

Herausgegeben im Auftrag der Rechtswissenschaftlichen Fakultät
der Universität Zürich von A. Donatsch, D. Jositsch, F. Meyer,
C. Schwarzenegger, B. Tag und W. Wohlers

Annina Baltisser

Datenbeschädigung und Malware im Schweizer Strafrecht

**Der Tatbestand des Art. 144^{bis} StGB
im Vergleich mit den Vorgaben
der Cybercrime Convention
und der deutschen Regelung**

Schulthess § 2013

Inhaltsverzeichnis

Vorwort	V
Inhaltsübersicht	VII
Inhaltsverzeichnis	IX
Literaturverzeichnis	XIX
Materialienverzeichnis	XXXV
Internetquellen	XXXVII
Abkürzungsverzeichnis	XXXIX
Kapitel 1 Einleitung	1
Kapitel 2 Einführung in die Computertechnik	3
I. Computersysteme und Netzwerke	3
1. Computer	3
2. Internet	5
2.1. Funktionsweise und Kommunikation	5
2.2. Internetdienste	7
II. Daten	9
1. Der Datenbegriff	9
2. Speicherung von Daten	10
3. Datendarstellung	11
3.1. Text	11
3.2. Bilder und Musik	12
3.3. Programme	12
4. Organisation von Daten	13
4.1. Dateiverwaltung	13
4.2. Datenbanksysteme	14
5. Datensicherheit und -integrität	14
5.1. Datensicherung	15
5.2. Zugriffskontrollen	15
5.3. Kryptografie	16
5.4. Data Loss Prevention	17

III. Bedrohungen des Computersystems.....	18
1. Malware.....	18
1.1. Viren.....	19
1.1.1. Virenarten.....	20
1.1.1.1. Bootviren.....	20
1.1.1.2. Makroviren.....	21
1.1.1.3. Dateiviren.....	21
1.1.2. Verschleierungstaktiken.....	23
1.1.2.1. Verschlüsselte Viren.....	23
1.1.2.2. Polymorphe Viren.....	23
1.1.2.3. Stealth Viren.....	23
1.1.3. Payload.....	24
1.2. Würmer.....	25
1.2.1. Arten von Würmern.....	25
1.2.1.1. E-Mail-Würmer.....	25
1.2.1.2. IRC- und IM-Würmer.....	26
1.2.1.3. P2P-Würmer.....	27
1.2.2. Payload.....	27
1.3. Trojanische Pferde.....	28
1.3.1. Begriff.....	28
1.3.2. Varianten.....	28
1.4. Mischformen: Zum Beispiel Logic Bombs.....	30
1.5. Exkurs: Malware für Smartphones.....	30
2. Denial of Service/Distributed Denial of Service.....	31
2.1. DoS-Angriff.....	31
2.2. DDoS-Angriff.....	32
3. Ausgewählte weitere Bedrohungen.....	33
3.1. Spyware.....	33
3.2. Adware.....	34
3.3. Spam- und Phishing-Mails.....	34
3.4. Hoaxes.....	35
4. Mögliche Schutzmassnahmen.....	35
4.1. Schutz vor Malware.....	36
4.1.1. Antivirensoftware.....	36
4.1.2. Firewalls.....	37
4.1.3. Einschränkung der Administratorrechte.....	38
4.2. Schutz vor DoS-/DDoS-Attacken.....	39
5. Malware-Programmierer.....	39

