

Inhaltsverzeichnis

Vorwort	9
Abbildungsverzeichnis	11
Tabellenverzeichnis	13
Abkürzungsverzeichnis	15
1. Einleitung	19
1.1 Untersuchungsgegenstand und Relevanz	22
1.2 Forschungsstand, Desiderate und Fragestellung	27
1.3 Aufbau der Studie	34
2. Theorie: Pragmatismus, Rollentheorie und Techniksoziologie	35
2.1 Wissenschaftstheoretische Grundannahmen: Pragmatismus und Rollentheorie	36
2.2 Analytische Bezugspunkte: Die symbolisch interaktionistische Rollentheorie in der Außenpolitikforschung	42
2.3 Rollentheorie zwischen Innen- und Außenpolitik: Ein rollentheoretisches Zwei-Ebenen-Spiel	54
2.4 Der Cyberspace als (sicherheits-)politisches Handlungsfeld: Theoretische Implikationen	63
2.4.1 Empirischer Exkurs: Die Entwicklung des Internets	75
3. Methodik und Konzeption	83
3.1 Auswahlentscheidungen: Fälle, Quellen und Untersuchungszeitraum	83
3.2 Die interpretative Analyse: Grounded-Theory-Methodologie und Practice Tracing	89
3.3 Rollen und Handlungskontexte	92
3.4 Forschungsleitende Annahmen	96
4. Strafverfolgung im globalen Netz	99
4.1 Deutschland	100

4.1.1	Das deutsche IT-Strafrecht: Domestische Etablierung eines neuen Rechtsrahmens	100
4.1.2	Kryptopolitik	104
4.1.3	Internationalisierung: Strafrechtliche Harmonisierung	109
4.1.4	Neue Ermittlungswerkzeuge: Die Etablierung der offensiven domestischen Beschützerrolle	114
4.2	Vereinigtes Königreich	124
4.2.1	Das britische IT-Strafrecht: Domestische Etablierung eines neuen Rechtsrahmens	124
4.2.2	Kryptopolitik	128
4.2.3	Internationalisierung: Strafrechtliche Harmonisierung	141
4.2.4	Neue Ermittlungswerkzeuge: Die Etablierung der offensiven domestischen Beschützerrolle	144
4.3	Zwischenfazit	153
5.	Die Snowden-Enthüllungen: Das Netz und die Nachrichtendienste	159
5.1	Deutschland	160
5.1.1	Die Snowden-Enthüllungen: Die Bundesregierung zwischen Verunsicherung, Abhängigkeit und zaghafter Selbstbehauptung	160
5.1.2	Die Bundesregierung unter Druck: Die domestische Aufarbeitung der Enthüllungen	175
5.1.3	Die Etablierung einer neuen Beschützer-Rolle: Reform des BND-Gesetzes	187
5.2	Vereinigtes Königreich	193
5.2.1	Die Snowden-Enthüllungen: Die britische Regierung zwischen Kritik und Selbstbehauptung	193
5.2.2	Die Regierung unter Druck: Selbstbehauptung unter wachsendem domestischen Druck	203
5.2.3	Stabilisierung und Ausbau der Beschützer-Rolle: Der Investigatory Powers Act 2016	211
5.3	Zwischenfazit	218
6.	Krieg im Cyberspace? Die militärische Nutzung des Netzes	223
6.1	Deutschland	223
6.1.1	Der Aufbau militärischer Kapazitäten: Defensive Ausrichtung und Schutz der eigenen Systeme	223
6.1.2	(Schonende) Offensive und aktive Verteidigung	227
6.2	Vereinigtes Königreich	238
6.2.1	Der Aufbau militärischer Kapazitäten: Neue offensive Möglichkeiten	238
6.2.2	Einsatz der offensiven Kapazitäten und Russland als neuer Referenzpunkt ...	244
6.3	Zwischenfazit	253

7. Fazit: Cybersicherheit zwischen Innen- und Außenpolitik	259
7.1 Empirische Befunde	260
7.1.1 Entwicklung der Cybersicherheitspolitiken	260
7.1.2 Implikationen für die internationale Cybersicherheitsordnung und das Netz	268
7.2 Theoretische Reflexion: Fruchtbarkeit des Zwei-Ebenen-Rollenspiels und alternative Erklärungen	270
7.3 Limitationen, Desiderate und Ausblick	274
8. Literatur- und Quellenverzeichnis	279