Inhaltsübersicht

Vorwort V

§ 1 Bots im Kontext von Cyberkriminalität – Eine Einführung 1

§ 2 Gang der Arbeit 3

§ 3 Zielsetzung 5

Erster Teil – Das Phänomen der Botnetz-Kriminalität 7

§ 4 Der Begriff „Bot“ 9

I. Sprachlicher Ursprung 9

II. Definitionsansätze 9

III. Abgrenzung zu humanoiden Robotern 10

IV. Botnetze, Social Bots und Cheatbots als wichtigster Teil der Bot-Kriminalität 11

§ 5 Botnetze 13

I. Begriff 13

II. Funktionsweise von Botnetzen 15

1. Programmierung der für Botnetze erforderlichen Schadsoftware 15
2. Infektion mit der Schadsoftware 15
   a) Infektion mittels getarnter Schadsoftware – Das trojanische Pferd des Internets 16
   b) Ausnutzung von Sicherheitslücken (Exploits) 18
   c) Manuelle Installation 19
   d) Anschließender Infektionsvorgang 19
3. Integration in das Botnetz 20
   a) Integrationsvorgang 20
   b) Integrationsfähige Systeme mit Fokus auf der Bedeutung von IoT-Geräten für den Botnetz-Aufbau 20

Inhaltsübersicht

4. Kommunikation mit dem System 21
a) Zentrale Botnetze 22
b) Hierarchische Botnetze 25
c) Dezentrale Botnetze 26
5. Nutzung der Botnetze 27
III. Einsatzbereiche der Botnetze 27
1. DDoS-Attacken 28
a) Funktionsweise von DDoS-Attacken 28
aa) Syn Flooding 30
bb) Ping Flooding 30
cc) Mailbombing 30
b) Distributed-Reflected-Denial-of-Service-(DRDoS-)Attacke 31
c) Motive für DDoS-Attacken 31
d) Durch DDoS-Attacken resultierende Gefahren 32
2. Zugriff auf die lokalen Daten der Nutzer 35
a) Snifferprogramme 36
b) Keylogger 37
3. Nutzung der Rechenleistung und der Bandbreite der gekaperten Systeme 37
a) Brute-Force- und Credential-Stuffing-Angriffe 38
b) Kryptomining 38
aa) Der technische Hintergrund des Bitcoinminings am Beispiel des Bitcoins 39
bb) Bitcoinmining durch Mobiltelefon und intelligente Endgeräte 42
cc) Der Bitcoin als attraktive Beute 42
dd) Gefährdungslage durch Kryptomining 43
4. Versand von Spam- und Phishing-Mails 45
5. Ransomware 49
a) Funktionsweise von Ransomware 49
b) Motivation und Auswirkungen von Ransomwareangriffen 52
6. Verbreitung von Malware 56
7. Nutzung einzelner Systeme eines Botnetzes 56
a) Proxy-Hosts 56
b) Hostspeicher 57
c) Flux-Server 58
d) Steuern einzelner Geräte, insbesondere IoT-Geräte 58
IV. Identifikation von Botnetzen 59
V. Durch Botnetze induzierte Gefährdungslage 60
VI. Fazit: Botnetze als größte Bedrohung des Cybercrimes 62

§ 6 Social Bots 63

I. Begriffsbestimmung 64
1. Kommunikationsspezifischer Ansatz 64
2. Einsatzbereichsspezifischer Ansatz 65
3. Zielsetzungsspezifischer Ansatz 65
4. Täuschungsspezifischer Ansatz 65

5. Bösartige und gutartige Social Bots 66
6. Fazit 67

II. Funktionsweise von Social Bots 68
1. Exkurs: Funktionsweise von sozialen Netzwerken 68
2. Soziale Netzwerke und Social Bots 71
3. Technische Hintergründe und Programmierung 71
a) Nutzerkonten 72
b) Application Programming Interface oder Browserautomatisierung 73
c) Steuerungsprogramme 74
aa) Einfache Social Bots 75
bb) Komplexe Social Bots 76
cc) Hochkomplexe Social Bots 77
d) Abgrenzung zu anderen Internetphänomenen 79

