

Cybercrime und Strafrecht in der Informations- und Kommunikationstechnik

von

Dieter Kochheim
Oberstaatsanwalt in Hannover

2. Auflage 2018



Inhaltsüberblick

Geleitwort	VII
Vorbemerkungen zur 2. Auflage	IX
Vorwort zur 1. Auflage	XI
Inhaltsverzeichnis	XV
Abkürzungsverzeichnis	XXVII
Teil 1: Duale Welt	1
Kapitel 1. Cybercrime und IuK-Strafrecht	15
Kapitel 2. Geschichte des Cybercrime	41
Kapitel 3. Formen und Methoden des Cybercrime	143
Kapitel 4. Gefahren und Hackteure in der dualen Welt	205
Teil 2: Materielles IuK-Strafrecht	227
Kapitel 5. Hacking	229
Kapitel 6. Malware	303
Kapitel 7. Botnetze	335
Kapitel 8. Missbräuchliche Datenverwertung und Rechtsverfolgung	341
Kapitel 9. Bargeldloser Zahlungsverkehr	353
Kapitel 10. Betrug, Irrtum und Schaden	399
Kapitel 11. Zahlungs- und Warenverkehr	429
Kapitel 12. Skimming	445
Kapitel 13. Urkunden und beweiserhebliche Daten	485
Kapitel 14. Phishing	527
Kapitel 15. Onlinehandel und Underground Economy	557
Kapitel 16. Arbeitsteiliges und modulares Cybercrime	603

Kapitel 17. Würde, persönliche Entfaltung und Meinung	623
Kapitel 18. Pornografische Abbildungen	635
Teil 3: Ermittlungen gegen das Cybercrime	645
Kapitel 19. Strafverfolgung, Verdacht und Ermittlungen	649
Kapitel 20. Das Internet und die IuK-Technik als Informationsquellen	707
Kapitel 21. Informationsquellen und Sachbeweise	727
Kapitel 22. Personale Ermittlungen	747
Kapitel 23. Technische Maßnahmen	763
Teil 4: Die Zukunft des Cybercrime und seiner Strafverfolgung	783
Kapitel 24. Cybercrime und der Umgang mit der IuK-Technik	785
Kapitel 25. Materielles IuK-Strafrecht	797
Kapitel 26. Strafverfahrensrecht	803
Kapitel 27. Vorläufiger Abschluss der Bestandsaufnahme?	805
Glossar	807
Rechtsprechungsübersicht	911
Stichwortverzeichnis	927

Inhaltsverzeichnis

Geleitwort	VII
Vorbemerkungen zur 2.Auflage	IX
Vorwort zur 1.Auflage	XI
Inhaltsüberblick	XIII
Abkürzungsverzeichnis	XXVII
Teil 1: Duale Welt	1
A. Jargon und Fachbegriffe	3
B. Zu Teil 1: Duale Welt	5
C. Zu Teil 2: Materielles IuK-Strafrecht	7
I. Quellen des materiellen IuK-Strafrechts	8
II. Gesetzlich ausgestaltetes Hacking-Strafrecht	9
III. Betrugsnahe Cybercrime	12
IV. Schweres Cybercrime	13
D. Zu Teil 3: Ermittlungen gegen das Cybercrime	14
Kapitel 1. Cybercrime und IuK-Strafrecht	15
A. Technische Gegenstände des IuK-Strafrechts	16
B. Abgrenzungen zu anderen Begriffssystemen	19
C. Besonderheiten des Cybercrime und des IuK-Strafrechts	21
D. IuK-Strafrecht im engeren Sinne	24
E. Bedeutung des Cybercrime	28
F. Quellen für die Bestandsaufnahme	32
I. Register aktueller Cyber-Gefährdungen	33
II. Bedrohungen gegen industrielle Anlagensteuerungen	35
1. Unberechtigte Nutzung von Fernwartungszugängen	35
2. Online-Angriffe über Office-/Enterprise-Netze	35
3. Angriffe auf eingesetzte Standardkomponenten im ICS-Netz	35
4. (D)DoS-Angriffe	36
5. Menschliches Fehlverhalten und Sabotage	36
6. Einschleusen von Schadcode über Wechseldatenträger und externe Hardware	36
7. Lesen und Schreiben von Nachrichten im ICS-Netz	36
8. Unberechtigter Zugriff auf Ressourcen	37
9. Angriffe auf Netzwerkkomponenten	37
10. Technisches Fehlverhalten und höhere Gewalt	37
G. Fazit: Cybercrime und IuK-Strafrecht	37

