

# Hacking in der Schweiz

im Spiegel des europäischen, des deutschen und des  
österreichischen Computerstrafrechts

von

**Dr. Christa Pfister**

Rechtsanwältin in Zürich

BWV · BERLINER  
WISSENSCHAFTS-VERLAG



Schulthess



# Inhaltsverzeichnis

Inhaltsverzeichnis.....	9
Vorwort der Herausgeber .....	5
Vorwort.....	7
Abkürzungsverzeichnis .....	19
<b>1 Einleitung und Übersicht.....</b>	<b>23</b>
<b>2 Technische Grundlagen.....</b>	<b>25</b>
<b>2.1 Vorbemerkung.....</b>	<b>25</b>
<b>2.2 Computer und Internet .....</b>	<b>25</b>
<b>2.3 Hacking .....</b>	<b>30</b>
2.3.1 Vorbemerkung .....	30
2.3.2 Stationen eines Hacks .....	30
2.3.2.a Footprinting: Informationssammlung.....	30
2.3.2.b Scanning: Abtasten des Zielsystems .....	31
2.3.2.c Auswertung.....	31
2.3.2.d Angriff .....	32
2.3.3 Einzelne Vorgehensweisen .....	32
2.3.3.a Zum Beispiel: Sniffing .....	32
2.3.3.b Zum Beispiel: Spoofing .....	32
2.3.3.c Zum Beispiel: Hijacking .....	33
2.3.3.d Zum Beispiel: Buffer Overflow .....	33
2.3.3.e Zum Beispiel: ActiveX-Manipulation .....	34
2.3.3.f Zum Beispiel: Social Engineering .....	34
<b>2.4 Computerviren und andere Malware.....</b>	<b>35</b>
2.4.1 Vorbemerkung .....	35
2.4.2 Computerviren .....	35
2.4.3 Würmer.....	36
2.4.4 Trojaner .....	36
<b>2.5 Denial of Service und Distributed Denial of Service .....</b>	<b>37</b>
2.5.1 Denial of Service (DoS) .....	37
2.5.2 Distributed Denial of Service (DDoS).....	37

<b>3</b>	<b>Einführung Computerkriminalität .....</b>	<b>39</b>
<b>3.1</b>	<b>Computerkriminalität allgemein .....</b>	<b>39</b>
3.1.1	Definition.....	39
3.1.2	Geschichte der Computerkriminalität.....	40
3.1.3	Das Internet .....	41
3.1.3.a	Vorbemerkung .....	41
3.1.3.b	Geschichte.....	41
3.1.3.c	Einfluss auf die Computerkriminalität.....	43
3.1.4	Aktuelle Entwicklungen.....	43
3.1.4.a	Zum Beispiel: Phishing .....	44
3.1.4.b	Zum Beispiel: Gezielte Industriespionage.....	44
3.1.4.c	Zum Beispiel: Botnetze.....	45
<b>3.2</b>	<b>Die Computerdelikte des StGB.....</b>	<b>46</b>
3.2.1	Entstehungsgeschichte der Computerstrafnormen.....	46
3.2.2	Notwendigkeit der Neuregelung .....	47
3.2.3	Systematik der neu geschaffenen Computertatbestände .....	48
3.2.4	Rechtsgutkonzept des schweizerischen Computerstrafrechts .....	49
3.2.4.a	Rechtsgut Information?.....	49
3.2.4.b	Art. 143 <sup>bis</sup> als Vermögensdelikt?.....	51
3.2.4.c	Weitere Ungereimtheiten .....	51
3.2.4.d	Zwischenergebnis .....	52
3.2.5	Internationaler Vergleich der Systematik .....	52
3.2.5.a	Deutschland.....	52
3.2.5.b	Frankreich.....	53
3.2.6	Rechtsgut und Systematik: Fazit .....	54
3.2.7	Definitionen der zentralen Begriffe des Computerstrafrechts .....	55
3.2.7.a	Daten .....	55
3.2.7.b	Datenverarbeitungsanlage.....	57
3.2.8	Ausmass .....	59
3.2.8.a	Kriminalstatistik.....	59
3.2.8.b	Dunkelfeld.....	62
<b>4</b>	<b>Strafhoheit bei grenzüberschreitender Computerkriminalität .....</b>	<b>65</b>
<b>4.1</b>	<b>Internationalität des Internets.....</b>	<b>65</b>
<b>4.2</b>	<b>Internationales Strafrecht .....</b>	<b>65</b>