III. Örtlicher Anwendungsbereich von Social Bots 80

IV. Effekte der Social Bots 81
1. Tarnungseffekt durch Nachahmung menschlichen Verhaltens 82
2. Multiplikationseffekt durch verdeckte Vervielfältigung von Beiträgen von Social Bots 84
3. Anonymisierungseffekt durch Zurücktreten des Verwenders hinter den Bot 86
4. Personalisierungseffekt durch personalisierte Anpassung an den Adressaten 86

V. Formen der Beeinflussung 87
1. Manipulation von Trends durch Verstärkung von Auffassungen 87
2. Verbreitung von Desinformation und Fake News 89
3. Unterdrückung von Diskussionen und Auffassungen 93
4. Künstliche Erhöhung von Followerzahlen/„Gefällt mir"-Angaben und Ähnlichem 94
5. Massenhafte Verbreitung sonstiger Beiträge 94
6. Verfälschung von Datenbeständen 95
7. Folgen 95
a) Manipulation der öffentlichen Meinungsbildung 95
aa) Bedeutung der sozialen Medien im Kontext der Meinungsbildung 96
bb) Gefahren der Einbeziehung von sozialen Medien im Kontext der Meinungsbildung 96
cc) Auswirkungen der Social Bots auf die Meinungsbildung 97
b) Einsatz von Social Bots zur Manipulation von Kundenverhalten 101
aa) Die künstliche Erhöhung von Populationsindikatoren auf sozialen Netzwerken, beispielsweise von Like- und Follower-Anzahlen 101
bb) Beeinflussung von Aktienmärkten 102
cc) Manipulationen im Bereich des Influencer-Marketings 103
dd) Verbreitung von Fake News zwecks Werbemittelgenerierung 104
c) Social Bots zur Verbreitung von Hatespeech und Cybermobbing 104
aa) Das Phänomen Hass und Mobbing im Internet 104
bb) Auswirkungen von Hass und Mobbing im Internet 106

cc) Hass und Mobbing im Internet und Social Bots 107
dd) Gefährdung von Leib und Leben durch Cybermobbing 108
d) Gefährdung von Gesundheit und Leben durch Fake News 108
e) Weitere Einsatzbereiche und Gefahren 109
aa) Terrorismus: Einsatz von Social Bots zur Verbreitung terroristischer Inhalte 109
bb) Vertrauensverlust 109
cc) Einsatz von Social Bots zum Locken in Abofallen 110
dd) Irreführung von Strafverfolgungsbehörden durch Fake News 111
ee) Scamming und Sextortion 111
ff) Verbreitung von Schadsoftware 112
VI. Akteure 112
VII. Fazit 113

§ 7 Cheatbots 115
I. Cheatbots als unerwünschter Bestandteil der Computerspielbranche 115
II. Grundlagen: Begriffsbestimmung 116
III. Funktionsweise 117
1. Freischaltung von Zusatzfunktionen 118
a) Zugriff auf Premiumfunktionen 118
b) Zugriff auf Funktionen, die im Spiel nicht vorgesehen wurden 118
2. Das Automatisieren von Spielerhandlungen 119
a) Weiterentwicklung von Spielcharakteren 119
b) Sammeln virtuellen Geldes oder virtueller Gegenstände 120
IV. Folgen 122
1. Sinkender Spielspaß 122
2. Daraus resultierendes wirtschaftliches Risiko für die Spieleindustrie 123
3. Regelwidrige Verwendung von Cheatbots im Rahmen des eSports 126
a) Cheatbots im eSport 126
b) Bedeutung des eSports 127
4. Problem der praktischen Nachweisbarkeit 129

§ 8 Weitere Bot-Formen 131
1. Bietroboter 131
2. Scalper-Bots 132
3. Ticket-Bots 132
4. Pokerbots 133
5. Umfrage- und Petitionsbots 133
6. Streaming-Bots 134
7. Gewinnspielbots 134
8. Klickbots 135
9. Bewertungsbots 141

