3. IT-Sicherheit: Digitale Grenzaushandlungen

Im Jahr 2019 wurde in einer Online-Auktion ein Kunstwerk namens *The Persistence of Chaos* für 1,345 Millionen US-Dollar versteigert. Es handelt sich um einen vergleichsweise alten Laptop mit dem Betriebssystem *Windows XP*, der mit sechs verschiedenen Schadprogrammen aus den letzten Jahrzehnten bestückt ist: *ILOVEYOU*, *MyDoom*, *SoBig*, *DarkTequila*, *BlackEnergy* und *WannaCry* (vgl. mschf.xyz o.J.). Kreiert wurde *The Persistence of Chaos* von dem chinesischen Internetkünstler Guo O Dong in Zusammenarbeit mit einer New Yorker IT-Sicherheitsfirma namens *Deep Instinct*, die dabei behilflich war, den Laptop so zu konfigurieren, dass die Malware keinen weiteren Schaden außerhalb desselben anrichten kann (vgl. Dozier 2019). Dies erscheint, gemessen an den einzelnen Programmen, mehr als ratsam – Guo O Dong gibt auf der zum Kunstwerk gehörenden Webseite an, dass sich der durch alle sechs Programme zusammen erwirkte finanzielle Schaden auf 95 Milliarden US-Dollar belaufe (vgl. mschf.xyz o.J.). *The Persistence of Chaos* ist in mehrfacher Hinsicht ein spannendes Kunstobjekt: Zum einen stellt sich die Frage, wie es technisch überhaupt möglich ist, sechs verschiedene Malwares auf demselben Computer zu installieren, da einige der Schadprogramme die Funktionalität desselben bereits so stark beeinträchtigen dürften, dass eine normale Benutzung des Computers nicht mehr möglich sein sollte. Weiterhin sind die durch das Kunstprojekt und seine Situierung verhandelten Grenzbestimmungen bemerkenswert. Grenzbestimmungen, zu denen das Kunstwerk einlädt, und die gleichermaßen an dieses herangetragen werden, damit es als Ware zirkulieren kann. Für die nüchtern aufgeschlüsselten Bestandteile »Airgapped Samsung NC10-14GB 10.2-Inch Blue Netbook (2008), Windows XP SP3, 6 pieces of malware, power cord, restart script, malware« heißt es in den Verkaufsbedingungen:

> »The sale of malware for operational purposes is illegal in the United States. As a buyer you recognize that this work represents a potential security ha-

> zard. By submitting a bid you agree and acknowledge that you're purchasing this work as a piece of art or for academic reasons, and have no intention of disseminating any malware. Upon the conclusion of this auction and before the artwork is shipped, the computer's internet capabilities and available ports will be functionally disabled.« (Ebd.)

Die Schadsoftware muss also, den rechtlichen Rahmenbedingungen folgend, auf dem Laptop eingeschlossen und dadurch stillgestellt werden: *Dissemination* darf unter keinen Umständen geschehen – vom intendierten Eintritt in der Malware als Kunstobjekt in den Warenkreislauf einmal abgesehen. Der Laptop als »potential security hazard« evoziert damit das Bild der Büchse der Pandora, die nicht geöffnet werden darf. Um eine absichtliche Öffnung zu unterbinden und eine versehentliche Öffnung auszuschließen, wird vor der Versendung an den_die Käufer_in die Fähigkeit zur Konnektivität des Laptops zunichte gemacht. Zum einen, indem der Laptop »airgapped« versendet wird, er also nicht mehr mit dem Internet verbunden werden, und auch nicht über eine direkte Verbindung mit einem zweiten Computer mit dem Internet in Kontakt kommen kann. *Air Gaps* galten lange Zeit als Sicherheitsmechanismus, mit dem sich ungewollter Datenaustausch zuverlässig unterbinden lässt, und wurden sowohl für militärische als auch geheimdienstliche Zwecke eingesetzt, sowie in Hochsicherheitsanlagen kritischer Infrastruktur (vgl. Zetter 2014). Spätestens mit dem Erfolg von *Stuxnet*, einer Schadsoftware, die um die 2010er Jahre die Zentrifugen einer iranischen Urananreicherungsanlage beschädigte, die ebenfalls airgapped war, wurde (erneut) deutlich, dass Schadsoftware nicht nur über das Internet verbreitet werden kann, sondern auch über mobile Datenträger (vgl. ebd.). Konsequenter Weise wurden daher bei *The Persistence of Chaos* auch die Ports des Laptops zerstört, die einen Datenaustausch mittels mobiler Datenträger ermöglichen würden. Das Chaos darf also nur innerhalb des Laptops fortbestehen, dessen Grenzen als undurchlässig konfiguriert wurden.

3.1 Diskursive Ansteckungspotentiale

Die Abgrenzungen, Ein- und Ausschließungen von *The Persistence of Chaos* bieten eine Möglichkeit, den Faden der »xenophobe[n] Fortifizierungslogik«, und vor allem den Aspekt der »Nichtansteckung« (Loick 2021, 271), die kennzeichnend sind für einen negativen Sicherheitsbegriff, wieder aufzunehmen,

den Blick aber diesmal auf vernetzte Computer zu richten. Im vorangegangenen Kapitel wurde, mit Fokus auf die Verschlüsselung und Übertragung von Nachrichten, der Sicherheitsbegriff der Kryptologie als negativer Sicherheitsbegriff bestimmt. Grundlegend für diesen vom technisch-postalischen Übertragungsmodell von Kommunikation informierten Sicherheitsbegriff ist im Fall der Kryptologie vor allem die Konzeptionalisierung des unsicheren Kanals als Übertragungsmedium einer Nachricht, die auf ihrem Weg der Gefahr eines *störenden Dritten* ausgesetzt ist. Die von der Kryptologie eingesetzte Lösung dieses Problems ist die Schaffung eines sicheren Kanals durch die Verschlüsselung der Nachricht, wodurch die Gefahr des *störenden Dritten* gebannt scheint. Eine solche Konzeptionalisierung von Sicherheit bestimmt Kommunikation als Informationsaustausch, der sich im Versenden und Empfangen einer Nachricht ereignet. Kommunikation hat damit einen klar definierten Anfang und ein klar definiertes Ende, und wird innerhalb der Kryptologie weitestgehend isoliert von anderen medialen Zusammenhängen betrachtet, insofern die Regulierung der Medialität von Kryptographie innerhalb digitaler Medien die Anschlussstellen zu diesen standardisiert.

Gemäß der zuvor eingezogenen Aufteilung der Anwendungsbereiche von Kryptographie, schließt das vorliegende Kapitel mit einer Diskussion von Sicherheit vernetzter IT-Systeme abseits von Kommunikationsprozessen menschlicher Akteur_innen an, denn mit der bereits skizzierten Entstehung des ARPANET Ende der 1970er Jahre veränderte sich nicht nur die Kommunikation zwischen Menschen, sondern begannen auch Maschinen jenseits menschlicher Lesbarkeiten und Handlungen miteinander zu kommunizieren. In den 1980er Jahren ereigneten sich einige technische Weiterentwicklungen auf dem Gebiet vernetzter digitaler Medien: So wurde unter anderem mit dem Adressvergabesystem IPv4 (vgl. Postel 1981a) sowie dem Transmission Control Protocol (TCP, vgl. Postel 1981b) die Grundlage für das heutige Internet gelegt, sowie durch günstigere und effizientere Hardware Mainframe-Computer Schritt für Schritt kleiner, bis sie schließlich in den 1990er Jahren zu Personal Computern (ggf. mit Internetanschluss) wurden. Gleichzeitig entstanden die ersten Sicherheitsprobleme vernetzter Computer: Computerviren, -würmer und -trojaner, wurden (mal mehr, mal weniger) kontrolliert durch die Leitungen gesendet, sowie theoretisch aufgearbeitet (vgl. exemplarisch Cohen 1987; Spafford 1994; Spafford 1989). Die 1990er Jahre waren sowohl von dem Einzug der Personal Computer in Privathaushalte als auch von der Vernetzung derselben über das Internet gekennzeichnet (vgl. Sprenger/Engemann 2015a, 10–11). Was zunächst ein aktives Sich-Einwählen und eine kabelgebundene

Ethernetverbindung voraussetzte, wurde in den darauffolgenden Jahren zu einer kabellosen Technologie, in der alle netzwerkfähigen Geräte immer online sind, oder es zumindest qua Design[1] sein sollen. Mit dieser dauerhaften Konnektivität trat ein neues Problem auf: Der *unsichere Kanal*, auf den sich die Herstellung von Sicherheit in der Kryptologie bezieht, hat sich vervielfältigt und verstetigt – unsichere Kanäle umgeben die einzelnen Maschinen, die in einem ständigen Austausch miteinander stehen – und eine Verschlüsselung des Informationsaustauschs von Computern untereinander ist nicht gegeben. Die umfassende Vernetzung skaliert darüber hinaus Sicherheitsprobleme in vernetzten Umgebungen, wie beispielsweise Computerviren, -würmer und -trojaner auf ungekannte Ausmaße (vgl. Krämer 2008, 146), wovon nicht zuletzt *The Persistence of Chaos* zeugt. Die Eckpfeiler der zu erzählenden Geschichte der IT-Sicherheit wären allerdings mit einem Blick, der sich nur auf die technischen Entwicklungen der letzten Jahrzehnte richtet, unzureichend umrissen. Die 1980er Jahre, die sich als formative Phase für die Herausbildung der IT-Sicherheit bestimmen lassen, waren in den USA darüber hinaus maßgeblich von der Zuspitzung des Kalten Kriegs, Ronald Reagans Präsidentschaft sowie der AIDS-Krise geprägt (vgl. Deuber-Mankowsky 2017b, 15–16), die an dieser Stelle im Sinne einer Grundlage für die folgenden Ausführungen skizzenhaft dargestellt werden soll.

1981 wurde an der Westküste der USA zum ersten Mal AIDS diagnostiziert,[2] allerdings zunächst unter einem anderen Namen. Nach dem Tod von fünf, dem damaligen Wissensstand entsprechend nicht vorerkrankten Personen in Los Angeles durch eine Pneumocystis-Pneumonie, wurde in einer Veröffentlichung der Centers for Disease Control[3] (kurz: CDC) die scheinbar einzige Gemeinsamkeit der Toten genannt, und gleichsam als möglicher Auslöser der Krankheit suggestiv hervorgehoben: alle Verstorbenen waren

1 Diese Entwicklung wird im Spannungsfeld der Schlagwörter *ubiquitous computing* und *Internet der Dinge* verhandelt. Weiterführend dazu siehe Sprenger und Engemann (2015b).

2 Der Autor und Aktivist Theodore Kerr weist in einem Gespräch mit der Filmemacherin und Aktivistin Alexandra Juhasz darauf hin, dass das HI-Virus bereits seit Beginn des 20. Jahrhunderts in Kamerun, und bereits seit den späten 1960er Jahren in den USA zirkulierte: »There are lived experiences of HIV well before 1981, but these occur outside of discourse. Even so, a then-unnamed illness impacts individuals and communities.« Diese Phase bezeichnet Kerr treffend als »AIDS before AIDS« (Juhasz/Kerr 2020).

3 Die Centers for Disease Control sind eine Behörde des US-amerikanischen Gesundheitsministeriums.

homosexuelle Männer (vgl. Treichler 1987, 276). Noch im selben Jahr wurden die Tode weiterer homosexueller Männer an seltenen, aber normalerweise nicht tödlich verlaufenden Krankheiten auf einen Zusammenbruch des Immunsystems zurückgeführt, aufgrund dessen der Körper nicht mehr in der Lage war, sich adäquat gegen diese Infektionen zu schützen, und das diagnostizierte Syndrom mit dem Akronym *GRID* bezeichnet: *Gay-Related ImmunoDeficiency* (vgl. ebd., 277). Erst nachdem im darauffolgenden Jahr dasselbe Krankheitsbild nicht mehr ausschließlich bei homosexuellen Männern, sondern unter anderem auch bei heterosexuellen Personen diagnostiziert wurde, wurde *GRID* durch die Bezeichnung *AIDS* ersetzt: *Acquired Immune Deficiency Syndrome* (vgl. ebd.). 1984 wurde HIV als Auslöser von AIDS festgestellt (vgl. Deuber-Mankowsky 2017b, 14). Was sich an dieser Stelle durch die Knappheit der Aufzählung als eine Fortschrittsgeschichte wissenschaftlicher Objektivität missverstehen lassen könnte, ist alles andere als das. Wie Paula Treichler in ihrem Aufsatz *AIDS, homophobia and biomedical discourse. An epidemic of signification* darlegt, handelt es sich beispielsweise bei der Ersetzung von GRID durch AIDS nicht um eine Bereinigung des Wissenschaftsdiskurses von homophoben Vorurteilen, werden nicht ›unwissenschaftliche‹ Vorurteile durch ›neutrale wissenschaftliche Fakten‹ ersetzt. Vielmehr unterstreicht Treichler (1987, 266–267),

> »that no clear line can be drawn between the facticity of scientific and non-scientific (mis)conceptions. Ambiguity, homophobia, stereotyping, confusion, doublethink, them-versus-us, blame-the-victim, wishful thinking: none of these popular forms of semantic legerdemain about AIDS is absent from biomedical communication.«

Was AIDS *ist*, so Treichlers zentrales Argument, ist ein anhaltender gesellschaftlicher Aushandlungsprozess zwischen den materiellen Aspekten der Krankheit und den (möglichen) Bedeutungen, die diesen zugewiesen werden. AIDS, so schreibt sie, »with its genuine potential for global devastation – is simultaneously an epidemic of a transmissible lethal disease and an epidemic of meanings or signification« (ebd., 263–264). AIDS als *epidemic of signification*[4] zeigt sich also in den (bis heute andauernden) mannigfaltigen

4 Es entbehrt nicht einer gewissen Absurdität, dass das Manuskript des vorliegenden Buchs während der Covid-19-Pandemie fertiggestellt wurde, zu deren Beginn Tedros Adhanom Ghebreyesus, der Direktor der WHO, vor einer *Infodemie* warnte (vgl. The Lancet Infectious Diseases 2020). Ghebreyesus' Anliegen wird zumeist darauf bezo-

Versuchen der Sinnproduktion, die sich an den beobachtbaren Elementen der Krankheit entzünden, und von absurd wirkenden Deutungen wie AIDS sei »[a]n Andromeda strain with the transmission efficiency of the common cold« über etwas nüchternere wie »[t]he most urgent and complex public health problem facing the world today« bis hin zu homophoben Deutungen wie »[a] gay plague, probably emanating from San Francisco« oder »[t]he price paid for anal intercourse« (ebd., 264–265) reichen.

Die bisher genannten, wenigen Beispiele für homophobe Formen der Wissens- und Sinnproduktion über AIDS sind symptomatisch für die »offene Homophobie [der] konservativ-neoliberalen Politik« (Deuber-Mankowsky 2017b, 16) der Reagan-Regierung und großer Teile der Bevölkerung, die sich darüber hinaus auch in Schweigen und Passivität manifestierte: In den nicht in die Wege geleiteten Maßnahmen zum Schutz der Bevölkerung, wie beispielsweise konzentrierter Forschung über die neue Krankheit und der schnellen Entwicklung von Therapiemöglichkeiten, in der nicht erfolgten Aufklärung über die Ansteckungswege durch öffentliche Behörden, sowie in den spärlichen oder falschen Informationen über und Framings von AIDS in den Medien (vgl. Crimp 1987b; Bersani 1987, 202). Was aus der medialen Berichterstattung dafür umso deutlicher hervorging, wie Leo Bersani (ebd.), darlegt, waren »heterosexual anxieties«: Angst vor Homosexualität und homosexuellen Personen, Angst vor AIDS, und den Zusammenhängen und Ansteckungspotentialen, die diesen zugeschrieben wurden. So wurde AIDS »zu einer Strafe und Homosexualität zu einer Sünde erklärt« (Deuber-Mankowsky 2017b, 16), und es entstand eine Epidemie gewaltigen Ausmaßes. Eine ausführliche und

gen, die Erkenntnisse der Wissenschaft umsichtig zu kommunizieren. So sollen in medialer Berichterstattung keine Erkenntnisse aus Pre-Print-Aufsätzen, die noch nicht den gängigen wissenschaftlichen Standards zur Qualitätssicherung unterzogen wurden, als Fakten geframed werden, und den in Sozialen Netzwerken entstehenden und verbreiteten Falschinformationen wiederum mit wissenschaftlicher Klarheit und angepassten Kommunikationsstrategien begegnet werden (vgl. Zarocostas 2020). Diese Auslegung des Begriffs Infodemie setzt eine mit Neutralität gleichbedeutende Objektivität von Wissenschaft voraus und positioniert diese gleichermaßen als gesellschaftlichen Zusammenhängen äußerlich, was sich mit Treichler als unzutreffend kritisieren lässt. Einzig in der zu Beginn der Pandemie thematisierten Namensgebung des neuen Virus, bei der Bezeichnungen, die die Zugehörigkeit zu bestimmten bereits bekannten Virenstämmen wie »SARS-CoV-2« oder »CoVid-19« gegenüber ortsbezogenen Namen wie etwa »Wuhan Virus« bevorzugt wurden, um Diskriminierung zu vermeiden, wurde ein direkter Anknüpfungspunkt an Treichlers Argumentation erkennbar (vgl. Webel 2020).

in ihrer Klarheit und Stärke bewundernswerte Dokumentation, Analyse und Kritik dieser Verhältnisse stellt die 43. Ausgabe des Journals *October* aus dem Jahr 1987 mit dem Schwerpunkt *AIDS: Cultural Analysis/Cultural Activism* dar, in deren Einleitung Douglas Crimp (1987b, 13) eindringlich auf die verschiedenen Ebenen des Schweigens hinweist, die die AIDS-Krise kennzeichnen:

> »The ignorance and confusion enforced by government and the dominant media; the disenfranchisement and immiseration of many of the people thus far hardest hit by AIDS; and the psychic resistence [sic!] to confronting sex, disease, and death in a society where those subjects are largely taboo – all of these conditions must be faced by anyone doing work on AIDS.«

In diesem Zitat lässt sich auch ein weiterer Punkt ausmachen: die Zuspitzung biopolitischer Aushandlungen darüber, wessen Leben betrauerbar ist, und wessen Leben dadurch als schützenswert gilt, und wer »dem Sterben überantwortet« (Deuber-Mankowsky 2017b, 16) wird. Zu Beginn der 1980er Jahre wurde AIDS auch als »4-H disease« bezeichnet, die in erster Linie »homosexuals, heroin addicts, hemophiliacs, and Haitians« (Gilman 1987, 87) treffen würde. Diese Teile der Bevölkerung wurden somit zu sogenannten Risikogruppen erklärt, was allerdings nicht dazu führte, dass sie verstärkt geschützt wurden, sondern dass der Rest der Bevölkerung besonders *vor ihnen* geschützt werden sollte. An dieser Stelle tritt, wie Deuber-Mankowsky (2017b, 16) ausführt, die Verflechtung von Homophobie mit Rassismus, Sexismus und, wie an dieser Stelle mit Bersani (1987, 201) ergänzt werden kann, auch *class*, deutlich hervor, denn gegen diese vier (sich teilweise überschneidenden) Gruppen richteten sich gesellschaftliche Ausschlussmechanismen im Besonderen.[5] Mit Bersani (ebd., 199) lässt sich weiterhin feststellen, dass diese Gruppen nicht nur durch Passivität dem Sterben überantwortet wurden, sondern auch physischer Gewalt und Angriffen ausgesetzt waren:

> »Doctors have refused to operate on people known to be infected with the HIV virus [sic!], schools have forbidden children with AIDS to attend classes, and recently citizens of the idyllically named town of Arcadia, Florida, set fire to the house of a family with three hemophiliac children apparently infected with HIV.«

5 Für eine weiterführende, detaillierte Analyse der Diskursivierung von HIV, AIDS und Homosexualität in Printmedien und Fernsehen siehe Watney (1996).