Kapitel 2. Geschichte des Cybercrime	41
A. Vor 1900. Technische und wirtschaftliche Anfänge	43
B. Bis 1950. Elektrotechnik und technische Großanlagen	46
C. Bis 1970. Beginn des elektronischen Zeitalters	47
D. Bis 1980. Gründerzeit der Mikroelektronik	50
E. Bis 1990. Expansion und Missbrauch	52
F. Bis 2000. Internet und Viren	55
I. Adressierung und Internetverwaltung	57
1. Telekommunikation	59
2. Datenkommunikation und Internet	64
3. Domain Name System	68
4. Hierarchische Internetverwaltung	69
5. Content Distribution Network	71
II. Informations- und Kommunikationstechnik bis 2000	71
III. Cybercrime und Anfänge der Rechtsprechung zur IuK	73
1. Dialer und Mehrwertdienste	73
2. Grabbing	74
3. Haftung für Links	74
4. Haftung des Providers	78
G. Seit 2000. Kommerzielles Internet und organisiertes Cybercrime	79
I. „Raubkopien“	82
II. Hacking und Malware	84
III. Botnetze. Hacktivismus	86
IV. Konvergenz zwischen Sprach- und Datendiensten	89
1. Mobilfunknetze und technische Innovationen	89
2. Mobiles Cybercrime	91
3. Konvergenz und technische Zusammenführung	94
V. Assistenten, KI und IoT	95
H. Cybercrime in der Neuzeit	98
I. Klaus Störtebeker	99
II. Cardingboards	99
III. Botnetze	102
IV. Stuxnet	107
V. Datenspionage	110
1. Shady Rat	111
2. Aurora	111
3. Night Dragon	112
4. High Roller	113
5. Anunak, Carbanak	113
6. The Man-in-the-Middle	115
7. Online-Seed-Generator	116
8. Kommerzielle und aktivistische Datenabgriffe	117
VI. Ransomware	125
VII. Abofallen	128
VIII. Webshops und Betrug	130
I. Technische und gesellschaftliche Hintergründe des IuK-Strafrechts	131
I. 2. WiKG	133
II. IuKDG	134

III. Bekämpfung der Computerkriminalität	136
IV. Stillstand bei der Kodierung des materiellen IuK-Strafrechts	137
J. Fazit: Wesentliche Formen des Cybercrime	138
Kapitel 3. Formen und Methoden des Cybercrime	143
A. Schema eines Hacking-Angriffs	146
B. Social Engineering	149
I. Farmen. Methodisches Vorgehen	150
II. Zuwendung und Gier: Chatbots	152
III. Neue Gefahren im IoT	154
C. Phishing	155
D. Finanzagenten und Beutesicherung	157
I. Unfreiwillige und unechte Finanzagenten	158
II. Warenagenten, Packstationen und Bezahlssysteme	159
E. Skimming	160
I. Merkmalstoffe und EMV-Chip	164
II. Formenwechsel beim Datenabgriff	165
III. Skimming unter Einsatz des Hackings	167
F. Malware	169
I. Basis-Malware und Infiltration	170
1. Präparierte Webseiten	174
2. E-Mails und E-Mail-Anhänge	176
3. Andere Formen der Anlieferung und Infiltration	176
4. Erkundung des Systems und Einnisten der Malware	177
II. Produktive Malware	178
1. Maliziöse Grundfunktionen	179
2. Ransomware	180
3. Bot Ware	182
4. Onlinebanking-Malware	182
5. Anlagensteuerungen	184
G. Crimeware-as-a-Service	185
I. Die RIG-Infrastruktur im Überblick	187
II. Sprungseiten und Weiterleitungen	188
III. Infiltration und Verwaltung der Bots	190
IV. Umleitung und Abgriff von Verkehrsdaten	190
H. Vom Klickbetrug zum Ad Fraud	192
I. Identitätstäuschung und Identitätsdiebstahl	194
I. Identitätstäuschung im Rechtssinne	196
II. Identitätsmerkmale und Identitätsübernahme	199
J. Carding und Kontobetrug	200
K. Fälschung von Zahlungskarten	202
Kapitel 4. Gefahren und Hackteure in der dualen Welt	205
A. Gefahren, Typen und Hackteure	205
I. Bedrohungsregister vom BSI	206
II. Typen und Strukturen	208
III. Vorsätzlich handelnde Angreifer laut BSI	214
B. Cyber-Aktivist (Hacktivist)	214
I. Hacker und Hacktivismus	215

