativ? Love (2010, 238) weist darauf hin, dass der Aufsatz sich nicht dafür ausspreche, ausschließlich reparative Positionen zu vertreten, und in weiten Teilen selbst paranoid strukturiert sei. Diese Ambivalenz ist jedoch hauptsächlich der reparativen Position zu verdanken: Wenn reparative Lesarten die Möglichkeit für Überraschungen offenhalten, so gilt dies nicht nur für positive, sondern ebenso für negative Überraschungen (vgl. Sedgwick 2003, 146). Damit geht, wie Love (2010, 239) anmerkt, auch einher, dass reparative Praktiken der Wissensproduktion die Tür vor paranoiden Praktiken nicht verschließen. Ihre eigene Lesart von Sedgwicks Aufsatz, bemerkt Love (ebd., 238–239), »vacillates between a schizoid-paranoid mode and a reparative mode. What the essay argues, and what it performs, is the impossibility of choosing between them.« Diese Leseerfahrung kann ich durchaus teilen: Sedgwicks Aufsatz spielt mit seinem eigenen Oszillieren, sowohl in den Modi der Adressierung als auch in den Modi der Bezugnahme auf seine Gegenstände, und hat sich in seiner Bedeutung für mich während des Schreibprozesses mehrfach verändert. Dennoch ist das Wechseln zwischen paranoiden und reparativen Lesarten kein Ausgeliefertsein an den Text, und auch bezogen auf weitere Texte und Gegenstände vielmehr eine Art aktiver Übung, die voller Überraschungen steckt. Das Einüben des Wechsels der Positionen lässt sich selbst als eine reparative Geste beschreiben, denn es ist eine Erfahrung geprägt von »*multiplicity, surprise, rich*

divergence, consolation, creativity, and *love*« (ebd., 237), die neue Perspektiven auf die eigenen Gegenständen ermöglicht, sowie andere Arten, sich zu diesen in Beziehung zu setzen. Sind die Diskurse der IT-Sicherheit und Kryptologie maßgeblich geprägt von paranoiden Praktiken, die zweifelsohne auch das vorliegende Buch *angesteckt* haben, lässt sich an dieser Stelle dennoch mit Michaelsen (2018, 107) resümieren: »Es ist nicht so, dass es keinen Anlass zur Paranoia gäbe. Mit Sedgwick stellt sich jedoch die Frage, ob unsere Energien am sinnvollsten in diesem Projekt des Aufspürens und Entlarvens eingesetzt sind.« Was wäre vor diesem Hintergrund also ein reparatives Projekt, auf das sich die Energien stattdessen fokussieren könnten? Wie ließe sich Sicherheit in Kryptologie und vernetzten Computersystemen reparativ denken? Oder, um Sedgwicks Einsatz mit Heather Love (2010, 236) noch einmal etwas offener zu formulieren: »I am enabled – but to do what?«

5.2 Queere (IT-)Sicherheit?

Als ein Beispiel für reparative Praktiken der Wissensproduktion, die, wie bereits mit Michaelsen (2018, 98) ausgeführt wurde, eine Verschiebung des Erkenntnisinteresses von struktureller, systemischer Gewalt hin zu Praktiken, »die eine Existenz unterdrückter und marginalisierter Subjekte ermöglichen – nicht erst nach Überwindung der bestehenden Gegebenheiten, sondern innerhalb dieser«, lässt sich der *Safe/r Sex*-Diskurs der 1980er Jahre anführen. Auch Daniel Loick (2021, 12) bespricht diesen im Zuge seiner Ausführungen zu einem *queeren Sicherheitsbegriff*, den er in Anlehnung an Christoph Menkes und Juliane Rebentischs Konzept der »ästhetischen Freiheit«, sowie anhand des *Safe/r Sex*-Konzepts entwickelt. Ein queerer Sicherheitsbegriff zeichnet sich Loick (ebd., 13) zufolge »durch die Dekonstruktion der strikten Opposition von Sicherheit und Unsicherheit, durch einen Platz für Negativität im Positiven« aus, mittels derer sich die xenophoben Mechanismen, sowie das Phantasma einer zu erreichenden absoluten Sicherheit des negativen Sicherheitsbegriffs vermeiden ließen. Diese Dekonstruktion der binären Opposition von Sicherheit und Unsicherheit beobachtet Loick (ebd., 13–14) vor allem in den Fürsorge- und Sicherheitspraktiken der AIDS-Aktivist_innen der 1980er Jahre:

> »Der AIDS-Aktivismus bringt die bürgerliche Einteilung in Privatheit und Öffentlichkeit zum Kollabieren, indem sie von vornherein die öffentli-

> che Bedeutung ›privater‹ Handlungen exponiert: Sexuelles Begehren und sexuelle Aktivitäten, die Sorge um und für Partner*innen, Trauer- und Begräbnisrituale hatten einen unmittelbar politischen Charakter, sie stehen zur Mehrheitsgesellschaft in einem konfrontativen oder polemischen Verhältnis. Dementsprechend ging es in der ›AIDS-Krise‹ auch nicht allein um das persönliche, sondern auch um das kollektive Überleben, das heißt um das Überleben einer Form von subalterner Sozialität und Kultur.«

In diesem Kontext weist Loick den Grundannahmen von *Safe/r Sex* besondere Relevanz zu: *Safe/r Sex* richtete sich, wie bereits in Kapitel 3 angerissen, gegen das dominante homophobe Narrativ der 1908er Jahre, HIV/AIDS sei eine Strafe für die Hand in Hand gehenden Sünden Homosexualität und Promiskuität. Loick verweist auf Douglas Crimps Aufsatz *How To Have Promiscuity in an Epidemic*, in dem Crimp (1987a, 253, Herv. i.O.) dieses dominante Narrativ angreift, und formuliert: »*it is our promiscuity that will save us*.« Crimp (ebd., 253) führt aus:

> »We were able to invent safe sex because we have always known that sex is not, in an epidemic or not, limited to penetrative sex. Our promiscuity taught us many things, not only about the pleasures of sex, but about the great multiplicity of those pleasures. It is that psychic preparation, that experimentation, that conscious work on our own sexualities that has allowed many of us to change our sexual behaviors – something that brutal ›behavioral therapies‹ tried unsuccessfully for over a century to force us to do – very quickly and very dramatically.«