Bersani führt noch einige weitere Beispiele für diese Formen von Gewalt an, die sich gegen Personen mit HIV und AIDS richten, und zeichnet die Verschiebungen nach, anhand derer die als zu einer der benannten Risikogruppen zugehörig gelesenen Personen, vor allem homosexuelle Männer, zu bereits angesteckten, infizierten und potenziell infizierenden Personen gemacht, und damit auch derselben Gewalt ausgesetzt wurden. Diese Situation reflektierend, schreibt er in seinem Aufsatz *Is the Rectum a Grave?*, der ebenfalls Teil der erwähnten Ausgabe des Journals *October* ist: »[…] given the nature of that starting point, analysis, while necessary, may also be an indefensible luxury. […] it is also important to say that, morally, the only *necessary* response to all of this is rage.« (Ebd., 200–201, Herv. i.O.) Und dennoch schreibt er, nimmt er eine Analyse vor, die ebenso eine Kritik dieser Verhältnisse ist, und gekennzeichnet von dem Wunsch nach einem besseren (Zusammen-)Leben und der Offenheit von Zukünften. Bersanis Aufsatz, die anderen Beiträge der *October*-Ausgabe, ebenso wie weitere Schriften der von HIV, AIDS und/oder der mit der AIDS-Krise einhergehenden Gewalt Betroffenen, lassen sich damit, Douglas Crimp (1987b, 7) folgend, als »cultural practices actively participating in the struggle against AIDS« begreifen.

Ein weiteres Beispiel solcher kulturellen Praktiken sind Performances und Kunstprojekte, die im Kontext der Widerstandsbewegung ACT UP (»AIDS Coalition to Unleash Power«) entstanden sind, aber auch ACT UP selbst. 1987 gegründet, war es das Ziel der Mitglieder, »›to act up‹, sich aufzulehnen, rauszugehen und im doppelten Sinn des Wortes Theater zu machen« (Deuber-Mankowsky 2017b, 14–15). Die Bewegung versteht sich selbst, wie Crimp (1987b, 7) anhand der Worte dokumentiert, mit denen die montagabendlichen Treffen eröffnet werden, als »a nonpartisan group of diverse individuals united in anger and committed to direct action to end the AIDS crisis.« Die Mitglieder von ACT UP organisierten Kunstausstellungen und Demonstrationen, führten Interventionen im öffentlichen Raum durch und leisteten Aufklärungsarbeit (vgl. Crimp 1987b), um AIDS zu politisieren und gegen die intersektional strukturierte Diskriminierung vorzugehen. Einen wichtigen Teil der Aufklärungsarbeit, aber auch der Selbstermächtigung Betroffener, machten audiovisuelle (Selbst-)Dokumentationen aus. Tragbare Videokameras mit eingebautem Videorekorder wurden ab 1983 verkauft, und wurden zum elementaren Bestandteil der ACT UP-Bewegung (vgl. Deuber-Mankowsky 2017b, 17). »Das Ziel des Video-Aktivismus war,«, führt Deuber-Mankowsky (ebd., 19) aus, »Menschen mit AIDS zu ermöglichen, sich selbst beim Machen von Geschichte zusehen zu können. Sie sollten sich nicht als

Opfer und als passiv wahrnehmen, sondern als Aktivist_innen.« So dokumentierten die Aktivist_innen, wie es war, mit HIV zu leben, an AIDS zu leiden oder zu sterben, oder geliebte Menschen mit der Krankheit zu begleiten, zu pflegen oder an diese zu verlieren, gegen die Politik und die Pharmaindustrie zu demonstrieren etc. Diese Aufnahmen richteten sich gegen »mainstream phobic portrayals of those with AIDS as pitiable victims, damnable threats, and as alone and *dying*« (Cifor/McKinney 2020, Herv. i.O.), ebenso wie gegen verbreitete Falschinformationen zu den Übertragungswegen von HIV und das Schweigen. Deuber-Mankowsky (2017b, 20) fasst pointiert zusammen: »Medien der Dokumentation, die Bild- und Tonerfassung, deren Bearbeitung und Distribution waren Teil der Politisierung von AIDS und sie waren Teil des Alltags mit AIDS.«[6]

Thematisch mit HIV und AIDS befasste medienwissenschaftliche Analysen, bemerken Marika Cifor und Cait McKinney (2020) in ihrem Aufsatz *Reclaiming HIV/AIDS in digital media studies*, konzentrieren sich zumeist auf audiovisuelle Phänomene.[7] Dies mag aufgrund der Bedeutung von Camcordern und der audiovisuellen (selbst-)dokumentarischen Praktiken der ACT UP-Bewegung nicht verwunderlich erscheinen. Dass digitale Medien in Bezug auf die AIDS-Krise oftmals als »unique format, site, or subject of study« (ebd.) von derselben getrennt betrachtet worden seien, hingegen schon – denn, so formulieren es Cifor und McKinney (ebd.), »AIDS, computing, and the Internet grew up together.« Diese Felder verbindet mehr als nur ein zeitlicher Zusammenfall: »HIV and digital media share a set of core concerns«, führen sie weiter aus, zu dem unter anderem »virality, risk, privacy, surveillance, and embodiment, to name a few« (ebd.) gehören. Die weitestgehende Absenz medienwissenschaftlicher Forschung zum Zusammenhang von AIDS und digitalen Kulturen sehen Cifor und McKinney (ebd.) als »part of a larger structural process of HIV stigma and abandonment – a cultural process that is classed, racialized, and gendered in the context of an ongoing epidemic driven by structural oppressions, from poverty to incarceration to xenophobia.« Ihren

6 Aus diesen Praktiken der (Selbst-)Dokumentation entwickelte sich schließlich, wie Deuber-Mankowsky (2017b, 14) unter Bezugnahme auf dessen Namensgeberin B. Ruby Rich darlegt, Anfang der 1990er Jahre das sogenannte *New Queer Cinema*. Für einen Überblick sowohl über die Entstehungsgeschichte als auch eine Diskussion des *New Queer Cinema* in Verschränkung mit dem Konzept des Post-Cinema, siehe Deuber-Mankowsky (2017b).

7 Cifor und McKinney (2020) betrachten für ihren Aufsatz ausschließlich Publikationen aus dem nordamerikanischen Raum.

Aufsatz verstehen Cifor und McKinney (ebd.) als einen »call to action«, dem ich gerne nachkomme, wenn auch vielleicht nicht in der Weise, die die beiden Autor_innen intendiert haben. Im Folgenden geht es weniger um Praktiken der (Selbst-)Dokumentation, des Archivs oder von Aktivismus in und mit digitalen Medien, sondern eher um eine Grundlagenarbeit für die von Cifor und McKinney eingeforderten medienwissenschaftlichen Auseinandersetzungen mit der gemeinsamen Geschichte von HIV, AIDS und digitalen Medien, oder anders formuliert: mit ihren diskursiven Ansteckungspotentialen. Das vorliegende Kapitel nimmt den Status der Übertragungen von Konzepten aus der HIV/AIDS-Forschung in die Informatik, und die damit entstandenen Politiken der Herstellung von Sicherheit in den Blick: Welcher Sicherheitsbegriff wurde in die Informatik übertragen und informiert die IT-Sicherheit? Welche Konsequenzen bringt dies mit sich?

3.2 Zwei Fallbeispiele von Ransomware

Über die Bedeutung der in den 1980er Jahren beginnenden AIDS-Krise für digitale Kulturen und ihren Zusammenhang mit IT-Sicherheit lässt sich wohl am naheliegendsten anhand von Computer*viren* nachdenken. Während Cifor und McKinney (2020) vor allem für die nordamerikanische medienkulturwissenschaftliche Publikationslandschaft diesbezüglich ein Manko diagnostizieren, wurden außerhalb derselben einige Überlegungen zu diesem Themenbereich veröffentlicht. Die umfangreichste Analyse dieser Verschränkung legt der finnische Medienwissenschaftler Jussi Parikka (2016) mit *Digital Contagions: A Media Archaeology of Computer Viruses* vor. Parikka nähert sich dem Zusammenhang von biologischen und informatischen Viren über eine medienarchäologische Herangehensweise, und bespricht nicht nur den Zusammenhang der AIDS-Krise mit der Herausbildung von IT-Sicherheit, sondern darüber hinaus auch die Diskursivierung von Computerviren als *Artificial Life* unter den Vorzeichen der Medienökologie.[8] Die australische Soziologin Deborah Lupton geht in ihrem Aufsatz *Panic computing: The viral metaphor and computer technology* (1994) darauf ein, inwiefern die Übertragung von Viralitätskonzepten, die im Zusammenhang mit der AIDS-Krise

8 Siehe dazu auch Parikkas (2005) Artikel *The Universal Viral Machine. Bits, Parasites and the Media Ecology of Network Culture.*

entstanden sind, gesellschaftliche Vorstellungen von Computernutzung prägen. Ausnahmen aus dem US-amerikanischen Raum stellen sowohl Stefan Helmreichs (2000) Aufsatz *Flexible Infections: Computer Viruses, Human Bodies, Nation-States, Evolutionary Capitalism* dar, in dem Helmreich die Sprache des IT-Sicherheitsdiskurses untersucht, und sowohl Zusammenhänge zu AIDS als auch zu weiteren körperbezogenen Grenzverhandlungen[9] wie beispielsweise der des Nationalstaates und seiner Außengrenzen im Fall eines Krieges nachweist; sowie Cait McKinney und Dylan Mulvins (2019) Aufsatz *Bugs: Rethinking the History of Computing*, in dem die Rolle der Diskursivierung von Computersicherheit mittels Metaphern aus dem HIV/AIDS-Diskurs für die mit dem Einzug von Computern in Privathaushalte verbundenen Aushandlungsprozesse untersucht wird. Im deutschsprachigen Kontext finden sich Bearbeitungen des Zusammenhangs von biologischen und informatischen Viren bei Sybille Krämer (2008), die in *Medium, Bote, Übertragung: Kleine Metaphysik der Medialität* anhand des Zusammenhangs der beiden Arten von Viren sowie des Ansteckungsvorgangs Erkenntnisse über das Konzept der Übertragung entwickelt; und auch bei Brigitte Weingart (2002), die in *Ansteckende Wörter. Repräsentationen von AIDS* ebenfalls kurz auf Computerviren zu sprechen kommt. Darüber hinaus enthält auch der von Brigitte Weingart gemeinsam mit Ruth Mayer herausgegebene Sammelband *Virus! Mutationen einer Metapher* zwei Aufsätze, die die Gemeinsamkeiten und Unterschiede biologischer und informatischer Viren besprechen (vgl. Knight 2004; Schmundt 2004).

Die vorliegende Untersuchung wird sich der Verflochtenheit von HIV, AIDS und digitalen Medien ebenfalls über Computerviren nähern, aber zusätzlich das in den genannten Publikationen unbeachtet gebliebene Phänomen der *Ransomware* in den Fokus rücken, das es erlaubt, in diesen Zusammenhang auch die Entwicklung der Kryptographie mit einzuflechten. Der Name *Ransomware* bezeichnet eine Sorte Schadsoftware, »which demands a payment in exchange for a stolen functionality« (Gazet 2010, 77), die also einen gegebenen Computer in einer Weise verändert, dass er nicht mehr zu verwenden ist, oder die auf ihm gespeicherten Dateien nicht mehr intakt sind, und mittels derer versucht wird, ein Lösegeld für die Wiederherstellung des Geräts/der Daten zu erpressen. Im Folgenden wird zunächst anhand einer

9 Der Zusammenhang von Kriegsmetaphern, Biologie und IT-Sicherheit wird hier nicht weiter ausgeführt. Weiterführend zu Krieg und Biologie siehe Haraway (1991b), und zu Krieg, Biologie und IT-Sicherheit Parikka (2016).

der in *The Persistence of Chaos* enthaltenen Schadsoftware namens *WannaCry* die Funktionsweise von Ransomware genauer erläutert sowie Ransomware als Phänomen situiert. Anschließend wird anhand des ersten dokumentierten Falls von Ransomware aus dem Jahr 1989, dem sog. *AIDS Information Trojaner*, die Verflechtung von Ransomware mit HIV und AIDS nachgewiesen. Im weiteren Verlauf des Kapitels wird auf einen Teilbereich der Kryptologie mit dem Namen *Kryptovirologie* eingegangen, die die technische Brücke zwischen dem *AIDS Information Trojaner* und *WannaCry* bildet, aber auch die Kryptographie in die von zweierlei Arten von Viren informierten Grenzaushandlungen der IT-Sicherheit einbindet.

3.2.1 *WannaCry*

> »The more Microsoft solidifies its global monopoly, the greater the chance for a single software exploit to bring down the entire grid. The more global health networks succeed in wiping out disease, the greater the chance for a single mutant strain to cause a pandemic.« (Galloway/Thacker 2007, 17)

Im Mai 2017 beschädigte eine Cyberattacke, die unter dem Namen *WannaCry*[10] bekannt wurde, innerhalb von wenigen Stunden mindestens 200.000 Computer in über 150 Ländern (vgl. Whittaker 2019).[11] Betroffen waren ausschließlich Computer mit dem Betriebssystem *Microsoft Windows*, da *WannaCry* eine betriebssystemspezifische Sicherheitslücke ausnutzte. Im Fall eines geglückten Angriffs wurde die Festplatte verschlüsselt, sodass Nutzer_innen aus ihren eigenen Computern ausgesperrt wurden, und nur noch eine Nachricht sahen, in der sie darüber informiert wurden, dass der Zugang zu ihren Dateien durch die Zahlung eines Lösegeldes in der pseudonymen Kryptowährung *Bitcoin* wiederhergestellt werden könne – jegliche andere Interaktion mit dem Computer war nicht mehr möglich. *WannaCry* hat nicht nur die Computer von Privatpersonen getroffen, sondern auch Computernetzwerke größerer Firmen überall auf der Welt, von der *Deutschen Bahn* über *FedEx*, und auch die Mehrheit der Krankenhäuser Großbritanniens, wodurch ein mehrere Tage andauernder Engpass in der Gesundheitsversorgung entstand (vgl. Briegleb 2017; Cameron

10 Die Software hat mehrere ähnlich klingende Namen, wie beispielsweise *WanaDecrypt0r 2.0* (vgl. Briegleb 2017) oder *WanaCrypt0r* (vgl. Khomami/Solon 2017), firmiert aber zumeist unter dem sprechenden Namen *WannaCry*.

11 Die genaue Zahl lässt sich schwer bestimmen, Angaben reichen von 200.000 (vgl. Perekalin 2017) bis zu »hundreds of thousands of computers« (Whittaker 2019).

2017): Die Krankenhäuser[12] verloren nicht nur den Zugang zu Patient_innendaten, sondern waren darüber hinaus auch nicht in der Lage, Behandlungen fortzuführen, da einige medizinische Geräte, die beispielsweise zur Verabreichung von Chemotherapie verwendet werden, über ein *Windows*-basiertes Betriebssystem verfügen (vgl. Fox-Brewster 2017; Marsh 2017).

Entgegen der medialen Berichterstattung ist *WannaCry* kein Virus, sondern ein Wurm, genauer: *WannaCry* wird als *ransomware cryptoworm* klassifiziert (vgl. Chua 2017), da sich die Software autonom über das Internet verbreitet und die Schadensroutine aus der Verschlüsselung sowie einer Lösegeldforderung zusammengesetzt ist. Die Software selbst besteht aus zwei Teilen: Einem Exploit[13] und einer Verschlüsselungsvorrichtung (vgl. Perekalin 2017). Der verwendete Exploit, mit dem *WannaCry* sich über ein gegebenes Netzwerk verbreitet und andere Systeme ›infiziert‹, heißt *EternalBlue* und nutzt eine Schwachstelle im *Windows Server Message Block-Protokoll* (kurz: SMB) aus. SMB ist ein Protokoll innerhalb des Applikationsschichtennetzwerks, mit dem Dateien oder Drucker innerhalb eines lokalen Netzwerks freigegeben und geteilt werden können. Dies ist aus zwei Gründen bemerkenswert: Erstens war *EternalBlue* der NSA zum Zeitpunkt des Angriffs bereits seit mindestens fünf Jahren bekannt (vgl. Nakashima/Timberg 2017), war aber nicht publik gemacht worden, um diese Sicherheitslücke weiter ausnutzen zu können (vgl. Wong/Solon 2017).[14] Erst als eine Hacker_innengruppe, die sich als *The Shadow Brokers* bezeichnet, den Exploit von der NSA stahl, informierte die NSA *Microsoft* über die Existenz von *EternalBlue*, woraufhin *Microsoft* im März 2017 einen Patch für die Sicherheitslücke im SMB veröffentlichte (das MS17-010 security bulletin, vgl. Goodin 2017; Microsoft 2017). Genau einen Monat später, am 14. April 2017, veröffentlichten *The Shadow Brokers EternalBlue* für alle zugänglich im Internet (vgl. Wong/Solon 2017). Computer von Nutzer_innen, die *Microsofts* Sicherheitspatch nicht installiert hatten, oder

12 Tatsächlich war der Gesundheitssektor bereits vor *WannaCry* die am stärksten von Ransomware betroffene Branche (vgl. Shah/Farik 2017).

13 Als Exploit wird eine Software bezeichnet, die speziell dafür geschrieben wurde, eine bestimmte Sicherheitslücke auszunutzen.

14 *EternalBlue* fällt damit in die sog. »NOBUS«-Kategorie der NSA. Das Akronym wird mit »nobody but us« aufgelöst und bezeichnet Sicherheitslücken, von deren Existenz nur die NSA weiß, und/oder die aufgrund der benötigten finanziellen und/oder technischen Ressourcen nur die NSA ausbeuten kann, die diese nicht meldet, um sie weiterhin ausnutzen zu können (vgl. Peterson 2013).