II. Anonymous und Payback	218
III. Die Zukunft des Hacktivismus	221
C. Subkulturen und Sprachen	223
Teil 2: Materielles IuK-Strafrecht	227
Kapitel 5. Hacking	229
A. Gegenstand und Grenzen des Hacking-Strafrechts	230
B. Ausspähen und Abfangen von Daten	239
I. Zugangssperren gegen das Ausspähen	242
1. Ungeschützte Daten	243
2. Systemstart und Kennwortschutz	245
3. Angriff im laufenden Betrieb	248
II. Wiederholte Überwindung von Zugangssperren	248
1. Vollendung und Beendigung	249
2. Zustands- und Dauerdelikt	250
3. Beitritt eines Dritten	251
III. Angriff gegen ein Local Area Network – LAN	251
1. Missbrauch indiskreter Kenntnisse	252
2. Wardriving	253
3. Inhaltlicher Schutzbereich von Daten aus dem LAN	256
4. Datenübermittlung im Internet und Webserver	258
5. Gesetzesinitiative zum „Digitalen Hausfriedensbruch“	260
C. Datenveränderung und Computersabotage	262
I. Datenveränderung	262
II. Computersabotage	267
1. Datenverarbeitung von wesentlicher Bedeutung	267
2. Schutz der Datenverarbeitung; DDoS	270
3. Grunddelikt und schwere Computersabotage	277
D. Computerbetrug	279
I. Datenmanipulation	280
II. Geldspielautomaten	282
III. Card-Sharing	284
IV. Dreieckscomputerbetrug	285
V. Manipulierte Sportwetten	286
VI. Cashing	287
VII. Systematische Struktur- und Wertgleichheit	287
1. Systematische Betrachtung	288
2. Kritik	289
E. IuK-Straftaten im Vorbereitungsstadium	291
I. Tatphasen	294
II. Computerprogramme	297
III. Einsatz von Hardware	298
IV. Passwörter und Zugangscodes	299
V. Kopierschutz, WareZ	300
VI. Verabredung von IuK-Verbrechen	300

Kapitel 6. Malware	303
A. Basis-Malware	306
B. Vorbereitungsstadium	309
I. Distanzdelikte	310
II. Vorbereitende IuK-Straftaten und Beginn des Versuchs	314
III. Zusammenfassung: Strafbarer Versuch	318
C. Anlieferung und Installation	319
D. Einnisten und Tarnung	327
I. Ransomware	328
II. Viren und Würmer	329
III. Backdoors	329
IV. Keylogger und Spyware	331
V. Verzögert und langfristig wirkende Malware	332
VI. Tarnung, Stealth	332
VII. Zusammenfassung	333
E. Crimeware-as-a-Service	334
Kapitel 7. Botnetze	335
A. Straftaten beim Betrieb eines Botnetzes	337
B. Steuerung eines Botnetzes	338
C. Spezialisierte Bot Ware gegen Kritische Infrastrukturen	339
Kapitel 8. Missbräuchliche Datenverwertung und Rechtsverfolgung	341
A. Dienstgeheimnisse	342
B. Privater Missbrauch von personenbezogenen Daten	343
I. Erhebung und Verarbeitung von Verkehrsdaten	343
II. Bewegungsprofile per GPS	344
III. Dashcam	345
C. Geschäfts- und Betriebsgeheimnisse	346
D. Steuerdaten-CDs	347
E. Fallen und Abmahnungen	348
F. Gesetz gegen die Datenhehlerei	350
Kapitel 9. Bargeldloser Zahlungsverkehr	353
A. SEPA. Eine Einführung	353
B. Authentifizierung, Autorisierung und Kundenkennung	354
I. Authentifizierung und Autorisierung	355
II. Garantiefunktion und Kundenkennung	355
III. Transaktionsnummer	356
C. Anweisung	358
D. Lastschriftverfahren	360
I. Vertragsverhältnisse im Lastschriftverfahren	361
II. Verfahrensabläufe und Fachbegriffe	363
III. Bankkonto und Zahlungsdienste	364
IV. Schadensrisiken und Schadensgemeinschaft	367
1. Inkassostelle	367
2. Kontoinhaber	368
3. Zahlstelle und Zahlungsdiensterahmenvertrag	369