§ 9 Akteure im Bereich der Bot-Kriminalität 145

1. Besondere Attraktivität des Tatmittels Internet 145
2. Täterstrukturen im Bereich der Bot-Kriminalität 147
3. Täterpersönlichkeiten 148
   a) Cyber-Aktivisten in Abgrenzung zu Cyberkriminellen 149
   b) Konkurrenzausspähung und Konkurrenzschädigung 150
   c) Geheimdienste und weitere staatliche Akteure 151
   d) Cyber-Terroristen 152
   e) Unbesonnene Systemnutzer 153
   f) Weitere mögliche Tätergruppen 153
4. Internetkriminalität als Dienstleistung 154

Zweiter Teil – Die strafrechtliche Behandlung von Bot-Kriminalität de lege lata 157

§ 10 Grundlagen einer Strafbarkeit de lege lata 159

I. Zuständigkeit der deutschen Justiz – Strafanwendungsrecht 159
   1. Die Internationalität des Botphänomens als Ausgangspunkt für strafanwendungsrechtliche Fragestellungen 159
   2. Anwendbarkeit des deutschen Strafrechts auf das Bot-Phänomen 160

II. Vorsatz 162
   1. Auswirkungen der Automatisierung auf das Vorliegen des Vorsatzes 162
   2. Vorsatz des nicht verwendenden Programmierers 164

§ 11 Botnetze de lege lata 165

I. Programmieren der Botware 165

II. Verbreitung der Botware 168
   1. Vorsätzliche Verbreitung von Malware 168
      a) Strafbarkeit wegen Ausspähen von Daten, § 202a Abs. 1 StGB 168
         aa) Die Firewall als besondere Zugangssicherung 169
         bb) Verantwortlichkeit: Strafbarkeit des Bots selbst? 171
         cc) Verantwortlichkeit des Bot-Nutzers – Durchbrechung der Kausalität und objektiven Zurechnung? 173
         dd) Zwischenergebnis 177
      b) Strafbarkeit wegen Abfangens von Daten, § 202b StGB 177
      c) Strafbarkeit wegen Datenveränderung, § 303a StGB 177
      d) Strafbarkeit wegen Computersabotage, § 303b StGB 181
   2. Versehentliche Verbreitung von Computerviren durch Programmierer 182
   3. Versehentliche Weiterverbreitung von Computerviren durch die Inhaber infizierter Systeme 182
   4. Zwischenergebnis 186

III. Verwendung eines Botnetzes 186
1. DDoS-Attacken 186
a) Strafbarkeit wegen Nötigung, § 240 StGB 186
b) Strafbarkeit wegen Erpressung, § 253 Abs. 1 StGB 187
c) Strafbarkeit wegen Sachbeschädigung, § 303 StGB 187
d) Strafbarkeit wegen Datenveränderung, § 303a StGB 188
e) Strafbarkeit wegen Computersabotage, § 303b StGB 192
f) Strafbarkeit wegen Störung von Telekommunikationsanlagen, § 317 StGB 193
g) Strafbarkeit wegen Ausspähens von Daten, § 202a StGB, Abfangens von Daten, § 202b StGB, und Vorbereitens des Ausspähens und Abfangens von Daten, § 202c StGB 194
h) Tötungs- und Körperverletzungsdelikte 194
i) Strafbarkeiten aus dem Einsatz von Botnetzen gegen kritische Infrastrukturen 195
j) Zwischenergebnis 195
2. Zugriff auf die Daten der gekaperten Systeme 196
a) Allgemeine Strafbarkeit des Zugriffs auf die Daten 196
aa) Strafbarkeit wegen Diebstahls, § 242 StGB 196
bb) Strafbarkeit wegen Ausspähens von Daten, § 202a Abs. 1 StGB 196
cc) Strafbarkeit wegen Abfangens von Daten, § 202b StGB 197
dd) Strafbarkeit wegen § 42 Abs. 2 BDSG 197
b) Zugriff auf Daten unter Verwendung von Snifferprogrammen 198
c) Zugriff auf Daten unter Verwendung von Keyloggern 198
d) Löschung oder Unbrauchbarmachung von Daten auf dem System 200
e) Zwischenergebnis 200
3. Nutzung der Rechenleistung und Bandbreite der gekaperten Systeme 200
a) Proxy Hosts 201
b) Brute Force und Credential-Stuffing-Angriffe 202
c) Kryptomining 203
aa) Strafbarkeit wegen Entziehung elektrischer Energie, § 248c StGB 203
bb) Strafbarkeit wegen Betrug, § 263 StGB 204
cc) Strafbarkeit wegen Computerbetrugs, § 263a StGB 204
dd) Strafbarkeit wegen Ausspähens und Abfangens von Daten, § 202a StGB bzw. § 202b StGB 205
ee) Strafbarkeit wegen Vorbereitens des Ausspähens und Abfangens von Daten, § 202c StGB 205
ff) Strafbarkeit wegen Datenveränderung, § 303a StGB 205
gg) Strafbarkeit wegen Computersabotage, § 303b StGB 206
hh) Strafbarkeit wegen Erschleichens von Leistungen, § 265a StGB 206
ii) Strafbarkeit wegen Sachbeschädigung, § 303 StGB 206
jj) Zwischenergebnis 207
d) Fernsteuerung von IoT-Gräten 207