Die Besonderheit des queeren Sicherheitsbegriffs, führt Loick (2021, 14–15, Herv. i.O.) basierend auf Crimp aus, bestehe in der Erkenntnis, dass queere Sicherheit nicht davon ausgehe, dass nicht-heteronormativer, nicht mit Reproduktion assoziierter Sex per se sicherer sei, sondern dass sich »Sicherheit nur dadurch her[stellt], *dass man sich der Unsicherheit aussetzt.* Damit wird die Dichotomie von Sicherheit und Risiko dekonstruiert: die Unmöglichkeit von Sicherheit ist zugleich die Bedingung ihrer Möglichkeit.« Ein queerer Sicherheitsbegriff, wie ihn Loick anhand von *Safe/r Sex* definiert, lässt sich darüber hinaus mit Sedgwick und Michaelsen als reparative Praktik einstufen: Er ermöglicht marginalisierten Personen ein Überleben, aber auch ein gutes Leben, *innerhalb* einer gesellschaftlichen Struktur, und nicht erst nach Überwindung derselben. Nicht durch die Versuche der Vermeidung von Negativität, was das Ziel paranoider Praktiken wäre, sondern durch die

Anerkennung von Negativität und Unsicherheit als Teil sowie notwendige Voraussetzung von Sicherheit lässt sich diese herstellen. Mit Loick (ebd., 16) lässt sich anschließen:

> »Die Relevanz des queeren Sicherheitsbegriffs – eines Sicherheitsbegriffs also, der sich bewusst ist, dass Sicherheit sich nur durch die Öffnung gegenüber der Unsicherheit realisieren lässt – ist dabei nicht auf die Frage des Sex beschränkt, sondern betrifft auch andere Themenbereiche.«

Während Loick an dieser Stelle mit einer Diskussion von queerer Sicherheit in Bezug auf *Safe/r Spaces* anschließt, kommt die vorliegende Untersuchung zu der Frage zurück, ob und wie eine reparative Perspektive auf Sicherheit vernetzter Computer geworfen werden kann, und formuliert die Frage neu: (Wie) kann ein queerer Sicherheitsbegriff für die IT-Sicherheit in Stellung gebracht werden?

5.2.1 *Queer OS/Queer Computation*

Aufgrund des Zusammenhangs des queeren Sicherheitsbegriffs mit dem Konzept von *Safe/r Sex*, und damit mit dem aktivistischen HIV/AIDS-Diskurs, sowie der Bestimmung von queerer Sicherheit als reparativer Praktik der Wissensproduktion und der Bezugnahme auf die Welt, soll der Frage nach der Produktivität eines queeren Sicherheitsbegriffs für die IT-Sicherheit in diesem Unterkapitel anhand einer Reihe von Aufsätzen nachgegangen werden, die sich explizit dem Zusammenhang von Queerness und Technik widmen, und sich lose unter den Schlagworten *Queer OS* und *Queer Computation* versammeln lassen. Dazu zählen die seit 2013 erschienenen Artikel Jacob Gabourys, die sich mit queeren Persönlichkeiten der Technikgeschichte befassen, jedoch nicht, um eine Ansammlung von Biografien im Sinne einer personifizierten Technikgeschichte vorzulegen, sondern um erstmals eine queere Genealogie der Computergeschichte zu schreiben (vgl. Gaboury 2013a; 2013b; 2013c; 2013d; 2013e). 2014 veröffentlichte Kara Keeling ihre Gedanken zu *Queer OS*, und zwei Jahre später folgte der korrespondierende Text *QueerOS: A User's Manual* von Fiona Barnett, Zach Blas, Micha Cárdenas, Jacob Gaboury, Jessica Marie Johnson und Margaret Rhee (2016). Wiederum zwei Jahre später folgte Jacob Gabourys (2018) Artikel *Critical Unmaking: Toward a Queer Computation*.[14] Gemein-

14 Es ließen sich durchaus noch weitere Texte zu dieser Gruppe zählen, beispielsweise Wendy Chuns (2012) *Race and/as Technology or How to Do Things to Race* oder Tara Mc-

sam ist all diesen Texten der Versuch, *Computation*, also die mathematisch-technischen Strukturen und Materialitäten von Computern, sowie deren Eigenheiten und Nutzungspraktiken mit *Queerness*,[15] den Lebensrealitäten, Philosophien, Utopien und Dystopien queerer Menschen, zusammenzudenken, und auf die Modi ihrer Überschneidungen hin zu befragen. Im Folgenden wird zunächst anhand kritischer Lektüren der drei für das vorliegende Unterkapitel zentralen Texte *Queer OS*, *QueerOS: A User's Manual* und *Critical Unmaking: Toward a Queer Computation* das Verhältnis von Queerness und *Computation* in den jeweiligen Aufsätzen diskutiert, und anschließend Anknüpfungspunkte an Sedgwicks *reparative reading* ausgemacht. Weiterhin werden die gewonnenen Erkenntnisse über den *Queer Computation*-Diskurs im Hinblick auf die zentrale Frage des vorliegenden Kapitels, das Nachdenken über einen queeren Sicherheitsbegriff für die IT-Sicherheit, produktiv gemacht.

Queer OS

Kara Keeling (2014, 152) beginnt ihren Artikel *Queer OS* mit der Feststellung, »[f]rom new media's eccentric temporalities and reliance on reading codes to their relationships to ephemera, publics, viruses, music, and subcultures, new media intersect with queer theories in a variety of ways.« An diesen Intersektionen sei bisher Wissen über »queer cybercultures« hergestellt worden, sowie »explorations of the role of new media in LGBT, and queer people's lives«, und wichtige Erkenntnisse zu »representation of LGBT people in, on, and through new media« (ebd.). Dennoch, bemerkt Keeling, gebe es eine Lücke: Während Arbeiten, die sich mit dem Zusammenhang von *race* und neuen Medien befassen, zwar anschlussfähig seien an Positionen der Queer Theory, so werde dieser Zusammenhang nur selten explizit gemacht. Und auch feministische Analysen von Phänomenen digitaler Kulturen, die von einer umfassenderen Beschäftigung mit Queer Theory profitieren könnten, liefern bisher in Keelings

---

Phersons (2012) *U.S. Operating Systems at Mid-Century. The Intertwining of Race and UNIX*, die an dieser Stelle jedoch ausgenommen werden sollen, da sie sich nicht explizit mit Queerness befassen. Die folgenden Überlegungen konzentrieren sich auf Keeling (2014), Barnett et al. (2016), und Gaboury (2018).

15 *Queer*, das sich mit »verdreht« oder »versaut« oder »merkwürdig« ins Deutsche übersetzen lässt, wurde in den 1980er Jahren als abwertende Bezeichnung für homosexuelle Männer und Frauen gebraucht (vgl. Deuber-Mankowsky 2017b, 12). Nach seiner Umdeutung durch Aktivist_innen wird der Begriff heute von Menschen, deren Geschlechtsidentität und/oder Begehren keinem heteronormativen Modell entsprechen, affirmativ als Selbstbezeichnung gebraucht (vgl. Plötz 2014).

