

Inhaltsverzeichnis

Erster Teil

Einleitung und Grundlagen

A.	Einleitung	29
I.	Einführung	29
II.	Theorie und Realität der Überwachung moderner Kommunikation	31
	1. Der „Staatstrojaner“	31
	2. Die Alternativlosigkeit des „Staatstrojaners“	33
	3. Eine Alternativmöglichkeit	34
	a) Die Alternativmöglichkeit aus technologischer Sicht	34
	b) Die Alternativmöglichkeit in der Praxis	35
	c) Die Alternativmöglichkeit aus rechtlicher Sicht	36
III.	Methodik	36
	1. Informationstechnologische Analyse	37
	2. Rechtliche Analyse	38
IV.	Gang der Darstellung	38
B.	Begrifflichkeiten und Grundlagen der Kommunikation über das Internet-Netzwerk	40
I.	Das Internet-Netzwerk	40
II.	Die Netzwerkprotokolle des Internet-Netzwerkes	42
	1. Referenzmodelle	42
	2. TCP/IP-Referenzmodell	43
	a) Aufbau des TCP/IP-Referenzmodells	43
	b) Die einzelnen Schichten des TCP/IP-Referenzmodells	44
	aa) Anwendungsschicht	44
	bb) Transportschicht	45
	cc) Internetschicht	45
	dd) Netzzugangsschicht (Sicherungs- und Bitübertragungsschicht)	46
	(1) IEEE 802.11 (WLAN) als Beispielprotokoll der Netzzugangsschicht	47
	(a) Betriebsmodus	47
	(b) Assoziation	48
	(c) Begleiterscheinungen der Funkübertragung	48
	(d) Authentifizierung/Verschlüsselung	49
	(aa) Sicherheitsmechanismen	49

	(bb) WPA2-Personal und WPA2-Enterprise . . .	49
	(e) Adressierung	50
	(2) Address Resolution Protocol	50
	(a) Intra-Netzwerk-Niveau	51
	(b) Inter-Netzwerk-Niveau	51
	3. Art der Übermittlung	52
III.	Protokolldateneinheiten: Überblick und Termini	52
C.	Kryptologische Grundlagen	55
I.	Kryptologie: Termini und Aufgaben	55
	1. Termini	55
	2. Aufgaben der Kryptologie	55
II.	Elementares Instrumentarium der Kryptographie	56
	1. Kryptographischer Algorithmus	56
	2. Schlüssel	57
	3. Kryptosystem, Verschlüsselungsverfahren, Algorithmus	57
	4. Symmetrische Algorithmen – Secret-Key-Verfahren	57
	a) Prinzip des symmetrischen Algorithmus	57
	b) Problem des Schlüsselaustausches	58
	5. Asymmetrische Algorithmen – Public-Key-Verfahren	59
	6. Hybride Algorithmen	61
III.	Kryptanalyse	62
	1. Angriffsarten	62
	2. Man-in-the-Middle-Angriff	63
IV.	Public-Key-Infrastrukturen	64
	1. Authentizität des öffentlichen Schlüssels	65
	2. Grundschema einer PKI	65
V.	Digitale Signaturen	66
VI.	Hashfunktionen	67

Zweiter Teil

Informationstechnologische Analyse

D.	Einleitung	69
I.	Erläuterung und Eingrenzung des Untersuchungsgegenstandes	69
	1. Eigenständigkeit und lokaler Ansatzpunkt der Überwachungs- maßnahme	69
	2. Vorgehen ohne Eindringen in das informationstechnische Endgerät	70
	3. Überprüfbarkeit des Vorgehens als methodische Voraussetzung	70
	4. Aktualität der Untersuchung	71
II.	Gang der Analyse	71
E.	Der Zugriff auf den Datenverkehr eines lokalen Funknetzwerks	72
I.	Einführung	72
II.	Der Zugriff auf lokale Funknetzwerke (Wireless LAN)	72
	1. Lokalisieren und Zuordnen des Access Points	73
	a) Grundlagen	73
	aa) Aktives und passives Scannen	74