ältere, offiziell nicht mehr unterstütze Versionen von *Microsoft Windows* verwendeten, blieben angreifbar.[15] Zweitens, da es sich bei *WannaCry*, wie bereits erwähnt, streng genommen um eine Wurmsoftware handelt. Der Unterschied von Virus und Wurm ist in diesem Zusammenhang nicht unbedeutend: Ein Computervirus ist an Programme oder Betriebssysteme ›angeheftet‹ wie an einen ›Host‹ oder ›Wirt‹, und kann nicht unabhängig von diesen laufen. Ist beispielsweise ein Computervirus in einem Word-Dokument enthalten, so richtet er keinen Schaden an, und kann sich auch nicht verbreiten, solange das Dokument nicht geöffnet wird. Ein Wurm hingegen kann sich unabhängig von einer Aktivierung durch andere Programme von einem Gerät auf ein anderes kopieren, sowie unabhängig von einem Host-Programm ausgeführt werden, was auch bedeutet, dass er unabhängig von User_inneninteraktion mit einem gegebenen Computer ist (vgl. Spafford 1989, 448). Die Nutzung von *EternalBlue* ermöglichte dem Wurmprogramm eine schnelle Verbreitung über das SMB-Protokoll innerhalb lokaler Netzwerke: Loggt sich ein mit *WannaCry* ›infizierter‹ Computer beispielsweise in einem Firmennetzwerk ein, so kann *WannaCry* sich über das SMB-Protokoll ohne weiteres Zutun verbreiten und alle anderen Computer im selben Netzwerk ›anstecken‹. *WannaCry* verbreitete sich allerdings auch über lokale Netzwerke hinaus, indem die Software zufällige IP-Adressen im Internet ansteuerte (vgl. Mackenzie 2019). Aufgrund der Verbreitungswege, aber auch der Eigenständigkeit des Wurmprogramms waren die üblicherweise empfohlenen Verhaltensweisen von User_innen zum Schutz vor Schadsoftware, wie beispielsweise keine unerwartet erhaltenen oder verdächtig aussehenden E-Mail-Anhänge zu öffnen, oder bestimmte Webseiten zu meiden, um sich vor sog. *Drive-by-Downloads*[16] zu schützen, im Fall von *WannaCry* wirkungslos. Ist ein Computer ›infiziert‹, lädt *WannaCry* die Verschlüsselungskomponente aus dem Internet herunter und beginnt damit,

15 Dies war, auch wenn es sich dabei um einen vergleichsweise geringen Anteil der befallenen Computer handelt, besonders problematisch im Fall von Microsoft Windows XP – einer älteren Windows-Version, die seit einigen Jahren offiziell nicht mehr unterstützt wird und für die es daher zunächst auch keinen Patch gab. Da Windows XP aber oftmals von Firmen genutzt wird, veröffentlichte Microsoft schlussendlich doch noch einen Patch für Windows XP (vgl. Warren 2017). Statistisch am häufigsten betroffen waren Computer mit dem Betriebssystem Windows 7 (vgl. Brandom 2017).

16 Als *Drive-by-Download* wird ein von User_innen unbemerkt ablaufender Download, meist von Schadsoftware, bezeichnet. Ein solcher Download wird durch Sicherheitslücken in Webbrowsern möglich, die von auf einer entsprechenden Webseite hinterlegten Skripten ausgenutzt werden (vgl. Hifinger 2019).

die Festplatte zu verschlüsseln. Diese Verschlüsselung kann nicht durch eine dritte Partei gebrochen werden,[17] da die Schadsoftware eine Kombination aus symmetrischer und asymmetrischer Kryptographie verwendet, was die Zahlung des Lösegelds als einziges Mittel erscheinen lässt, mit dem man im besten Fall den Zugang zu den eigenen Dateien wiedererlangt.[18]

Genauso plötzlich wie *WannaCry* sich verbreitete, kam diese Verbreitung zunächst zu einem Stopp: Der britische IT-Sicherheitsforscher Marcus Hutchins bemerkte bei der Analyse des Codes der Schadsoftware, dass diese stets vor Beginn des Verschlüsselungsvorgangs eine Domain namens https://www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com ansteuerte. Hutchins fiel weiterhin auf, dass diese Domain noch nicht registriert war. Er registrierte sie, in der Hoffnung, durch eine Beobachtung der dort eintreffenden Anfragen ein genaueres Bild von der Verbreitung der Schadsoftware zu erhalten. Zu seinem eigenen Erstaunen beendete er mit der Registrierung der Domain jedoch die Ausbreitung der Schadsoftware, da diese sich, sofern sie eine Antwort von der angefragten Domain bekam, einfach abschaltete. Dies machte zwar bereits geschehene Verschlüsselungen nicht rückgängig, unterbrach aber die Verbreitung der Ransomware (vgl. Clark 2017; Hutchins 2017) – jedenfalls fürs Erste. Leicht veränderte Versionen von *WannaCry*, die nicht mehr über die Abfrage der von Hutchins registrierten Domain anzuhalten sind, sind auch heute noch im Umlauf. Zum jetzigen Zeitpunkt (Stand: Oktober 2020) führt *WannaCry* seit seinem ersten Auftauchen ungebrochen die Statistik der meistverbreiteten Ransomwares der Welt an (vgl. Chebyshev et al. 2018; Kaspersky 2020, 9; Kaspersky 2019). Wie kam es zu dieser Entwicklung?

3.2.2 Der *AIDS Information Trojaner*

Der erste dokumentierte Ransomware-Fall ereignete sich im Dezember 1989 mit einem Programm namens *AIDS Information Trojaner.*[19] Ihren Namen hat

17 Eine statistisch unbedeutende Ausnahme bildet hier das Programm *WanaKiwi*, das in manchen Fällen die Verschlüsselung rückgängig machen konnte. Voraussetzung dafür ist, dass der Computer seit Beginn des Verschlüsselungsvorgangs nicht neu gestartet wurde, da *WanaKiwi* den Arbeitsspeicher ausliest (vgl. Delpy 2017).

18 Grundsätzlich raten Polizei und Sicherheitsexpert_innen von einer Lösegeldzahlung jedoch ab (vgl. The No More Ransom Project o.J.b).

19 In manchen Publikationen wird der *AIDS Information Trojaner* lediglich als *AIDS Trojan* bezeichnet, bspw. bei Ferbrache (1992) oder Solomon (1991).

diese Schadsoftware daher, dass sie in einem interaktiven Informationsprogramm über HIV und AIDS versteckt war, das auf Floppy Disks in Umlauf gebracht wurde (vgl. Simone 2015). Die mit »AIDS Information – an Introductory Diskette Version 2.0« beschrifteten Floppy Disks der fiktiven Firma *PC Cyborg Corporation* wurden an mehrere Tausend Personen gesendet, die entweder Abonnent_innen des Magazins *PC Business World* oder Teilnehmer_innen einer WHO-Konferenz des Jahres 1988 zum Thema AIDS waren (vgl. Ferbrache 1992, 25; McKinney/Mulvin 2019, 483).[20] Mit der Installation der Software installierte der_die unwissende User_in gleichzeitig auch die Schadsoftware, die wie in einem Trojanischen Pferd in der Floppy Disk versteckt war. Nur ein Blick in die beigefügten Lizenzbedingungen — 1989 offenbar ebenso unbeliebt wie heute — hätte den Verdacht aufkommen lassen können, dass das Programm ein Scam sei: Die EULA beinhaltet mehrere unseriöse Warnungen davor, dass die Software nicht kostenfrei zu nutzen sei, listet mögliche Kosten auf und warnt potentielle Nutzer_innen davor, dass eine Installation der auf der Floppy Disk enthaltenen Software die anderen Programme des betreffenden Computers und den Computer selbst nicht unberührt lassen würde. Ein Auszug liest sich folgendermaßen:

> »You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement; your conscience may haunt you for the rest of your life; you will owe compensation and possible damages to PC Cyborg Corporation; and your microcomputer will stop functioning normally.« (Ferbrache 1992, 261)

Falls man sich (dennoch) dazu entschloss, die Software zu installieren, so wurde gleichzeitig die Schadsoftware sowie ein Bootcounter installiert, der in diesem Fall als Trigger einer Art Logikbombe (vgl. Gazet 2010, 78) fungierte und beim 90. Reboot des Computers die Schadensroutine auslöste. Diese besteht aus zwei Teilen: Zuerst werden alle Dateinamen auf der Festplatte verschlüsselt und anschließend eine neue Datei erstellt, um den auf der Festplatte verbliebenen Platz aufzufüllen (vgl. Solomon et al. o.J.). Nachdem dieser Prozess abgeschlossen war, wurde der_die User_in vom Computer aufgefordert, den

20 Die genaue Anzahl der versendeten Disketten variiert stark je nach der zu Rate gezogenen Publikation, was vermutlich daran liegt, dass das Ausmaß des Schadens in den frühen Publikationen, die schnell auf den Trojaner folgten, noch nicht absehbar oder zusammengetragen war. Die höchste Anzahl gibt Solomon (1991, 16) mit 20.000 Adressat_innen an.

Drucker einzuschalten, und ein Erpressungsschreiben im Stil eines Formulars für eine Lizenzerneuerung mit einer Zahlungsforderung über 189 USD für eine Jahreslizenz oder 378 USD für zeitlich unbegrenzten Zugang zur eigenen Festplatte wurde ausgedruckt (vgl. ebd.). Die Zahlung sollte an die *PC Cyborg Corporation* gesendet werden, die auch als Lizenzgeberin der Floppy Disk aufgetreten war, und ein panamaisches Postfach wurde als Zahlungsadresse angegeben (vgl. ebd.). Nur kurze Zeit nach dem Erscheinen der Lösegeldforderung versuchte die Software, verschreckte User_innen mit der Angabe auszutricksen, dass mit der Installation der Malware auf einem weiteren Computer 30 Tage Zeit erkauft werden konnten, bevor die Zahlung fällig würde – eine Prozedur, die ohne ihr Versprechen einzulösen lediglich einen weiteren Computer beschädigte (vgl. ebd.).

Die Verflechtung dieser ersten Ransomware mit HIV/AIDS erschöpft sich jedoch nicht in dem zur Tarnung des Trojaners verwendeten Programm: Höchstwahrscheinlich[21] war der Urheber des Trojaners Dr. Joseph Lewis Popp, seines Zeichens Harvard-Absolvent für Evolutionsbiologie und zur Zeit des Ransomware-Angriffs HIV/AIDS-Forscher und Consultant der WHO in Kenia (vgl. Simone 2015).[22] Zwei Wochen nach der Veröffentlichung des *AIDS Information Trojaners* erregte Popp durch sein seltsames Verhalten die Aufmerksamkeit der Behörden am Flughafen Schiphol Amsterdam, als er auf der Rückkehr von einer WHO-Konferenz in Nairobi die Worte »Dr. Popp has been poisoned« in den Koffer einer_eines Mitreisenden kratzte (vgl. ebd.). Als sein Gepäck durchsucht wurde, fand man ein Siegel der *PC Cyborg Corporation* bei ihm. Kurze Zeit später wurde Popp in Ohio festgenommen und nach Großbritannien ausgeliefert, um sich dort wegen Erpressung und Vandalismus vor Gericht zu verantworten. Allzu viel Licht ins Dunkel konnte die Verhandlung

21 Obwohl Popp der Einzige war, der sich aufgrund des Trojaners vor Gericht verantworten musste, bemerken Solomon, Nielson und Meldrum (o.J.) in ihrer Analyse, dass der Code des *AIDS Information Trojaners* gleichermaßen aus sehr simplen und sehr anspruchsvollen Codezeilen besteht, woraus sie folgern, der Code könne mehrere Autor_innen haben – oder mindestens mehrere Quellen, aus denen er zusammenkopiert wurde.

22 Zur Joseph Popps Beruf und Rolle bei der WHO finden sich divergierende Angaben: McKinney und Mulvin (2019, 483) schreiben, Popp sei »an anthropologist with a doctorate from Harvard who had been denied a position at the World Health Organization«; Ferbrache (1992, 27) wiederum schreibt: »Popp was a zoologist who had conducted research into animal behaviour for UNICEF and WHO, and who had examined the initial links between monkeys carrying AIDS and the human population.«

jedoch nicht bringen: Popp leugnete, mit der Floppy Disk irgendeinen Profit gemacht zu haben und beschuldigte Beschäftigte der WHO, die Direktor_innen der *PC Cyborg Corporation* zu sein. Er behauptete weiterhin, die AIDS Information Diskette 2.0 sei Teil eines geheimen Plans gewesen, Gelder für HIV/AIDS-Forschung zusammenzutragen (vgl. Wilding 1990, 2), was angesichts der Tatsache, dass hauptsächlich Organisationen, die zu HIV und AIDS forschten oder Aufklärungsarbeit leisteten, von der Schadsoftware betroffen waren, und die Forschung dadurch Rückschläge in Form von Datenverlust erlitt (vgl. Simone 2015), eher zynisch wirkt. Darüber hinaus wurde Popp nie verurteilt – der vorsitzende Richter erklärte ihn für unzurechnungsfähig, da Popp wiederholt dabei beobachtet wurde, wie er sich einen Pappkarton über den Kopf und Kondome über seine Nase stülpte, sowie sich Lockenwickler in den Bart drehte, angeblich als Schutzmaßnahme gegen Strahlung (vgl. ebd.). Nachdem die Wogen des Prozesses sich geglättet hatten, eröffnete Popp mit seiner Tochter ein Schmetterlingskonservatorium in Oneonta, NY, das auch heute noch geöffnet ist und neben Schmetterlingen auch tropische Reptilien beherbergt (vgl. Joseph L. Popp, Jr. Butterfly Conservatory o.J.; Simone 2015).

3.3 Ansteckungen/Übertragungen/Grenzaushandlungen

Der *AIDS Information Trojaner* wirft Fragen nach dem Status der Übertragungen biologischer Konzepte in die Informatik auf: In welchem Verhältnis stehen Schadprogramme und das HI-Virus, oder etwas allgemeiner: biologische Viren? Und wie wirken sich diese Übertragungen auf die Herstellung von IT-Sicherheit aus?

»Der enorme Marktwert des Virus«, schreibt Brigitte Weingart (2002, 78) in ihrem Buch *Ansteckende Wörter. Repräsentationen von AIDS*,

> »zeigt sich einerseits daran, daß der Begriff aus der Spezialisten-Domäne des wissenschaftlichen, genauer: des medizinischen (molekularbiologischen, immunologischen) Diskurses, herausgetreten und zur allgegenwärtigen Metapher geworden ist.«

So habe das Virus als Metapher »die Grenze zum Spezialdiskurs der Informationstechnologie überschritten und zirkuliert seitdem als Computervirus« (ebd.). »Erwartungsgemäß«, so schreibt Weingart (ebd., 80) weiter, »gibt es auch in der Geschichte der Computerpathologien ein Virus, dem man den Namen ›AIDS‹ gegeben hat.« Weingart (ebd.) bezieht sich an dieser Stelle auf den

AIDS Information Trojaner, gibt aber an, dass die Verknüpfung keine strukturelle sei, »denn anstelle des AIDS-Fragebogens hätte auch ein anderes Angebot stehen können.« Dieser Aussage lässt sich sowohl anhand der bereits dargelegten Verbindungen Joseph Popps zur HIV- und AIDS-Forschung, den zu großen Teilen mit AIDS-Forschung und -Aufklärung befassten Empfänger_innen, als auch basierend auf der geschilderten Funktionsweise des *AIDS Information Trojaners* widersprechen. Der Trojaner lässt sich als den Krankheitsverlauf einer HIV-Infektion bis hin zum Ausbruch von AIDS nachahmend lesen, und das nicht nur, wie Cait McKinney und Dylan Mulvin (2019, 484) in ihrem Aufsatz *Bugs: Rethinking the History of Computing* spitz bemerken, mit einem »particularly distanced squint«: Angefangen bei der Infektion/Installation, über die ihr folgende symptomlose Latenzperiode, wie sie nach einer HIV-Infektion auftritt, die ihr Äquivalent in der Zeit bis zum 90. Reboot des Computers findet. Schlussendlich kommt es zum Auftreten von Symptomen, entweder in der Form von verschiedenen Krankheiten, die zusammengenommen das Krankheitsbild AIDS ausmachen, oder durch die ablaufende Schadensroutine. Ein entscheidender Aspekt, in dem die Verbindung nicht aufgeht, ist die Frage nach Intentionalität der jeweiligen Phänomene: Während der *AIDS Information Trojaner* oder andere Computerviren oder -würmer von Menschen geschrieben und in Umlauf gebracht werden, und sich eine Intention feststellen lässt, trifft dies auf HIV/AIDS nicht zu (vgl. Helmreich 2000, 482). Es lassen sich, abgesehen von dieser Einschränkung, also sowohl personelle als auch strukturelle Verbindungen zwischen HIV, AIDS und dem *AIDS Information Trojaner* herstellen. Eine weitere Verbindung, die sie als »Verwicklung der Ansteckungsverfahren« bezeichnet, liefert Weingart (2002, 80) selbst:

> »Wer jede x-beliebige Diskette nicht als per se mit Vorsicht zu behandelnden ›Fremdkörper‹ erachtet, sondern in den ›intimen Öffnungen‹ seines Computers zuläßt, ist beim ersten Test – auf ›gesundes Mißtrauen‹ – schon durchgefallen. Er/sie hat sich mit dieser Fahrlässigkeit gewissermaßen schon in die ›Risikogruppe‹ katapultiert.«

Bereits in diesem kurzen Zitat – stets in Anführungszeichen geschrieben, um uneigentliche Rede zu markieren[23] – ist eine Fülle von Ausdrücken enthalten,

23 Weingart (2002, 11–12) thematisiert die Verwendung von vorsichtiger, uneigentlicher Rede mehrfach in ihrem Buch, und bezeichnet diese Verwendung von Anführungszeichen als Markierung derselben mit Hubert Fichte als »Zungenpräser«: »›Zungenpräser‹ kann auch als Metapher für ›diskursive Verantwortung‹ interpretiert werden,

die den IT-Sicherheitsdiskurs bis heute prägende Konzepte ansprechen, und die am öffentlichen Diskurs um HIV und AIDS orientiert sind. Interessant ist darüber hinaus, dass Weingart eine Übertragung vornimmt: Es handelt sich beim *AIDS Information Trojaner* keineswegs um einen Computervirus, sondern, wie der Name schon sagt, um einen Trojaner – was Weingart (ebd.) auch kurz bemerkt, nur um dann darüber hinwegzugehen, indem sie schreibt, dass man von dem Trojaner »mit der Infektion durch ein Computervirus bestraft« werde. Auf technischer Ebene ist diese Bemerkung inkorrekt: Was Weingart als Virus identifiziert, ist vielmehr die Schadensroutine, die die Dateinamen mit einer monoalphabetischen Substitutionschiffre verschlüsselt (vgl. Gazet 2010, 78). Über Eigenschaften von Computerviren, wie sie in der Informatik definiert werden (vgl. Cohen 1987), verfügt der *AIDS Information Trojaner* keine. Weingart ist mit dieser Sorte Übertragung jedoch nicht allein: Mit einiger Regelmäßigkeit werden die Begriffe Virus und Wurm in medienkulturwissenschaftlichen Texten, aber auch in Zeitungsartikeln durcheinandergebracht oder synonym verwendet. So bezeichnet im Sammelband *Virus! Mutationen einer Metapher* bspw. Hilmar Schmundt (2004, 170) den *AIDS Information Trojaner* als »AIDS-Virus«. Im selben Band schreibt Peter Knight (2004, 196, Herv. MS) über den ILOVEYOU-Wurm: »Beim Ausbruch des ILOVEYOU-*Virus* wurden die Netzwerk-Server zwar mit E-Mails verstopft, die der *Wurm* massenhaft generiert hatte […].« Der Soziologe Andrew Ross (1991) schreibt in seinem Essay *Hacking Away At The Counterculture* abwechselnd über den »Morris virus« und den »Morris worm«. Es würden sich noch zahlreiche weitere Beispiele für diese Verwechselung anbringen lassen. Von größerem Interesse für die folgenden Betrachtungen, als den genannten Autor_innen etwaige Ungenauigkeiten nachzuweisen, ist die Frage, wie und weshalb diese Gleichsetzung

---

die gleichermaßen auf diejenigen übergeht, die eine Analyse des Diskurses über AIDS unternehmen (als Anweisung, ein Blatt vor den Mund zu nehmen). Auch wenn Anführungszeichen, diese ›Präservative des *speech act*‹, immerhin markieren, daß man bezüglich der Worte wählerisch ist, reichen sie kaum aus, um Diskurse abzusichern, *safer text* zu produzieren. […] Das gilt auch und erst recht für die ›ansteckenden Wörter‹, die im Diskurs über AIDS zirkulieren und deren epidemische Verbreitung ebenso zum Gegenstand dieses Buches gehört wie die Versuche ihrer Kontrolle.« Auch in der vorliegenden Publikation habe ich bisher zumeist ähnliche Vorsichtsmaßnahmen verwendet, und mich etwa bemüht, in den technischen Beschreibungen so wenig wie möglich umgangssprachlich zu schreiben. Dennoch lässt sich mit Donna Haraways Konzept der *Trope* berechtigter Zweifel an diesen Vorsichtsmaßnahmen anbringen, die den Versuch begleiten, Viralität explizierend kontrollieren zu wollen.

von Ransomware, Wurm und Virus möglich wird (und sich in die Texte einschleicht). Eine naheliegende Vermutung ist, dass diese Phänomene über Gemeinsamkeiten mit Computerviren verfügen, die im Folgenden untersucht werden sollen.