4.2.1	Ausführungsort .....	67
4.2.2	Erfolgort .....	68
4.2.2.a	Die bundesgerichtliche Rechtsprechung zum Erfolgsbegriff im Internationalen Strafrecht.....	69
4.2.2.b	Der Erfolgsbegriff in der Lehre.....	69
<b>4.3</b>	<b>Problematische Ausdehnung der Strafhoheit.....</b>	<b>72</b>
<b>4.4</b>	<b>Lösungsansätze zur Begrenzung der Strafhoheit.....</b>	<b>73</b>
4.4.1	Dogmatische Ansätze zur Begrenzung des Ubiquitätsprinzips .....	73
4.4.2	Massnahmen auf nationaler Ebene .....	74
4.4.3	Massnahmen auf internationaler Ebene .....	75
4.4.4	Fazit zur Strafhoheit.....	76
<b>5</b>	<b>Einführung Hacking .....</b>	<b>77</b>
<b>5.1</b>	<b>Definitionen .....</b>	<b>77</b>
5.1.1	Definitionen der Wörterbücher .....	77
5.1.2	Definitionen der Hacker .....	77
5.1.3	Definitionen der Gesetzgeber .....	78
5.1.4	„Richtige“ Definition? .....	78
5.1.5	Definition für die vorliegende Arbeit.....	79
<b>5.2</b>	<b>Geschichte des Hacking .....</b>	<b>79</b>
5.2.1	Die Ursprünge .....	79
5.2.2	Der Einfluss des Internet .....	80
<b>5.3</b>	<b>Die Hackerszene .....</b>	<b>81</b>
5.3.1	Die öffentliche Wahrnehmung .....	81
5.3.2	Entwicklung der Hackerszene .....	83
5.3.2.a	Vorbemerkung .....	83
5.3.2.b	Die Perspektive der Hacker .....	83
5.3.2.c	Die Perspektive der Strafverfolger .....	85
5.3.3	Besondere Strömungen.....	85
5.3.3.a	Hackivism .....	85
5.3.3.b	Open Source .....	87
<b>5.4</b>	<b>Ausmass .....</b>	<b>88</b>
5.4.1	Kriminalstatistik.....	88
5.4.2	Dunkelfeld.....	88

<b>5.5</b>	<b>Täter .....</b>	<b>89</b>
5.5.1	Profil des „typischen“ Hackers .....	89
5.5.2	Hacker-Kategorien .....	90
5.5.2.a	Klassische Hacker .....	90
5.5.2.b	„Interne“ Hacker .....	91
5.5.2.c	Cracker .....	92
5.5.2.d	Hacktivisten .....	93
5.5.2.e	Überläufer .....	93
5.5.2.f	Script Kiddies .....	93
5.5.2.g	Cyber-Terroristen und Information Warfare .....	93
5.5.3	Hacker-Gruppen .....	95
5.5.4	Hacking und Gender .....	95
5.5.5	Altersstruktur .....	96
<b>6</b>	<b>Hacking gemäss Art. 143<sup>bis</sup> StGB .....</b>	<b>99</b>
<b>6.1</b>	<b>Wortlaut .....</b>	<b>99</b>
<b>6.2</b>	<b>Rechtsgut und Deliktsnatur .....</b>	<b>99</b>
6.2.1	Rechtsgut .....	99
6.2.2	Deliktsnatur .....	100
6.2.2.a	Gefährdungs- oder Verletzungsdelikt? .....	100
6.2.2.b	Tätigkeits- oder Erfolgsdelikt? .....	102
<b>6.3</b>	<b>Objektiver Tatbestand .....</b>	<b>103</b>
6.3.1	Tatsubjekt .....	103
6.3.2	Tatobjekt Datenverarbeitungssystem .....	103
6.3.3	Das Tatbestandsmerkmal der Fremdheit .....	105
6.3.4	Das Tatbestandsmerkmal der besonderen Sicherung .....	106
6.3.4.a	Bauliche oder betriebliche Schranken als besondere Sicherungen .....	108
6.3.4.b	Passwörter und PIN als besondere Sicherungen .....	108
6.3.4.c	Kryptographie als besondere Sicherung .....	110
6.3.4.d	Firewall als besondere Sicherung .....	112
6.3.4.e	Differenzierung anhand des Opfers? .....	113
6.3.4.f	Schlussbemerkung .....	114
6.3.5	Tathandlung .....	115
6.3.5.a	Grundsatz .....	115
6.3.5.b	Hacking .....	115
6.3.5.c	Cracking .....	116
6.3.5.d	Crashing .....	116
6.3.5.e	Ethical Hacking .....	116
6.3.5.f	Social Engineering .....	116
6.3.5.g	Phreaking .....	117