Augen bestenfalls Anschlusspunkte an diese (vgl. ebd., 152–153). In Anbetracht dieser von ihr diagnostizierten Lücke in der Theoriebildung schlägt Keeling (ebd., 153) ein »scholarly political project« vor, das sie »Queer OS« nennt, und »at the interfaces of queer theory, new media studies, and technology studies« situiert. Keeling (ebd.) schreibt dazu ausführlicher:

> »Queer OS would take historical, sociocultural, conceptual phenomena that currently shape our realities in deep and profound ways, such as race, gender, class, citizenship, and ability (to name those among the most active in the United States today), to be mutually constitutive with sexuality and with media and information technologies, thereby making it impossible to think any of them in isolation. It understands queer as naming an orientation toward various and shifting aspects of existing reality and the social norms they govern, such that it makes available pressing questions about, eccentric and/or unexpected relationships in, and possibly alternatives to those social norms.«

Wissenschaftliche Arbeiten, die sich unter dem Begriff Queer OS versammeln ließen, führt Keeling (ebd.) aus, seien bereits im Entstehen begriffen, und werden von ihr im Verlauf ihres Artikels besprochen. Ohne Keelings Schilderungen zu diesen Arbeiten detailliert wiedergeben zu wollen, soll zunächst noch einmal genauer nachgezeichnet werden, welche Implikationen Keelings Queer OS beinhaltet. Wie ist der Begriff Queer OS, also ein Queer *Operating System*, ein queeres *Betriebssystem*, angesichts Keelings Vision zu situieren? Handelt es sich dabei um ein Betriebssystem für Maschinen oder für Gesellschaft, oder beides? Keeling (ebd., 153–154) schließt mit diesem Begriff an den drei Jahre zuvor erschienenen Artikel *U.S. Operating Systems at Mid-Century. The Intertwining of Race and UNIX* von Tara McPherson an, und begreift damit Betriebssysteme nicht als bloß technische Systeme, sondern als ›Betriebssysteme einer höheren Ordnung‹. Spezifisch bezieht sich Keeling auf McPhersons (2012, 22) Formulierung »[…] UNIX is widely understood to embody particular philosophies and cultures of computation, ›operating systems‹ of a larger order […].« Im Verlauf ihres Artikels expliziert McPherson, in welcher Weise mit UNIX als Betriebssystem eine dazugehörige Philosophie verbunden sei, eine Idee davon, wie *Computation* aussehen könnte, und eine Gesellschaft, die diese ermöglicht hat, und in die sie gleichsam zurückwirkt. Diese Übertragungsprozesse zeichnet McPherson sehr sorgsam nach, und achtet darauf, die zwei Wissenskulturen, als die sie die Informatik und die Geisteswissenschaft identifiziert, in ihren Unterschieden genau zu erfassen, aber miteinander in einen Dialog zu

bringen. Eine so strikte Trennung von Informatik/Naturwissenschaften und Geisteswissenschaften, wie sie von C.P. Snow (2012) in *The Two Cultures* vorgenommen, oder auch im Zuge des Sokal Hoax formuliert wurde, bezeichnet McPherson (2012, 33) zwar als Mythos, bemerkt aber weiter:

> »[…] powerful operating systems have surged beneath the surface of what and how we know in the academy for well over half a decade. It would be foolish of us to believe that these operating systems – in this paper best categorized by UNIX and its many close siblings – do not at least partially overdetermine the very critiques we imagine that we are performing today.«

McPhersons *operating systems* sind damit nicht nur im wörtlichen Sinne als informatische Betriebssysteme zu begreifen, sondern auch als die Effekte der Betriebssysteme von Computern, die sich bis hinein in die (geistes-)wissenschaftliche Theoriebildung bemerkbar machen,[16] und damit im metaphorischen Sinne als gesellschaftliche Organisationsstrukturen benannt werden können.

Durch die Übernahme der Formulierung des Betriebssystems höherer Ordnung, das sie mit McPhersons zuvorderst zitierter Bemerkung als gesellschaftliche Organisationsstruktur identifiziert, bringt Keeling *Queer* als eine gesellschaftliche Organisationsstruktur in Stellung: »Queer OS makes this formulation of *queer* function as an operating system along the lines of what Tara McPherson describes as ›operating systems of a larger order‹ than the operating systems that run on our computers.« (Keeling 2014, 153) Darüber hinaus verwendet Keeling *Queer* auch als ein Element eines solchen Ordnungssystems. So schreibt sie weiter: »[…] Queer OS seeks to make *queer* into the logic of ›an operating system of a larger order‹«, und bestimmt *queer* damit als Element eines gesellschaftlichen Ordnungssystems »that unsettles the common senses that secure those presently hegemonic social relations that can be characterized by domination, exploitation, oppression, and other violences.« (Ebd., 154) Das Ziel eines *Queer OS* definiert Keeling (ebd.) im Anschluss als

> »[…] to provide a society-level operating system (and perhaps an operating system that can run on computer hardware) to facilitate and support imaginative, unexpected, and ethical relations between and among living beings

16 Auch McPhersons Text selbst unterliegt den Effekten der Modularisierung, die sie in ihrem Aufsatz zu kritisieren versucht (vgl. McIlwain 2020).

> and the environment, even when they have little, and perhaps nothing, in common.«