3.3.1 Metaphorische Grenzaushandlungen

Liest man über *WannaCry*, den *AIDS Information Trojaner*, oder andere Schadsoftware, so fällt auf, dass die Sprache, die zur Beschreibung dieser Phänomene genutzt wird, durchzogen ist von Elementen des uneigentlichen Sprechens, die sich größtenteils als Alltagssprache naturalisiert haben, aber bei genauerem Hinhören doch herausstechen: Computer*viren infizieren*, oder *greifen an*, Verschlüsselung wird *gebrochen*, in gehackte Systeme wurde *eingebrochen* – überall scheint die Sprache, mit der Phänomene aus dem Bereich der IT-Sicherheit beschrieben werden, von Metaphern der Grenzaushandlungen durchsetzt zu sein. Der Begriff der Metapher ist, so ließe sich sagen, in der Theoriebildung überbesetzt.[24] »[E]ine ausführliche Aufarbeitung metaphorologischer Positionen«, bemerkt Christina Brandt (2004, 28) dazu in *Metapher*

24 Medienwissenschaftliche Arbeiten, die sich dezidiert mit Metaphern auseinandersetzen, sind beispielsweise Marianne van den Boomens (2014) *Transcoding the Digital: How Metaphors Matter in New Media*, Matthias Bickenbachs und Harun Mayes (2009) *Metapher Internet. Literarische Bildung und Surfen*, sowie Georg Christoph Tholens (2002) *Die Zäsur der Medien. Kulturphilosophische Konturen*. Bei Tholen lassen sich durchaus Anknüpfungspunkte an Krämer finden, dennoch weist sein Anliegen, das Verhältnis von Medien und Menschen zu bestimmen, in eine andere Richtung als das der vorliegenden Publikation, und wird daher nicht eingebunden. Während Bickenbach/Maye und van den Boomen extrem detaillierte Überlegungen zum Verhältnis von Metaphern und den von ihnen untersuchten Medien präsentieren, verzichtet die vorliegende Publikation auf eine Einbindung ihrer Texte, da diese dazu tendieren, die von ihnen untersuchten Phänomene in der exakten Einteilung in bestimmte metaphorische Phänomene stillzustellen. Der vorliegenden Publikation geht es genau nicht um die Herstellung von festen Kategorisierungen, sondern um die Nachzeichnung der Ansteckungspotentiale von Metaphern, die mit Krämer, Treichler und Haraway als andauernde Aushandlungsprozesse begriffen werden sollen. Als weiterführende Grundlagentexte zur Metapher sind unter anderem Hans Blumenbergs (1997) begriffsgeschichtliche Studie *Paradigmen zu einer Metaphorologie*, George Lakoffs und Mark Johnsons (1996) neurolinguistische Untersuchung *Metaphors We Live By*, sowie die philosophischen Ausführungen *Models and Metaphors: Studies in Language and Philosophy* von Max Black (1962), sowie Jacques Derridas (1983) Ausführungen zur Metapher in *Grammatologie* (auf die sich auch Sybille Krämer bezieht) zu nennen.

und Experiment. Von der Virusforschung zum genetischen Code, wäre »selbst ein Unternehmen in Buchumfang.« Auch die vorliegende Untersuchung möchte, Brandts Geste folgend, eine solche Aufarbeitung an dieser Stelle nicht leisten, da sie dem Erkenntnisinteresse dieser Untersuchung nur bedingt zuträglich wäre. Ein lockerer Metaphernbegriff, der eher in die Richtung von Donna Haraways bereits eingeführtem Konzept der *Trope* strebt, ist für die folgenden Betrachtungen ausreichend und soll im Hinblick auf das Erkenntnisinteresse dieser Untersuchung kurz umrissen werden.

Das in den deutschen Sprachgebrauch überführte Wort *Metapher* stammt vom griechischen Wort *metaphorā* ab, das mit »Übertragung« übersetzt werden kann (Kluge 2012a), und befindet sich damit bereits an einem neuralgischen Punkt für medientheoretische Überlegungen. Mit Sybille Krämer (2003, 84) wurden bereits in Kapitel 2 *Übertragung* und *Inkorporation* als Eigenschaften von Medien eingeführt. Das Zusammenwirken beider Begriffe ermöglicht es, auf die von Krämer (ebd., 84–85, Herv. MS) ausgemachte »Gretchenfrage« der Medientheorie, ob Medien Sinn erzeugen oder vermitteln, zu antworten, dass »Medien im Akt der *Übertragung* dasjenige, was sie übertragen, zugleich mitbedingen und prägen.« In der Übertragung liegt also die Konstitutionsleistung von Medien begründet. An dieser Stelle lohnt es sich, noch mal einen Schritt zurückzugehen: »Der für die Medientheorie relevante Begriff der ›Übertragung‹«, schreibt Krämer (ebd., 84), »kann am Vorbild jener Art von Übertragung gewonnen werden, welche für die Metapher (meta-phora) grundlegend ist.« Umgekehrt bedeutet dies für die Metapher, dass diese eine Übertragung vornimmt, und damit über ein generatives Moment verfügt, sowie zwei voneinander getrennte Bereiche voraussetzt, zwischen denen eine solche Übertragung stattfinden kann. Wie bereits in der Einleitung dargelegt, ist die vorliegende Publikation daran interessiert, die Übertragungsprozesse von Konzepten und Begriffen zwischen wissenschaftlichen Sphären nachzuvollziehen, deren Wissensproduktion unterschiedlichen Rationalitäten folgt. Deuber-Mankowsky (2020, 135) folgend wurden diese Rationalitäten als von unterschiedlichen »Regeln und Prozessen« gekennzeichnet bestimmt, und die jeweiligen Wissensbestände damit als unterschiedlichen Ordnungen angehörend. Für das vorliegende Material bedeutet dies: Bei der Übertragung des Konzepts *Virus* aus der Immunologie in den Zusammenhang der Informatik wird nicht einfach nur ein dort angesiedeltes Phänomen erläutert, sondern entsteht es erst in und durch metaphorische Übertragung. Im Fokus steht also die Medialität von Metaphern, die sich in einer Art fraktaler Baumstruktur ebenfalls durch Übertragung und Inkorporation auszeichnet. Der Aspekt der

Inkorporation, dem Krämer ebenfalls Eigenschaften zuschreibt, die über ein bloßes *Ver*körpern hinausgehen, lässt sich mit Haraways Konzept der *trope* und dem Ausdruck *materiell-semiotisch* noch weiter stärken: Zwar sind Metaphern bei Haraway »tools and tropes« (Haraway 2018, 39), und Wörter »thick, living, physical objects that do unexpected things« (Haraway 1997, 125), aber die Phänomene, die sie bezeichnen, werden nicht einfach nur in sprachlichen Zusammenhängen verwoben, sondern arbeiten an diesen Zusammenhängen mit. So schreibt Haraway (2018, 97) im Zuge ihrer Betrachtungen der *OncoMouse*:

> »The collapse of metaphor and materiality is a question not of ideology but of modes of practice among humans and nonhumans that configure the world – materially and semiotically – in terms of some objects and boundaries and not others.«

Eine Lesart Haraways, die den Prozess der Herstellung von Wissen nur auf die Rolle von Sprache konzentriert, würde ihrem Einsatz nicht gerecht werden. An der Herstellung von Wissen ist also nicht nur Sprache mit ihrer Körperlichkeit beteiligt, sondern auch die Materialitäten der beschriebenen Objekte, die daran mitarbeiten, wie sie beschrieben werden können, und Sprache eben nicht nur im Sinne einer passiven Verkörperung erdulden. Die Konsequenz, die sich daraus ableitet, formuliert Haraway (ebd., 39) folgendermaßen: »The point is to learn to remember that we might have been otherwise, and might yet be, as a matter of embodied fact.« Bevor es im nächsten Kapitel um die spekulativen Zukünfte gehen kann, die Haraways Konzept des Materiell-Semiotischen eröffnen, soll allerdings nun endlich ein Überblick über die Geschichte und den Status Quo der IT-Sicherheit gegeben werden.

3.3.2 Zur Medialität von Viren und Würmern

1984 veröffentlichte der Informatiker Fred Cohen[25] einen Aufsatz, in dem er »a major computer security problem called a virus« (Cohen 1987, 22)[26] vorstellt.

25 Die Bezeichnung der geschriebenen Software als Virus geht auf Cohens Mentor Len Adleman zurück (vgl. Cohen 1987, 31), der den Leser_innen hier bereits als einer der drei Erfinder des ersten auf Diffies und Hellmans Konzept aufbauendem asymmetrischen Verschlüsselungsverfahren RSA bekannt ist, aber dies soll nur am Rande bemerkt sein.

26 In dieser Publikation wird die 1987 im Journal *Computers & Security* veröffentlichte Version zitiert.

»The virus is interesting«, schreibt Cohen (ebd.) weiter, »because of its ability to attach itself to other programs and cause them to become viruses as well.« Ein weiterer technischer Faktor, der Computerviren interessant macht, ist die zum damaligen Zeitpunkt noch weit verbreitete Nutzung von Time-Sharing-Computern durch jeweils mehrere User_innen. Die bisher implementierten Sicherheitsmechanismen dieser Systeme konzentrierten sich auf das Verhindern von »illicit dissemination of information« (ebd.): Es wurden für alle Nutzer_innen passwortgeschützte, eigene Bereiche angelegt, innerhalb derer sie ihre Dateien speichern konnten, was bereits mit Paul Ferdinand Siegert (2008, 191) als eine erste Form der Herstellung von Sicherheit als *access control* eingeführt wurde. Computerviren setzten an der Kehrseite dieses Phänomens an, denn, wie Cohen (1987, 22, Herv. MS) ausführt, »little work has been done in the area of keeping information *entering* an area from causing damage.« Die Definition des neuen Sicherheitsproblems lautet folgendermaßen:

> »We define a computer ›virus‹ as a program that can ›infect‹"[27] other programs by modifying them to include a possibly evolved copy of itself. With the infection property, a virus can spread throughout a computer system or network using the authorizations of every user using it to infect their programs. Every program that gets infected may also act as a virus and thus the infection grows.« (Ebd., 23)

Computerviren sind also Programme, die andere Programme infizieren, anstecken, das heißt: sich auf andere Programm *übertragen*, indem sie diese umschreiben. Der Begriff Virus als Bezeichnung für ein biologisches Phänomen kommt aus dem Lateinischen und bedeutet so viel wie *Saft* oder *Gift* (vgl. Kluge 2012b). Auch die Infektion hat ihre Wurzeln im Lateinischen, genauer dem lateinischen Verb *inficere*, das mit »vergiften, verpesten, beflecken« übersetzt wird (Krämer 2008, 138). Auf einen umfassenden wissenschaftsgeschichtlichen Überblick, wie das Virus zum Gegenstand der Bakteriologie und Medizin wurde, wird an dieser Stelle zugunsten der Stringenz der Argumentation verzichtet,[28] die lediglich das Wissen um Viren als ansteckende Elemente, durch die Infektionskrankheiten übertragen werden, voraussetzt. Durch die von ihnen geleistete Übertragung sind Viren auch medienwissenschaftlich ein

27 Der Virus und seine Eigenschaft der Infektion, die an dieser Stelle noch in Anführungszeichen geschrieben sind, werden im Verlauf des Aufsatzes von diesen befreit und damit im Sprachgebrauch naturalisiert.

28 Für einen solchen Überblick siehe exemplarisch Brandt (2004, 55–103).

interessantes Phänomen. So widmet auch Sybille Krämer biologischen und informatischen Viren ein Unterkapitel in *Medium, Bote, Übertragung*. »Wenn von ›Computerviren‹ gesprochen wird«, schreibt sie, »scheint hier das medizinische Vokabular auf äußerste Weise ins Metaphorische gedehnt« (ebd., 145). Dennoch betrachtet Krämer (ebd., 158) Computerviren und biologische Viren im Hinblick auf ihre Gemeinsamkeiten, um anhand dieser beider Viren ein Konzept dessen zu entwickeln, was sie als »Übertragen durch Ansteckung« ausmacht, und was sich in Anlehnung an den Begriff Medialität als *Viralität* beschrieben ließe. Die Übertragung durch Ansteckung umfasst Krämer zufolge fünf Punkte, die im Folgenden spezifisch im Hinblick auf Computerviren diskutiert werden: Somatizität, Heterogenität, Nichtreziprozität/Unidirektionalität, Umschrift und Gewaltsamkeit (vgl. ebd.).[29]

Unter *Somatizität* versteht Krämer (ebd.), dass die Übertragung durch Ansteckung ein körperliches Phänomen ist, insofern sie Körper ebenso wie Kontakt zwischen diesen voraussetzt. »To talk of viruses«, schreibt auch Parikka (2016, 94), »is to talk of embodiment, but not merely involving human bodies.« Für Computerviren bedeutet dies, dass Computer als Körper gedacht und konzipiert werden, was, wie er darlegt, bereits in den 1950er Jahren mit der Analogie von CPU und Gehirn begonnen hat (vgl. ebd., 111), aber auch, dass einzelne Programme innerhalb desselben Computers analog zu Körpern verstanden werden können (vgl. Ferbrache 1992, 44). Das bekannte UNIX-Diktum »Everything is a file«[30] ließe sich als »Everything is a body« neu formulieren, insofern Computerviren innerhalb ein und desselben Computers von Programm zu Programm übertragen werden können.

Unter dem Punkt *Heterogenität* erläutert Krämer (2008, 158), dass Ansteckungen nur zwischen »äußerst differierenden Systemen« geschehen können, »sei diese Differenz nun beschrieben als eine zwischen Eigenem und Fremdem, Gesundem und Krankem […].« Dies begründet Krämer in der Immunisierung, mit der Ansteckung verhindert werden kann, indem die

29 Die Diskussion um die Ähnlichkeit von Computerviren und biologischen Viren innerhalb der Informatik bezieht sich eher darauf, wie stark die Analogie zu biologischen Viren tatsächlich trägt, indem versucht wird, die biologischen Vorgänge exakt mit den informatischen zusammenzubringen (vgl. exemplarisch Ferbrache 1992; Forrest et al. 1997; Spafford 1989). Eine Diskussion der Ähnlichkeit der Medialität von Computerviren und biologischen Viren erscheint an dieser Stelle zielführender.

30 »Everything is a file« weist darauf hin, dass sowohl gespeicherte Dateien wie Bilder, Texte oder Musik als auch die Programme, mit denen sie angezeigt werden, Text*dateien* sind, und gleichermaßen bearbeitet werden können.

Unterschiede zwischen dem infizierten und dem noch nicht infizierten System aufgehoben werden. Dies trifft auf Computerviren nur bedingt zu, denn Viren, die beispielsweise innerhalb des *Microsoft Windows*-Betriebssystems funktionieren, tun dies nicht auf UNIX-basierten Systemen. Die Systeme dürfen also nicht so heterogen sein, dass die zwischen ihnen ausgetauschten Daten nicht auf beiden Systemen auch *ausgeführt* werden können, eine gewisse gemeinsame Sprache muss gegeben sein.

Der Aspekt der Heterogenität ist direkt anschlussfähig an den der *Umschrift*: Verfügen differente Systeme über eine gemeinsame Sprache, oder vielmehr über einen gemeinsamen Code, so können Viren zwischen ihnen übertragen werden, und sich in das noch nicht infizierte System einschreiben, es also umschreiben. Die Übertragung durch Viren, so formuliert Krämer (ebd., 159), ist »mit Prozessen der Informationsverarbeitung verbunden«. Bei der Informationsverarbeitung heterogener Systeme schließen auch Galloway und Thacker (2007, 86) an: »What counts is not that the host is a ›bacterium,‹ an ›animal,‹ or a ›human.‹ What counts is the code – the number of the animal, or better, the numerology of the animal.« Auch wenn bereits in Kapitel 2 darauf hingewiesen wurde, dass die Ausdeutung dieses Codes als kryptographisch (vgl. ebd.) unzutreffend ist, und das Element des Satanistisch-Okkulten, das in der Anspielung auf die Numerologie/Zahl des Tieres aufscheint, in der vorliegenden Publikation nicht mitgetragen wird, so lässt sich dennoch nicht abstreiten, dass Übertragung durch Ansteckung, und damit Viren die – informatisch ausgedrückt – Interoperabilität differenter Systeme voraussetzen. Ein Beispiel dafür ist der gelungene Hack einer DNA-Sequenziermaschine, bei dem mit einem in DNA codierten Computervirus im Vorgang der Sequenzierung die Maschine infiziert wurde (vgl. Fischer 2017; Ney et al. 2017).

Der Aspekt der *Nichtreziprozität/Unidirektionalität* ist spannend, weil er sich bei Computerviren einerseits auf den technischen Vorgang beziehen lässt: Die Weitergabe des Virus geschieht nur in eine Richtung zur selben Zeit, d.h. ein Computervirus kann nur ein anderes Programm mit diesem infizieren, aber nicht gleichzeitig sich selbst, da es bereits infiziert ist. Andererseits kann die Unidirektionalität mit McKinney und Mulvin auch auf das diskursive Ansteckungspotential zwischen Informatik und HIV/AIDS bezogen werden: »[T]he homology between computing and HIV is asymmetrical. Examples of HIV used in computer network discourses are abundant, while we found only a small set of examples of AIDS activists responding to or refracting this metaphor.« (McKinney/Mulvin 2019, 482)

Damit bleibt als letzter Aspekt der der *Gewaltsamkeit* von Übertragung durch Ansteckung, den Krämer (2008, 159) einerseits im invasiven und passivierenden Moment der Ansteckung ausmacht – wer oder was angesteckt wird, dem_der widerfahre etwas, das größtenteils nicht von ihm_ihr kontrolliert werden könne – und andererseits in den Präventions- oder Gegenmaßnahmen wie der Immunisierung oder etwa der Quarantäne.