(1) Service Set Identifier (SSID)	74
(2) Aktives Scannen	74
(3) Passives Scannen	74
bb) Beacon-Frame und Probe-Response-Frame	75
b) Lokalisieren funkbasierter Netzwerke	75
c) Hidden Network	75
d) Zuordnung zum Ziel der Infiltration	77
e) Zusammenfassung: Lokalisieren und Zuordnen des Access Points	78
2. Der Zugang zum (fremden) Wireless LAN	78
a) WLAN ohne Sicherheitsvorkehrungen	79
aa) Authentifizierung und Assoziierung	79
bb) Access Control List	79
cc) Zusammenfassung: WLAN ohne Sicherheitsvorkehrungen	80
b) WEP-verschlüsseltes WLAN	80
aa) Verschlüsselung bei WEP	80
(1) Shared Key	81
(2) WEP-Seed/Gesamtschlüssel (=RC4-Schlüssel)	81
(3) Verschlüsselungsvorgang	81
(4) Versendeter Datenteil bei WEP	81
bb) Authentifizierung und Assoziierung bei WEP	82
(1) Verfahren	82
(2) Fake Authentication	82
cc) Attacks on WEP	83
(1) FMS/KoreK-Method	83
(a) FMS	83
(b) KoreK	84
(2) PTW-Method	84
(a) Klein- bzw. Jenkins-Korrelation	84
(b) Extension to Multiple Key Bytes	84
(3) Schätzung der ersten 16 Bytes des RC4-Schlüsselstroms	85
(4) Umsetzung einer WEP-Attack	86
dd) Zusammenfassung: WEP-verschlüsseltes WLAN	87
c) WPA/WPA2-verschlüsseltes WLAN (Pre-Shared-Key)	87
aa) Verschlüsselung bei WPA/WPA2	88
(1) WPA – Temporary Key Integrity Protocol	88
(2) WPA2 – AES-CCMP	89
bb) Schlüsselmanagement in WPA/WPA2	90
cc) Authentifizierung und Assoziierung bei WPA/WPA2	90
dd) Attacks on WPA/WPA2	91
(1) Brute-Force-Attack	91
(a) Offline-Dictionary-Attack (als Ausprägung der Brute-Force-Attack)	91
(b) Dictionary Files	92
(c) Precomputed Hash Files (Rainbow Tables)	93
(d) Erfolgsaussichten eines Dictionary-Angriffs auf WPA/WPA2	94
(e) Erweiterung: Deauthentication attack	94
(f) Umsetzung der Brute-Force-Attack	95

	(2) Schwachstelle: Vorkonfigurierter WPA/WPA2-Schlüssel (PSK)	95
	(3) Schwachstelle: Wi-Fi Protected Setup (WPS)	96
	(4) Schwachstelle: Router-Remote Management	98
	(5) Sonstige Attacken auf WPA/WPA2	99
	(a) WPA-TKIP	99
	(aa) <i>Beck/Tews</i>	99
	(bb) <i>Beck und Vanhoef/Piessens</i>	100
	(cc) Umsetzung	101
	(b) WPA2	101
	(aa) Hole196 Vulnerability	101
	(bb) KRACK	101
	ee) Zusammenfassung: WPA/WPA2-verschlüsseltes WLAN	102
	d) Evil-Twin-Attack	103
	e) Zusammenfassung: Der Zugang zum (fremden) Wireless LAN	105
	3. Mitschneiden des Datenverkehrs im Wireless LAN	105
	a) Sniffen des unverschlüsselten Netzwerkverkehrs (WLAN ohne Sicherheitsvorkehrungen)	106
	b) Sniffen des WEP-verschlüsselten Netzwerkverkehrs	106
	c) Sniffen des WPA/WPA2-verschlüsselten Netzwerkverkehrs	107
	d) Sniffen am Evil Twin	109
	e) Zusammenfassung: Mitschneiden des Datenverkehrs im Wireless LAN	109
III.	Zusammenfassung: Der Zugriff auf den Datenverkehr	110
	1. Lokalisieren und Zuordnen des Access Points	110
	2. Der Zugang zum (fremden) Wireless LAN	111
	3. Mitschneiden des Datenverkehrs im Wireless LAN	111
F.	(Inhaltliche) Untersuchung des Netzwerkverkehrs	113
I.	Einführung und Eingrenzung	113
II.	Bestimmung des anvisierten Endgerätes	113
III.	Auswerten der Daten und Herausfiltern der Kommunikationsinhalte	114
	1. Methoden des Mitschneidens und Speicherns der Daten	115
	2. Inhaltsdaten und Zugangsdaten	115
	a) Inhaltsdaten	115
	b) Zugangsdaten/Passwörter	115
	3. E-Mails	116
	a) E-Mail-Client	116
	aa) E-Mails versenden: Simple Mail Transfer Protocol	116
	bb) E-Mails empfangen: POP3/IMAP	116
	b) Webmail	116
	4. Soziale Netzwerke/Webforen/Sonstiges HTTP	117
	5. Instant Messaging/Chat	117
IV.	Besonderheit: Verschlüsselung oberhalb der Netzzugangsschicht	118
	1. Verschlüsseltes World Wide Web	119
	a) Transport Layer Security (SSL/TLS)	119
	b) HTTP über eine SSL/TLS-Verbindung (HTTPs)	121
	c) Angriffe auf HTTPs	121
	aa) Ausgangspunkt: Man-in-the-Middle-Angriff	123