4. Versand von Spam- und Phishing-Mails 208
a) Spam-Mails 208
b) Phishing-Mails 209
aa) Strafbarkeit wegen Betrugs, § 263 StGB 209
bb) Strafbarkeit wegen Computerbetrugs, § 263a StGB 212
cc) Strafbarkeit wegen Fälschung beweiserheblicher Daten, § 269 StGB 212
dd) Strafbarkeit wegen Ausspähens von Daten, § 202a StGB 214
ee) Strafbarkeit wegen Abfangens von Daten, § 202b StGB 215
ff) Strafbarkeit wegen Nötigung, § 240 StGB 215
gg) Strafbarkeit wegen Datenveränderung, § 303a StGB, und Computersabotage, § 303b StGB 215
hh) Strafbarkeiten aus §§ 143, 143a MarkenG und §§ 106 ff. UrhG 216
ii) Weitere Strafbarkeiten im Zusammenhang mit Phishing 216
jj) Zwischenergebnis 216
5. Ransomware 217
a) Strafbarkeit wegen Erpressung (durch Unterlassen gemäß §§ 253 Abs. 1, 3, 22, 23 StGB) 217
b) Strafbarkeit wegen Betrugs, § 263 StGB 219
c) Strafbarkeit wegen Datenveränderung gemäß § 303a StGB 219
d) Strafbarkeit wegen Computersabotage gemäß § 303b StGB 220
e) Strafbarkeit wegen Ausspähens von Daten, § 202a StGB 220
f) Strafbarkeit wegen Unterstützung krimineller Vereinigungen gemäß § 129 Abs. 1 S. 2 StGB 221
g) Weitere Straftatbestände 223
h) Zwischenergebnis 223
IV. Strafbarkeit derjenigen, von deren Rechner ohne ihr Wissen die Ausbreitung des Botnetzes erfolgt oder Angriffe ausgehen 223
V. Bewertung der Rechtslage de lege lata 224

§ 12 Social Bots de lege lata 227

I. Strafrechtliche Bewältigung von Social Bots 227
1. Keine ausdrückliche Strafbarkeit der Verwendung eines Social Bots 227
2. Strafbarkeit wegen §§ 106, 108 UrhG? 227
3. Ergebnis 230