Keelings *Queer OS* ist damit eine ambivalente Konstellation: Zum einen ein Betriebssystem höherer Ordnung, womit Keeling in loser Anlehnung an McPherson ein gesellschaftliches Ordnungssystem bezeichnet, zum anderen möglicherweise auch ein informatisches Betriebssystem für Computer. Obgleich die Formulierung eines queeren Betriebssystems auf gesellschaftlicher Ebene durchaus charmant klingt, lässt sich die Idee eines gesellschaftlichen Betriebssystems als eine recht flache Lesart von McPhersons (2012, 22) Verwendung des Begriffs verstehen, die die Betriebssysteme höherer Ordnung bereits bei ihrer ersten Nennung durch Anführungszeichen als uneigentliche Rede markiert. Im Verlauf von McPhersons Artikel sind mit Betriebssystemen in erster Linie informatische Betriebssysteme gemeint, die anhand von UNIX zusammen mit ihren Medieneffekten einer genaueren Betrachtung unterzogen werden. Dabei fokussiert sich McPherson (ebd., 29–31) hauptsächlich auf die Modularisierung von Abläufen innerhalb von Computern, die sie in gesellschaftlichen Wissensbeständen und Sphären gespiegelt sieht, beispielsweise in der Aufteilung des öffentlichen Raumes durch die *racial segregation*-Politik der 1960er Jahre. Ein weiterer Schauplatz, an dem die Logik von Computern auf die Gesellschaft zurückwirke, in der sie entstanden und situiert sei, stellt für McPherson die wissenschaftliche Theoriebildung dar. So charakterisiert sie insbesondere die Filmwissenschaft als gekennzeichnet von weißen Flecken in Bezug auf digitale Kulturen, was sie als (Medien-)Effekte derselben begreift (vgl. ebd., 34–36). Bei Keeling (2014, 154) fallen nicht nur die von McPherson gesetzten Anführungszeichen um das Betriebssystem als Metapher weg, wodurch dieses eigentümlich naturalisiert wird, sondern ereignet sich auch eine in zwei Schritten verlaufende Operationalisierung von *queer* in der Formulierung »Queer OS seeks to make *queer* into the logic of ›an operating system of a larger order‹«, die mit Deuber-Mankowsky (2017a, 160, 165) als ein »ontologisches Debakel«, und damit als eine konzeptuelle Verflachung von *queer* begriffen werden kann: Der erste Schritt ist die Konzeptualisierung von Gesellschaft als Betriebssystem. Durch diese Übertragung informatischen Vokabulars auf die Gesellschaft erscheint diese als bereits intrinsisch modularisiert, sowie in starren Zusammenhängen logisch organisiert, als Ausführbares und Ausführendes. Der zweite Schritt ist die Reformulierung von *queer*, eines politischen und philosophischen Konzepts, als informatisches Konzept: als algorithmisch ausführbar, automatisierbar,

was *queer* operationalisiert (vgl. ebd., 160). Diese Verschiebungen, lässt sich an dieser Stelle bemerken, dürfte Keeling nicht beabsichtigt haben, sind sie doch gegenläufig zu ihrer Verwendung des Begriffs *queer* als dezidiert offenem Projekt, das sie als neue und überraschende Relationen ermöglichend beschreibt, was in Sedgwicks Sinne als reparativ aufgefasst werden kann. Das »ontologische Debakel«, wie es Deuber-Mankowsky (2020; 2017a) darlegt, schließt hingegen Zukünfte, da es die operationalisierten Konzepte durch die Algorithmisierbarkeit und Ausführbarkeit deterministisch werden lässt.

QueerOS: A User's Manual

Ausgehend von diesen Operationalisierungen von *queer* ist es ein vergleichsweise kleiner Schritt zu einem *Queer OS* als Betriebssystem von Computern. Mit ihrem Text *QueerOS: A User's Manual* legen Fiona Barnett, Zach Blas, Micha Cárdenas, Jacob Gaboury, Jessica Marie Johnson und Margaret Rhee (2016) eine Lesart von *Queer OS* vor, die Kara Keelings Überlegungen zum Ausgang nimmt, aber stärker auf ein Verständnis von Queer OS als Betriebssystem von Computern oder mobilen Endgeräten hin denkt. Barnett et al. (ebd., 50) markieren ihren Anfangspunkt als Keelings Definition, »QueerOS would make it impossible to think of phenomena of identitarian difference as separate from information technologies.« Während sie die von Keeling geleistete Auflistung rezenter und im Entstehen begriffener Projekte schätzen, die sich mit der Intersektion und Verstricktheit von Queerness und Technik befassen, diagnostizieren sie dennoch, »QueerOS remains a largely speculative project«, und begreifen diese Unschärfe als »a challenge set forth by Keeling to those who have begun to think these worlds together« (ebd.), derer sie sich in ihrem Aufsatz annehmen.

Was zunächst auffällt ist die Schreibweise *QueerOS*: War bei Keeling noch ein Leerzeichen zwischen *Queer* und dem *Operating System*, so wird hier durch die stilisierte Schreibweise ohne Leerzeichen, die im Artikel durch Zitationen bereits Keeling zugeschrieben wird, schon angedeutet, welche Richtung die Weiterführung von Keelings Konzept einschlägt. *QueerOS* erinnert in dieser Schreibweise an *MacOS*, sowie an die Namen verschiedener Linux-Distributionen.[17] Dennoch positionieren sich die Autor_innen (ebd., 50) explizit als Gegenentwurf zur dominant *weißen* und männlichen, wie auch rassistisch-sexistischen Kultur, die sie mit GNU/Linux assoziieren: »However, our

17 Für eine Auflistung ähnlicher Namen siehe die Webseite *ArchiveOS* (o.J.).

OS doesn't come in the form of GNU/Linux's man pages with detailed descriptions of switches, pipes, and flags.« Die Geste der Absetzung von den GNU/Linux »man pages«, also den *manual pages*, dem Handbuch, entfaltet ihre volle Kraft vor dem Hintergrund des in Linux-Hilfsforen oft verwendeten Akronyms »RTFM«, das ausgeschrieben für »read the fucking manual« steht. RTFM wird oftmals auf von der Community als unnötig oder zu basal empfundene Fragen geantwortet (vgl. The Jargon File o.J.e), und stellt insofern einen Gatekeeping-Mechanismus dar, als außer Acht gelassen wird, dass die GNU/Linux *man pages* oftmals für Anfänger_innen schwer zu verstehen sind. Barnett et al. (2016, 50) möchten ein inklusiveres Projekt entwerfen, das über das Ausborgen der »language of popular software to present an accessible introduction« ein Handbuch für ein neues Betriebssystem bereitstellen möchte, »with each component given a poetic and theoretical description of its features and limitations.« In der Fußnote, mit der dieser Satz versehen ist, weisen die Autor_innen darauf hin, dass manche der von ihnen beschriebenen technischen Features zum Zeitpunkt ihrer Arbeit an dem *User's Manual* (noch) nicht existieren. Nichtsdestotrotz nehmen sie bestehendes Vokabular auf und spinnen dieses mit »performative and disruptive intent« (ebd., 58) weiter. Als Einflüsse für ihr *QueerOS* benennen die Autor_innen neben Kara Keeling auch Vertreter_innen aus Queer Theory, Science-Fiction und Aktivismus, sowie feministische Medienprojekte von Schwarzen Menschen, People of Color und trans Personen (vgl. ebd., 50–51). Im Zuge dessen beziehen sich Barnett, Blas, Cárdenas, Gaboury, Johnson und Rhee (ebd., 51) auf *Queerness* als »socially constructed, promiscuous, political, and discomfiting«, aber auch als »technological, operative, and systemic, derived from individual interests, mutual concern, and discussions that have emerged from collective presentations, virtual discussions, and queer dreams.« An dieser Stelle wiederholt sich die Operationalisierbarkeit von *Queer*, die bereits bei Keeling angelegt war, womit sich die Frage aufwirft, zu welchem Zweck das es operationalisiert wird. Der Einsatz der Autor_innen lässt sich als Versuch, aber auch als Wunsch interpretieren, durch die Operationalisierbarkeit von *Queer* eine Stärkung dieses Konzepts innerhalb einer informatischen Logik zu erzielen: Gehören das philosophische Konzept *Queer* und die informatische Logik beide derselben Ordnung an, so würde sich das Ansteckungspotential von *Queer* auf die Informatik erhöhen (vgl. ebd.). Dennoch ist erkennbar, dass die Autor_innen ein Bewusstsein für die zu vermeidende Verkürzung von *Queer* innerhalb einer solchen Logik haben. So bemerken sie beispielsweise: »Our hope is not to present a unified theory of what a queer operating system should be

