

Asymmetrien in Cyberkonflikten

Wie Attribution und der Einsatz von Proxies
die Normentwicklung beeinflussen



Die Reihe „Außenpolitik und Internationale Ordnung“
wird herausgegeben von

Prof. Dr. Hanns W. Maull, Berlin

Prof. Dr. Sebastian Harnisch, Universität Heidelberg

AUSSENPOLITIK UND INTERNATIONALE ORDNUNG

Kerstin Zettl | Sebastian Harnisch
Mischa Hansel [Hrsg.]

Asymmetrien in Cyberkonflikten

Wie Attribution und der Einsatz von Proxies
die Normentwicklung beeinflussen



Nomos



Onlineversion
Nomos eLibrary

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-8487-7382-4 (Print)

ISBN 978-3-7489-1357-3 (ePDF)

1. Auflage 2022

© Nomos Verlagsgesellschaft, Baden-Baden 2022. Gesamtverantwortung für Druck und Herstellung bei der Nomos Verlagsgesellschaft mbH & Co. KG. Alle Rechte, auch die des Nachdrucks von Auszügen, der fotomechanischen Wiedergabe und der Übersetzung, vorbehalten. Gedruckt auf alterungsbeständigem Papier.

INHALTSVERZEICHNIS

| | |
|-----------------------|---|
| Abbildungsverzeichnis | 7 |
| Tabellenverzeichnis | 8 |

EINLEITUNG

| | |
|--|----|
| <i>Sebastian Harnisch, Kerstin Zettl und Mischa Hansel</i> Einleitung: Asymmetrien und Cyberkonflikte | 11 |
|--|----|

CYBERKONFLIKTAKTEURE

| | |
|--|----|
| <i>Stefan Steiger</i> Auf leisen Pfoten oder brüllend laut: Chinesische und russische Cyberangriffe im Vergleich | 45 |
|--|----|

| | |
|---|----|
| <i>Kerstin Zettl</i> Der Einsatz von Cyberproxies zur Wahrung autokratischer Regimesicherheit – Iran und Nordkorea im Vergleich | 69 |
|---|----|

| | |
|---|-----|
| <i>Matthias Schulze</i> Asymmetrien zwischen Cyber-Offensive und -Defensive. Eine empirische Annäherung | 105 |
|---|-----|

ATTRIBUTION

| | |
|---|-----|
| <i>Sebastian Harnisch</i> Cyber Fiasko: Populismus, proaktive Selbstverteidigung und die gescheiterte Cybersicherheitspolitik der Trump-Regierung | 137 |
|---|-----|

| | |
|--|-----|
| <i>Rebecca Beigel</i> Attribution von Cyberoperationen – Deutschlands öffentliche Zuschreibungen | 169 |
|--|-----|

Inhaltsverzeichnis

NORMBILDUNG

Mischa Hansel

Cybernorbildung in den Vereinten Nationen. Welche Rolle spielt der asymmetrische Gebrauch von Proxies? 201

Alexander Klimburg

Whole of What? Kooperationsansätze in der internationalen Cybersicherheit 229

SCHLUSSBETRACHTUNG

Mischa Hansel, Kerstin Zettl und Sebastian Harnisch

Schlussbetrachtung 257

VERZEICHNIS DER AUTORINNEN UND AUTOREN 279

Abbildungsverzeichnis

| | |
|--|-----|
| Abbildung 2.1: Cyberangriffe pro Jahr | 52 |
| Abbildung 2.2: Cyberangriffe nach Angreifertyp | 54 |
| Abbildung 3.1: Iranische Cyberoperationen 2007-2019 | 85 |
| Abbildung 3.2: Iranische Cyberproxy-Operationsformen | 85 |
| Abbildung 3.3: Ziele iranischer Cyberproxy-Operationen | 86 |
| Abbildung 3.4: Interaktionsstrukturen zwischen iranischen Cyberproxies | 89 |
| Abbildung 3.5: Nordkoreanische Cyberoperationen 2004-2019 | 91 |
| Abbildung 3.6: Nordkoreanische Cyberoperationsformen | 92 |
| Abbildung 3.7: Ziele nordkoreanischer Cyberoperationen | 92 |
| Abbildung 3.8: Nordkoreanische Cybergruppierungen | 95 |
| Abbildung 5.1: Cyberkonfliktdyade VR China vs. USA, 2008-2019 | 149 |
| Abbildung 5.2: Cyberoperationsformen VR China-US-Dyade, 2008-2019 | 150 |
| Abbildung 5.3: Cyberkonfliktdyade Russische Föderation vs. USA, 2008-2019 | 155 |
| Abbildung 5.4: Cyberoperationsformen Russische Föderation vs. USA, 2008-2019 | 156 |

Tabellenverzeichnis

| | | |
|--------------|---|-----|
| Tabelle 1.1: | Verständnis von Asymmetrien in der internationalen Politik | 18 |
| Tabelle 1.2: | Informationsasymmetrien in Cyberkonflikten: Ziele und Instrumente | 23 |
| Tabelle 2.1: | Proxynutzung im Vergleich | 53 |
| Tabelle 2.2: | Ziele staatlicher und staatlich beauftragter Cyberangriffe | 55 |
| Tabelle 2.3: | Angriffstypen | 55 |
| Tabelle 2.4: | Angriffstypen staatlicher Angriffe | 55 |
| Tabelle 3.1: | (Technische) Intensitätsbemessung des HD-CY.CON | 83 |
| Tabelle 3.2: | Iranische Proxygruppierungen | 88 |
| Tabelle 3.3: | Nordkoreanische CyberGruppierungen | 94 |
| Tabelle 4.1: | Ausgewählte TTPs und Kosten von Cyberangriffen je Akteurstyp | 121 |
| Tabelle 4.2: | Angreifer Idealtypen und hypothetische Kostenfaktoren für die Offensive | 123 |
| Tabelle 4.3: | Berechnung der Angriffskosten für die Idealtypen basierend auf Marktpreisen | 124 |
| Tabelle 5.1: | Angriffsintensitäten VR China-US-Dyade (2008-2019) | 151 |
| Tabelle 5.2: | Angriffsintensitäten Russische Föderation-US-Dyade (2008-2019) | 157 |
| Tabelle 6.1: | Interne vs. externe Attributionspraktiken | 171 |
| Tabelle 6.2: | Übersicht der Analysekriterien | 176 |
| Tabelle 6.3: | Die untersuchten Attributionen im Vergleich | 180 |