(1) Address Resolution Protocol Spoofing	123
(2) Domain Name System Spoofing	124
bb) SSL-Stripping	125
cc) Man-in-the-Middle-Angriff über eigene digitale Zertifikate	126
dd) SSL/TLS-Session-Cookie-Hijacking	129
ee) Schutzmaßnahmen: HSTS und HPKP	131
(1) HTTP Strict Transport Security (HSTS)	131
(a) Funktionsweise von HSTS	131
(b) Schwachstellen und Verbreitung von HSTS	132
(2) HTTP Public Key Pinning (HPKP)	133
ff) Weitere Beispiele für Schwachstellen und Zero-Day-Exploits	134
(1) BEAST	135
(2) POODLE	136
(3) RC4-Verzerrungen	137
gg) Sonstige Angriffe (Spear-Phishing, Brute-Force-Attack) .	138
2. Weitere offene Forschungsfelder beim Einsatz von Verschlüsselung	139
V. Zusammenfassung	140
1. Auswerten der Daten und Herausfiltern der Kommunikationsinhalte	140
2. Verschlüsseltes World Wide Web	140
G. Folgerungen für die nachfolgende rechtliche Analyse	142

Dritter Teil

Rechtliche Analyse

H. Einleitung	149
I. Einführung	149
II. Abgrenzung zu Quellen-TKÜ und Online-Durchsuchung	150
I. Die Überwachung lokaler Funknetzwerke („WLAN-Catching“)	152
I. Überwachung lokaler Funknetzwerke aus technischer Perspektive	152
1. Differenzierende Betrachtungsweise des Vorgangs	152
2. Erläuterung der unterschiedlichen Maßnahmen	155
3. Einheitliche Betrachtungsweise des Vorgangs?	160
II. Überwachung lokaler Funknetzwerke aus rechtlicher Perspektive	162
1. (Kurze) Erläuterung der maßgeblichen Normen	162
a) Maßgebliche Grundrechte	162
aa) Recht auf informationelle Selbstbestimmung, Art. 2 I	
i.V.m. Art. 1 I GG	163
bb) Brief-, Post- und Telekommunikationsgeheimnis, Art.	
10 I GG	163
cc) Gewährleistung der Vertraulichkeit und Integrität infor-	
mationstechnischer Systeme (GVIIS), Art. 2 I i.V.m. Art.	
1 I GG	164
dd) Unverletzlichkeit der Wohnung, Art. 13 I GG	165
b) Maßgebliche strafprozessuale Normen	166
2. Eine (erste) rechtliche Einordnung	167
a) Allgemeines	167

b)	Die Primärmaßnahme: Mitschneiden und Speichern des Datenverkehrs eines lokalen Funknetzwerks (Abhören des WLAN) inkl. Überwachung des Surfverhaltens	169
c)	Sekundärmaßnahmen	171
aa)	Sekundärmaßnahmen I: Maßnahmen ohne Überwindung von Sicherheitsvorkehrungen	172
bb)	Sekundärmaßnahmen II: Maßnahmen zur Überwindung von Sicherheitsvorkehrungen (insb. Verschlüsselung)	173
cc)	Sekundärmaßnahmen III: „Informationstechnologische Täuschungen“ im Rahmen der Überwachung lokaler Funknetzwerke	175
III.	Überwachung lokaler Funknetzwerke in Lit. und Rspr.	175
1.	<i>Jordan</i>	176
2.	<i>Kleih</i>	179
3.	Weitere Erwähnungen	183
4.	Fazit	185
J.	Analyse der einzelnen Kategorien von Ermittlungsmaßnahmen	186
I.	Die Primärmaßnahme	186
1.	Erläuterung der Ermittlungsmaßnahme	186
2.	Verfassungsrechtliche Vorgaben	187
a)	Telekommunikationsgeheimnis, Art. 10 I GG	189
aa)	Reichweite des Schutzbereichs des Telekommunikationsgeheimnisses	189
(1)	Die Übermittlung von Informationen (die Transportkomponente des Telekommunikationsgeheimnisses)	189
(a)	Beginn/Ende/Unterbrechung des Übermittlungsvorganges (Behandlung der beim Provider zwischengespeicherten E-Mails)	190
(b)	Übertragung der Vorgaben auf Daten in lokalen Funknetzwerken (Netzbetreiberlose Telekommunikation)	192
(aa)	Technologische Aspekte	192
(bb)	Rechtliche Aspekte	192
(2)	Die Überwachung des gesamten Surfverhaltens (die Kommunikationskomponente des Telekommunikationsgeheimnisses)	194
(a)	Die Kommunikationskomponente in der Definition des <i>BVerfG</i>	195
(b)	Abgrenzung von Individual- und Massenkommunikation	196
(aa)	Subjektives Kriterium	196
(bb)	Objektives Kriterium	196
(cc)	Beschränkung auf klassische, interpersonale Kommunikation?	196
(c)	Potentielle Betroffenheit von interpersonaler Kommunikation	199
(d)	Nichtannahmebeschluss des <i>BVerfG</i>	199