[…] this is a speculative proposition for a technical project that does not yet exist and may never come to exist, a project that does not yet function and may never function.« (Ebd.) Als Ziel von *QueerOS* beschreiben Barnett, Blas, Cárdenas, Gaboury, Johnson und Rhee (ebd.), »to address what we perceive as a lack of queer, trans, and racial analysis in the digital humanities, as well as the challenges of imbricating queer/trans/racialized lives and building digital/technical architectures that do not replicate existing systems of oppression.« In dem Wissen, dass *Queer* und *Computation* als Konzepte sich beim Versuch, sie in derselben Ordnung zu situieren, als widerständig erweisen, bezeichnen Barnett et al. (ebd.) ihre Ergebnisse mehr als Denkanstöße, als »theoretical vaporware, speculative potentialware, ephemeral praxis.« *QueerOS* lässt sich damit als ein aktivistisch-ästhetisches Projekt begreifen, das sich gegen die Fortschreibung bestehender sozialer Ungerechtigkeiten in technischen Strukturen richtet, sowie geisteswissenschaftliche Analysen um marginalisierte Positionen erweitern möchte. Dennoch stellt sich die Frage, wie produktiv *QueerOS* für dieses Anliegen sein kann, wenn die Autor_innen einerseits um die Begrenztheit der Operationalisierbarkeit von *Queer* wissen, diese aber trotzdem vornehmen; sowie sich an verschiedenen Stellen gegen die grundsätzliche Logik des informatischen Diskurses richten, aber dennoch dessen Vokabular, und damit dessen Logik übernehmen. *QueerOS* ist damit von einer Unschärfe gekennzeichnet, die Schwierigkeiten mit sich bringt, und im Folgenden genauer betrachtet werden soll.

Im Verlauf ihres Aufsatzes gehen die Autor_innen in sechs Sinnabschnitten auf *Interface*, *User*, *Kernel*, *Applications*, *Memory* und *I/O* ein. Diese werden hier nicht im Detail diskutiert, dennoch sollen exemplarisch die Vermengungen und Unschärfen von *Queer* und Informatik nachgezeichnet werden. Das erste Beispiel befindet sich im Abschnitt zu Interfaces. Barnett et al. (ebd., 52) beziehen sich auf das Interface als zentralen Ort der Zusammenkunft von Menschen und Maschinen, sowie als Ort der Übertragungen zwischen diesen beiden. Trotz dieser besonderen Rolle seien Interfaces »prophylactic, accepting only that which has been made hygienic through a translation from the material world into information.« (Ebd.) Abgesehen von dem anzubringenden Einwand, dass auch Informationen über Materialität verfügen, wird jedoch klar, was Barnett et al. hier adressieren: Informationen, die in einen Computer eingegeben werden können, müssen einer bestimmten Form gehorchen, über eine Medialität verfügen, die bestimmte qualitative Elemente derselben ausschließt. In diesem Sinne fragen die Autor_innen danach, wie ein Interface aussehen könnte, das nicht auf »Shannon's mathematical

theory of communication, but on something disarticulated from Western epistemologies« (ebd.) basiert, in dem die Figur des *störenden Dritten* nicht als ausgeschlossenes Element reproduziert würde, sondern als »that which connects and transforms us, an infectious intimacy in which bodies are open to the transformation that arises from one to another« (ebd.) konfiguriert wäre. Die an dieser Stelle artikulierte Idee, User_innen und Maschine verschmelzen zu lassen, indem die starren und als formatierend erlebten *Grammars of Action* (vgl. Agre 1994) zugunsten eines Interfaces aufgebrochen werden, bei dem »interaction […] might transform both the user and the system« (Barnett et al. 2016, 52), wird kurz darauf zugunsten der Idee eines Interfaces verworfen, das sich unsichtbar macht, aber dennoch nicht naturalisiert (vgl. ebd., 53).[18] *QueerOS* wird im Verlauf des Textes immer wieder in ähnlich paradoxer Weise charakterisiert, entweder durch Stilblüten wie »QueerOS rejects the body and yet requires it« (ebd.), oder durch einander widersprechende Aussagen über technische Möglichkeiten des Systems. So fordern die Autor_innen zwar eine Abkehr von der Shannon'schen Logik der Informationsverarbeitung sowie eine Zurückweisung von Funktionalität und eine Privilegierung von Instabilität (vgl. ebd.), formulieren aber gleichermaßen den Anspruch plattformübergreifender Interoperabilität von Apps (vgl. ebd., 55), die ohne die von ihnen zurückgewiesenen Prinzipien informatischer Logik nicht möglich wären. Es ließen sich noch verschiedene weitere Beispiele anführen, doch diese Untersuchung möchte nicht selbst in ein *paranoid reading* verfallen, in dem akribisch nach den technischen Unmöglichkeiten eines bereits als unscharf und spekulativ markierten ästhetischen Projekts gesucht wird.

Bezugnehmend auf José Esteban Muñoz' (2009) Konzept der *Queer Futurity* formulieren Barnett et al. (2016, 53): »Both user and OS agree there will be no finite in the OS. The OS will be emergent, transformative, and ›not yet here‹.« Zusammenfassend lässt sich an dieser Stelle sagen, dass es sich bei *QueerOS* um ein in erster Linie ästhetisches Projekt handelt, das daher ebenfalls in Sedgwicks Sinne als *reparative reading* verstanden werden kann, insofern es einige Überraschungen bereithält, sowie die Beziehung der Leser_innen zu den beschriebenen Gegenständen neu gestaltet, und in dem sich trotz, oder vielmehr: aufgrund der Unschärfen neue Denkanstöße ergeben. In diesem Sinne bietet *QueerOS* »no permanent solutions, only tactical interventions that

18 Angesichts der bereits in Kapitel 2 mit Krämer und Bolter/Grusin besprochenen Logik von Medialität ist zweifelhaft, ob irgendein Medium auf diese Weise existieren könnte, doch um die reine Machbarkeit geht es *QueerOS* nicht.