Kapitel 3 Cybercrime	41
I. Einleitung.....	41
II. Terminologie.....	44
III. Die einschlägigen Tatbestände des schweizerischen StGB.....	46
1. Verlagerung klassischer Straftaten ins Internet.....	46
2. Die Computerdelikte des StGB	46
IV. Statistik.....	47
1. Meldungen bei der KOBİK.....	47
2. Polizeilich registrierte Straftaten	50
3. Verurteilungen.....	53
4. Auswertung des statistischen Datenmaterials	54
4.1. Grafische Übersicht	54
4.2. Begrenzte Aussagekraft und Schlussfolgerungen.....	54
4.3. Datenbeschädigung und Malware als verkannte Probleme	55
Kapitel 4 Die Datenbeschädigung im Schweizer Recht.....	59
I. Allgemeines.....	59
II. Wortlaut des Art. 144^{bis} StGB	60
III. Grundlagen	60
1. Begriffserläuterungen.....	60
1.1. Daten.....	61
1.1.1. Allgemeines.....	61
1.1.2. Definition	61
1.1.2.1. Einbezug von Bildern und Ton	61
1.1.2.2. Datenverarbeitungsanlage und Datenverarbeitung	62
1.1.2.3. Gespeicherte und übermittelte Daten	63
1.2. Programme.....	64
2. Stellung im Strafgesetzbuch.....	64
2.1. Hintergrund.....	64
2.2. Kritik.....	65
3. Geschütztes Rechtsgut.....	66
3.1. Begriff des Rechtsgutes	66
3.2. Geschützte Rechtsgüter des Art. 144 ^{bis} StGB	67
3.2.1. Das geschützte Rechtsgut bei der Datenbeschädigung nach Art. 144 ^{bis} Ziff. 1 StGB.....	67
3.2.1.1. Ungestörte Verfügungsmacht über Daten.....	67

3.2.1.2.	Technischer Aspekt: Information als Rechtsgut	69
3.2.1.3.	Fazit.....	70
3.2.2.	Das geschützte Rechtsgut beim Vorbereitungstatbestand nach Art. 144 ^{bis} Ziff. 2 StGB	71
4.	Deliktatur.....	72
IV.	Der Tatbestand des Art. 144^{bis} Ziff. 1 StGB.....	72
1.	Objektiver Tatbestand	72
1.1.	Täter	73
1.2.	Angriffsobjekt.....	73
1.2.1.	Einschränkung des Angriffsobjektes.....	73
1.2.2.	Definition des Verfügungsberechtigten	74
1.3.	Tathandlungen.....	74
1.3.1.	Die einzelnen Tathandlungen.....	75
1.3.1.1.	Verändern.....	75
1.3.1.2.	Löschen	78
1.3.1.3.	Unbrauchbarmachen	80
1.3.2.	Erheblichkeit der Beeinträchtigung?.....	83
1.3.3.	Ausgewählte Erscheinungsformen der Cyberkriminalität als tatbestandsmässige Handlungen nach Art. 144 ^{bis} Ziff. 1 StGB.....	88
1.3.3.1.	DoS-/DDoS-Attacken	88
1.3.3.2.	Website Defacement	89
1.3.3.3.	Spamming	91
1.3.3.4.	Datenbeschädigung durch Passwörter?.....	92
1.4.	Unbefugtes Handeln.....	94
1.5.	Taterfolg und Kausalität	94
2.	Subjektiver Tatbestand.....	95
V.	Der Tatbestand des Art. 144^{bis} Ziff. 2 StGB.....	96
1.	Objektiver Tatbestand	96
1.1.	Täter.....	96
1.2.	Tatmittel.....	96
1.2.1.	Objektiver Charakter des Programms	97
1.2.2.	Datenbeschädigung als wesentliche Funktion.....	98
1.2.2.1.	Beschränkung der Programme auf Computerviren?	98
1.2.2.2.	Fazit.....	101
1.2.3.	Programme mit doppeltem Verwendungszweck.....	101
1.2.4.	Fazit und Ausblick	102
1.2.5.	Exkurs: Antiviren- und Datenrettungssoftware.....	103
1.2.5.1.	Verneinung einer Tatbestandsmässigkeit.....	103
1.2.5.2.	Fehlende Strafbarkeit der Anwender	104