Bevor im nächsten Unterkapitel genauer auf die Immunisierung eingegangen wird, soll der Blick noch einmal kurz auf Computerwürmer gerichtet werden, also auf Programme, die sich autonom und ohne dabei andere Programme zu verändern durch ein Netzwerk bewegen. Während Computerviren explizit als Sicherheits*problem* eingeführt wurden, was Handlungsbedarf impliziert, so bespricht Cohen (1987, 22) Würmer eher wohlwollend: Über den Xerox Wurm beispielsweise schreibt er, dieser habe »accidentally« zu einem *Denial of Service*, also einer Überlastung des Netzwerks geführt. Diese Gleichgültigkeit gegenüber Würmern lässt sich einerseits als strategisch interpretieren, schließlich geht es um die Absteckung des neuen Phänomens, und den damit verbundenen Expertenstatus bezüglich notwendiger Sicherheitsmaßnahmen für das neue Problem, und den daraus erwachsenden Möglichkeiten finanzieller Förderung der Forschung. Aus heutiger Perspektive lässt sich diese Haltung allerdings auch mit Parikka (2016, 20) darauf zurückführen, dass die Ursprünge von Würmern »in the needs of network computing in general« liegen: Manche sich wiederholenden Abläufe, die beispielsweise zur Systempflege notwendig sind, wurden als weitestgehend autonom agierende Programme automatisiert, die damit nicht als »anomalies in the simple sense of the word but [as] part and parcel of the emergence of network systems« (ebd.) einzustufen sind. Für Würmer und für Viren gilt damit eine Ambiguität, die in den nächsten Jahrzehnten sukzessive vereindeutigt werden sollte: »[E]ssentially the same program can be defined as a utility program in one context and as a malware program in another.« (Ebd.) Festzuhalten ist an dieser Stelle zunächst, dass Viren und Würmer nicht als vernetzten Systemen äußerliche Störfaktoren begriffen,[31] sondern vielmehr als »a phenomenon of time-

31 In seinem Aufsatz *The Universal Viral Machine. Bits, Parasites and the Media Ecology of Network Culture* macht Parikka (2005) dasselbe Argument stark, jedoch nicht aus einer medienarchäologischen, sondern aus einer medienökologischen Perspektive. Eine affirmative Verwendung des Begriffs *environment* ist jedoch aufgrund der Verstrickung dieses Konzepts mit der Politik des Nationalsozialismus mit Sprenger (2019) kritisch neu zu evaluieren.

sharing, networking, and, broadly speaking, connectivity« (ebd.) im Allgemeinen betrachtet werden müssen.[32] Weiterhin überschneiden sich die Phänomene Computerviren und -würmer also einerseits in der Ambiguität ihrer Nutzungspraktiken, sowie in ihren ähnlichen Verbreitungsdynamiken: Von den mit Krämer ausgeführten Kriterien für Viralität teilen sie Somatizität, Heterogenität, Unidirektionalität und Gewaltsamkeit, während Umschrift[33] bei Würmern nur bedingt gegeben ist. Diese Überschneidungen beantworten die eingangs aufgeworfene Frage, wie die synonyme Verwendung oder unabsichtliche Verwechselung von Computerviren und -würmern möglich wird.

Die Ambiguität von Computerviren stellt die noch verhältnismäßig junge IT-Sicherheit vor ein nicht zu unterschätzendes Problem, das Cohen (1987, 34) nach einigen Überlegungen zur Prävention, aber auch Reparatur von durch Computerviren entstandenen Schäden, in seinen abschließenden Bemerkungen zur Herstellung von Sicherheit in vernetzten Systemen thematisiert:

> »To be perfectly secure against viral attacks, a system must protect against incoming information flow, while to be secure against leakage of information a system must protect against outgoing information flow. In order for systems to allow sharing, there must be some information flow. It is therefore the major conclusion of this paper that the goals of sharing in a general purpose multilevel security system may be in such direct opposition to the goals of viral security as to make their reconciliation and coexistence impossible.«

Wie können vernetzte Systeme, mit ihren körperlichen Qualitäten, vor einem Phänomen geschützt werden, das in denselben begründet liegt? Wie kann Informationsverarbeitung vor dem Missbrauch ihrer zentralen Funktionselemente, dem Lesen und Um/Schreiben, geschützt werden? Und wie wird dieser definiert, also, was ist normale und nicht-normale Computernutzung?

---

32 Eine solche Lesart steht Konzeptualisierungen von Computerviren als terroristischen Entitäten, die ein geschlossenes System infiltrieren oder von außen bedrohen, und damit der Gleichsetzung von Computernetzwerken mit Nationalstaaten, wie sie beispielsweise das FBI in den 1990er veranschlagte (vgl. Helmreich 2000, 485), diametral entgegen.

33 Ob Umschrift als eine Eigenschaft von Computerwürmern definiert wird, oder nicht, hängt von der eingenommenen Perspektive ab. Würmer schreiben im Gegensatz zu Viren keine Programme um, um sich in diese hineinzuschreiben. Aus der Perspektive, dass alle Aktionen in digitalen Medien *schriftliche* Operationen sind, nimmt der Wurm sehr wohl eine Umschrift von Daten auf der Festplatte eines Computers vor.

Die von Cohen diagnostizierte Unvereinbarkeit von vernetzten Systemen, die Informationsaustausch erlauben, mit (Sicherheit vor) Computerviren scheint mit der Formulierung, »reconciliation and coexistence« seien unmöglich, zunächst für eine Unterbrechung des Informationsaustauschs zu plädieren, und damit in die Richtung der von Loick (2021, 271) benannten »Fortifizierungslogik« eines negativen Sicherheitsbegriffs zu zeigen. Dies ist offensichtlich nicht passiert – aber was stattdessen?

3.3.3 Liberale Abwehrmechanismen

Wie der Soziologe Andrew Ross in seinem Aufsatz *Hacking Away at the Counterculture* ausführt, nahm die Verstrickung von biologischen Viren und computerbezogenen Phänomenen in der medialen Berichterstattung und damit auch der breiten Öffentlichkeit Ende der 1980er Jahre ausgerechnet mit einem Computer*wurm* Fahrt auf: Der sogenannte *Morris Worm*, benannt nach seinem Autor Robert Morris,[34] verbreitete sich Anfang November 1988 über das Internet und ARPANET auf ungefähr 6000 Computer (vgl. Ross 1991, 75). Dies ist, folgt man der Schätzung in Eugene Spaffords (1989, 446) Aufsatz *The Internet Worm Incident*, dass ungefähr 60.000 Computer zu der damaligen Zeit vernetzt waren, eine beachtliche Menge, die dadurch generiert wurde, dass der Wurm auf mehreren verschiedenen Betriebssystemen laufen konnte. Der Morris Worm richtete keinen irreparablen Schaden an: Es wurden weder Dateien gelöscht noch die Funktionalität der Betriebssysteme verändert oder zerstört. Was allerdings passierte, war eine starke Verlangsamung der befallenen Maschinen, die den Wurm teilweise mehrfach ausführten, was schlussendlich den Arbeitsspeicher verstopfte und zu Abstürzen oder längeren Ausfällen der betroffenen Geräte führte (vgl. ebd., 446–447). Nach nur zwei Tagen wurde die Verbreitung des Wurms gemeinsam von den IT-Abteilungen der Universitäten Berkeley und Purdue gestoppt (vgl. ebd., 447). Spafford (ebd.) verliert ebenfalls einige Worte zur medialen Berichterstattung über den Wurm, und vermutet, dass Vertreter_innen der Presse den Morris Worm als Virus bezeichneten, »possibly because their experience to date has been only with that form of security problem.« Dies mag eine Erklärung für die Verwechselung sein – eine andere wäre, dass die Medialität des Wurms der von Computerviren in einem entschei-

34 Die folgende Geschichte ist doppelt so unterhaltsam, wenn man weiß, dass Robert Morris der Sohn des damals leitenden Wissenschaftlers des National Computer Security Center (NCSC) der National Security Agency (NSA) ist (vgl. Kocher 1989, 3).

denden Punkt – der Verbreitung über ein Netzwerk – ähnelt, was ausschlaggebend für diese Verwechselung oder bewusste Komplexitätsreduktion in der Berichterstattung war. Mit Ross lässt sich noch ein weiterer Grund ausmachen: Die Berichterstattung über den Morris Worm, so seine These, forcierte die Intersektion von Informatik und Medizin, da das Thema Computerviren leicht mit dem bereits etablierten und die Medien der damaligen Zeit dominierenden Diskurs über HIV/AIDS verknüpft werden konnte:

> »[M]edia commentary on the virus scare has run not so much tongue-in-cheek as hand-in-glove with the rhetoric of AIDS hysteria – for example, the common use of terms like killer virus and epidemic; the focus on highrisk personal contact (virus infection, for the most part, is spread through personal computers, not mainframes); the obsession with defense, security and immunity; and the climate of suspicion generated around communitarian acts of sharing.« (Ross 1991, 76)

Ross führt seine Überlegungen zum gemeinsamen Vokabular von HIV/AIDS und Computerviren anhand eines Artikels aus dem *Times Magazine* mit dem Titel *Invasion of the Data Snatchers* (vgl. Elmer-Dewitt 1988) weiter aus. Der Titel ist, wie Parikka (2016, 48) bemerkt, eine Anspielung auf Don Siegels Film Invasion of the Body Snatchers (USA 1956), eine Adaption des zwei Jahre zuvor erschienenen Romans *The Body Snatchers* von Jack Finney. Invasion of the Body Snatchers erzählt die leise, fast schon heimliche Invasion einer beschaulichen US-amerikanischen Kleinstadt in den 1950er Jahren durch Aliens, die die Bewohner_innen der Stadt durch identisch aussehende, sogenannte »pod people« austauschen, die keine Gefühle haben und daher der einzigen Eigenschaft beraubt sind, die sie menschlich gemacht hätte. Diese Geschichte kann als eine Parabel gelesen werden, in der Kommunismus und die Angst vor einer kommunistischen Infiltration der McCarthy-Ära anhand von Körperlichkeit und Un/Sichtbarkeit verhandelt werden (vgl. Ebert 1994).[35] Durch die Verwendung von Science Fiction-Motiven wie die Invasion, und in diesem Fall

35 Der Filmkritiker Roger Ebert schrieb über Abel Ferraras Remake des Films im Jahr 1994, das nur Body Snatchers (USA 1993) heißt, dass, während jedem der insgesamt drei Verfilmungen des Stoffs eine unterschiedliche Motivation zu Grunde liege (von »the paranoia of McCarthyism« über einen Generationsunterschied), in diesem Fall »fear of AIDS« den Film informiert haben könne (Ebert 1994). Dies zeigt, dass das immunologisch strukturierte Narrativ des Stoffes in seiner konkreten Bedeutung historisch variabel und in seiner letztendlichen Ausgestaltung dem jeweiligen Zeitgeist unterworfen ist.

auch die Kolonisierung durch Außerirdische, verbindet der *Times*-Artikel, wie Ross (1991, 76) es formuliert, Computerviren mit »those historical fears about bodily invasion, individual and national, that are endemic to the paranoid style of American political culture.« Mit Parikka (2016, 48, Herv. MS) lässt sich darauf hinweisen, dass die Aliens, die unsichtbar und schwelend die US-amerikanische Kleinstadt unterwandern, als »threats to the idea of American *liberal freedom*« begriffen werden können, »and the allegory of viruses represented them as somewhat similar: they were threats to the basis of organized society, democracy, and civil rights.« Die liberale Vorstellung von Freiheit bildet, wie bereits mit Daniel Loick (2021, 267) ausgeführt wurde, die Grundlage für den negativen Sicherheitsbegriff, der den Staat in die Position der Kontrollinstanz der Einhaltung von Gesetzen, und damit der Aufrechterhaltung von Grenzen rückt. Zentraler Schauplatz dieses Grenzschutzes ist das Privateigentum (vgl. ebd., 270). Dies zeigt sich sowohl in der sich in den 1980er Jahren herausbildenden gesetzlichen Regulierung von Hacking als auch in den auf den Morris Worm folgenden Diskussionen über ethische Grundsätze der Computernutzung. 1986 wurde in den USA der *Computer Fraud and Abuse Act*, der die unautorisierte Computernutzung unter Strafe stellt, als Ergänzung des bestehenden Strafrechts zur Regulierung der Nutzung von Telekommunikationsmedien verabschiedet. Diese Entwicklung beschreibt Paul Taylor (2001, 115–118) als zusammenhängend mit der Professionalisierung der Computerbranche als Wirtschaftszweig, und der daraus erwachsenden Forderung nach dem Schutz ihrer wirtschaftlichen Interessen:

> »Hackers, along with viruses, can be portrayed as an external threat to security against which computer security professionals and their products are needed as a safeguard. At the same time, however, there also seems to be an implicit recognition that computer systems are inherently susceptible to bugs and intrusions but that some sort of social solution to such vulnerabilities is more realistic than finding the necessary technical resources to fix the problems.« (Ebd., 117)

Was die Herausbildung von ethischen Grundsätzen der Computernutzung innerhalb liberaler gesellschaftlicher Strukturen angeht, wurde Hacking vornehmlich mit Tropen und Metaphern der Grenzverletzung und -überschreitung belegt. Eine dieser Tropen, die sich bis heute gehalten hat, ist die des *Wilden Westens*. Ein aktuelles Beispiel findet sich auf der Webseite des *No More Ransom Project*, einer Initiative der Sicherheitsfirmen *Kaspersky Lab* und *McAfee*, der niederländischen Polizei und *Europol*. Dort hilft ein »Crypto She-

riff« (vgl. The No More Ransom Project o.J.a), den eigenen Computer im Fall eines Ransomware-Befalls zu reparieren, indem die Ransomware identifiziert und, wenn möglich, eine Software zur Entschlüsselung der eigenen Daten angeboten wird. Der »Crypto Sheriff« kann als eine Anspielung auf das Bild von Hacker_innen als Cowboys betrachtet werden, das, wie Taylor (2001, 37–38) beschreibt, hauptsächlich auf William Gibsons 1984 erschienenen Science Fiction-Roman *Neuromancer* zurückzuführen ist. Das Wild West-Narrativ verbindet eine romantisierte Idee individualistischer Männlichkeit mit »frontier-based concepts« (ebd., 38), in denen *jungfräuliches* Territorium betreten wird und Grenzen verschoben oder verletzt werden (vgl. ebd., 37–38).[36] Weitere »frontier-based concepts« sind die des »breaking and entering«, also des Einbrechens, des Knackens, des Brechens, die es erlauben, Eigentumsrecht für immaterielle Güter zu denken und geltend zu machen (vgl. ebd., 145–151), sowie Metaphern aus dem Bereich der Körperlichkeit. Da der zentrale Schauplatz des Liberalismus die staatliche Regelung von Privateigentum ist, ist die Kriminalisierung von Hacking von elementarer Bedeutung, da der Staat nun auch die Grenzen immaterieller Güter schützen kann und muss.

Noch bevor Robert Morris die Autorschaft des Wurms bestätigte oder es ein entsprechendes Gerichtsurteil gab, das ihn eindeutig als Urheber desselben identifizierte, wurde der Nachweis über seine Autorschaft erbracht, da in seinen Useraccounts auf mehreren Computern der Cornell University ältere Versionen des Wurm-Codes gefunden wurden (vgl. Spafford 1989, 462). Was unklar blieb, und zu Spekulationen einlud, war Morris' Motivation. Während der Wurm von einigen als ein Dummer-Jungen-Streich abgetan wurde, war der Kanzler der Cornell University ganz vom Gegenteil überzeugt. Sein Bericht unterstellte Morris bösartige Absichten, und befand sein Verhalten für »unethical and contrary to the standards of the computer profession« (ebd., 463). Ross (1991, 85) konzentriert sich auf den Teil des Berichts, in dem Morris' bisherige Universitätslaufbahn besprochen wird: »[T]he report regrets that Morris was educated in an ›ambivalent atmosphere‹ where he ›received no clear guidance‹ about ethics from ›his peers or mentors‹ (he went to Harvard!).« In Kombination mit den gegen Morris erhobenen Anschuldigungen identifiziert

36 Taylor versammelt in *Hackers. Crime in the digital sublime* die Aussagen zahlreicher Hacker_innen, mit denen er E-Mail-Interviews geführt hat. Im Verlauf des Buches wird deutlich, dass die Wild West-Trope zwar von manchen affirmiert wird, aber auch starke Kritik an dieser und den anderen Tropen der Grenzaushandlung formuliert wird (vgl. Taylor 2001, 156–158).

Ross (ebd., 85–86) den Bericht als einen liberalen Abwehrmechanismus: Indem Morris vorgeworfen wird, *trotz* seiner liberalen Werten folgenden Erziehung keine ethischen Standards, kein klares Bewusstsein für Recht und Unrecht zu haben, wird Morris als schuldig, die Institution aber als schuldlos konfiguriert, ohne den Liberalismus selbst zu adressieren:

> »Generally speaking, the report affirms the genteel liberal ideal that professionals should not need laws, rules, procedural guidelines, or fixed guarantees of safe and responsible conduct. Apprentice professionals ought to have acquired a good conscience by osmosis from a liberal education, rather than from some specially prescribed course in ethics and technology.« (Ebd., 86)

Morris wurde für ein Jahr von der Universität suspendiert, und musste sich in Syracuse, New York vor Gericht verantworten (vgl. Ferbrache 1992, 23; Spafford 1989, 464). Die Anklage basierte auf dem *Computer Fraud and Abuse Act*, und Morris wurde im Frühling 1990 schuldig gesprochen und zu drei Jahren Bewährung, sowie 400 Sozialstunden und einer Geldstrafe von 10.000 US-Dollar verurteilt (vgl. Galloway 2004, 183).

3.4 AIDS und Computer

Der erste Computervirus, so erzählt es jedenfalls Fred Cohen, wurde im Gegensatz zu den bereits in Netzwerken heimischen Computerwürmern nicht ebenfalls dort beobachtet, sondern gewissermaßen unter Laborbedingungen hergestellt: Am 03.11.1983, schreibt Cohen (1987, 31), wurde er im Zuge eines Experiments konstruiert, das Teil eines wöchentlich stattfindenden Seminars über Computersicherheit war.[37] Die Durchführung des Virus-Experiments inklusive der getroffenen Sicherheitsmaßnahmen, mit denen eine unkontrollierte Vermehrung der neuen Software verhindert wurde, werden ausführlich beschrieben: Alle ›Infektionen‹ mussten von einer Person manuell bestätigt werden, und die Virussoftware war darüber hinaus so programmiert, dass sie keinen Schaden anrichten, sondern lediglich einen Nachweis über ihre Verbreitung erbringen sollte – nicht zuletzt auch, um eine unbemerkte Verbreitung zu verhindern (vgl. ebd.). Die erste Software, die in diesem Experiment

37 Spafford (1989, 449) hingegen weist darauf hin, dass bereits 1982 erste Computerviren im Umlauf waren.

mit dem Virus ausgestattet wurde, war ein Programm zur graphischen Darstellung des UNIX-Dateisystems mit dem Namen *vd*. Stefan Helmreich (2000, 476) folgend, zeigt sich an dieser Stelle zum ersten Mal ein »metaphorical link between computer viruses and sexually transmitted diseases« – Helmreich deutet *vd* in diesem Zusammenhang als die Abkürzung für *venereal disaease*, dem (mittlerweile veralteten) englischen Ausdruck für Geschlechtskrankheit. In den darauffolgenden Jahren sollte sich diese Verstrickung anhand von HIV/AIDS auf der Ebene der Imagination von Computern als Körpern, sowie der Herstellung von Sicherheit fortschreiben, und zwar sowohl im öffentlichen als auch im innerfachlichen Diskurs. Nennenswert für letzteren ist, wie Ross ausführt, dass die Verknüpfung von medizinischer Forschung und Informatik im Nachgang des Morris Worm aktiv von den Informatiker_innen hergestellt wurde, die den Computerwurm untersuchten und zu dem Schluss kamen, dass direkte Analogien zwischen den Verbreitungsmechanismen biologischer und elektronischer Viren (oder in diesem Fall: Würmer) bestünden, und basierend auf dieser Erkenntnis Sicherheitspläne entwarfen:

> »The epidemiology of biological virus (especially AIDS) research is being studied closely to help implement computer security plans. In these circles, the new witty discourse is laced with references to antigens, white bloodcells [sic!], vaccinations, metabolic free radicals, and the like.« (Ross 1991, 76)

Dies kann zweifelsohne als ein Effekt der medialen Gemeinsamkeiten von biologischen Viren und Computerwürmern, vor allem im Hinblick auf ihre Verbreitung in Netzwerken, gedeutet werden.[38] Als Reaktion auf den Morris Worm, führt Ross (ebd.) weiter aus, versuchten verschiedene Behörden der USA, ein »Center for Virus Control« einzurichten, das, wie er bemerkt, »Atlanta's Centers for Disease Control, notorious for its failures to respond adequately to the AIDS crisis« nachempfunden war. In der zweiten Hälfte der

38 Parikka (2016, 103) bemerkt, dass AIDS als eine »epidemic in non-scalar networks« betrachtet werden könne. Auch Albert-László Barabási (2002, 123–142) weist in *Linked. The New Science of Networks* darauf hin, dass sowohl HIV als auch Computerviren sich in skalenfreien Netzwerken verbreiten, was die ähnlichen Dynamiken der beiden bedinge. Seine sensationalistische Darstellung des Sexuallebens des homosexuellen Flugbegleiters Gaetan Dugas, anhand dessen Barabási seine Argumentation über die Verbreitung von HIV entfaltet, sowie seine moralistische Abwertung von Promiskuität zeugen jedoch von den in der Wissensproduktion über HIV tief verwurzelten homophoben Narrativen, die Barabási leider unreflektiert übernimmt.