strive toward a future, becoming a utility that assumes its own obsolescence but which may be refigured, rearranged, and executed once again.« (Ebd., 58) Aus einer technisch informierten Perspektive lässt sich dennoch einwenden, dass die Unschärfe in erster Linie dadurch bedingt ist, dass die *attachments* und Erkenntnisweisen der Informatik zugunsten von *Queer* als philosophisch-aktivistischem Konzept vernachlässigt, oder etwas spitzer formuliert, nicht ernst genommen werden. Barnetts, Blas', Cárdenas', Gabourys, Johnsons und Rhees Versuch, *Queer* nicht vollständig zu operationalisieren und damit einer verflachenden, algorithmischen Logik zu unterwerfen, hat stattdessen zu einer Verflachung des informatischen Diskurses geführt. Für den dritten zu diskutierenden Text der Reihe stellt sich damit die Frage, ob und wie *Queer* und *Computation* in einer Weise miteinander verschränkt werden können, die die jeweiligen Eigenheiten der Diskurse berücksichtigt und anerkennt.

Queer Computation

In seinem 2018 erschienen Artikel *Critical Unmaking: Toward a Queer Computation* fragt Jacob Gaboury nach der Existenz von *Queer Computation* und ihren Modalitäten. Gaboury geht auf verschiedene Möglichkeiten ein, wie *Computation*, also die Art, wie Computer rechnen und funktionieren, aber auch wie sie verwendet und imaginiert werden, queer sein oder gequeert werden könnte. Dazu sei es notwendig, formuliert er, »that we find new ways to make queer theory speak to technology on its own terms.« (Gaboury 2018, 484) Im Zuge dessen nimmt auch Gaboury (ebd.) unter Bezugnahme auf Alexander Galloway explizit eine Operationalisierung von *Queerness* vor:

> »[T]his chapter looks to ›compute queerness‹ by both making it subject to the logic of computation and asking it to act computationally; that is, to become executable. In doing so, it proposes a practice of critical unmaking, foregrounding queer techniques of refusal, misuse, and disruption that must nonetheless work with and through contemporary digital technologies.«

Wie *Queerness* berechenbar und ausführbar gemacht werden könne, führt Gaboury anhand von vier Bereichen aus, die er als Schauplätze von *Queer Computation* identifiziert: den Fail, den Glitch, Normen – in Form von Protokollen – und Code selbst.

Anhand von Jack Halberstams Konzept von *queer failure* beschreibt Gaboury *Queer Computation* in Bezug auf den *Fail* als Möglichkeit, Technik aus einem teleologischen Fortschrittsnarrativ zu lösen. So würde *Queer Computation* sich die Widerständigkeit von *Queerness* zunutze machen, die sich (ironischer Weise) in

dem »refusal to be made useful or productive« (ebd.) ausdrücke. »To compute queerly«, führt Gaboury (ebd., 485) weiter aus,

> »is to acknowledge, embrace, and enact a practice of radical technological failure. It is to engage in critical unmaking: to make central those externalities – exploits, bugs, breakdown, abuse, and misuse – of our digital culture that, while pervasive, we nonetheless disavow. […] In acknowledging, accepting, and even producing failure, queer computation seeks to make clear the values and assumptions that drive our culture of technological development and to offer alternate modes for living with and through technology.«

Aber was kann es eigentlich bedeuten, absichtlich Fehler in digitalen Systemen herzustellen? Um dieser Frage nachzugehen, wendet sich Gaboury dem *Glitch* zu. Ein Glitch ist eine »temporary malfunction« (ebd.), die unerwartet auftritt, und als Störung die Materialität des Mediums offenbart. Nach einigen Überlegungen zur Rolle des Glitchs in Medienkunst bemerkt Gaboury (ebd., 486), die »proliferation of glitch as an aesthetic practice […] diminishes its radical potential«. Betrachtet man Glitches als gewollte ästhetische Phänomene, so riskiere man, ihnen ihr disruptives Moment zu nehmen und normalisiere sie fernab eines radikalen und damit queeren Potentials, das in diesem Beispiel nur ein tatsächlicher Fail haben könne. An dieser Stelle entsteht eine grundlegende Schwierigkeit von *Queer Computation* als Projekt, die Gaboury besonders in Bezug auf *Normen* und *Protokolle* herausarbeitet: Da IT-Systeme standardisiert, und Kommunikation zwischen Computern mit Protokollen, die die Grenzen und Regeln des Sagbaren herstellen (vgl. ebd., 488), bestimmt ist und sein muss, um überhaupt zu funktionieren, kurz: weil digitale Systeme ohne mathematische Exaktheit zum Scheitern verurteilt sind, biete eine Verweigerung dieser Normen wenig Ansatzpunkte für eine queere Kritik von *Computation* abseits von »complete annihilation« (ebd., 486) oder des Luddismus.[19] Beide Optionen betrachtet Gaboury (ebd.) jedoch als nicht zielführend:

> »[…] while it may be compelling to smash our computers in an act of queer rebellion, the radical potential of such a gesture ends there. A broken machine cannot compute, queerly or otherwise. It is a brick, a doorstop; it has no radical potential for computation as it has no computational function.

19 Gerade der Luddismus, denkt man bspw. an das Manifest des sog. »Unabombers« Theodore Kaczynski, zeigt auch eher in die Richtung einer toxischen Männlichkeit als einer queeren Kritik. Vgl. dazu Kaczynski (2010).

> Likewise, it may be compelling to simply opt out of digital technologies altogether, supposing that digital media are irreconcilable with a radical queer politics. While Luddism is certainly a form of critique, it is deeply limited in its efficacy here.«

Dies führt zu *Code* als letztem Bereich von Gabourys Überlegungen zu *Queer Computation*. Anhand einer Diskussion verschiedener Medienkunstprojekte, in deren Zentrum Programmiersprachen stehen, die nicht den für die Informatik gängigen Regeln der Funktionalität folgen, schlägt Gaboury (ebd., 488) vor: »[O]ur queer imperative must be to identify the ideological assumptions that produce protocologial [sic!] norms and then subvert them – to make visible through a queer critical practice the values that structure our technology.« Der Logik von *protocol*, die Alexander Galloway (2004) in seinem gleichnamigen Buch dargelegt hat, folgend, bemerkt Gaboury (2018, 488) weiter: »If it is not possible to work outside the conditions for engagement produced by a given technology, then we must work with technical practices to critique and disrupt the values and assumptions that structure that technology.« Experimentelle Programmiersprachen eignen sich Gaboury (ebd.) zufolge besonders für ein solches Unterfangen, da sie »at the limits of computational logic« operieren, diese aber grundsätzlich erhalten. Eines der von Gaboury (ebd., 489) angeführten Beispiele ist *transCoder*, eine von Zach Blas konstruierte Programmiersprache, die auf »queer linguistic traditions of coded and obfuscated language« basiert, sowie auf Strukturen der Programmiersprache C, und in der Lage sei, ein »double coding« zu erzeugen. »To compute queerness«, schließt Gaboury (ebd., 490) seine Ausführungen,