1.3. Tathandlungen.....	105
1.3.1. Herstellen	105
1.3.2. Einführen.....	106
1.3.3. Inverkehrbringen und Zugänglichmachen	106
1.3.4. Anpreisen oder Anbieten.....	107
1.3.5. Geben von Herstellungsanleitungen.....	107
2. Subjektiver Tatbestand.....	108
2.1. Allgemeines	108
2.2. Vorsatzform	109
2.2.1. Tathandlungen.....	109
2.2.2. Verwendung im Sinne von Ziffer 1.....	109
2.2.2.1. Übersicht	109
2.2.2.2. Würdigung.....	111
2.3. Die Formulierung „weiss oder annehmen muss“.....	115
VI. Rechtswidrigkeit und Schuld	118
1. Rechtfertigungsgründe zu Art. 144 ^{bis} Ziff. 1 StGB	119
2. Rechtfertigungsgründe zu Art. 144 ^{bis} Ziff. 2 StGB	119
VII. Versuch und Vollendung	120
1. Versuch.....	120
1.1. Dogmatik.....	120
1.2. Versuchte Datenbeschädigung nach Art. 144 ^{bis} Ziff. 1 StGB...	120
1.3. Versuchte Vorbereitungshandlungen nach Art. 144 ^{bis} Ziff. 2 StGB	121
2. Vollendung	122
VIII. Täterschaft und Teilnahme.....	122
1. Täter und Teilnehmer der Datenbeschädigung nach Art. 144 ^{bis} Ziff. 1 StGB.....	122
2. Täter und Teilnehmer der Vorbereitungshandlungen nach Art. 144 ^{bis} Ziff. 2 StGB	122
IX. Strafdrohung und Antragserfordernis.....	123
1. Strafdrohung und Antragserfordernis bei der Datenbeschädigung nach Art. 144 ^{bis} Ziff. 1 StGB.....	123
2. Strafdrohung und fehlendes Antragserfordernis beim Vorbereitungstatbestand nach Art. 144 ^{bis} Ziff. 2 StGB.....	124
X. Qualifikationen und Privilegierung.....	124
1. Grosser Schaden (Qualifikation nach Art. 144 ^{bis} Ziff. 1 Abs. 2 StGB).....	124
2. Gewerbsmässigkeit (Qualifikation nach Art. 144 ^{bis} Ziff. 2 Abs. 2 StGB).....	126

3.	Geringfügige Vermögensdelikte (Privilegierung nach Art. 172 ^{ter} Abs. 1 StGB).....	127
XI.	Konkurrenzen und Abgrenzungsfragen	128
1.	Verhältnis von Art. 144 ^{bis} Ziff. 1 und Ziff. 2 StGB.....	128
2.	Konkurrenzen zu den übrigen Computerdelikten des StGB	129
2.1.	Art. 143 StGB	129
2.2.	Art. 143 ^{bis} StGB	130
2.3.	Art. 147 StGB	131
2.4.	Art. 150 StGB	131
3.	Verhältnis zu Art. 144 StGB	132
4.	Verhältnis zu Art. 251 und 254 StGB	132
XII.	Rechtsprechung	133
1.	Bundesgerichtliche Rechtsprechung: BGE 129 IV 230	133
1.1.	Sachverhalt und Erwägungen	133
1.2.	Würdigung	134
2.	Kantonale Rechtsprechung.....	135
2.1.	Vorbemerkung	135
2.2.	Beispiele.....	136
2.2.1.	Datenbeschädigung durch den Ex-Partner oder einen Bekannten.....	136
2.2.2.	Datenbeschädigung im Zusammenhang mit dem Arbeitsverhältnis	138
2.2.3.	Datenbeschädigung im Rahmen der Begehung einer anderen Straftat	139
2.3.	Schlussfolgerung.....	140
XIII.	Exkurs: Die Verletzung des Schutzes von technischen Massnahmen nach Art. 69a URG	141
1.	Vorbemerkung.....	141
2.	Wortlaut von Art. 69a URG	142
3.	Geschütztes Rechtsgut und Deliktnatur	143
4.	Art. 69a Abs. 1 lit. b URG im Besonderen.....	143
5.	Verhältnis des Art. 69a URG zu Art. 144 ^{bis} StGB	145
Kapitel 5	Datenbeschädigung in der Cybercrime Convention	147
I.	Die Cybercrime Convention.....	147
1.	Ziel und Ausgestaltung der Konvention.....	147
2.	Zusatzprotokoll.....	148
3.	Stand der Unterzeichnungen und Ratifikationen.....	148
4.	Bedeutung der Cybercrime Convention	149