4. Schadensgemeinschaft zwischen Zahlstelle und Kontoinhaber . . .	371
E. Autorisierung bei Zahlungskarten und Clearing	373
F. Sicherheitsmerkmale von Zahlungskarten	376
G. Bargeldlose Zahlungen ohne Karte	378
H. Neue Instrumente im Zahlungsverkehr	380
I. Originäre Zahlungsverfahren	380
II. Abgeleitete Zahlungsverfahren	381
III. Aktuelle Bezahl- und Verrechnungsverfahren	384
1. Virtualisierte Zahlungs- und Bankdienste	384
2. Kontokorrentsysteme	384
3. Kreditäre Abrechnungssysteme	385
4. Gutscheinhändler	385
5. Proprietäre Verrechnungssysteme und Bitcoins	385
6. Wechselstuben	385
IV. Kryptowährungen. Bitcoin	386
1. Überblick	387
2. Blockchain	389
3. Bitcoin-Client; Wallet	391
4. Mining	392
5. Bewertung	393
6. Missbrauch von Kryptowährungen durch Hacking	396
V. Fazit	398
Kapitel 10. Betrug, Irrtum und Schaden	399
A. Kaufvertrag und Irrtum	401
B. Besondere Formen des Betruges	405
C. Täuschung über die Zahlungsfähigkeit	407
D. Risikogeschäfte und Schaden	409
E. Schadenseintritt und Vermögensgefährdung	411
F. Kreditbetrug und Rückzahlungsanspruch	413
G. Debitkonto und Kartenmissbrauch	415
H. Kontoeröffnungsbetrug	417
I. Gefälschte Schecks	422
J. Manipulationen mit Bankkonten	423
K. Fazit	426
Kapitel 11. Zahlungs- und Warenverkehr	429
A. Beschaffung von Daten	430
B. Beschaffung von Tatausführungsmitteln	432
C. Tatausführung	434
D. Beuteerlös und -sicherung	437
E. Verbotene Bankgeschäfte	440
I. Bargeldtransfer und Hawala	440
II. Treuhand	442
Kapitel 12. Skimming	445
A. Skimming als mehrgliedriges Delikt	445
I. Cashing als finales Tatziel	447
II. Fälschungsdelikte	448

III. Zahlungskarten	450
IV. Grundlagen zum Skimming	451
B. Tatphasen, Versuch und Vorbereitung	453
I. Beteiligung am Versuch	456
II. Umgangsdelikte in der Vorbereitungsphase	461
1. Skimminggeräte	461
2. Computerbetrug und Computerprogramme	462
3. Werkzeuge und Werkstoffe	463
4. Tatphasenmodell für das Vorbereitungsstadium	466
III. Skimming im engeren Sinne	467
IV. Datenbeschaffung per Hacking	471
V. Angriffe gegen Karten und Geldausgabeautomaten	472
VI. Verabredung zum Skimming	473
1. Gewerbsmäßiges Handeln	474
2. Bande	475
3. Beteiligung an einer Straftat	476
4. Täter hinter dem Täter	477
5. Zwischenergebnisse	478
6. Tatvarianten bei der Beteiligung am Skimming	479
VII. Deliktische Einheiten und Konkurrenzen	481
Kapitel 13. Urkunden und beweishebliche Daten	485
A. Urkunde und Abbild	488
B. Amtliche Ausweise und Persobuilder	493
C. Identitätstäuschung	495
I. Anonymität, Pseudonym und Identität	496
II. Datenlüge und Identitätstäuschung	498
1. Strafbare Täuschung: Kammergericht Berlin	499
2. Strafloze Datenlüge: OLG Hamm	499
3. Offene und verdeckte Pseudonyme; Lehnnamen	500
D. Falsche beweishebliche Daten	502
E. Fakes, falsche und Lehnnamen	506
I. Fake Account und Fake-Identität	506
II. Lehnnamen	506
III. Bankdrops	508
IV. Fazit	509
F. Virtuelle Kommunikation und Abbilder	510
I. Quasiurkunden	511
II. Spam-Mails und Schutzrechte	512
III. Technische Stempel und Adressen	513
IV. Namens- und Identitätstäuschung	514
G. Urkunde und Quasiurkunde	518
I. Abbild und Verkörperung	518
II. Lüge oder Identitätstäuschung	521
H. Fälschung technischer Aufzeichnungen	523
Kapitel 14. Phishing	527
A. Finanzagenten	529
I. Vollendung und Beendigung	530