II. Die strafrechtliche Einordnung von Social Bots 230
1. Strafrechtliche Einordnung der einzelnen Einsatzbereiche 230
a) Manipulation von Trends 230
aa) Strafbarkeit wegen Datenveränderung, § 303a Abs. 3 StGB 230
bb) Strafbarkeit wegen Ausspähens von Daten, § 202a Abs. 1 StGB, Abfangens von Daten, § 202b StGB, und Vorbereitens des Ausspähens und Abfangens von Daten, § 202c Abs. 1 Nr. 2 StGB 232
cc) Strafbarkeit wegen Computersabotage, § 303b Abs. 1 Nr. 2 StGB 232
dd) Ergebnis 234

b) Verbreitung von Fake News 234
aa) Strafbarkeit wegen landesverräterischer Fälschung, § 100a StGB 234
bb) Strafbarkeit wegen Wählernötigung, § 108 StGB, und Wählertäuschung, § 108a StGB 235
cc) Strafbarkeit wegen Störpropaganda gegen die Bundeswehr, § 109d StGB 235
dd) Strafbarkeit wegen Störung des öffentlichen Friedens durch Androhung von Straftaten, § 126 Abs. 2 StGB 236
ee) Strafbarkeit wegen Volksverhetzung, § 130 StGB 237
ff) Strafbarkeit wegen Vortäuschens einer Straftat, § 145d StGB 240
gg) Strafbarkeit wegen falscher Verdächtigung, § 164 StGB 241
hh) Strafbarkeit wegen Beleidigungsdelikten, § 185 ff. StGB 242
ii) Strafbarkeit wegen verhetzender Beleidigung, § 192a StGB 242
jj) Strafbarkeit wegen Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen, § 201a StGB 242
kk) Weitere Straftatbestände 243
ll) Zwischenergebnis 244
c) Unterdrückung von Diskussionen und massenhafte Verbreitung sonstiger Beiträge 245
d) Künstliche Erhöhung von Publikationsindikatoren zur Manipulation von Kundenverhalten 245
e) Manipulationen der öffentlichen Willensbildung 249
aa) Strafbarkeit wegen Wahlfälschung, § 107a StGB 249
bb) Strafbarkeit wegen Wählernötigung, § 108 StGB 250
cc) Strafbarkeit wegen Wählertäuschung, § 108a StGB 251
dd) Weitere Strafbarkeiten 251
f) Manipulation von Kundenverhalten 251
g) Social Bots zur Verbreitung von Hatespeech und zum Cybermobbing 252
aa) Strafrechtlicher Schutz 252
(1) Strafbarkeit wegen der Beleidigungsdelikte, §§ 185 ff. StGB 252
(2) Strafbarkeit wegen gefährdenden Verbreitens personenbezogener Daten, § 126a StGB 260
(3) Strafbarkeit wegen Körperverletzungsdelikten, §§ 223 ff. 261
(4) Strafbarkeit wegen öffentlicher Aufforderung zu Straftaten, § 111 StGB 262
(5) Strafbarkeit wegen Verletzung der Vertraulichkeit des Wortes, § 201 StGB, und Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen, § 201a StGB 263
(6) Nachstellung, § 238 StGB, Nötigung, § 240 StGB, und Bedrohung, § 241 StGB 264
(7) Strafbarkeit wegen § 33 KUG 264
(8) Weitere Straftatbestände 265
bb) Zivilrechtlicher Schutz 265
cc) Fazit 266
h) Weitere Einsatzbereiche von Social Bots und deren strafrechtliche Einordnung 266

2. Probleme auf Seiten der Strafverfolgung 268
a) Mangelnde Erkennbarkeit als Problem der Strafverfolgung 268
b) Fehlende Möglichkeit der Zuordnung als Problem der Rechtsdurchsetzung 274
3. Ergebnis und Ausblick auf den dritten Teil der Arbeit 275
III. Andere rechtliche Regelungen 276
1. Vertragsrecht 276
2. Wettbewerbsrecht 276
3. Verhaltenskodex zur Bekämpfung von Desinformation 277
4. Telemedienrecht 277
5. Netzwerkdurchsetzungsgesetz 279
6. Fazit 280