1980er Jahre gelangten, abgesehen vom Morris Worm, auch einige Computerviren zu größerer Bekanntheit: der *Lehigh*[39] *Virus,* der *Jerusalem*[40] *Virus* und der *Cascade*[41] *Virus.* Diese neuen Computerviren wurden zunächst innerhalb der Fachöffentlichkeit mit AIDS verglichen: Der Lehigh Virus beispielsweise bekam den Beinamen »PC AIDS« (Parikka 2016, 113). Zum *Jerusalem Virus* zitiert Parikka (ebd., 112) aus *The Risk Digest*, einem Forum über IT-Sicherheit, das vom *ACM Committee on Computers and Public Policy* betrieben wurde, in dem es heißt: Der *Jerusalem Virus* »might do to computers what AIDS has done to sex. […] The current free flow of information will stop. Everyone will be very careful who they come into contact with and with whom they share their information.« 1990 kursierten außerdem der *AIDS II*-Virus für das Betriebssystem MS-DOS, sowie *CyberAIDS* für Apple-Computer (vgl. McKinney/Mulvin 2019, 476–477).

Die bisherigen Ausführungen zum Zusammenhang von HIV, AIDS und Sicherheitsproblemen vernetzter Systeme haben sich hauptsächlich auf die Gemeinsamkeiten der Medialität dieser Phänomene, sowie die innerfachliche Perspektive der Informatik konzentriert. Mit der im letzten Unterkapitel umrissenen Herausbildung von ethischen Grundsätzen für die Nutzung von Computern, die an einem liberalen Freiheitsbegriff orientiert sind, sowie der Professionalisierung der Herstellung von Computersicherheit als Industriezweig Ende der 1980er/Anfang der 1990er Jahre und dem ungefähr zeitgleichen Einzug von PCs in Privathaushalte rückten zusätzlich User_innen als Adressat_innen der HIV/AIDS-Metaphorik in den Blick. »[N]ew and would-be computer users«, führen McKinney und Mulvin (ebd., 485) aus, »often confronted explanations of their vulnerability to technological systems through

39 Der *Lehigh Virus* (Betriebssystem: DOS) ist nach seiner Entdeckung im Jahr 1987 an der Lehigh University benannt. Dieser Virus zerstörte die COMMAND-Routine des DOS-Systems, die dafür zuständig ist, den Computer hochzufahren. Bemerkenswert an diesem Virus ist, dass er so schädlich war, dass er sich nicht effektiv außerhalb der Universität verbreiten konnte. Dennoch führte er zu der Einrichtung einer USENET-Gruppe über Computerviren (vgl. Parikka 2016, 33).

40 Der *Jerusalem Virus* (Betriebssystem: DOS) verfügte über eine eingebaute ›Zeitbombe‹: Am 13. Mai 1988, zum 40jährigen Bestehen des Staates Israel, sollte die Schadensroutine des Virus aktiviert werden, die darin bestand, alle aufgerufenen Dateien (und Software) zu löschen (vgl. danooct1 2012b; Parikka 2016, 81, Fußnote 147).

41 Der *Cascade Virus* (Betriebssystem: DOS) sorgte dafür, dass alle 30 Sekunden alle angezeigten Buchstaben auf einem Display alle nacheinander auf den Boden der Anzeige fallen (vgl. danooct1 2012a; Parikka 2016, 33–34).

the heuristics of HIV/AIDS […].« McKinney und Mulvin (ebd., 494) weisen zudem darauf hin, dass zu Beginn der 1990er Jahre die Bedeutung von Computernutzung und Vernetzung über das Internet einem gesellschaftlichen Aushandlungsprozess unterworfen war:

> »In the global North, the 1990s marked a period of heightened flexibility in the interpretation of what computing meant and would come to mean. With every new promise of what a networked computer could do came corresponding fears and threats. Analogies and metaphors were instrumental in simplifying and stabilizing the meaning of new technologies and the practices surrounding them. HIV/AIDS provided a ready template for interpreting the future of computing's domestication.«

Die scheinbare Selbstverständlichkeit dieser Metaphorisierung, und die ihr zugeschriebe Rolle der diskursiven Absicherung birgt jedoch, gemessen an der Geschichte von HIV und AIDS, ein verhältnismäßig großes Irritationspotential. In Aussagen wie »It might do to computers what AIDS has done to sex« (Parikka 2016, 112) scheint klar zu sein, was HIV/AIDS bedeutet, und scheint die Analogie dementsprechend eine klare Handlungsanweisung zu erzeugen: die Reduktion von Vernetzung. Nimmt man Treichlers Bestimmung von AIDS als *epidemic of signification* allerdings ernst, und rechnet man die Tatsache mit ein, dass die Versuche, zu bestimmen was AIDS sein könnte, von großen Unsicherheiten und anhaltenden gesellschaftlichen Aushandlungsprozessen gekennzeichnet waren (und es noch sind), so muss ein Prozess am Werk sein, der die Analogie von Computersicherheit und Schutz vor HIV/AIDS als eindeutig erscheinen lässt. Das vorliegende Unterkapitel wird diesen Prozess diskutieren, und darlegen, dass die Ambivalenzen des HIV/AIDS-Diskurses zugunsten einer liberalen Idee von Eigenverantwortung verflacht wurden, die sich in den homophoben Narrativen des HIV/AIDS-Diskurses zeigte, und die auf die Herstellung von IT-Sicherheit übertragen wurde. Dies wird im Folgenden anhand der Bedeutung des Immunsystems als Figur der Differenzgenerierung im Konzept der »Digital Immunology«, sowie der Begriffe »Digital Hygiene« und »Safe Hex« nachvollzogen.

3.4.1 Technische Lösungsansätze: *Computer Immunology*

Mit Computerviren, -würmern und der Imagination von Computern als Körpern gewann das Konzept der *Computer Immunology* an Popularität. Diese Anwendung immunologischer Konzepte auf Maschinen drückte sich zunächst in

der Vorstellung aus, Computer könnten gegen Schadsoftware *geimpft* und damit *immunisiert* werden, wie die sprechenden Namen der ersten Antivirenprogramme zeigen, die beispielsweise »Flu Shot +, ViruSafe, Vaccinate, Disk Defender, Certus, Viral Alarm, Antidote, Virus Buster, Gatekeeper, Ongard, and Interferon« (Ross 1991, 79) lauteten. Obgleich die Wirksamkeit dieser ersten Antivirenprogramme relativ begrenzt war, da es nicht lange dauerte, bis Hacker_innen neue Viren programmiert hatten, gegen die die Antivirenprogramme keinen Schutz bieten konnten (vgl. ebd.), hat sich die Idee von Antivirus-Software als Impfung lange gehalten. Ferbrache (1992, 45) führt sie genauer aus:

> »Vaccination provides an extremely powerful technique in biological systems, promoting the development of natural immunity using attenuated viral material. Within the computer environment fragments of viral material may also be used – in this case the signature recognition strings which the virus uses to prevent repeated replication. These fragments may safely be added to existing cells (computer programs) and will protect against the virus.«[42]

Ferbrache (ebd.) spekuliert weiterhin über die Möglichkeit von Antikörpern in Computersystemen: Diese Rolle könnte »specific disinfection software« zukommen, »which would recognise the infected program and destroy the virus.« Heutige Antivirenprogramme verfügen über eine Kombination dieser beiden Eigenschaften. Die von Ferbrache angestellten Vergleiche von biologischen und informatischen Viren betreffen noch die Punkte Isolation und Quarantäne, Latenz und Inkubation, Träger, Diagnose, Eintrittspunkte und Vektoren, auf die an dieser Stelle allerdings nicht eingegangen werden soll, da sie für die weitere Analyse nicht zielführend sind. Umso zentraler ist allerdings der letzte Punkt seiner Liste mit dem Titel »AIDS«:

---

42 Zeitgenössische Antivirenprogramme funktionieren effizienter als die von Ferbrache imaginierten: Anstatt jedes einzelne Programm durch einen Einschluss des zu bekämpfenden Materials zu ›immunisieren‹, scannen Antivirenprogramme in regelmäßigen Abständen die Festplatte eines Computers. Finden sie dabei ein Programm, dessen Signatur mit einer in ihrer Datenbank befindlichen Signatur übereinstimmt, melden sie dies dem_der User_in. Die in den letzten Jahren bekannt gewordene Schadsoftware EMOTET konnte genau diesen Vorgang umgehen, indem der Code der Malware sich immer wieder verändert hat, und so unter dem Radar der Antivirenprogramme blieb. In diesem Fall spricht man von einem *polymorphen Virus* (vgl. CISO 2018).

> »Finally, the organism's internal protective systems may recognise legitimate cell material (erroneous decisions resulting from a scan for a virus, or analysis of system activity logs) and may remove legitimate programs. Equally, the virus may alter the operation of the anti-virus software in such a manner as to cause the deletion or corruption of valid data or programs. This could be compared to the Acquired Immuno-Deficiency Syndrome (AIDS) in humans.« (Ebd., 46)

Ein mögliches Gefahrenszenario liegt für Ferbrache also darin, dass das Immunsystem des Computers, sprich: das Antivirenprogramm, durch einen Computervirus beschädigt werden, und infolgedessen nicht mehr genau zwischen legitimen und illegitimen Programmen unterscheiden könne. Dies würde zu einer weiteren Schädigung des Computers führen, ebenso wie zu einer Anfälligkeit für andere Viren, ähnlich wie dies nach einer HIV-Infektion bei Menschen geschähe. Diese Art der Metapher, konstatiert Helmreich (2000, 487), und auch ihre Ausweitung auf vernetze Computer, »make[s] sense only when biological organisms and computers are both envisioned as ›coded texts‹ pasted together with the glue of information.« Diese diskursive Herstellung einer Vergleichbarkeit, die suggeriert, dass Computer und Körper der gleichen Ordnung angehörten, wird in Diskussionen von Computerviren als *Artificial Life* fortgeführt, die jedoch für die folgende Untersuchung nicht von Interesse sind.[43] Stattdessen soll genauer auf die Figur des Immunsystems eingegangen werden.

Der Begriff *Immunität* ist seit einigen Jahrtausenden in Gebrauch und verbindet, wie der Wissenschaftshistoriker Johannes Türk (2014, 107) ausführt, »medizinisches Wissen um den Körper mit einem Wissen um dessen Interaktionen mit seiner Außenwelt […].« Immunität stammt vom lateinischen *immunitas*, das wiederum vom Wort *munus* abstammt, das Verpflichtung, öffentliches Amt oder Aufgabe bedeutet (vgl. ebd.). Nach römischem Recht waren immune Einzelpersonen oder Gruppen von den Aufgaben befreit, die zur Aufrechterhaltung der Gesellschaft notwendig waren, wie beispielsweise der Ausübung öffentlicher Ämter oder der Abgabe von Steuern (vgl. ebd., 108). Im mittelalterlichen Europa kam dem Begriff der Immunität eine neue Dimension zu: Immunität bedeutete nicht mehr nur eine Befreiung von gesellschaftlichen Aufgaben, sondern auch die Fähigkeit, eigene Gesetze sowie eine

43 Vergleiche dazu exemplarisch Spafford (1994), sowie Parikka (2016, 173–237).

eigene Gerichtsbarkeit einzusetzen, und vermittelte so zwischen den Interessen von Kirche und Adeligen (vgl. ebd., 110). In der Phase der Herausbildung von Nationalstaaten entstand schließlich das Konzept der diplomatischen Immunität, das die Grundlage des internationalen Rechts darstellt – wer in diplomatischer Mission unterwegs war, war im fremden Staat straffrei (vgl. ebd., 111). »Der Begriff der Immunität«, fasst Türk (ebd., 112, Herv. i.O.) zusammen, »bezieht sich daher hier zunächst auf den *Staats*organismus, bevor er eine Eigenschaft des biologischen Organismus bezeichnet.« Ende des 19. Jahrhunderts formiert sich schließlich die Immunologie als Wissenschaft, und überträgt den Begriff der Immunität metaphorisch auf das körperliche Phänomen der Resistenz (vgl. ebd.). All diesen Bedeutungszusammenhängen ist gemeinsam, dass Immunität sich als Ausnahme auf eine Norm bezieht (vgl. ebd., 107), also eine Differenz herstellt.

An diesem Punkt lässt sich mit Donna Haraways Aufsatz *The Biopolitics of Postmodern Bodies: Constitutions of Self in Immune System Discourse* anschließen, in dem sie das Immunsystem als ein Objekt des 20. Jahrhunderts sowie als »elaborate icon for principal systems of symbolic and material ›difference‹ in late capitalism« (Haraway 1991b, 204) bestimmt. Der Prozess der Differenzgenerierung ist notwendig für die Herstellung von Bedeutung – ohne Differenz gibt es keine Zeichen, keine Sprache, keine Positionen, und vor allem keine Subjekte. Haraway (ebd.) geht es spezifisch um die Subjektivierungsprozesse von »biomedical, biotechnical bodies and selves in post-modern scientific culture in the United States in the 1980s.« Ausgehend von Treichlers Bestimmung von AIDS als *epidemic of signification* nähert sich Haraway den Feldern und Versatzstücken, die über das Immunsystem als differenzgenerierende Figuration verbunden sind: HIV/AIDS, Krieg, Verkörperung, feministische Science Fiction-Literatur, medizinische Praktiken und viele weitere (auf die an dieser Stelle leider nicht eingegangen werden kann, da sie zu weit weg führen). Das Immunsystem fungiert in all diesen Kontexten Haraway (ebd.) zufolge als

> »a map drawn to guide recognition and misrecognition of self and other in the dialectics of Western biopolitics. That is, the immune system is a plan for meaningful action to construct and maintain the boundaries for what may count as self and other in the crucial realms of the normal and the pathological.«

Die Unterscheidung von, und damit die Grenzziehung zwischen *self* und *other* lässt sich somit als Grundfunktion immunologischer Logik begreifen, was diese an die Grenzaushandlungen des Liberalismus anschlussfähig macht.

Dies schlägt sich auch im IT-Sicherheitsdiskurs nieder: Auf die Spitze getrieben wurde die Idee eine *Computer Immunology* Ende der 1990er Jahre im gleichnamigen Paper von Stephanie Forrest, Steven Hofmeyr und Anil Somayaji. Die Autor_innen beginnen ihren Text mit einer rhetorischen Volte, in der nicht mehr die Informatik Bezug auf die Immunologie nimmt, sondern umgekehrt: »Natural immune systems protect animals from dangerous foreign pathogens, including bacteria, viruses, parasites, and toxins. Their role in the body is analogous to that of computer security systems in computing.« (Forrest et al. 1997, 88) Durch diese mechanistische Beschreibung des Lebens erscheinen Computer als belebt, und als derselben Ordnung angehörend wie Tiere, und damit auch Menschen. Bereits im nächsten Satz wird dieser Zusammenhang jedoch in einer Immunisierungsstrategie des Textes gegen Kritik teilweise aufgelöst: »Although there are many differences between living organisms and computers, the similarities are compelling and could point the way to improved computer security.« (Ebd.) Das von Ferbrache identifizierte und mit AIDS verglichene Problem der Sicherheitsmechanismen in Computern, Schadsoftware unter Umständen nicht korrekt erkennen zu können, sehen auch Forrest, Hofmeyr und Somayaji (ebd., 90) als grundlegend, und formulieren es in der bereits mit Haraway diskutierten Formel des Immunsystems, die in der Unterscheidung von *self* und *other* liegt: »The problem of protecting computer systems from malicious intrusions can similarly be viewed as the problem of distinguishing self from dangerous nonself.« Zeitgenössische, durch Software implementierte Sicherheitsmechanismen, wie beispielsweise Firewalls, so schreiben sie weiter, »have largely failed to take advantage of what is known about how natural biological systems protect themselves from infection.« (Ebd.) Für elaboriertere Sicherheitsmaßnahmen eines Computer-Immunsystems definieren Forrest, Hofmeyr und Somayaji (ebd., 91) sechs grundlegende Aufgaben, über die eine Software, der die Rolle des Immunsystems zukommt, verfügen solle:

> »[…] a stable definition of self, the ability to prevent or detect and subsequently eliminate dangerous foreign activities (infections), memory of previous infections, a method for recognizing new infections, autonomy in managing responses, and a method of protecting the immune system itself from attack […].«

Im Verlauf ihres Artikels stellen die drei Autor_innen einige Überlegungen zu der technischen Realisierung eines solchen Systems vor, die aber durchaus noch weiterer Entwicklung bedürfen. Dazu gehört unter anderem die Mit-

einbeziehung autorisierter User_innen in das *self* des Computers, die, so spekulieren sie, beispielsweise über »user behaviour patterns, or even keyboard typing patterns« (ebd., 91) erkannt werden könnten, obwohl diese Herangehensweise die Gefahr berge, ein zu restriktives System zu entwickeln. Der Artikel endet mit einer Evaluierung der Forschungsergebnisse, gemessen an den zeitgenössischen Möglichkeiten der IT-Sicherheit, in der die Autor_innen darauf hinweisen, dass der Erfolg oder Misserfolg von *Computer Immunology* darin begründet liege, den korrekten Abstraktionsgrad der Immunsystem-Analogie zu bestimmen (vgl. ebd., 96). Als ein kritisches Unterscheidungsmerkmal von Immunologie und auf Computer bezogener Sicherheit machen sie aus, »that the immune system is not concerned with the important problems of protecting secrets, privacy, or other issues of confidentiality.« (Ebd.) Dies deutet darauf hin, dass sie einen fundamentalen Unterschied zwischen kryptographischer Sicherheit und IT-Sicherheit sehen. Aber ließe sich nicht auch das Schützen von Geheimnissen mit immunologischen Analogien ausdrücken? Wird beispielsweise eine Nachricht verschlüsselt, um nur von einer bestimmten Person gelesen werden zu können, muss die Unterscheidung von *self* und *other* zuverlässig funktionieren, denn sonst wäre die Verschlüsselung nicht zu gebrauchen. Das Element des *störenden Dritten* ließe sich in diesem Fall als *other* bezeichnen, wobei *self* Sender_in und Empfänger_in, sowie deren Computer meint. Dies verkompliziert Forrest, Hofmeyr und Somayajis Modell, das nur die Definition von *self* innerhalb *eines* Computers (in Verbindung mit dem_der dazugehörigen User_in) in den Blick nimmt. Doch selbst wenn eine solche Erweiterung möglich wäre: Ganz so eindeutig geht es auch Ende der 1990er Jahre in der Kryptographie nicht mehr zu.