> »we must begin by acknowledging what queerness offers to a critique of computation. In doing so, we are left with few clear answers and are instead asked to imagine new ways to work against the normalizing influence of our technical culture while maintaining the general functionality of the systems we inhabit.«

Queerness bestimmt Gaboury (ebd.) ebenfalls in Anlehnung an Muñoz »as a means of imagining a future that is not yet here«, weist aber zugleich darauf hin, dass ebendiese Zukünfte durch die »cultural logic of contemporary technology« kolonisiert worden seien, und daher nicht mehr als »primary vector for queer computational critique« funktionieren könnten. Gaboury (ebd.) folgert, »rather than mobilize queerness as a useful technological apparatus, we might deploy it as part of a critical practice of unmaking.« Während der

Ablehnung von »queerness as a useful technological apparatus«, also der Operationalisierung von Queerness, durchaus zuzustimmen ist, soll an dieser Stelle dennoch kritisch angemerkt werden, dass auch die Vorstellung, die Zukunft sei bereits kolonisiert worden, als ein Effekt der Verflachung durch Operationalisierung betrachtet werden kann, die also immer noch am Werk ist: Nur, wenn Queerness als derselben Ordnung wie die Informatik angehörend vorgestellt wird, erscheint ihr Potential als durch diese aufgehoben, erscheinen die Zukünfte als bereits determiniert.

Beide Ansätze Gabourys, sowohl die Operationalisierung von Queerness, die er als nicht zielführend betrachtet, als auch die von ihm vorgeschlagene Auflösung dieses Vorschlags durch die Positionierung von Queerness als »critical practice of unmaking«, sind in Sedgwicks Sinne nicht als reparativ einzustufen. Gegen seine Einordnung von Queerness als »critical practice of unmaking«, also als normative Ordnungen destabilisierendes und denaturalisierendes Element, lässt sich ebenfalls mit Michaelsens (2018, 105) Sedgwick-Lektüre einwenden, dass eine solche Konzeptionalisierung von Queerness auch in anderen Kontexten mit Sedgwick nicht als reparativ verstanden werden kann:

> »Für Sedgwick handelt es sich um eine Fehldeutung, queere Kultur lediglich als Parodie, De-Naturalisierung und Verspottung von dominanter Kultur zu betrachten. […] Einer Perspektive, die sich auf das Entlarven und das ›Immerschon‹ von Macht und Gewaltförmigkeit fokussiert, entgehen diese reparativen Elemente queerer Existenz.«

Reparativ wäre stattdessen, wie Michaelsen (ebd., 112) ausführt, eine »Betonung des Medienspezifischen und Materiellen«, die zum sinnlichen und ästhetischen Überschuss zurückführe. »Möglicherweise«, bemerkt Michaelsen (ebd., 114) an anderer Stelle, »beziehen sich Scheitern und Überschuss auf dasselbe, nur einmal in paranoidem und einmal in reparativem Vokabular.« Zum Überschuss schreibt sie weiter:

> »Medientheoretisch ist mit Überschuss der Anteil des Medialen an dem gemeint, was es vermittelt bzw. was nicht ganz in dem Vermittelten aufgeht. Als solches ist es für die Konstitution des Vermittelten entscheidend und produziert einen Sinn-Überschuss. Dieser manifestiert sich insbesondere in Momenten der Störung, in denen sich die Materialität des Mediums zeigt, im Rauschen, in Pixeln etc.« (Ebd., 112)

Dieser Hinweis ist vor allem vor dem Hintergrund von Gabourys Perspektive auf den Glitch von Interesse: Wenn Gaboury den Glitch als Moment von Queer-

ness verwirft, da dieser Queerness scheinbar normalisiere und seines disruptiven Potentials beraube, ist dies ebenso eine nicht-reparative Perspektive auf Queerness wie ihre Operationalisierung.

Mit Deuber-Mankowsky (2017a, 163–164, 167) wurde bereits darauf hingewiesen, dass die Operationalisierung analytischer Begrifflichkeiten zu einer Unschärfe in der Theoriebildung führt, die gerade in Bezug auf digitale Medien mit einem instrumentellen Technikverständnis einhergeht, in dem Technik als Werkzeug und damit als beherrschbar erscheint. Bei Gaboury, so ließe sich argumentieren, liegt die Gefahr eines durch die Operationalisierung erzeugten instrumentellen Verständnisses von Queerness vor, die damit vorrangig als Mittel, als bloßes Werkzeug zur denaturalisierenden Machtanalyse konzeptualisiert, und infolgedessen als philosophisches Projekt und als Lebensrealität stillgestellt wird. Eine reparative Perspektive würde jedoch außerhalb einer Operationalisierung von Queerness und dem aus der Operationalisierung gesuchten Ausweg, Queerness als die informatische Logik denaturalisierend zu begreifen, stattfinden. Denn, wie Michaelsen (2018, 113) in Bezug auf eventuelle reparative Anschlüsse in medienwissenschaftlicher Geschlechterforschung konstatiert, werden diese gerade durch das »besondere Interesse am medialen und materiellen Überschuss« möglich:

> »Gerade die dabei in den Blick rückenden Ästhetiken und Affekte, die auf Bedeutung jenseits hegemonialer semantischer Inhalte hinweisen, sind als lebenserhaltende Ressourcen u.a. für unterdrückte und marginalisierte Gruppen zu verstehen. Die Frage wäre nicht nur, welchen Anteil das Mediale an Konzepten von Geschlecht hat bzw. wie sich Gender und Medien wechselseitig konstituieren. Das Interesse würde sich stattdessen auf den medialen Anteil richten, der über die Wiederholung und Verfestigung normativer Geschlechter hinausgeht. Das dadurch produzierte Wissen kann als reparativ verstanden werden, da es einen anderen, weniger ausschließlich auf Machteffekte ausgerichteten Blick ermöglicht bzw. deren allumfassende Wirkmächtigkeit infrage stellt.« (Ebd.)

