

# Inhalt

---

<b>Vorwort</b> .....	9
<b>Abkürzungsverzeichnis</b> .....	11
<b>1. Einleitung: Die Übertragung der Staat-Proxy-Logik auf den Cyberspace</b> .....	15
1.1 Autokratien und Demokratien: unterschiedliche Proxy-Nutzung im Cyberspace? .....	15
1.2 Bisheriger Forschungsstand zu Proxys im Cyberspace .....	19
1.3 Vergleich konventioneller und Cyberproxy-Funktionslogiken .....	26
1.4 Staatliche Cyberproxy-Nutzung als rein offensives Metier? .....	28
1.5 Bisheriger Forschungsstand zum Attributionsproblem im Cyberspace .....	29
1.6 Forschungsdesign .....	31
<b>2. Der neue Liberalismus zur Erklärung staatlicher Außenpolitiken</b> .....	35
2.1 Der neue Liberalismus als sozialwissenschaftlich-analytische Theorie .....	36
2.1.1 Normen und Werte als politische Leitlinien im ideellen Liberalismus .....	40
2.1.2 Der Primat der Wirtschaft im ökonomischen Liberalismus .....	43
2.1.3 Die Rolle nationaler Institutionenarrangements im republikanischen Liberalismus ....	45
2.2 Das Management asymmetrischer Interdependenzen aus Sicht des neuen Liberalismus: »Politicians still matter« .....	46
2.2.1 Verhandlungsmacht nach innen und außen .....	47
2.2.2 Sensitivität und Vulnerabilität im Cyberspace .....	49
2.2.3 Der strategische Handlungsspielraum autokratischer AnführerInnen .....	53
2.2.4 Der strategische Handlungsspielraum demokratischer AnführerInnen .....	57
2.3 Fazit: Der Cyberspace als regimetypenübergreifende Chance und Herausforderung zugleich .....	60
<b>3. Ein liberales Erklärungsmodell staatlicher Cyberproxy-Strategien</b> .....	63
3.1 Why Cyberproxys Matter: Das Attributionsproblem als asymmetrische Interdependenzsituation .....	64
3.2 Funktion und Art der Cyberproxys: Wer macht was? .....	67
3.2.1 Funktion und Art autokratischer Cyberproxys .....	67

3.2.2 Funktion und Art demokratischer Cyberproxys .....	71
3.3 Gesellschaftliche Präferenzkonstellationen als unabhängige Variable .....	75
3.3.1 Autokratien .....	75
3.3.2 Demokratien .....	77
3.4 Die nationale Cyberakteursumwelt als konditionierende Variable .....	78
3.4.1 Autokratien .....	79
3.4.2 Demokratien .....	80
3.5 Der Einfluss konventioneller Konfliktdynamiken als intervenierende Variable .....	81
3.5.1 Autokratien .....	81
3.5.2 Demokratien .....	83
3.6 Staaten und ihre Proxys: Die Suche nach dem perfekten Match .....	84
<b>4. Das Mixed-Methods-Forschungsdesign .....</b>	<b>85</b>
4.1 Methodische Herausforderungen im Bereich der Cyberkonfliktforschung .....	85
4.2 Der HD-CY.CON-Datensatz .....	88
4.2.1 Theoretische Annahmen und Implikationen .....	88
4.2.2 Allgemeine Kennzahlen zum Datensatz im Vergleich .....	100
4.3 Theoriegeleitete Fallauswahl mithilfe deskriptiver Statistik .....	100
4.4 Konzeptoperationalisierung im Rahmen eines strukturiert- fokussierten Vergleiches .....	103
4.4.1 Funktionen autokratischer Cyberproxys .....	104
4.4.2 Arten autokratischer Cyberproxys .....	105
4.4.3 Funktionen demokratischer Cyberproxys .....	106
4.4.4 Arten demokratischer Cyberproxys .....	107
4.4.5 Domesticke Präferenzkonstellationen .....	107
4.4.6 Die nationale Cyberakteursumwelt .....	112
4.4.7 Das allgemeine Konfliktniveau .....	113
4.5 Auswahl der Leitfragen .....	114
<b>5. Die empirische Cyberkonfliktlandschaft von 2000–2019: Der HD-CY.CON-Datensatz ....</b>	<b>117</b>
5.1 Cyberkonflikte und deren Darstellungen in russisch- und chinesischsprachigen Quellen ....	117
5.2 Regimetypespezifische Cyberproxy-Nutzungsmuster im HD-CY.CON .....	121
5.2.1 Kennzahlen offensiver Cyberoperationen im HD-CY.CON .....	124
5.2.2 Autokratische Fallauswahl: China und Russland im Vergleich .....	133
5.2.3 Kennzahlen politischer und technischer Attributionen im HD-CY.CON .....	141
5.2.4 Demokratische Fallauswahl: Die USA und Israel als <i>Best Cases</i> .....	148
5.3 Autokratisches Fallbeispiel I: China .....	149
5.3.1 Chinesische Cyberproxy-Operationen: Wer macht was? .....	150
5.3.2 Chinas Cyberakteursumwelt .....	176
5.3.3 Chinas domesticke Präferenzkonstellationen und der Einfluss des allgemeinen Konfliktniveaus .....	180
5.4 Autokratisches Fallbeispiel II: Russland .....	202
5.4.1 Russische Cyberproxy-Operationen: Wer macht was? .....	202
5.4.2 Russlands Cyberakteursumwelt .....	226

5.4.3 Russlands domestische Präferenzkonstellationen und der Einfluss des allgemeinen Konfliktniveaus .....	229
5.5 Chinesische und russische Cyberproxy-Nutzung im Vergleich .....	248
5.6 Demokratisches Fallbeispiel I: USA .....	254
5.6.1 US-Cyberattributionen: Wer macht was? .....	254
5.6.2 Die Cyberakteursumwelt der USA .....	269
5.6.3 Die domestischen Präferenzkonstellationen der USA und der Einfluss des allgemeinen Konfliktniveaus .....	272
5.7 Demokratisches Fallbeispiel II: Israel .....	297
5.7.1 Israelische Cyberattributionen: Wer macht was? .....	297
5.7.2 Israels Cyberakteursumwelt .....	306
5.7.3 Israels domestische Präferenzkonstellationen und der Einfluss des allgemeinen Konfliktniveaus .....	309
5.8 Amerikanische und israelische Cyberproxy-Nutzung im Vergleich .....	323
<b>6. Befunde und Implikationen .....</b>	<b>331</b>
6.1 Autokratien und ihre Cyberproxys .....	331
6.2 Demokratien und ihre Cyberproxys .....	333
6.3 Theoretische Implikationen .....	334
6.4 Anknüpfungspunkte für künftige Forschungsvorhaben .....	337
6.5 Policy-Implikationen .....	340
<b>Literaturverzeichnis .....</b>	<b>345</b>
<b>Abbildungsverzeichnis .....</b>	<b>421</b>
<b>Tabellenverzeichnis .....</b>	<b>423</b>