Exkurs: Kryptovirologie

Die vom *AIDS Information Trojaner* verwendete Verschlüsselung war, gemessen an heutigen Standards, recht schwach: Es wurde eine monoalphabetische Substitutionschiffre verwendet (vgl. Gazet 2010, 78), was bedeutet, dass, einmal dechiffriert, die Lösung auf jede weitere Installation der Malware anwendbar war. Und tatsächlich wurde die Verschlüsselung schnell gebrochen: Nachdem die Herausgeber_innen des Magazins *PC Business World*, an dessen Abonnent_innen der auf der AIDS Information Diskette 2.0 enthaltene Trojaner postalisch zugestellt wurde, von dem Missbrauch ihrer Adressliste erfuhren, engagierten sie einen Experten für Computerviren, um den Schaden wieder rückgängig zu machen. Dieser schrieb ein Programm mit dem Namen AIDSOUT, mit dem die Verschlüsselung des Trojaners wieder entschlüsselt werden

konnte (vgl. McKinney/Mulvin 2019, 484). Dies ist in zweifacher Hinsicht bemerkenswert: Einerseits, da der Trojaner durch die Angabe einer scheinbar einzigartigen Referenznummer (vgl. Solomon et al. o.J.) in der als Lizenzerneuerungsformular gestalteten Lösegeldforderung suggerierte, dass jeder betroffene Computer einzeln freigeschaltet werden müsse, und andererseits, da es deutlich werden lässt, wie prekär die AIDS-Analogie für Computer ist: Während es keine erfolgreichen[44] Therapiemöglichkeiten für HIV und AIDS[45] bei Menschen gab, war AIDS im Computer vollständig und nahezu instantan ›heilbar‹.[46] Dies sollte sich schon bald ändern: Nur sieben Jahre nach dem *AIDS Information Trojaner* erreichte die Grundidee der Ransomware ihre nächste Stufe, die gleichsam das technologische Bindeglied zwischen dem *AIDS Information Trojaner* und *WannaCry* darstellt. 1996 veröffentlichten Adam Young und Moti Yung ein Paper über eine Vermischung von Computerviren und kryptographischen Verfahren, die sie *Kryptovirologie* (englisch: *cryptovirology*) nannten. Die dazugehörige Angriffsvariante bezeichnen sie als »cryptoviral extortion attack« (Young/Yung 2017, 25). Dieses Phänomen ist heute unter dem Namen *Ransomware* bekannt (vgl. ebd.).

Kryptovirologie markiert seinen beiden Erfindern zufolge einen Shift im Feld der Kryptographie weg von dem Schutz vor Computerviren hin zum Angriff auf Daten (vgl. Young/Yung 1996, 129). In einem jüngeren Paper mit dem Titel *Cryptovirology: The Birth, Neglect, and Explosion of Ransomware*, das Young

44 Das Medikament Azidothymidine (AZT), das in den USA ab 1986 in klinischen Studien verabreicht wurde, wirkte zunächst vielversprechend, stellte sich aber im Verlauf der Studie als nur kurzzeitig wirksam, sowie von enormen Nebenwirkungen begleitet heraus, was zu heftigen Auseinandersetzungen zwischen Pharmaindustrie, Medizin und Aktivist_innen führte (vgl. Schock/Würdemann 2017; Treichler 1991).

45 (Präventive) Behandlungen der opportunistischen Infektionskrankheiten, wie etwa der Pneumocystis-Pneumonie, wurden allerdings bereits erfolgreich durchgeführt, und hatten auch verlangsamende Auswirkungen auf den Krankheitsverlauf insgesamt (vgl. Treichler 1991, 66–67).

46 Der *AIDS II*-Virus lässt sich als Spiel mit diesem Gegensatz deuten, da die Schadensroutine explizit auf die Un/Möglichkeit der Heilung Bezug nimmt. Dies geschieht in Form einer von schwarzen und weißen Smileys eingerahmten Nachricht: »I have been elected to inform you that throughout your process of collecting and executing files, you have accidentally ƓHÜ¢KΣ► yourself over; again, that's PHUCKED yourself over. No, it cannot be; YES, it CAN be, a vîtûs [virus] has infected your system. Now what do you have to say about that? HAHAHAHAHA. Have ƓHÜÑ [phun] with this one and remember, there is NO cure for AIDS« (McKinney/Mulvin 2019, 477).

und Yung anlässlich der *WannaCry*-Welle verfassten, stärken sie diese Behauptung und weiten sie aus:

> »Cryptography, for millennia, had been perceived as a purely protective technology, and in particular as a way to hide the content of messages, secure data at rest, and authenticate users.« (Young/Yung 2017, 24)

Kryptovirologische Angriffe hingegen »weaponize cryptography as an attack tool as opposed to the previous uses that were defensive in nature.« (Ebd., 25) Dies mag zunächst verwundern, denn seit dem Zweiten Weltkrieg wurde Kryptographie in den USA rechtlich als eine Form von Munition eingestuft, also vorrangig als Militärtechnologie angesehen (vgl. Diffie/Landau 2007, 728). Diese Behauptung erklärt sich allerdings aus der Funktionsweise kryptovirologischer Angriffe. Über die ursprüngliche Zielsetzung ihres Forschungsvorhabens schreiben Young und Yung (1996, 131):

> »We are interested in making the host dependent on the virus. Thus, we design cryptovirology from the point of view of survivability. That is, a virus can survive in the host if it makes the host depend in a critical way on the very presence of the virus itself. If we cannot achieve this, we may approximate it by writing a virus such that its effect on the host is only reversible by the virus writer (so the dependence is approximated by making the host depend on the author rather than the virus).«

Letzteres ist ihnen durch die Kombination von asymmetrischer Kryptographie mit Computerviren[47] auch gelungen – der kryptovirologische »high survivability virus« (ebd., 130) zeichnet sich aus Sicht des Virus durch eine hohe Überlebensfähigkeit aus: Von dem Computer, den er infiziert hat, kann er nicht einfach entfernt werden. Als Inspiration für ihr Vorhaben nennen Young und Yung (ebd., 131) unter anderem den *AIDS Information Trojaner*, den sie trotz seiner leicht zu brechenden Verschlüsselung als einen ersten Schritt in die Richtung eines »high survivability virus« bezeichnen, aber auch den von H.R. Giger entworfenen *Facehugger*[48] aus Ridley Scotts Film Alien (UK/USA 1979).

47 Young und Yung (1996, 131) verwenden Virus als Überbegriff für Computerviren, Trojaner, Würmer und andere Sorten Malware.

48 Der *Facehugger* ist die erste Stufe des *Xenomorph*, also des titelgebenden Aliens, der, wenn er sich einmal an das Gesicht eines Menschen (oder Androiden) geheftet hat, um dessen Körper als Wirt für die nächste Stufe des *Xenomorph* zu gebrauchen, nicht mehr entfernt werden kann, ohne dabei den Wirt zu töten. Young and Yung (2017, 25) kommentieren: »We sought a digital analogue of the facehugger, namely, a forced

Ein bereits eingeführtes Beispiel für eine »cryptoviral extortion attack« ist die Ransomware *WannaCry*, die genau nach den von Young und Yung beschriebenen Kriterien funktioniert: Der_die Angreifer_in generiert ein asymmetrisches Schlüsselpaar, hinterlegt den öffentlichen Schlüssel in der Schadsoftware, und behält den privaten Schlüssel. Die Schadsoftware infiziert einen Computer und verschlüsselt dessen Dateien mit einem auf dem Computer hergestellten symmetrischen Schlüssel, der im Anschluss an diesen Vorgang mit dem öffentlichen Schlüssel des_der Angreifer_in asymmetrisch verschlüsselt wird.[49] Schlussendlich erscheint die Lösegeldforderung, die neben den Kontaktinformationen des_der Angreifer_in und einer Zahlungsanweisung auch den symmetrischen Schlüssel als Ciphertext beinhaltet, der ebenfalls zwecks Entschlüsselung mitgesendet werden muss (vgl. Young/Yung 2017, 25). Theoretisch sollte im Fall der Bezahlung des Lösegelds der symmetrische Schlüssel als Plaintext an die erpresste Person zurückgesendet werden, sodass diese wieder Zugang zu ihren Daten erhält (vgl. ebd.). Damit ist der Effekt des »high survivability virus« also nur durch den_die Angreifer_in rückgängig zu machen.[50] Immunologisch ausgedrückt wird es mit der Verbindung von Schadsoftware und asymmetrischer Kryptographie in der Kryptovirologie also möglich, durch Verschlüsselung das *self*, das bei Forrest, Hofmeyr und Somayaji aus User_in und Computer, oder in der Kryptographie aus Sender_in, Empfänger_in und deren Computern bestand, auf den_die Angreifer_in, dessen_deren Computer und den Computer der

---

symbiotic relationship between a computer virus and its host where removing the virus is more damaging than leaving it in place.«

49 Das hybride Verfahren wird verwendet, da symmetrische Verschlüsselung schneller und weniger ressourcenaufwändig als asymmetrische Verschlüsselung ist. Ein ausreichend langer symmetrischer Schlüssel kann nicht in Polynomialzeit gebrochen werden, wie bereits in Kapitel 2 dargelegt wurde. Darüber hinaus muss bei diesem hybriden Verfahren nur der asymmetrisch verschlüsselte symmetrische Schlüssel an den_die Angreifer_in versendet werden, um eine mögliche Entschlüsselung zu gewährleisten, und nicht die gesamten verschlüsselten Daten der Festplatte.

50 Obwohl dieses Verfahren bereits seit 1996 bekannt ist, dauerte es noch ca. 20 Jahre, bis kryptovirologische Angriffe in großem Maß durchgeführt wurden, da Angreifer_innen Gefahr liefen, durch den Empfang des Lösegelds ins Visier der Strafverfolgungsbehörden zu geraten. Pseudonyme Kryptowährungen wie Bitcoin oder Ethereum lösten dieses Problem, und verwandelten Ransomware in ein regelrechtes Geschäftsmodell mit einem geschätzten Jahresumsatz von einer Milliarde US-Dollar (vgl. Young/Yung 2017, 25).

erpressten Person[51] zu beschränken, wodurch letztere zum *störenden Dritten* gemacht wird.

3.4.2 User_innenzentrierte Lösungsansätze: *Digital Hygiene/Safe Hex*

Mit dem *Digital Immunology*-Konzept wurde ein informatischer Ansatz vorgestellt, der die Herstellung von IT-Sicherheit in erster Linie softwarebasiert zu erreichen versucht: User_innen tauchen bei Forrest, Hofmeyr und Somayaji nur indirekt auf, nämlich in Form ihrer Effekte auf die Maschine, die, sofern sie von autorisierten User_innen kommen, irgendwie als dem *self* der Maschine zugehörig markiert werden müssen. Anhand der Funktionsweise von Kryptovirologie wurde eine Spielart von Schadsoftware vorgestellt, die die Relation von autorisierten User_innen und ihren Computern unterläuft und stört, indem erstere als das *störende Dritte* markiert und ausgeschlossen werden. Darüber hinaus wurde die Rolle von User_innen im vorliegenden Kapitel bisher nicht weiter bestimmt, was aber an dieser Stelle anhand der Konzepte *Digital Hygiene* und *Safe Hex* nachgeholt werden soll. Sowohl *Digital Hygiene* als auch *Safe Hex* zielen auf eine Regulierung des Verhaltens der Computernutzer_innen ab, die für die Herstellung von IT-Sicherheit mit verantwortlich gemacht werden.

Digital Hygiene

»The notions of digital hygiene«, schreibt Parikka (2016, 2), »orderly computing, and clean communication has [sic!] appeared in the vocabulary of computer culture since the 1980s.« Dies führt er auf das mit dem technologischen Fortschritt ab den 1980er Jahren einhergehende Körperideal zurück: »The clean body of modernization found its imaginary ideal in the computer organism.« (Ebd., 119) Verknüpft mit den Bildern digitaler Hygiene, ordentlicher Computernutzung und sauberer Kommunikation ist also das Konzept des Computers als maschinischem, sauber-elektronischem Körper. Helmreich (2000, 477) verbindet dieses Körperideal darüber hinaus mit dem Liberalismus der US-amerikanischen Gesellschaft, und konstatiert:

> »Computers are imagined as pristine, autonomous entities that exist prior to their embedding in networks – an idea that echoes the liberal conception

51 Der_die Angreifer_in hat zwar keinen Zugriff auf die Daten der erpressten Person, greift aber in ausreichendem Maß in die Funktionsweise von deren_dessen Computer ein, um Teil dieser Trias zu sein.

> of society as made up of individuals who exist prior to the society of which they are a part, an ideology deeply written into U.S. political culture.«

Doch der Körper des Computers blieb, wie in diesem Kapitel deutlich geworden ist, nicht lange diesem Ideal treu: »Just as the body biologic (and politic) was, from the end of the nineteenth century, the object of constant attacks by minuscule viruses and bacteria, so the computer soon had its own share of dirt.« (Parikka 2016, 119) Eine besonders bemerkenswerte Reaktion auf den ›Dreck‹ und die damit einhergehenden ›Krankheiten‹ der sauberen Systeme ist die Forderung nach *Public Health* für die vernetzte Gesellschaft (vgl. ebd.). Public Health lässt sich als »die Wissenschaft und die Praxis der Verhinderung von Krankheiten, Verlängerung des Lebens und Förderung der Gesundheit durch organisierte Anstrengungen der Gesellschaft« (Robert Koch-Institut 2016) definieren, und wird damit als eine biopolitische Maßnahme erkennbar. In ihrer Analyse von Foucaults Konzeptionen von Sicherheitsdispositiv und Biopolitik konstatiert Maria Muhle (2008, 261, Herv. i.O.) unter Bezugnahme auf Georges Canguilhems Begriff des Lebens: »Die Bio-Macht bezieht sich nicht nur *auf das Leben*, sondern sie tut dies zugleich *nach dem Modell des Lebens*.« Dies bedeutet konkret, dass die Bio-Macht das Leben reguliert, nicht indem sie es diszipliniert, oder gezielt auf einen Aspekt des Lebens wirkt, sondern indem sie sich multifaktoriell aufstellt, und über das Milieu die Bedingungen für das Leben reguliert. »Ein solchermaßen regularisierbares und indirekt erfassbares Leben«, so schreibt Muhle (ebd., 263) weiter, »verweist auf die spezifisch organische Dimension eines Lebensbegriffs, so wie ihn auch die moderne Biologie kennt.« Die vermutlich prominenteste Forderung innerhalb der Informatik für diese Form der Herstellung von Sicherheit, die sich an dem Wissen der modernen Biologie, vor allem der Immunologie orientiert, sowie über das Milieu die Bedingungen für sichere Informationstechnologie regulieren möchte, stammt von Bryan Kocher, der Ende der 1980er Jahre Präsident der *Association for Computing Machinery* (ACM) war. In seinem kurzen, aber viel zitierten Text mit dem Titel *A Hygiene Lesson*, den Kocher (1989, 3) als Einleitung zur offiziellen Publikation der ACM verfasst hat, reagiert er direkt auf den *Morris Worm*, den er als einen Streich, aber auch als Warnsignal begreift: Habe der Morris Worm zwar keinen Schaden angerichtet, so sei durch ihn doch unmissverständlich klar geworden, wie verletzlich vernetzte Systeme seien. Bemerkenswert ist, dass auch Kocher (ebd.) den Morris Worm als Virus bezeichnet, und zunächst Parallelen zu HIV/AIDS zieht: »The parallels between contracting a PC ›virus‹ and a sexually transmitted disease are

painfully obvious«, nur um wenig Sätze später die »UNIX epidemic«, also den Morris Worm, mit der Cholera-Epidemie des 19. Jahrhunderts gleichzusetzen. IT-Sicherheit, also *Security*, wird bei Kocher (ebd., 3–6) damit gleichbedeutend mit Hygiene, und somit Prävention:

> »Just as in human society, hygiene is critical to preventing the spread of disease in computer systems. Preventing disease requires setting and maintaining high standards of sanitation throughout society, from simple personal precautions (like washing your hands or not letting anyone know your password), to large investments (like water and sewage treatment plants or reliably tested and certified secure systems).«

Auf die Herkunft der hier von Kocher aufgerufenen Hygienemaßnahmen zur Prävention von Krankheiten, wie beispielsweise das Händewaschen oder die Einrichtung einer geregelten Frisch- und Abwasserversorgung innerhalb von Städten, geht auch Michel Foucault in seiner von 1977–1978 am Collège de France gehaltenen Vorlesung *Sicherheit, Territorium, Bevölkerung. Geschichte der Gouvernementalität I* ein, in der er die Bio-Macht untersucht. Bereits im ersten Teil zeichnet er die Entstehung des Sicherheitsdispositivs nach, und grenzt dieses von juristischen, juridischen und Disziplinarmechanismen ab. Während letztere durch Überwachungs- und Korrekturmechanismen gekennzeichnet sind, etabliert das Sicherheitsdispositiv statt einer binären Aufteilung in erlaubte und verbotene Ereignisse einen »als optimal angesehene[n] Mittelwert« (Foucault 2006, 20) für das Vorkommen bestimmter Ereignisse, sowie »Grenzen des Akzeptablen« (ebd.), jenseits derer ein bestimmtes Ereignis nicht mehr geschehen dürfe. Sicherheit ist also befasst mit der statistischen Verteilung von Elementen und Ereignissen. Daher arbeitet sie mit den materiellen Gegebenheiten eines Territoriums: »mit der Lage, dem Ableiten von Abwässern, mit den Inseln, mit dem Freiland usw. Sie bearbeitet folglich ein Gegebenes.« (Ebd., 38) Im Fall von Computersicherheit wären die materiellen Gegebenheiten sowohl die Hard- als auch die Software und die Vernetzung der Computer untereinander – oder für Kocher (1989, 6) »reliably tested and certified secure systems«. Ein entscheidendes Merkmal des Sicherheitsdispositivs ist allerdings, dass Sicherheit nicht als perfekt, nicht als absolut gedacht wird. Stattdessen

> »[…] geht [es] einfach darum, die positiven Elemente zu maximieren, so daß man auf bestmögliche Weise vorankommt, und im Gegensatz dazu Risiko und Mißstand, wie den Diebstahl, die Krankheiten usw., auf ein Mindestmaß zu beschränken, wobei man genau weiß, daß man sie niemals besei-

> tigen wird. […] Das wird nie aufzuheben sein, also bearbeitet man Wahrscheinlichkeiten.« (Foucault 2006, 38)

Auch Kochers Forderung bewegt sich in eine ähnliche Richtung. Es geht ihm weniger um absolute Sicherheit, als um eine andauernde Arbeit an ihrer Herstellung, was erkennen lässt, dass absolute Sicherheit nie ganz erreicht werden kann. Er bemerkt, dass nicht vernetzte Computer, ähnlich wie Einsiedler, die außerhalb von gesellschaftlichen Zusammenhängen stehen, so gut wie nie erkranken würden, für eine vernetzte Gesellschaft aber andere Regeln gelten müssten:

> »[…] if we are to become a networked society, we must treat computer diseases as a real threat to that society. We must heed the public health warnings from NSA, practice personal systems hygiene, adhere to sanitary standards, and support the development of secure systems to keep the germs out. Electronic epidemics should be like cholera epidemics – something you only read about in history books.« (Kocher 1989, 3–6)

Kochers Vision folgend, sollte die NSA eine ähnliche Rolle übernehmen wie die Centers for Disease Control und regelmäßige Gesundheitswarnungen aussprechen (der Versuch der Einrichtung eines den CDC ähnlichen Center for Virus Control als Reaktion auf den Morris Worm wurde bereits mit Ross (1991, 75–76) erwähnt), und müssten die Nutzer_innen vernetzter Computer keine neuen Techniken der Problemlösung erlernen, sondern könnten sich an dem gesellschaftlich vorhandenen Alltagswissen um die eigene Körperhygiene orientieren, das sie eigenverantwortlich auf ihre Maschinen anwenden sollen. Das Programm von »personal systems hygiene« bedeutet also, die eigene Körperhygiene auf die eigene Maschine auszudehnen, und so beide Körper als *self* vor allen biologischen und informatischen Formen von *other* zu schützen. Computer werden so nicht nur als Körper gedacht, sondern dem eigenen Körper gleichgestellt – eine Annäherung, die im Folgenden noch wichtig sein wird. Die Forderung nach einer Computerhygiene beinhaltet »a range of practices, demands, advice, and precautions« (Parikka 2016, 129), die bei Kocher von der Geheimhaltung von Passwörtern bis hin zu regelmäßigen Sicherheitszertifizierungen von IT-Systemen reicht. Auf diese Weise werden nicht nur Institutionen in die Pflicht genommen, für Sicherheit zu sorgen, sondern auch, wie Parikka (ebd.) schreibt, »the user and her way of interacting with the computer«, die zum »safe link in the networking chain«

werden sollen. Kochers Wunsch, über ›elektronische Epidemien‹ nur noch in Geschichtsbüchern zu lesen, hat sich dennoch nicht realisiert.

