

Inhaltsverzeichnis

Vorwort.....	V
A. Einführung	1
B. Cyber-Versicherungsvertragsstatut und international-privatrechtliche Grundlagen	7
I. Internationale Zuständigkeit für Cyber-Deckungsstreitigkeiten	9
1. Gerichtsstandsvereinbarungen in Cyber-Versicherungsverträgen.....	10
2. Zuständigkeit für (Deckungs)Klagen gegen den Versicherer.....	12
II. Internationales Cyber-Versicherungsvertragsrecht unter der Rom I-VO.....	14
1. Grundanknüpfung nach Art. 7 Rom I-VO	15
a) Großrisiken nach Art. 7 Abs. 2 UAbs. 1 i.V.m. Art. 3 Rom I-VO	16
b) Massenrisiken: KMU unterhalb der Großrisiko-Schwelle	19
c) Sonderfrage: Einzuhaltende Sicherheitsvorschriften und vertragliche Obliegenheiten bei Auslandsbezügen	21
2. Art. 7 Abs. 4 Rom I-VO	29
3. Eingriffsnormen und ordre public Art. 9, Art. 21 Rom I-VO	30
III. Ergebnis	32
C. Internationale Cyber-Haftpflicht und Verbindungs- linien zur Cyber-Haftpflichtdeckung.....	34
I. Haftungsverhältnisse im Überblick.....	35
1. (Vor)vertragliche Haftung des angegriffenen Versicherungsnehmers gegenüber Dritten	36

2. Deliktische Haftung des angegriffenen Versicherungsnehmers gegenüber Dritten	38
II. Internationale Zuständigkeit für Cyber-Haftpflicht- streitigkeiten	42
1. Gerichtsstände nach der Brüssel Ia-VO für die Inanspruchnahme des Angegriffenen durch geschädigte Dritte	43
a) Haftung im Gefolge (halb)staatlicher Cyber- Attacken: acta iure imperii i.S.d. Art. 1 Abs. 1 S. 2 Brüssel Ia-VO ?	44
b) Zuständigkeit für Haftpflichtansprüche in Vertragsbeziehungen: Art. 25 und Art. 7 Nr. 1 Brüssel Ia-VO	49
c) Deliktserichtsstand nach Art. 7 Nr. 2 Brüssel Ia-VO	51
d) Gerichtsstände nach Art. 7 Nr. 5, Art. 8 Nr. 1 Brüssel Ia-VO	64
2. Art. 79 DSGVO bei Datenschutzverletzung infolge des Cyber-Vorfalles	66
3. Grenzüberschreitende kollektive Anspruchs- durchsetzung infolge eines Cyber-Incidents	67
III. Kollisionsrecht der Cyber-Haftpflicht	69
1. IPR der Cyber-Haftpflicht gegenüber Unter- nehmen	70
a) Rom I-VO und Rom II-VO als maßgebliches Kollisionsrechtsregime	71
b) Kollisionsrechtliche Anknüpfung (vor)vertrag- licher Haftpflichtansprüche	77
c) Kollisionsrechtliche Anknüpfung außervertrag- licher Haftpflichtansprüche	78

