

Inhalt

1. Einleitung	7
1.1 Attachments und die Frage nach der eigenen Methode	10
1.2 Wie medienwissenschaftlich über Technik schreiben?	13
1.3 Ungehörige Übertragungen	16
1.4 <i>Mit</i> der Technik schreiben	19
2. Kryptographische Sicherheitsbestimmungen	23
2.1 Zum Status des Wissens über Kryptographie	25
2.2 Zur Medialität von Kryptographie	28
2.3 <i>Klassische</i> und <i>moderne</i> Kryptographie	33
2.4 Zwei Schlüsselprobleme der Kryptographie	36
2.4.1 Grundbegriffe der Kryptographie	37
2.4.2 Erstes Schlüsselproblem: Das Kerckhoffs'sche Prinzip	40
2.4.3 Zweites Schlüsselproblem: Asymmetrische Kryptographie	48
2.5 Kryptographische Modellbildung	60
2.5.1 Der <i>unsichere Kanal</i>	60
2.5.2 Alice und Bob	66
2.5.3 Sicherheit in der Kryptographie	76
3. IT-Sicherheit: Digitale Grenzaushandlungen	89
3.1 Diskursive Ansteckungspotentiale	90
3.2 Zwei Fallbeispiele von Ransomware	98
3.2.1 <i>WannaCry</i>	100
3.2.2 Der <i>AIDS Information Trojaner</i>	103
3.3 Ansteckungen/Übertragungen/Grenzaushandlungen	106
3.3.1 Metaphorische Grenzaushandlungen	109
3.3.2 Zur Medialität von Viren und Würmern	111
3.3.3 Liberale Abwehrmechanismen	117

3.4	AIDS und Computer	121
3.4.1	Technische Lösungsansätze: <i>Computer Immunology</i>	124
3.4.2	User_innenzentrierte Lösungsansätze: <i>Digital Hygiene/Safe Hex</i>	133
4.	Backdoors	145
4.1	Was sind Backdoors?	146
4.1.1	Die kleptographische Backdoor in DUAL_EC_DRBG	153
4.2	Von Türen, Hintertüren und Schlüsseln	163
4.3	›In through the back door...‹: Mögliche Umdeutungen	168
4.3.1	<i>Back Orifice</i>	171
4.3.2	Über den Anus	173
5.	Für einen queeren Sicherheitsbegriff	187
5.1	Paranoide und Reparative Praktiken	188
5.1.1	Paranoide Praktiken in IT-Sicherheit und Kryptologie	191
5.1.2	Reparative Praktiken	205
5.2	Queere (IT-)Sicherheit?	208
5.2.1	<i>Queer OS/Queer Computation</i>	210
5.2.2	Queere Sicherheit	223
6.	Schluss	227
	Literatur und weitere Quellen	231
	Danksagungen	253