(e) Drohender Wertungswiderspruch	200
(3) Zusammenfassung: Reichweite des Schutzbereichs des Telekommunikationsgeheimnisses	201
bb) Eingriff in das Telekommunikationsgeheimnis	202
b) Gewährleistung der Vertraulichkeit und Integrität informati- onstechnischer Systeme, Art. 2 I i.V.m. Art. 1 I GG	202
aa) Lokale Funknetzwerke als IT-Systeme	203
(1) Netzwerkkomponenten als informationstechnisches System	203
(2) Rechnernetze als informationstechnisches System	204
bb) Zwei Schutzrichtungen und Eingriffe in das GVliS	205
cc) Abgrenzung von GVliS zu Art. 10 I GG	205
(1) „Laufender Telekommunikationsvorgang“	206
(2) Nutzung der gesamten Bandbreite des Internet- Netzwerks als „laufende Telekommunikation“?	207
dd) Zusammenfassung: Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 I i.V.m. Art. 1 I GG	209
c) Unverletzlichkeit der Wohnung, Art. 13 I GG	209
d) Recht auf informationelle Selbstbestimmung, Art. 2 I i.V.m. Art. 1 I GG	212
e) Zusammenfassung: Verfassungsrechtliche Vorgaben	212
3. Strafprozessuale Zulässigkeit der Primärmaßnahme	214
a) Anwendbarkeit der §§ 94 ff. StPO?	215
aa) Daten als Gegenstände	215
bb) Behandlung der beim Provider zwischengespeicherten E-Mails in der Rechtsprechung des <i>BVerfG</i>	217
cc) Übertragung der Vorgaben auf andere Daten und diffe- rente Übertragungsphasen?	218
b) Anwendbarkeit von § 102 StPO?	218
c) Anwendbarkeit von § 110 III StPO?	218
d) Anwendbarkeit der §§ 99, 100 StPO?	219
aa) Behandlung der beim Provider zwischengespeicherten E-Mails in der Rechtsprechung durch das <i>BVerfG</i> und den <i>BGH</i>	220
bb) Übertragung der Vorgaben auf andere Kommunika- tionenanwendungen?	222
cc) Bewertung der von der Rechtsprechung entwickelten Ergebnisse	222
dd) Übertragung der Vorgaben auf Daten in lokalen Netzwerken? (1) Gewahrsam des Providers an den Daten im lokalen Netzwerk?	224
(2) Daten im lokalen Netzwerk als dynamischer Vorgang	225
e) Anwendbarkeit von § 100a I S. 1 StPO?	226
aa) „Telekommunikation“ i.S.v. § 100a I S. 1 StPO	227
(1) Definition von „Telekommunikation“?	227
(2) Definition des Bundesgerichtshofs	228