2.	IPR der Cyber-Haftpflicht bei DSGVO-Verstößen gegenüber natürlichen Personen.....	84
a)	Verweisungsumfang des Art. 3 DSGVO	86
b)	Anknüpfung der nicht in Art. 82 DSGVO geregelten Fragen	87
c)	Zwischenfazit.....	101
3.	Kollektive Rechtsdurchsetzung und anwendbares Recht.....	101
IV.	Haftungsrechtlich maßgebliche Cyber-Sicherheitsstandards in grenzüberschreitenden Fällen.....	104
1.	Berücksichtigung abweichender Cyber-Sicherheitsstandards am Handlungsort	106
2.	Angemessenheit der Berücksichtigung von Sicherheitsstandards jenseits der lex causae	108
3.	Drittstaatliche Handlungsorte, Intra-EU-Konstellationen und der Eingriffsnormcharakter von Cyber-Sicherheitsstandards	110
a)	Cyber-Sicherheitsstandards am Handlungsort in Nicht-EU-Staaten.....	111
b)	Intra-EU-Konstellationen	113
4.	Zwischenfazit	117
V.	Ergebnis	118
D.	Versicherbarkeit von Geldbußen wegen Verstößen gegen Cybersicherheits- und Datenschutzbestimmungen	123
I.	Rechtsvergleichende Umschau: Kaum explizite Versicherungsverbote – viel Rechtsunsicherheit.....	127
1.	Deutschland	128
a)	§ 134 BGB i.V.m. Straftatbeständen des StGB..	128
b)	§ 138 Abs. 1 BGB und (in- und ausländische) Geldbußen.....	129

c) Zwischenergebnis: Unionale und nationale Präventionsrichtung als Maßstab	140
2. Italien: Allgemeines Verbot	141
3. Frankreich: Rechtsunsicherheit	143
4. England und Wales	146
5. USA	150
II. International-privatrechtliche Herausforderungen von Geldbußendeckungen in marktüblichen Klauseln	152
1. Klauselvariante Nr. 1: Verbote in der das Bußgeld verhängenden Rechtsordnung	155
2. Klauselvariante Nr. 2: Verbote des Vertragsstatuts und des Rechts am Erfüllungsort	158
3. Zwischenergebnis: Verbote aus multiplen Rechts- ordnungen – auch jenseits der „ordre public“- Klausel	163
III. Unionale Dimension der Versicherbarkeit: sanktionen- rechtlicher Effektivitätsgrundsatz	165
1. Ausgangslage: EU-Effektivitätsgrundsatz und Geldbußen	167
2. Sanktionenrechtliche Effektivität und Versicherungsschutz für Geldbußen	169
IV. Versicherbarkeit von Geldbußen durch „fine-wraps“ und „most favorable jurisdiction/venue“?	176
1. Von der „Puni-“ zur „Fine-Wrap-Policy“?	176
2. Keine „most favorable jurisdiction/venue“ bei Geldbußendeckungen	180
V. Ergebnis	183

E.	Versicherbarkeit und Erstattungsfähigkeit von „Lösegeldern“ bei Ransomware-Attacken	186
I.	Verbotsgesetze i.S.d. § 134 BGB: Straftatbestände und Sanktions- und Embargobestimmungen.....	188
1.	Beihilfe zur Unterstützung krimineller Vereinigungen oder zur Terrorismusfinanzierung als strafrechtliche Verbotsgesetze	191
a)	Unterstützung einer kriminellen Vereinigung: § 129 Abs. 1 S. 2 Var. 1, § 27 StGB als Verbotsgesetz	191
b)	Terrorismusfinanzierung: § 89c Abs. 1 Nr. 3, Abs. 3, § 27 StGB als Verbotsgesetz	194
2.	Nationale und unionale Sanktions- und Embargobestimmungen	195
II.	Drittstaatliche Verbotstatbestände: Art. 9 Rom I-VO und § 138 Abs. 1 BGB als Einfallstore.....	199
1.	Vermeintliche und tatsächliche Verbote von Lösegeldzahlungen in ausländischen Rechtsordnungen	201
a)	Italien: Klare Unklarheit	201
b)	Frankreich: Bedingte Zulässigkeit	203
c)	US-Bundesstaaten: Beispiele für punktuelle Verbote und weitergehende Gesetzesentwürfe	207
2.	Eingriffsnormen des Erfüllungsortes.....	209
3.	Materiell-rechtliche Berücksichtigung ausländischer Verbotsnormen über § 138 Abs. 1 BGB	214
a)	Reflexhafter Schutz (auch) deutscher Interessen.....	215
b)	Schutz „allgemein zu achtender Interessen aller Völker“	216
III.	Ergebnis	218