II. Doppelter Gehilfenvorsatz	531
III. Begünstigung	533
IV. Geldwäsche und Hehlerei	534
V. Ergebnisse	535
B. Klassisches Phishing	535
I. Tatphasen beim Kontohacking	537
II. Werbung von Finanzagenten	539
III. Webdesign und Werbetexte	540
C. Nachgemachte Webseiten	541
D. Direkter Eingriff in das Onlinebanking	544
E. Vollautomatisches Phishing	548
F. Fazit: Phishing in verschiedenen Phasen	552
Kapitel 15. Onlinehandel und Underground Economy	557
A. Webshops	557
B. Abofallen	561
I. Kompakte Handlungsmodelle	564
II. Distanzdelikt und sukzessive Tatausführung	566
III. Göttinger Abofälle und Bewertung	569
C. Nummertricks	569
I. Klassische Nummertricks (Spoofing)	570
II. Erfolgreiche Regulierung	571
III. Rückruftrick. Ping-Anrufe	571
D. Einzeltrick und Schockanrufe	574
E. Carding- und andere Boards	576
I. Cardingboards	579
II. Kriminelle Geschäfte	579
1. Eigene kriminelle Geschäfte	580
2. Öffentliche Aufforderung zu Straftaten	582
F. Bullet Proof-Dienste	583
G. Anonymisierungsdienste	586
H. Clearnet, Deepnet und Darknet	594
I. Zahlungsdienste und Geldwäsche	599
Kapitel 16. Arbeitsteiliges und modulares Cybercrime	603
A. Infrastrukturelle Tatbeteiligung und Begünstigung	606
I. Streaming: Internetradio und urheberrechtlich geschützte Filme	606
II. Hacking- und Cardingboards	607
III. Bullet Proof-Dienste	608
IV. Zulieferer und Crimeware-as-a-Service	609
V. Tatherrschaft und Beteiligung	611
B. Mittäterschaft und Bande	612
C. Mittelbare Täterschaft und uneigentliches Organisationsdelikt	615
D. Kriminelle Vereinigung	617
E. Kriminelle Vereinigung im IuK-Strafrecht	621
F. Ergebnisse	622
Kapitel 17. Würde, persönliche Entfaltung und Meinung	623
A. Nachstellung und Entwürdigung	625

B. Äußerungsdelikte	628
C. Haftung der Telemediendienste	632
Kapitel 18. Pornografische Abbildungen	635
A. Nacktheit. Posing. Pornografie	637
B. Schutzzwecke	638
C. Herstellungs-, Verschaffungs- und Verbreitungsverbote	639
D. Zwischenspeicher	640
E. Zugänglichmachen. Besitzverschaffung	642
Teil 3: Ermittlungen gegen das Cybercrime	645
Kapitel 19. Strafverfolgung, Verdacht und Ermittlungen	649
A. Aufgaben der Strafverfolgung	650
B. Ermittlungshandlungen	654
I. Auskunftersuchen oder Rasterfahndung?	655
II. Klassische Erkenntnisquellen	656
III. Verdeckte Ermittlungen	656
C. Anhaltspunkte und Verdacht	659
I. Spurenkritik und zulässige Eingriffsmaßnahme	660
II. Anfangsverdacht	662
III. Verhältnismäßigkeit, Eingriffstiefe und Schwere der Kriminalität	664
IV. Geltung von Tatsachen und Erfahrungen	666
V. Eignung, Erfolgserwartung und Ermittlungskonzept	668
VI. Gefahr im Verzug	671
D. Ermittlungsmaßnahmen im Überblick	672
I. Polizeiliche Eingriffsmaßnahmen	672
II. Beschränkte Eingriffsmaßnahmen ohne Katalogbindung	674
III. Personale Ermittlungen gegen die erhebliche Kriminalität	675
IV. Technische Eingriffsmaßnahmen	676
E. System der technischen Ermittlungsmaßnahmen	676
I. Neugestaltung der §§ 100a ff. StPO	679
II. Straftatenkataloge im Überblick	680
1. Betrugs- und Fälschungsdelikte	681
2. Erpressung	682
3. Absatzkriminalität	682
4. Hehlerei, Geldwäsche	683
5. Kriminelle Vereinigung, Volksverhetzung	683
6. Kritische Infrastrukturen	683
III. Repressive Datenzugriffe und Straftatenkataloge	684
F. Verwertungsgrenzen und -verbote	686
I. Erhebungs- und Verwertungsverbote	686
II. Erhebungs- und Verwertungsgrenzen in der StPO	688
1. Kernbereich der persönlichen Lebensgestaltung	690
2. Beweisverwertungsverbote	691
3. Zusammenfassung	693
III. Hypothetischer Ersatzeingriff	695
1. Doppeltürmodell	696