§ 13 Cheatbots de lege lata 281
1. Kein ausdrückliches strafrechtliches Verbot von Cheatbots 281
2. Strafrechtliche Relevanz der Verwendung von Cheatbots im eSport 281
a) Strafbarkeit wegen Betruges, § 263 StGB 281
aa) Betrug zum Nachteil des Veranstalters 282
bb) Betrug zum Nachteil eines Preisspenders 283
cc) Betrug zum Nachteil des Konkurrenten 283
dd) Betrug zum Nachteil des Zuschauers 286
ee) Betrug zum Nachteil des Sponsors 286
ff) Betrug zum Nachteil des Clans 286
gg) Betrug zulasten von Wettpartnern im eSport 287
b) Strafbarkeit wegen Sportwettbetrugs, § 265c StGB 288
c) Strafbarkeit wegen Manipulation berufssportlicher Wettbewerbe, § 265d StGB 291
d) Verstoß gegen das AntiDopG 292
e) Zwischenergebnis 293
3. Strafrechtliche Behandlung von Cheatbots außerhalb des eSports 293
a) Verwender von Cheatbots 293
b) Zweitmarkthändler 294
c) Hersteller von Cheatbots 295
d) Zwischenergebnis 295
4. Zivilrechtliche Behandlung von Cheatbots 295
a) Ansprüche gegen die Nutzer von Cheat-Software 295
b) Ansprüche gegen die Hersteller von Cheatbots 296
aa) Vertragliche Ansprüche 296
bb) Wettbewerbsrechtliche Ansprüche 297
cc) Deliktische Ansprüche 298
dd) Urheberrechtliche Ansprüche 298
ee) Markenrecht 299
c) Ansprüche gegen die Zweitmarkthändler 299
5. Problem der Erkennbarkeit von Cheatbots 300
6. Ergebnis 301

§ 14 Crime-as-a-Service de lege lata **303**

I. Strafbarkeit der Plattformbetreiber, welche die Infrastruktur zum Bot-Handel bereitstellen 303
1. Mittäterschaftliches Handeln der Plattformbetreiber 304
2. Bandenabrede oder kriminelle Vereinigung 305
3. Anstiftung und Beihilfe 306
4. Strafbarkeit des Betreibens krimineller Handelsplattformen im Internet, § 127 StGB 308
5. Fazit 311

II. Strafbarkeit weiterer Akteure 311
1. Strafbarkeit der Verkäufer und Vermieter von Bot-Software 311
2. Strafbarkeit der Käufer und Mieter eines Botnetzes 312

§ 15 Rechtswidrigkeit und Schuld **315**

§ 16 Prozessuale und praktische Hindernisse im Bereich der Bot-Kriminalität **317**

§ 17 Abschließende Betrachtung der rechtlichen Behandlung von Bot-Kriminalität de lege lata **319**

Dritter Teil – Die rechtliche Behandlung von Bot-Kriminalität im Internet de lege ferenda **321**

§ 18 Grundlagen einer strafrechtlichen Behandlung von Bots de lege ferenda **323**

I. Das Strafrecht als Lösung des Problems der Bot-Kriminalität 323
1. Regulierungsversuche im Internet 323
2. Effektivität des Strafrechts im Bereich der Bot-Kriminalität 324

II. Voraussetzungen einer gelungenen Regelung – insbesondere Technikneutralität als Grundvoraussetzung dauerhaft effektiver Regelungen 325

III. Adressat 326

§ 19 Strafrechtliche Behandlung der verschiedenen Bot-Arten mittels gemeinsamer Regelung **329**

I. Generelles Verbot von Bots 329

II. Strafbarkeit der unbefugten Benutzung informationstechnischer Systeme – Der digitale Hausfriedensbruch als Lösung des Bot-Problems? 331

III. Zwischenergebnis 338

§ 20 Botnetze de lege ferenda 341

I. Strafrechtliches Verbot von Botnetzen 341

II. Änderungen der §§ 202a, 202b, 202c StGB 342

1. Änderung des § 202a StGB 342

a) Erhöhung des Strafrahmens 342

b) Ausdehnung der Schutzwirkung auf Daten, die aufgrund mangelnder Sorgfalt nicht gegen den unberechtigten Zugang besonders gesichert sind 346

c) Ergänzung des § 202a StGB auf Ausnutzung von durch Dritte unbefugt geschaffene Zugänge 347