II. Eingriff in Daten nach Art. 4 CCC und Missbrauch von Vorrichtungen nach Art. 6 CCC	151
1. Einleitung	151
2. Geschütztes Rechtsgut und Deliktnatur	152
3. Der Tatbestand des Art. 4 CCC	153
3.1. Wortlaut	153
3.2. Objektiver Tatbestand.....	153
3.2.1. Täter	153
3.2.2. Angriffsobjekt	154
3.2.3. Tathandlungen	154
3.2.4. Unbefugtes Handeln.....	155
3.3. Subjektiver Tatbestand.....	155
3.4. Vorbehalt nach Art. 4 Abs. 2 CCC	155
4. Der Tatbestand des Art. 6 CCC.....	156
4.1. Wortlaut	156
4.2. Objektiver Tatbestand.....	157
4.2.1. Täter	157
4.2.2. Tatmittel	157
4.2.3. Tathandlungen	158
4.2.4. Einschränkung zugunsten der berechtigten Verwendung nach Art. 6 Abs. 2 CCC.....	159
4.3. Subjektiver Tatbestand.....	160
4.4. Vorbehalt nach Art. 6 Abs. 3 CCC	160
5. Versuch und Teilnahme.....	161
6. Strafdrohung.....	161
Kapitel 6 Die Umsetzung der Cybercrime Convention im Schweizer Strafrecht	163
I. Überblick über das Gesetzgebungsverfahren	163
II. Anpassung des Art. 144^{bis} StGB	164
1. Datenbeschädigung nach Art. 144 ^{bis} Ziff. 1 StGB	164
1.1. Ergebnisse des Gesetzgebungsverfahrens.....	164
1.1.1. Vernehmlassung unter besonderer Berücksichtigung der Stellungnahme der ISSS.....	164
1.1.2. Botschaft/Entwurf EJPD	165
1.2. Würdigung	166
1.2.1. Kein Anpassungsbedarf in Bezug auf Art. 4 CCC.....	167
1.2.2. Exkurs: Anpassungsbedarf hinsichtlich Art. 5 CCC?	168
1.2.3. Fazit.....	169
2. Vorbereitungshandlungen nach Art. 144 ^{bis} Ziff. 2 StGB	170

2.1. Vorbemerkung	170
2.2. Ergebnisse des Gesetzgebungsverfahrens.....	170
2.2.1. Vernehmlassung unter besonderer Berücksichtigung der Stellungnahme der ISSS.....	170
2.2.2. Botschaft/Entwurf EJPD	171
2.3. Würdigung	173
2.3.1. Objektiver Tatbestand	174
2.3.1.1. Tatmittel Computerprogramm	174
2.3.1.2. Passwörter als Tatmittel?	175
2.3.1.3. Tathandlungen.....	176
2.3.2. Subjektiver Tatbestand.....	177
2.3.3. Fazit.....	178
III. Weitere Anpassungen im Rahmen der Umsetzung des	
Art. 6 CCC	178
1. Ergebnisse des Gesetzgebungsverfahrens	179
1.1. Vernehmlassung unter besonderer Berücksichtigung der Stellungnahme der ISSS	179
1.2. Botschaft/Entwurf des EJPD.....	180
1.3. Diskussion in den Räten.....	182
2. Würdigung.....	182
2.1. Kriminalisierung von Vorbereitungshandlungen zum Hacking.....	183
2.2. Qualifikation bei Gewerbsmässigkeit und bei krimineller Organisation.....	184
2.3. Erfüllung der Mindestanforderungen nach Art. 6 Abs. 3 CCC	185
Kapitel 7 Datenbeschädigung im deutschen Strafrecht	189
I. Einführung.....	189
II. Statistik.....	190
1. Polizeilich registrierte Straftaten	190
2. Verurteilungen.....	191
3. Vergleich mit den Schweizer Kennzahlen	192
III. Datenveränderung nach § 303a dStGB.....	193
1. Wortlaut.....	193
2. Objektiver Tatbestand	194
2.1. Angriffsobjekt	194
2.2. Tathandlungen.....	195
2.2.1. Löschen	196