6.3.5.h	Computerviren .....	117
6.3.5.i	Backdoor .....	118
6.3.5.j	Spyware.....	119
6.3.5.k	Denial of Service (DoS) / Distributed Denial of Service (DDoS).....	120
6.3.5.l	Wardriving .....	121
6.3.5.m	Cookies.....	121
6.3.6	Das Tatbestandsmerkmal des unbefugten Handelns .....	122
6.3.7	Erfolg .....	123
6.3.8	Kausalität.....	123
<b>6.4</b>	<b>Subjektiver Tatbestand .....</b>	<b>124</b>
6.4.1	Vorsatz .....	124
6.4.2	Das Tatbestandsmerkmal der fehlenden Bereicherungsabsicht.....	125
<b>6.5</b>	<b>Versuch und Vollendung.....</b>	<b>126</b>
6.5.1	Versuch und Vorbereitung .....	126
6.5.1.a	Strafrechtliche Versuchsdogmatik .....	127
6.5.1.b	Footprinting.....	128
6.5.1.c	Portscan .....	129
6.5.1.d	Hacking-Tools.....	130
6.5.1.e	Fazit.....	131
6.5.2	Vollendeter Versuch .....	131
6.5.3	Untauglicher Versuch .....	132
6.5.4	Vollendung.....	132
<b>6.6</b>	<b>Täterschaft und Teilnahme .....</b>	<b>132</b>
<b>6.7</b>	<b>Rechtfertigungs- und Schuldausschlussgründe.....</b>	<b>134</b>
<b>6.8</b>	<b>Abgrenzungen/Konkurrenzen.....</b>	<b>134</b>
6.8.1	„Datenveruntreuung“ .....	134
6.8.2	Art. 143: Unbefugte Datenbeschaffung (Datendiebstahl) .....	135
6.8.3	Art. 144 <sup>bis</sup> : Datenbeschädigung .....	136
6.8.3.a	Ziff. 1: Datenbeschädigung.....	136
6.8.3.b	Ziff. 2: Computerviren .....	136
6.8.4	Art. 147: Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Computerbetrug) .....	137
6.8.5	Art. 150: Erschleichen einer Leistung (Zeitdiebstahl).....	137
6.8.6	Art. 150: Erschleichen einer Leistung (Grundtatbestand).....	137
6.8.7	Art. 162: Fabrikations- oder Geschäftsgeheimnis.....	138