(3)	„Genuin strafverfahrensrechtliche Begriffsbestimmung“ – Beschränkung auf zwischenmenschliche (interpersonale) Kommunikation?	229
(a)	Einschränkende Auslegung in der Literatur	229
(b)	Weites Verständnis in der Literatur	231
(c)	Rechtsprechung	231
(4)	Schlussfolgerung unter Orientierung am grundrechtlichen Schutz durch Art. 10 GG	232
(5)	„Telekommunikation“ und das Abhören des WLAN (WLAN-Catching)	233
(a)	Betroffenheit des gesamten Surfverhaltens	234
(b)	Übertragungsweg beendet/noch nicht begonnen?	235
(c)	Betroffenheit von Datenpaketen, die nur innerhalb des lokalen Netzwerks zirkulieren	237
bb)	„Überwacht und aufgezeichnet“	238
(1)	Zulässigkeit der selbständigen Durchführung einer Überwachungsmaßnahme durch die Strafverfolgungsbehörden im Rahmen von § 100a I S. 1 StPO	238
(2)	„Überwacht und aufgezeichnet“	240
cc)	„Auch ohne Wissen“	240
dd)	„Betroffene“	240
ee)	Sonstige Anordnungsvoraussetzungen von § 100a I S. 1 StPO	242
ff)	Zusammenfassung: Anwendbarkeit von § 100a I S. 1 StPO für das Mitschneiden und Speichern des Datenverkehrs eines lokalen Netzwerks (Abhören des WLAN) inkl. Überwachung des Surfverhaltens	243
f)	Anwendbarkeit von § 100a I S. 2 StPO?	244
aa)	Strafprozessuale Begriffsbestimmung des Merkmals „in informationstechnische Systeme eingegriffen“	245
bb)	Ergänzende Anhaltspunkte aus dem Verfassungsrecht?	247
cc)	Ergänzende Anhaltspunkte durch die Begriffsbestimmung in § 201 II BKAG?	248
dd)	Übertragung auf die Primärmaßnahme	248
g)	Anwendbarkeit von § 100a I S. 3 StPO?	249
h)	Anwendbarkeit von § 100b I StPO?	250
4.	Exklusive Wahrnehmung von WLAN-Verkehrsdaten	250
a)	Technologische Einzelheiten	250
b)	Rechtliche Einordnung	252
aa)	Erhebung <i>zusätzlich</i> zu der inhaltlichen Wahrnehmung nach § 100a I S. 1 StPO	252
bb)	Separate Erhebung <i>anstelle</i> der inhaltlichen Wahrnehmung	253
(1)	Verfassungsrechtliche Vorgaben	253
(2)	Strafprozessuale Zulässigkeit	254
(a)	Strafprozessuale Zulässigkeit der selbständigen Erhebung von Verkehrsdaten	254
(b)	Erhebung nicht beim Erbringer öffentlich zugänglicher Telekommunikationsdienste, § 100g V StPO	254

	(c) Kategorien von Verkehrsdaten, § 100g I - III StPO	255
5.	Zusammenfassung: Zulässigkeit des Mitschneidens und Speicherns des Datenverkehrs eines lokalen Funknetzwerks (Abhören des WLAN) inkl. Überwachung des Surfverhaltens	257
II.	Sekundärmaßnahmen	259
1.	Sekundärmaßnahmen I: Maßnahmen ohne Überwindung von Sicherheitsvorkehrungen	259
	a) Erläuterung der Ermittlungsmaßnahmen	259
	b) WLAN lokalisieren und zuordnen; Ermittlung der MAC-Adresse des Access Points	260
	aa) Technologische Einzelheiten	260
	bb) Rechtliche Einordnung	261
	(1) Verfassungsrechtliche Vorgaben	261
	(2) Strafprozessuale Zulässigkeit	263
	c) Maschine-zu-Maschine-Kommunikation: Ermittlung der MAC-Adressen der assoziierten Endgeräte mittels passiver Scanner; Hidden Networks	263
	aa) Technologische Einzelheiten	263
	bb) Rechtliche Einordnung	264
	(1) Verfassungsrechtliche Vorgaben	264
	(2) Strafprozessuale Zulässigkeit	266
	(a) § 100i StPO?	266
	(b) Ermittlungsgeneralklausel gem. §§ 161, 163 StPO?	267
	d) Das Senden von Datenpaketen an den Access Point: Verwendung aktiver Scanner; Einloggen in offenes WLAN	268
	aa) Technologische Einzelheiten	268
	bb) Rechtliche Einordnung	269
	(1) Verfassungsrechtliche Vorgaben	269
	(2) Strafprozessuale Zulässigkeit	272
	e) Zusammenfassung: Sekundärmaßnahmen I: Maßnahmen ohne Überwindung von Sicherheitsvorkehrungen	272
2.	Sekundärmaßnahmen II: Maßnahmen zur Überwindung von Sicherheitsvorkehrungen (insb. Verschlüsselung)	273
	a) Erläuterung der Ermittlungsmaßnahmen	273
	b) Technologische Einzelheiten	274
	c) Alleiniges Überwinden von Sicherheitsvorkehrungen von Telekommunikation (das „Knacken“ von Verschlüsselung)	276
	aa) Verfassungsrechtliche Vorgaben	277
	bb) Strafprozessuale Zulässigkeit	279
	(1) Überwinden der Verschlüsselung von Telekommunikation als „Überwachen und Aufzeichnen“ i.S.v. § 100a I S. 1 StPO?	279
	(2) Überwinden der Verschlüsselung von Telekommunikation als Annexkompetenz zu § 100a I S. 1 StPO?	281
	d) Eingriffe in den Datenverkehr einer Netzwerkinfrastruktur zur Überwindung von Sicherheitsvorkehrungen	285
	aa) Verfassungsrechtliche Vorgaben	285
	(1) Telekommunikationsgeheimnis, Art. 10 I GG	285