F.	Cyber-Versicherungen und Cumul-Risiken: Ausschluss von Krieg und Cyber-Operationen, Territorial-Ausschlüsse und „widespread events“	220
I.	Cyber-Krieg und konventionelle Kriegsausschluss- klauseln: History (not) repeating?	223
1.	Historische Entwicklung der Kriegsausschlüsse: Lehren aus statischen Wordings und der Sieges- zug von NMA 464	224
2.	Keine Erfassung des „reinen“ Cyber-Krieges durch Ausschlussklauseln der „NMA 464“-Generation wie Ziff. A1-17.2 AVB-Cyber a.F. (2017)	226
II.	Internationale Aspekte der neuen Ausschlüsse von „Cyber-Operationen“ im Gefolge von LMA 5564(a,b) bis 5567(a,b)	233
1.	Übersicht über gängige Klauselvarianten	235
a)	Ausschluss von „Cyber-Operation“ nach LMA 5564(a,b)	235
b)	LMA 5565(a,b) bis 5567(a,b): „KRITIS-Ansatz“	236
c)	Reaktionsbezogener Ansatz im Markt	238
2.	Grad staatlicher Involvierung und Transparenz- kontrolle: „on behalf of“, „im Auftrag“ oder „unter Kontrolle eines Staates“	239
3.	„Attribution“ und Klauselkontrolle	244
a)	Intransparenz der „Attribution“-Klausel in LMA 5564(a) bis 5567(a)	245
b)	Intransparenz in internationalen Fallgestaltungen: Cloud-Dienste und „physische Belegenheit des IT-Systems“	247
4.	Belegenheit des Computersystems für den Wiedereinschluss nach Ziff. 1 UAbs. 2 LMA 5565(a,b) bis 5567(a,b)	248
5.	Zwischenfazit	249

III. GDV-Musterbedingungen: Ausschluss von „Krieg und staatlichen Angriffen“ nach Ziff. A1-17-2 AVB-Cyber 2024	249
1. Cyber als Instrument eines „klassischen“ Krieges: Ziff. A1-17-2 lit. a) AVB-Cyber 2024	250
2. Reine Cyber-Attacken mit KRITIS-Bezug: Ziff. A1-17-2 lit. b) AVB-Cyber 2024	253
a) Sachlich-territoriale Auswirkungen auf KRITIS-Infrastruktur	254
b) „Beeinträchtigungen“ von KRITIS-Infrastruktur i.S.d. BSIG	256
3. Erleichterungen von Darlegung und Beweis der Voraussetzungen des Ausschlusses nach Ziff. A1-17-2 AVB-Cyber 2024	260
4. Darlegung und Beweis der staatlichen Provenienz der Cyber-Attacke: „Zuschreibung“ und Klauselkontrolle	262
5. Bedarf nach einer objektiven „Zuschreibung“ bzw. „attribution“	265
IV. Weitere Ansätze zur Vermeidung von Cumul-Risiken im Cyber-Bereich: „Widespread Event“ und „Territorial Exclusions“	267
1. „Weiterverbreitetes Ereignis“ und die AGB-Klauselkontrolle	267
2. Territoriale Ausschlüsse und internationale Cyber-Versicherung	270
V. Ergebnis	272
G. Zusammenfassung der Ergebnisse	275
I. Cyber-Versicherungsvertragsstatut und international-privatrechtliche Grundlagen	275
II. Internationale Cyber-Haftpflicht und Verbindungslinien zur Cyber-Haftpflichtdeckung	276

III. Versicherbarkeit von Geldbußen wegen Verstößen gegen Cybersicherheits- und Datenschutz- bestimmungen.....	281
IV. Versicherbarkeit und Erstattungsfähigkeit von „Lösegeldern“ bei Ransomware-Attacken	283
V. Cyber-Versicherungen und Cumul-Risiken: Ausschluss von Krieg und Cyber-Operationen, Territorial-Ausschlüsse und „widespread events“	284
Literaturverzeichnis	289