6. Schluss

> Eine reparative Perspektive geht von dem offensichtlichen Umstand aus, dass unsere Welt beschädigt und gefährlich ist, aber anstelle einer *bloßen Wiederholung* von ›bad news‹ zielt sie darauf, eine unterstützende Beziehung zu den Objekten in unserer Umgebung zu ermöglichen, was die ungewöhnliche Forderung nach Liebe als Grundlage der eigenen wissenschaftlichen Arbeit begründet. *(Michaelsen 2018, 99, Herv. i.O.)*

Angefangen bei der Kryptologie über die Geschichte der IT-Sicherheit, über das Zusammentreffen der beiden Bereiche in Kryptovirologie (Ransomware) und Kleptographie (Backdoors) bis hin zu den Versuchen, Queerness und Technik zusammenzudenken, hat die vorliegende Untersuchung entlang der Achsen negativer und queerer Sicherheitsbegriffe sowie paranoider und reparativer Praktiken der Wissensproduktion die Frage diskutiert, wie Sicherheit in digitalen Kulturen organisiert ist und sein könnte. Dabei wurden Brücken zwischen differenten Fachkulturen, und damit unterschiedlichen Formen der Wissensproduktion und -organisation, zwischen unterschiedlichen Rationalitäten und Attachments geschlagen: Zwischen mathematisch-informatischem Wissen und einer stark durch die Queer Theory beeinflussten Medienwissenschaft, was nicht zuletzt durch die reparative Praktik, Liebe als Grundlage der eigenen wissenschaftlichen Arbeit zu begreifen, möglich wurde.

Der Sicherheitsbegriff von Kryptologie und IT-Sicherheit wurde im Verlauf der Untersuchung als negativer Sicherheitsbegriff bestimmt. Anhand der kryptographischen Modellbildung im Fachbereich *Beweisbare Sicherheit* und vor dem Hintergrund der Medialität von Kryptographie wurde der Vorgang der Reduktion besprochen, sowie die Figur des *störenden Dritten*, die aus dem unsicheren Kanal eines gegebenen Systems ausgeschlossen werden muss, als leitende Idee der Kryptologie beschrieben. Für die Phase der Herausbildung der IT-Sicherheit in den 1980er Jahren spielt das *störende Dritte* und dessen Ausschluss aus den mittlerweile vervielfachten unsicheren Kanälen ebenfalls eine maßgebliche Rolle, und wurde anhand einer starken Bezugnahme auf den heteronormativen Mainstream-Diskurs über HIV und AIDS, und damit auf das Immunsystem als Figuration der Differenzgenerierung und auf die Herstellung von Sicherheit für vernetzte Computer übertragen. IT-Sicherheit, so konnte anhand der Konzeptionalisierung von Schadsoftware sowie des Umgangs mit derselben gezeigt werden, imaginiert Computer als Körper, die angesichts dessen allerhand diskursiven und materiellen Ansteckungspotentialen ausgesetzt sind. Den homophoben Elementen des zur Zeit der AIDS-Krise dominanten Diskurses folgend, nimmt die IT-Sicherheit die User_innen in die Pflicht, eigenverantwortlich für die Sicherheit ihrer Maschinen zu sorgen, und, durch die bereits genannten Ansteckungspotentiale, auch für ihre eigene.

Mathematisch-technische Konzeptualisierungen von Sicherheit in digitalen Kulturen folgen also einem negativen Sicherheitsbegriff, und sind darüber hinaus durch paranoide Praktiken der Wissensproduktion gekennzeichnet. Paranoia erfüllt in diesem Zusammenhang sowohl für die Kryptologie als auch die IT-Sicherheit eine doppelte Rolle: Zum einen kann negative Sicherheit nur durch das Antizipieren einer Bedrohung gedacht werden. Zum anderen dient die durch paranoide Praktiken versuchte Vermeidung negativer Affekte der Selbstversicherung des Diskurses, in den die Unsicherheit, und damit die negativen Affekte, trotz aller Bemühungen immer wieder einbrechen. Die paranoiden Praktiken der Wissensproduktion sind damit konstitutiv für die den Kryptologie- und IT-Sicherheitsdiskurs kennzeichnende Überbietungslogik negativer Sicherheit.

Nachdem durch die Diskussion von Backdoors dieser Diskurs für Fragen nach einem möglichen anderen Sicherheitsbegriff geöffnet wurde, konnte anhand von *QueerOS* und *Queer Computation* zunächst herausgearbeitet werden, dass der Versuch, reparative Praktiken in der Form einer Einführung von Queerness in die Logik der Informatik zu denken, kein gangbarer Weg für

eine Neubestimmung von Sicherheit in digitalen Kulturen sein kann. Infolgedessen hat die vorliegende Untersuchung den Fokus von dem Versuch, einen queeren Sicherheitsbegriff innerhalb der IT-Sicherheit zu etablieren, hin zu den Modalitäten queerer Sicherheit in und mit digitalen Kulturen verschoben, sowie tentative Ideen für die Möglichkeit eines solchen skizziert. Der Einsatz eines queeren Sicherheitsbegriffs würde darin liegen, im Gegensatz zu einem paranoid strukturierten, negativen Sicherheitsbegriff, genau nicht einer fortifizierenden Überbietungslogik zu folgen, in der die für die Herstellung von Sicherheit permanent erforderlichen Grenzaushandlungen zwischen vernetzten Computern untereinander, aber auch zwischen Computern und User_innen letztlich in der Eigenverantwortung derselben liegen. Ein queerer Sicherheitsbegriff legt stattdessen Wert auf eine solidarische Herstellung von Sicherheit, an der Menschen und Computer gemeinsam beteiligt sind, und die nur durch die Anerkennung von immer schon gegebener Unsicherheit als Bedingung für die Herstellung von Sicherheit möglich wird. Weiterführend gilt es, Praktiken queerer Sicherheit in und mit digitalen Medien und Systemen zu entwerfen, die nicht auf der Ebene des Technischen angesiedelt sind, aber dennoch über ein genaues Wissen der technischen Funktionsweisen verfügen. Infolgedessen bleibt an dieser Stelle nur noch, zu weiteren Überlegungen und Unternehmungen aufzurufen, die sich in reparativer Weise mit Fragen nach Sicherheit in und mit digitalen Kulturen auseinandersetzen. Damit schließt diese Untersuchung so, wie sie auch mit Marais und Haraway (1997, 123) begonnen hat: »For thus, all things must begin with an act of love.«