2. Spurenansatz	699
IV. Gemengelage; legendierte Kontrolle	700
Kapitel 20. Das Internet und die IuK-Technik als Informationsquellen	707
A. BVerfG zur Onlinedurchsuchung	707
B. Persönlichkeitsschutz durch Grundrechte	709
I. Telekommunikationsgeheimnis und Verkehrsdaten	713
II. Informationelle Selbstbestimmung	716
III. Vertraulichkeit und Integrität informationstechnischer Systeme	717
IV. Unverletzbarkeit der Wohnung	718
V. Eingriffstiefe und additive Grundrechtseingriffe	719
C. Dokumentationsermächtigung und Akten	720
D. Technischer Fortschritt und Eingriffsmaßnahmen	724
Kapitel 21. Informationsquellen und Sachbeweise	727
A. Öffentliche Quellen und behördliche Auskünfte	728
I. Öffentliche Quellen und Kommunikation	729
II. Behördliche Auskünfte	730
III. Registerauskünfte	731
B. Auskünfte und Zwangsmittel	732
C. Bestandsdaten	734
D. Durchsuchung	737
I. Durchsicht und Sicherstellung	738
II. Ferndurchsicht	741
E. Beschlagnahme von E-Mail-Konten	743
Kapitel 22. Personale Ermittlungen	747
A. Informanten und Vertrauenspersonen	748
B. NoeB und Verdeckte Ermittler	751
I. Verdeckte Ermittler	751
II. Nicht offen ermittelnde Polizeibeamte	753
III. Abgrenzung zwischen NoeB und VE	754
IV. Verdeckte personale Ermittlungen gegen das Cybercrime	757
C. Zugangsverschaffung	759
I. Nutzung fremder Zugangsdaten	759
II. Zugangsbeschränkungen und Keuschheitsproben	760
III. Scheinkauf	761
Kapitel 23. Technische Maßnahmen	763
A. Observation und technische Mittel	764
B. Verkehrsdaten und Vorratsdaten	766
I. Verkehrsdaten	768
II. Vorratsdaten	770
III. Funkzellendaten	772
IV. Standortdaten	773
C. TKÜ und Serverüberwachung	773
I. Überwachung der Telekommunikation	773
II. Auslandskopfüberwachung	775
III. IMSI-Catcher	776

D. Zugriff auf die Cloud	776
E. Onlinedurchsuchung und Quellen-TKÜ	779
F. Spyware und Crawler	780
 Teil 4: Die Zukunft des Cybercrime und seiner Strafverfolgung	 783
Kapitel 24. Cybercrime und der Umgang mit der IuK-Technik	785
A. Gezielte Angriffe mit verfeinerten (und robusteren) Instrumenten	786
B. Schwachstellen und Gefahren	789
C. Technik, Mensch, Security	793
 Kapitel 25. Materielles IuK-Strafrecht	 797
A. Ausspähen und Abfangen von Daten	798
B. Datenveränderung und Computersabotage	800
C. Vorbereitungs- und Verwertungshandlungen	800
D. Computerbetrug	801
E. Datenfälschungen	801
 Kapitel 26. Strafverfahrensrecht	 803
 Kapitel 27. Vorläufiger Abschluss der Bestandsaufnahme?	 805
 Glossar	 807
 Rechtsprechungsübersicht	 911
 Stichwortverzeichnis	 927