2.2.2. Unterdrücken und Unbrauchbarmachen.....	196
2.2.3. Verändern.....	197
2.3. Rechtswidriges Handeln.....	197
3. Subjektiver Tatbestand.....	198
4. Rechtswidrigkeit.....	198
5. Vorbereitung, Versuch und Vollendung.....	199
6. Konkurrenzen und Antragserfordernis.....	199
IV. Vorbereiten des Ausspäbens und Abfangens von Daten nach § 202c dStGB.....	200
1. Wortlaut.....	200
2. Objektiver Tatbestand.....	200
2.1. Tatmittel.....	200
2.1.1. Passwörter und sonstige Sicherheitscodes.....	200
2.1.2. Computerprogramme.....	201
2.2. Tathandlungen.....	203
3. Subjektiver Tatbestand.....	204
4. Tätige Reue.....	205
5. Konkurrenzen und fehlendes Antragserfordernis.....	206
6. Exkurs: Die Dual-Use-Problematik – Bestreben der deutschen IT-Branche um Rechtssicherheit.....	206
6.1. Strafanzeige gegen das BSI und Verfassungsbeschwerde gegen § 202c dStGB.....	207
6.2. Selbstanzeige wegen Anbieten von „Hacker-Tools“.....	208
V. Würdigung der deutschen Umsetzung der Cybercrime Convention.....	209
1. Datenveränderung nach § 303a dStGB.....	209
2. Vorbereitungshandlungen nach § 202c dStGB.....	209
Kapitel 8 Schlussfolgerungen und Regelungsvorschläge.....	213
I. Schlussfolgerungen.....	213
II. Regelungsvorschläge.....	215
Kapitel 9 Zusammenfassung.....	219
Abbildungsverzeichnis.....	223
Stichwortverzeichnis.....	225
Anhang.....	231

Abbildungsverzeichnis

Abb. 1: Die drei wichtigsten Malware-Formen.....	19
Abb. 2: Meldungen KOBIK, 2007-2011	48
Abb. 3: Registrierte Straftaten, Schweiz und Kanton Zürich, 2009-2011..	50
Abb. 4: Registrierte Straftaten, Kanton Zürich, 2007-2008	51
Abb. 5: Verurteilungen, Schweiz und Kanton Zürich, 2007-2010.....	53
Abb. 6: Computerdelikte in der Schweiz, 2007-2011	54
Abb. 7: „You got hacked“ – Beispiel eines Website Defacements	90
Abb. 8: „Defend your country“ – Beispiel eines Website Defacements	90
Abb. 7: Art. 4 CCC und Art. 144 ^{bis} Ziff. 1 StGB im Vergleich	166
Abb. 8: Art. 6 CCC und Art. 144 ^{bis} Ziff. 2 StGB im Vergleich	173
Abb. 9: Umsetzung Art. 6 CCC, Problemkreise	187
Abb. 10: Registrierte Straftaten, Deutschland, 2007-2011	190
Abb. 11: Verurteilungen, Deutschland, 2007-2010.....	191
Abb. 12: Registrierte Straftaten, Deutschland-Schweiz, pro 100'000 Ew..	192
Abb. 13: Verurteilungen, Deutschland-Schweiz, pro 100'000 Ew.....	193