2. Änderung des § 202b StGB 347

3. Strafbarkeit des Versuchs nach §§ 202a und 202b StGB 348

4. Gestaltung der Computer- und Internetdelikte als Offizialdelikte 349

5. Änderung des § 202c StGB 349

a) Ergänzung um die Tatbestandsvariante der gezielten Infektion mit Malware 349

b) Erhöhung des Strafrahmens und Strafschärfungen 350

III. Änderung des § 202d StGB 350

IV. Änderung der §§ 303a und 303b StGB 351

1. Änderung des § 303a StGB 351

2. Änderung des § 303b StGB 352

V. Erweiterung des Straftatenkatalogs des § 126 StGB 353

VI. Ergebnis 354

§ 21 Die Rolle von Präventivmaßnahmen, Detektion und Reaktion im Kampf gegen Botnetze 357

I. Verhinderung von Infektionen mit Bot-Software 357

1. „Schwachstelle Mensch" 357

a) Aufklärungsarbeit und Transparenz 358

b) Transparenz 360

c) Virenschutzprogramme 360

d) Regelmäßige Sicherheitsupdates 361

e) Reduktion der Angriffsfläche 362

f) Weitere Maßnahmen, die Inhaber von IT-Systemen anwenden können, um sich zu schützen 362

2. Schwachstelle Technik 363

a) Verbesserter Schutz von IT-Systemen, insbesondere von IoT-Geräten 363

b) Entnetzung und in sich geschlossene Systeme 366

II. Detektion und Reaktion, Begrenzung der Folgen von Bot-Kriminalität 367

1. Seitens der Nutzer (potenziell) betroffener Systeme 367

a) Erhöhte Aufmerksamkeit 367

b) Bereinigung betroffener Systeme 368

c) Datensicherung 368

2. Auf technischer Seite 369
a) Ausschalten von Botnetzen durch einen „digitalen Rettungsschuss" 369
b) Honeypots 369
c) Sinkhole-Server 373
3. Bug-Bounty-Programme anstelle einer Lizenz zum Hacken 374
4. Besondere technische Sicherheitsvorkehrungen 374
5. Cyberwehr Baden-Württemberg: Ein Beispiel gelungener staatlicher Reaktion auf die wachsende Cyberkriminalität 376
III. Ergebnis 377

§ 22 Social Bots de lege ferenda 379

I. Generelles oder partielles strafrechtliches Verbot von Social Bots 379
1. Generelles Verbot von Social Bots 379
a) Ein (strafrechtliches) Verbot von Social Bots als unzulässiger Eingriff in die Meinungsfreiheit aus Art. 5 Abs. 1 S. 1 1. Alt. GG? 380
b) Fehlende Erforderlichkeit aufgrund ausreichender rechtlicher Instrumente und der Selbstregulierung der Plattformen 387
c) Legitime Einsatzbereiche von Social Bots 389
2. Partielles Verbot bösartiger Social Bots, strafrechtliche Regulierung der Verbreitung von Desinformation mithilfe von Social Bots, Verbot von Bots mit dem Zweck der Desinformation und Manipulation 392
II. Verbot der Verbreitung von Desinformation 393
III. Bewältigung des Einsatzes von Social Bots zur Manipulation der öffentlichen Willensbildung im Wahlkampf 397
1. Bedarf an einer Änderung 397
2. Strafrechtliche Regulierungsvorschläge von Social Bots im Wahlkampf: Verbot der Verbreitung von Unwahrheiten zur politischen Einflussnahme, Ergänzung des § 108a StGB 398
3. Wahlrechtliches Verbot von Social Bots 400
4. (Selbst-)Verpflichtung der Parteien, keine Social Bots im Wahlkampf anzuwenden, als Alternative zu einer straf- oder wahlrechtlichen Regelung? 401
IV. Bekämpfung des Einsatzes von Social Bots zu Cybermobbing 402
1. Bedürfnis einer Änderung 402
a) Begrenzte Schutzwirkung der Beleidigungsdelikte 403
b) Mangelnde Berücksichtigung der Besonderheiten des Cybermobbings unter Rückgriff auf Social Bots 403
aa) Besonderheiten der Beleidigung im Internet 403
bb) Besonderheiten der Beleidigung unter Rückgriff auf Social Bots 406
cc) Berücksichtigung der Besonderheiten vor der Einführung des Gesetzes zur Bekämpfung des Rechtsextremismus und der Hasskriminalität 407
dd) Reformvorschläge 408
c) Gesetz zur Bekämpfung des Rechtsextremismus und der Hasskriminalität als Schließung der aufgeführten Lücken? 409