Safe Hex

Die zweite Ebene, auf der User_innen als für IT-Sicherheit Verantwortliche adressiert werden, ist eng mit der Idee von »personal systems hygiene« verbunden, rückt aber HIV und AIDS, die bei Kocher eine eher untergeordnete Rolle spielen, als Metaphern für schädliche Phänomene in vernetzten Computern ins Zentrum. Mit der metaphorischen Übertragung von AIDS auf Computerviren gehen nicht nur die medialen Gemeinsamkeiten der Übertragung durch Ansteckung einher, denn, wie Deborah Lupton (1994, 560) in ihrem Artikel *Panic computing: The viral metaphor and computer technology* konstatiert, »[v]iewing computer malfunction as a viral illness unavoidably invokes a moral framework.« Basierend auf Susan Sontags Untersuchung *Illness as Metaphor and AIDS and Its Metaphors* beobachtet Lupton (ebd., 561) in Bezug auf HIV und AIDS, dass der öffentliche Diskurs vor allem von Fragen nach Moral, Verantwortung und Schuld geprägt sei, wobei die letzten beiden stets den Kranken selbst zugewiesen werden.[52] Lupton (ebd., 561) schreibt weiter:

> »Public health discourse now emphasizes the responsibility of the individual to stay healthy, avoid risk and resist indulgence in certain behaviours defined as ›dangerous‹. It is believed that one does not become ill merely out of bad luck; one becomes ill because one has courted illness in some way, whether it be going out in the rain without an umbrella, eating too few vegetables and too much fat, suppressing anger in an inappropriate manner, or engaging in socially proscribed sexual acts.«

Für den HIV/AIDS-Diskurs der 1980er Jahre ist vor allem das Partizipieren in »socially proscribed sexual acts«, also verbotenen und verpönten Sexualpraktiken, von Bedeutung, das mit einer »homophobic representation of homosexuality« (Bersani 1987, 209) verknüpft ist. Bereits zu Beginn dieses Kapitels wurde mit Deuber-Mankowsky (2017b, 16) angerissen, dass in der AIDS-

52 Ein Beispiel für diese Moralisierung, die eine Infektion mit HIV als eigenes Verschulden formuliert, und gleichzeitig in einer zynischen Geste die Kontrollierbarkeit der eigenen Krankheit verspricht, ist die *New Age*-Bewegung und deren wohl prominenteste Vertreterin Louise Hay. »Die Ursache der Krankheit [AIDS, MS], so Hays Botschaft, ist Selbsthass, sie kann, so ihr Versprechen, geheilt werden durch Selbstliebe und Vergebung.« (Deuber-Mankowsky 2017b, 41)

Krise durch die konservative US-amerikanische Politik die »Krankheit […] zu einer Strafe und Homosexualität zu einer Sünde erklärt« wurde. Leo Bersani (1987, 210) analysiert die mit dieser Zuschreibung einhergehende diskursive Verschiebung: Schwule Männer seien nicht nur selbst schuld, wenn sie sich durch ihr Sexualverhalten mit HIV infiziert haben, mehr noch: »It is as if gay men's ›guilt‹ were the real agent of infection.« Aber worin genau, fragt sich Bersani weiter, besteht diese bereits vor einer HIV-Infektion da gewesene Schuld eigentlich? Bezugnehmend auf Simon Watney und weitere, von ihm nicht genannte Theoretiker_innen, bemerkt Bersani (ebd.), »[e]veryone agrees that the crime is sexual, and […] define[s] it as the imagined or real promiscuity for which gay men are so famous.« Sich dieser phantasmatisch-homophoben Verknüpfung weiter nähernd, kommt Bersani (ebd.) zu dem Schluss, »the act […] may itself be associated with insatiable desire, with unstoppable sex.« Dabei weisen die Vorstellungen von Mediziner_innen, die in der medialen Berichterstattung zu sehen und hören sind, wie Bersani (ebd., 211) mit Watney analysiert, Anklänge an die Diskursivierung weiblicher Prostituierter auf, die als Behältnisse für Geschlechtskrankheiten (konkret: Syphilis) imaginiert wurden, die sie angeblich an ›unschuldige Männer‹ weitergaben. Bersani (ebd.) schreibt weiter:

> »[T]he similarities between representations of female prostitutes and male homosexuals should help us to specify the exact form of sexual behavior being targeted, in representations of AIDS, as the criminal, fatal, and irresistibly repeated act. This is of course anal sex […].«

Konkret handelt es sich also um penetrativen Analsex, der, verschränkt mit der tatsächlichen und imaginierten Promiskuität homosexueller Männer zum Problem erklärt wird. Gerade die Vorstellung von homosexueller Promiskuität, von »gay men having sex twenty to thirty times a night, or once a minute«, führt Bersani (ebd.) aus, sei weniger mit den Fantasien männlicher als mit denen weiblicher Promiskuität belegt, die wiederum mit einer »fantasy of female sexuality as intrinsically diseased« zusammenhingen. Auf diese Weise werde Promiskuität nicht als das Infektionsrisiko erhöhend diskursiviert, sondern direkt zum »*sign of infection*« (ebd., Herv. i.O.). Die damit einhergehende Stigmatisierung von Promiskuität drückte sich auch in den am heteronormativen Ideal der *weißen* Kleinfamilie ausgerichteten Gesundheitsempfehlungen aus, die die Medienlandschaft dominierten (vgl. ebd., 203). So wurden unter anderem Monogamie und Abstinenz als wirksamer Schutz vor einer HIV-Infektion diskutiert, und *safe partners* sicheren

Sexpraktiken, also *Safe/r Sex*,[53] vorgezogen (vgl. Crimp 1987a, 252–253). Diese Empfehlungen sind, wie Douglas Crimp (ebd., 253) spitz bemerkt, an dem Mythos orientiert, »that monogamous relationships are not only the norm but ultimately everyone's deepest desire« – und darüber hinaus schützen sie, wie auch Bersani (1987, 218) schreibt, nicht zuverlässig vor einer HIV-Infektion. Doch in den Empfehlungen von Monogamie oder gar Abstinenz lässt sich nicht nur das heteronormative Familienideal erkennen, sondern auch der Versuch, HIV über eine Einschränkung der Verbreitungswege einzudämmen, nur mit, wie sich gezeigt hat, den absolut falschen Mitteln. Die Stigmatisierung ganzer Personengruppen als scheinbar einzigen Gefahrenherden für die Übertragung von HIV, und die Einschränkungen der körperlichen Verbindungen, die diese mit anderen eingehen könnten, statt der Sicherung dieser Verbindungen, hat sich als falsch und gefährlich erwiesen, »because people do not abstain from sex, and if you only tell them ›just say no‹, they will have unsafe sex.« (Crimp 1987a, 252–253)

Eine ähnliche Dynamik zeigt sich auch im IT-Sicherheitsdiskurs der 1980er und 1990er Jahre in den Versuchen der Regulierung körperlicher Verbindungen zwischen Computern: Auf die Unvereinbarkeit von Sicherheit vor viraler Software in vernetzten Systemen mit denselben hatte bereits Cohen (1987, 34) in *Computer Viruses. Theory and Experiments* hingewiesen. Dennoch ist ihm klar, dass Vernetzung nur durch Informationsaustausch realisiert werden kann, was also eine Koexistenz viraler Elemente und sicherer Computernetze unter »significant constraints« (ebd., 35) voraussetzt. Diese Einschränkungen werden durch die HIV/AIDS-Metaphorik auf die Nutzer_innen ausgelagert, die als Verantwortliche für die Sicherheit ihrer eigenen Computer, und vermittelt darüber auch der anderen Computer eines Netzwerks positioniert werden. »Where AIDS had created a new culture of bodily anxiety and political paranoia«, schreibt Parikka (2016, 34), »computer sex diseases were thought to create similar fears about communication and digital contact.« Ähnlich wie der medial dominante HIV/AIDS-Diskurs konzentrierte sich auch der IT-Sicherheitsdiskurs auf die Prävention von Ansteckungen, und die mediale

53 Die Bezeichnung *Safe Sex* entstand in den 1980er Jahren (vgl. Crimp 1987a). Heute hat sich in manchen Kontexten die Bezeichnung *Safer Sex* durchgesetzt, um zu betonen, dass es auch mit dem Einsatz von adäquaten Verhütungsmitteln keinen restlos sicheren Sex gibt – nur *sichereren Sex*. Die von den Aktivist_innen intendierte Bedeutung des Konzepts wird dadurch nicht verändert.

Berichterstattung über Computersicherheit, Werbematerialien für Antivirensoftware, Computerfachzeitschriften sowie Ratgeberliteratur zeichneten das Bild des unschuldig-reinen Computers, dessen Gesundheit in den Händen von sich potenziell gefährlich verhaltenden Nutzer_innen liege (vgl. ebd., 132–133). So formierte sich »the idea of a responsible user, who practiced digital hygiene and *safe hex*« (ebd., 179). *Safe Hex* ist jedoch im Gegensatz zu *Safe/r Sex* nicht mit der Entstigmatisierung von Promiskuität/hoher Konnektivität verbunden, sondern beinhaltet in erster Linie Verbots- und Verzichtsratschläge. Damit folgt *Safe Hex* weiterhin der Maxime der Eigenverantwortung der Nutzer_innen, die, falls sie dieser Verantwortung nicht gerecht werden sollten, eventuelle Schäden selbst verschuldet haben. Vor diesem Hintergrund lohnt sich ein erneuter Blick auf Brigitte Weingarts (2002, 80) Beschreibung der »Verwicklung der Ansteckungsgefahren« beim *AIDS Information Trojaner*:

> »Wer jede x-beliebige Diskette nicht als per se mit Vorsicht zu behandelnden ›Fremdkörper‹ erachtet, sondern in den ›intimen Öffnungen‹ seines Computers zuläßt, ist beim ersten Test – auf ›gesundes Mißtrauen‹ – schon durchgefallen. Er/sie hat sich mit dieser Fahrlässigkeit gewissermaßen schon in die ›Risikogruppe‹ katapultiert.«

Was Weingart hier als Subtext des *AIDS Information Trojaners* beschreibt, illustriert nicht nur die mit den HIV/AIDS-Metaphern einhergehende Verwicklung der Ansteckungsverfahren, sondern auch die Verwicklung der dominanten gesellschaftlichen Reaktionen, sowie die dem IT-Sicherheitsdiskurs eingeschriebene Homophobie: Haben die Nutzer_innen kein *Safe Hex* praktiziert, und ihren Computer ungeschütztem Verkehr mit einer fremden Diskette ausgesetzt, so sind sie auch selbst schuld an dem entstandenen Schaden. Als sichere Computernutzungspraktiken werden allerdings weniger Strategien für einen sicheren Umgang mit fremden Disketten oder (raub-)kopierter Software angeführt, als vielmehr der Appell, auf diese besser zu verzichten:

> »›Do not copy programs,‹ ›do not bring program disks from home to work,‹ ›do not boot your computer from an unknown disk,‹ ›check all disks before using them,‹ ›check all downloaded software before using it‹ – these and a range of similar recommendations were used to guide the user to proper PC habits.« (Parikka 2016, 136)

Die meisten dieser Ratschläge lassen sich mit Crimp als Verbote im Sinne einer unrealistischen »just say no«-Abstinenz begreifen, wohingegen wenigstens der Ratschlag, heruntergeladene Software vor dem ersten Ausführen zu

überprüfen, der Idee von *Safe/r Sex* so nahekommt, wie dies in Bezug auf Computer möglich ist. Gekoppelt mit den Verboten bei gleichzeitiger Forderung nach sicheren Computernutzungspraktiken war die Etablierung des Softwaremarkts. Sicherheitsprobleme wie Computerviren und -würmer werden damit, wie Parikka (ebd., 137) ausführt, verwendet um zwischen »healthy capitalist consumer products and software programs distributed as shareware or even freeware« zu unterschieden, sowie letztere als potenziell gefährlich zu markieren. Die bereits diskutierte Kriminalisierung von Hacking stellt einen weiteren Schritt in diese Richtung dar. Parikka (ebd.) schreibt weiter: »[C]leanliness and hygiene are what the consumer pays for. Trust has a cost. This demonstrates how consumer products succeed in their role as ›anxiety relievers.‹« Oder, wie sich mit Andrew Ross (1991, 76) polemisch hinzufügen lässt: »The underlying moral imperative is this: you can't trust your best friend's software any more than you can trust his or her bodily fluids. Safe software or no software at all!« Vertrauen ist also nur in kapitalistischen Strukturen denkbar, und so lässt sich *Safe Hex* bestenfalls als eine Schwundstufe des Konzepts von *Safe/r Sex* begreifen: In den meisten Fällen meint *Safe Hex* entweder Verzicht oder *Safe Partners*, wie beispielsweise vertrauenswürdige Softwarefirmen. Mit McKinney und Mulvin (2019, 487–488) lässt sich resümieren: »[I]n the 1990s, self-regulation and personal responsibility governed both mainstream public pedagogies around HIV and user responsibility in computing (and continue to do so today).«

Negative Sicherheit

> »The only computer that's completely secure […] is a computer that no one can use.« (Kaplan 2016)

Das vorliegende Kapitel hat bisher sowohl einen Blick auf die Anfänge von Schadsoftware geworfen als auch auf zeitgenössische Phänomene, um mit diesen in einer Kreuzstichbewegung Überlegungen zum Diskurs der IT-Sicherheit vorzustellen. Innerhalb dieses Spannungsfelds wurde sowohl grundlegendes Wissen der Informatik zur Beschaffenheit von Computerviren, -würmern und Kryptovirologie/Ransomware vermittelt, als auch medienwissenschaftliche Überlegungen zur Medialität derselben entwickelt. Darüber hinaus wurde die Verbindung des IT-Sicherheitsdiskurses mit dem AIDS-Diskurs der 1980er Jahre nachgezeichnet. Als kurzes Resümee lässt sich an dieser Stelle festhalten, dass die Herstellung von Sicherheit in IT-Systemen, die hier als vernetzte Computer gefasst wurden, immunologisch strukturiert

ist, insofern sie beständig mit Grenzaushandlungen beschäftigt ist. Donna Haraway folgend, die das Immunsystem als diskursive Figuration des 20. Jahrhunderts für die Differenzgenerierung, und damit die Unterscheidung von *self* und *other* analysiert hat, wurden die Grenzaushandlungen der IT-Sicherheit anhand der ersten Antivirenprogramme, aber insbesondere anhand des Konzepts der *Computer Immunology* von Stephanie Forrest, Steven Hofmeyr und Anil Somayaji sichtbar, bei dem ein computereigenes Immunsystem in Form von Software realisiert werden sollte. *Computer Immunology* markiert Schadsoftware als das *störende Dritte*, das aus den rechnerischen Prozessen von Computern ausgeschlossen und an seiner Verbreitung gehindert werden muss. Eine solche Herangehensweise, die die Herstellung von Sicherheit primär auf Software auslagert, musste notwendiger Weise scheitern, da die Unterscheidung erwünschter und unerwünschter Prozesse in vielen Fällen nicht eindeutig bestimmt werden kann. Dies liegt einerseits darin begründet, dass, wie mit Sybille Krämer aufgezeigt wurde, die Medialität von Computerviren und -würmern sich stark ähnelt, was hauptsächlich auf den beiden Phänomenen eigenen Prozess der Übertragung durch Ansteckung zurückzuführen ist. So werden diese Phänomene vergleich-, und mitunter verwechselbar, auch wenn sie aus informatischer Perspektive unterschiedlich definiert werden (vgl. Spafford 1989). Zusammengenommen mit Jussi Parikkas Feststellung, dass Schadsoftware als Bestandteil vernetzter digitaler Systeme begriffen werden müsse und nicht als ein ihnen äußerlicher Störfaktor, wird klar, dass das Immunsystem als strukturierende Metapher der IT-Sicherheit, was die Abwendung von Schaden angeht, in seiner Effektivität begrenzt ist: Aufgrund der Ambiguität viraler Prozesse, die sich sowohl in Schadsoftware als auch in erwünschter Software beobachten lassen, hat sich eine rein softwarebasierte Lösung für die Sicherheitsprobleme vernetzter Systeme als unzureichende Schutzmaßnahme herausgestellt. Mit den Konzepten der *Personal Systems Hygiene* und der HIV/AIDS-Metaphorik von *Safe Hex* wurde die Funktionsweise des Immunsystems auf die Nutzer_innen ausgedehnt, die so verantwortlich für die Gesundheit ihrer Computer wurden. Die immunologische Verfasstheit des IT-Sicherheitsdiskurses entfaltet auf diese Weise über die Verbindung von vernetzten Computern und HIV/AIDS eine normalisierende Wirkung, die bestimmte Formen der Computernutzung als normal und andere als nicht normal diskursiviert. Nahezu all diese Strategien und Praktiken basieren auf Grenzschutz, Exklusion und Abschottung, die kennzeichnend sind für den negativen Sicherheitsbegriff des Liberalismus (vgl. Loick 2021, 268–272). Dieser liegt damit, wie gezeigt werden konnte, nicht nur der Kryptologie,

sondern auch der IT-Sicherheit zugrunde. Das Wettrennen von Hacks und Sicherheitsupdates, wie es bei zeitgenössischen Ransomware-Wellen wie *WannaCry* zu beobachten ist, ist nur ein Beispiel unter vielen, anhand dessen sich das dem IT-Sicherheitsdiskurs ebenso wie der medizinischen Immunität eigene »Paradigma einer Logik der Steigerung« (Deuber-Mankowsky 2017b, 38) ausdrückt. Mit Sybille Krämer (2008, 149) lässt sich feststellen: »Computerwürmer regen zur ›Heilung‹ – oder sollen wir sagen: zur ›Immunisierung‹ – von Betriebssystemen an.« Diese Immunisierung von Betriebssystemen besteht in ebenjener Überbietungslogik zwischen Hacker_innen und Softwareindustrie. Es stellt sich dennoch die Frage, ob nicht andere Formen von Sicherheit für die Nutzung vernetzter Systeme denkbar wären. In den nächsten Kapiteln soll der Diskussion dieser Frage nachgegangen werden, indem zunächst anhand von Backdoors eine Umdeutung des hier analysierten homophoben HIV/AIDS-Diskurses unternommen wird, und im Anschluss daran einige Überlegungen zu *Queer Computation* vorgestellt werden.