6.8.8	Art. 179 <sup>novies</sup> : Unbefugtes Beschaffen von Personendaten .....	138
6.8.9	Art. 272-274: Nachrichtendienst .....	138
6.8.10	Art. 320, 321 und 321 <sup>bis</sup> : Amts- und Berufsgeheimnis .....	139
6.8.11	Straftatbestände des DSG und kantonaler Datenschutzgesetze .....	139
6.8.12	Straftatbestände des UWG .....	139
6.8.13	Straftatbestände des URG .....	139
<b>6.9</b>	<b>Strafdrohung .....</b>	<b>140</b>
6.9.1	Geltendes Recht .....	140
6.9.2	Regelung bis Ende 2006 und Übergangsrecht .....	140
<b>6.10</b>	<b>Antragserfordernis .....</b>	<b>141</b>
6.10.1	Die Antragsberechtigung .....	141
6.10.2	Ein abstraktes Gefährdungsdelikt als Antragsdelikt? .....	143
6.10.3	Bewertung des Antragserfordernisses .....	143
6.10.4	Ausblick .....	144
<b>6.11</b>	<b>Rechtsprechung.....</b>	<b>144</b>
6.11.1	Vorbemerkung und Vorgehen.....	144
6.11.2	Ein Entscheid zum Tatbestandsmerkmal der besonderen Sicherung.....	145
6.11.3	Rechtsprechung zu Konkurrenzfragen .....	145
6.11.4	Ein Entscheid zu Hacking und Mobiltelefon .....	146
6.11.5	Gesamteindruck.....	146
<b>6.12</b>	<b>Revisionsbedarf?.....</b>	<b>147</b>
<b>7</b>	<b>Hacking gemäss Art. 2 des Übereinkommens über Computerkriminalität des Europarates .....</b>	<b>149</b>
<b>7.1</b>	<b>Das Übereinkommen über Computerkriminalität (Cybercrime Convention).....</b>	<b>149</b>
7.1.1	Entstehungsgeschichte.....	149
7.1.2	Zusatzprotokoll .....	150
7.1.3	Rechtsnatur .....	151
7.1.4	Unterzeichnungen und Ratifikationen .....	151
7.1.5	Inhalt.....	152
7.1.5.a	Begriffsbestimmungen (erstes Kapitel) .....	152

7.1.5.b	Harmonisierung des materiellen Rechts (zweites Kapitel, Abschnitt 1).....	152
7.1.5.c	Strafprozessrecht (zweites Kapitel, Abschnitt 2).....	153
7.1.5.d	Zuständigkeitsfragen (zweites Kapitel, Abschnitt 3).....	153
7.1.5.e	Internationale Zusammenarbeit (drittes Kapitel) .....	154
7.1.5.f	Viertes Kapitel der Cybercrime Convention .....	155
7.1.6	Ziele .....	155
7.1.7	Würdigung .....	156
<b>7.2</b>	<b>Hacking in der Cybercrime Convention.....</b>	<b>158</b>
7.2.1	Wortlaut Art. 2 (englisch) .....	158
7.2.2	Wortlaut Art. 2 (deutsch).....	158
7.2.3	Objektiver Tatbestand und Rechtsgut.....	159
7.2.4	Subjektiver Tatbestand .....	160
7.2.5	Zulässige Einschränkungen.....	160
7.2.6	Versuch, Teilnahme, Sanktionen .....	161
7.2.7	Tatwerkzeuge .....	162
<b>7.3</b>	<b>Hacking gemäss Cybercrime Convention und gemäss StGB im Vergleich .....</b>	<b>163</b>
7.3.1	Rechtsgut und Deliktstypus .....	163
7.3.2	Objektiver Tatbestand.....	164
7.3.3	Subjektiver Tatbestand .....	164
7.3.4	Versuch, Teilnahme .....	165
7.3.5	Antragserfordernis .....	165
7.3.6	Hacking-Tools.....	166
7.3.7	Fazit.....	167
<b>8</b>	<b>Hacking gemäss Art. 2 des Rahmenbeschlusses über Angriffe auf Informationssysteme .....</b>	<b>169</b>
<b>8.1</b>	<b>Der Rahmenbeschluss über Angriffe auf Informationssysteme: Einführung .....</b>	<b>169</b>
8.1.1	Vorbemerkung: Europäisches Strafrecht? .....	169
8.1.2	Rechtsnatur .....	172
8.1.3	Inhalt.....	174
8.1.3.a	Gründe.....	174
8.1.3.b	Definitionen (Art. 1).....	174
8.1.3.c	Strafbestimmungen (Art. 2 bis 4) .....	175
8.1.3.d	„Allgemeiner Teil“ und Sanktionen (Art. 5 bis 9) .....	175
8.1.3.e	Zuständigkeit und internationale Zusammenarbeit (Art. 10 und 11).....	176