2. Verbleibender Reformbedarf 410
a) Strafrechtliche Würdigung von (Cyber-)Mobbing im StGB 410
b) Integration von automatisiert formulierten oder verbreiteten Diffamierungen als Qualifikationstatbestand der Beleidigung 415
3. Reform der §§ 201 und 201a StGB 415
4. Weitere Maßnahmen 416

IV. Bekämpfung des Einsatzes von Social Bots beim Einsatz zu wirtschaftlichen Zwecken 417

V. Weitere strafrechtliche Maßnahmen zur Eindämmung der Risiken von Social Bots 417
1. Wiedereinführung des Straftatbestands „Befürwortung von Straftaten" 417
2. Straftatbestand der unberechtigten Nachahmung 418
3. Wiedereinführung der Strafbarkeit der Sympathiewerbung für Terrororganisationen 419

VI. Weitere rechtliche Lösungsvorschläge 420
1. Klarnamenpflicht 420
2. Erweiterte Kennzeichnungspflicht 422
3. Rechtsgrundlage für Accountsperrungen 423
4. Verpflichtung der sozialen Medien zur verstärkten Mitwirkung 423
5. Transparente Ausgestaltung von Algorithmen 425

§ 23 Medienkompetenz, glaubwürdige Medien und Fakedetektoren zur Bekämpfung der negativen Auswirkungen von Social Bots 427

I. Stärkung der Medienkompetenz und Information der Nutzer als wichtigster Baustein im Kampf gegen die Folgen von Social Bots 427

II. Glaubwürdige Medien als Gegengewicht zur wachsenden Desinformation 430

III. Die Relevanz von Fake-Detektion, Gegenaufklärung und Richtigstellungen 431
1. Fake-Detektion als Grundlage der Gegendarstellung 431
2. Löschungen von Inhalten auf der Basis der Fake-Detektion 432
3. Gegenaufklärung und Richtigstellung von Desinformation 432
4. Technische Begrenzung von Social Bots mittels (verbesserter) Captchas 434
5. Social Bots als Gegenmittel im Kampf gegen Social Bots 436

IV. Ergebnis 437

§ 24 Cheatbots de lege ferenda 441

I. Strafrechtliches Vorgehen gegen Cheatbots mittels eines neuen Tatbestands 441
1. Schummeln als Straftat 441
2. Schaffung eines generellen Verbots von Cheatbots 441
3. Strafrechtliche Verhinderung des Einsatzes von Cheatbots im eSport 442

II. Anerkennung des eSport als Sport 443

III. Integration des eSports in die Tatbestände des §§ 265c, 265d StGB 455

IV. Eigener strafrechtlicher Sportbegriff 455
V. Integration von eSports in das AntiDopG 458
VI. Ergebnis 460

§ 25 Technische Maßnahmen zur Verhinderung des Einsatzes von Cheatbots 461

§ 26 Allgemeine Maßnahmen zur Bekämpfung von Bot-Kriminalität 463

I. Verbesserung der Strafverfolgung 463
1. Verbesserung, Ausweitung und Bündelung von Fachkompetenzen 463
2. Ausbau der internationalen Zusammenarbeit 464
3. Intensivierung der nationalen Zusammenarbeit 465
II. Verbesserungen auf Rechtsfolgenseite: Vorschlag eines Internetverbots 466
III. Förderung von Forschung 468

Vierter Teil: Schlussbetrachtung und Ausblick 471

Literaturverzeichnis 473