5.2.2 Queere Sicherheit

Anhand der bisher angestellten Überlegungen zu *Queer OS*, *QueerOS* und *Queer Computation* lässt sich folgern, dass die diskutierten Versuche, *Queer* und *Computation* zusammenzudenken, zwar an manchen Stellen über reparative Momente verfügen, aber dennoch in weiten Teilen durch die Unschärfen der Theo-

riebildung tendenziell eher in die gegenläufige Richtung zeigen. In allen diskutierten Texten ist eine Operationalisierung von Queerness zu beobachten, die von dem Wunsch getragen ist, Queerness und Informatik in einen Dialog zu bringen, dabei allerdings einen tatsächlichen Austausch verhindert, da beide als bereits denselben Rationalitäten angehörend, das heißt: denselben »Regeln und Prozessen« (Deuber-Mankowsky 2020, 135) folgend, gedacht werden. Diese unscharfe Vermengung führt, wie mit Deuber-Mankowsky argumentiert wurde, zu einer Bedeutungsverschiebung, an deren Ende entweder ein verkürztes Verständnis von *Queer/ness* oder von Technik steht. Das Insistieren der letzten beiden diskutierten Aufsätze, Queerness mit Muñoz (2009, 1) als zukünftig, als »not yet here«, als offene, utopische Zukünfte beinhaltend denken zu wollen, erweist sich damit als durch die Theoriebildung verstellt. Dabei wäre der Einsatz von Queerness als offen und Zukünfte ermöglichend, wie Muñoz (ebd., 12) selbst bemerkt, »aligned with what Sedgwick would call reparative hermeneutics.« Für den Erhalt von Queerness als offen gilt es also, eine ungenaue Übertragung von Konzepten zwischen Queer Theory und Informatik zu vermeiden – beide gehören differenten Bereiche der Wissensproduktion und damit getrennten Wissensordnungen an, die in einer »diskontinuierliche[n] Struktur« (Deuber-Mankowsky 2020, 136) verbunden sind. Unter Bezugnahme auf Sedgwick lässt sich an dieser Stelle noch hinzufügen, dass eine Vermengung beider Bereiche für das Einnehmen einer reparativen Perspektive nicht einmal notwendig ist. Mit Sedgwicks (2003, 124) Bemerkung, ein Verständnis für einen Sachverhalt »does not intrinsically or necessarily enjoin that person to any specific train of epistemological or narrative consequences«, soll an dieser Stelle zur eingangs gestellten Frage nach der Möglichkeit eines queeren, reparativen Sicherheitsbegriffs für die IT-Sicherheit zurückgekehrt werden.

Ein Verständnis für die Rationalität der technisch-informatischen Zusammenhänge, deren Wissensproduktion bereits mit Sedgwick als einer paranoiden Struktur folgend charakterisiert wurde, bedeutet auch, nicht per se an die »epistemological or narrative consequences« des IT-Sicherheitsdiskurses gebunden zu sein. Dies erlaubt es, die eingangs gestellte Frage noch einmal im Wortlaut aufzugreifen: (Wie) kann ein queerer Sicherheitsbegriff für die IT-Sicherheit in Stellung gebracht werden? Auf diese Frage soll basierend auf den bisherigen Überlegungen in drei Punkten geantwortet werden.

Erstens: Es kann nicht darum gehen, IT-Sicherheit mit einem queeren Sicherheitsbegriff neu zu konzeptualisieren, da die Funktionsweise von IT-Sicherheit, wie sie in der vorliegenden Untersuchung beschrieben wurde, ein

Produkt der Kryptologie und der Informatik ist, und bei allen problematischen Eigenschaften des paranoid strukturierten Diskurses nicht einfach anders gedacht werden kann. Ein solcher Versuch würde unweigerlich, wie in diesem Kapitel anhand von *QueerOS* und *Queer Computation* gezeigt wurde, eine Operationalisierung des queeren Sicherheitsbegriffs zur Folge haben, die zu vermeiden ist. Kurz: *Es kann nicht um eine technische Implementierung eines queeren Sicherheitsbegriffs gehen*.

Zweitens: *Statt über queere IT-Sicherheit nachzudenken, lohnt es sich eher, über queere Sicherheitspraktiken im Zusammenhang mit digitalen Kulturen nachzudenken*. Auf diese Weise wird der negative Sicherheitsbegriff der informatischen Logik der IT-Sicherheit als *Sicherheit vor* aufrechterhalten, und gleichzeitig anerkannt, dass das »anti-soziale und damit risikoreiche Moment« (Loick 2021, 278) digitaler Kulturen im Sinne einer »Dekonstruktion der strikten Opposition von Sicherheit und Unsicherheit, durch einen Platz für Negativität im Positiven« (ebd.), notwendiger Bestandteil des Lebens in und mit digitalen Kulturen ist, sowie die Voraussetzung dafür, Sicherheit überhaupt herstellen zu können. Das Wissen um die paranoide Strukturierung der IT-Sicherheit bedeutet damit weiterführend mit Sedgwick nicht, dass diese sich in den Nutzungspraktiken digitaler Medien fortsetzen muss, auch, wenn paranoide Strukturen, wie sie anmerkt, durchaus ansteckend sein können.

Dies führt zu Drittens: Der Verortung von queerer Sicherheit in Bezug auf IT-Sicherheit in den Denkweisen von Sicherheit in digitalen Kulturen, und damit den Umgangsweisen mit vernetzten Computern, und Technik im Allgemeinen. In Anlehnung an Loicks (ebd., 279) Ausführungen über von der queeren Community angesichts der AIDS-Krise entwickelten »konkrete[n] solidarische[n] Fürsorge- und Pflegetätigkeiten«, möchte ich an dieser Stelle vorschlagen, *solidarische Fürsorge- und Pflegepraktiken für das Leben in digitalen Kulturen und mit vernetzten Computern zu entwickeln*. Dies würde bedeuten, kein instrumentelles Technikverständnis zu veranschlagen, in dem (digitale) Medien als bloße Werkzeuge in Erscheinung treten, sowie anzuerkennen, dass das Leben in und mit Technik ebenfalls (System-)Pflegepraktiken beinhalten muss. Diese Fürsorgepraktiken entsprächen damit nicht den Praktiken von *Safe Hex*, die letztlich vereinzelnd wirken, da sie lediglich auf die Eigenverantwortung der User_innen rekurrieren. Stattdessen geht es um reparative, solidarische Praktiken, die unter anderem gekennzeichnet sind von gemeinsamen, unterstützenden (Ein-)Übungen von Nutzungsweisen, von Offenheit für Überraschungen, von anerkannten geteilten Verantwortlichkeiten, sowie davon, Neues auszuprobieren, mit Technik zu spielen, Infrastrukturen

gemeinschaftlich zu konzipieren, zu bauen und zu pflegen, und schließlich über die Anerkennung der Differenzen von Menschen und Maschinen der Unsicherheit, der Negativität, einen Platz in der Herstellung von Sicherheit einzuräumen.