8.1.3.f	Umsetzung und Inkrafttreten (Art. 12 und 13).....	176
<b>8.2</b>	<b>Hacking im Rahmenbeschluss .....</b>	<b>177</b>
8.2.1	Wortlaut Art. 2.....	177
8.2.2	Objektiver Tatbestand und Rechtsgut.....	177
8.2.3	Subjektiver Tatbestand .....	178
8.2.4	Zulässige Einschränkungen.....	178
8.2.5	Versuch, Teilnahme, Sanktionen .....	178
<b>8.3</b>	<b>Hacking gemäss Rahmenbeschluss und gemäss StGB im Vergleich .....</b>	<b>179</b>
8.3.1	Vorbemerkung .....	179
8.3.2	Objektiver Tatbestand.....	179
8.3.3	Subjektiver Tatbestand .....	180
8.3.4	Versuch und Teilnahme.....	180
8.3.5	Antragserfordernis .....	181
8.3.6	Strafmass .....	181
8.3.7	Fazit.....	181
<b>8.4</b>	<b>Mehrwert des Rahmenbeschlusses? .....</b>	<b>182</b>
8.4.1	Kein Kollisionsrecht .....	182
8.4.2	Ähnlichkeit mit der Cybercrime Convention .....	182
8.4.3	Fehlende direkte Erzwingbarkeit.....	183
8.4.4	Fazit.....	184
<b>9</b>	<b>Hacking im deutschen Strafrecht .....</b>	<b>185</b>
<b>9.1</b>	<b>Einführung.....</b>	<b>185</b>
<b>9.2</b>	<b>§ 202a dStGB vor der Revision.....</b>	<b>185</b>
9.2.1	Wortlaut (alt) § 202a dStGB.....	185
9.2.2	Entstehungsgeschichte des (alt) § 202a dStGB .....	185
9.2.3	Rechtsgut des (alt) § 202a dStGB .....	186
9.2.4	Objektiver Tatbestand des (alt) § 202a dStGB .....	186
9.2.5	Subjektiver Tatbestand des (alt) § 202a dStGB.....	188
<b>9.3</b>	<b>§ 202a dStGB nach der Revision.....</b>	<b>188</b>
9.3.1	Wortlaut (neu) § 202a dStGB .....	188
9.3.2	Wortlaut § 202c dStGB .....	189

9.3.3	Die Revision .....	189
9.3.4	Ausgewählte Aspekte der Neuregelung.....	190
9.3.4.a	Hacking-Strafbarkeit .....	190
9.3.4.b	Straflosigkeit des Hacking-Versuchs .....	191
9.3.4.c	Hacking-Tools.....	191
9.3.4.d	Antragserfordernis .....	191
9.4	<b>Würdigung der deutschen Umsetzung der internationalen Instrumente.....</b>	<b>192</b>
10	<b>Hacking im österreichischen Strafrecht .....</b>	<b>195</b>
10.1	Wortlaut § 118a StGB .....	195
10.2	Entstehungsgeschichte von § 118a öStGB.....	195
10.3	Objektiver Tatbestand .....	195
10.4	Subjektiver Tatbestand .....	196
10.5	Ermächtigungserfordernis.....	197
10.6	Würdigung und Ausblick .....	197
11	<b>Strafwürdigkeit des Hacking .....</b>	<b>199</b>
11.1	Einführung.....	199
11.2	Hacker als Wohltäter für die Gesellschaft?.....	199
11.3	Schadenspotenzial des Hacking .....	200
11.4	Die <i>ultima ratio</i> -Funktion des Strafrechts .....	202
11.5	<b>Straflosigkeit bei Selbstanzeige als Alternative? .....</b>	<b>204</b>
11.5.1	Ein Vorschlag aus Hackerkreisen.....	204
11.5.2	Gleicher Effekt durch das Antragserfordernis? .....	206
11.6	<b>Fazit .....</b>	<b>207</b>
12	<b>Zusammenfassung und Ergebnisse.....</b>	<b>209</b>
	Literaturverzeichnis .....	213
	Stichwortverzeichnis .....	223