(2)	GVIIS und Abgrenzung zum Telekommunikations- geheimnis	287
(3)	Sonstige Grundrechte	289
bb)	Strafprozessuale Zulässigkeit	289
(1)	Anwendbarkeit von § 100a I S. 1 StPO?	290
(2)	Anwendbarkeit von § 100a I S. 2 StPO?	291
(a)	„Die Überwachung und Aufzeichnung der Tele- kommunikation darf auch in der Weise erfolgen“	292
(b)	„Eingreifen in informationstechnische Systeme“	292
(c)	„Mit technischen Mitteln“	293
(d)	„Von dem Betroffenen genutzte“ (informati- onstechnische Systeme)	294
(e)	„Wenn dies notwendig ist, um die Überwa- chung und Aufzeichnung insbesondere in un- verschlüsselter Form zu ermöglichen“	294
(f)	Voraussetzungen des § 100a V und VI StPO	295
(g)	Schlussfolgerung	296
(3)	Anwendbarkeit von § 100a I S. 3 StPO?	296
(4)	Anwendbarkeit von § 100b I StPO?	296
(a)	„Eingreifen in ein informationstechnisches System“	297
(b)	„Erheben von Daten aus dem informations- technischen System“	298
(c)	Verhältnis von § 100b StPO zu § 100a StPO?	299
(d)	Schlussfolgerung	301
e)	Maßnahmen mit Auswirkungen auf IT-Endgeräte (aber ohne Infiltration) zur Überwindung von Sicherheitsvorkehrungen	301
aa)	Verfassungsrechtliche Vorgaben	301
(1)	Aussagen des <i>BVerfG</i>	302
(a)	Urteil zum „IMSI-Catcher“	302
(b)	Urteil zum NWVerfSchG	302
(c)	Urteil zu den neuen Befugnissen im BKAG	305
(d)	Schlussfolgerung	308
(2)	Übertragung auf die WLAN-Überwachungsmaßnahme mit Auswirkungen auf IT-Endgeräte (aber ohne Infiltration)	308
(a)	Ausschließlich punktuelle Veränderung am IT- System	308
(b)	Ausschließliche Betroffenheit von Daten mit Bezug zu einer laufenden Telekommunikation	310
(3)	Schlussfolgerung	310
bb)	Strafprozessuale Zulässigkeit	311
(1)	Anwendbarkeit von § 100a I S. 1 StPO?	311
(2)	Anwendbarkeit von § 100a I S. 2 StPO?	312
(a)	Auswirkungen der verfassungsrechtlichen Vor- gaben auf § 100a I S. 2 StPO	312
(b)	Notwendigkeit einer verfassungskonformen Auslegung von § 100a I S. 2 StPO?	313
(c)	Übertragung auf Maßnahmen mit Auswirkun- gen auf IT-Endgeräte	314

(3)	Anwendbarkeit von § 100a I S. 3 StPO?	314
(4)	Anwendbarkeit von § 100b I StPO?	314
(a)	„Eingreifen in ein informationstechnisches System“	315
(b)	„Erheben von Daten aus dem informations- technischen System“	315
(c)	Weitere Merkmale	316
(d)	Sonstige Anordnungsvoraussetzungen von § 100b StPO	317
(e)	Schlussfolgerung	318
f)	Zusammenfassung: Sekundärmaßnahmen II: Maßnahmen zur Überwindung von Sicherheitsvorkehrungen	318
3.	Sekundärmaßnahmen III: „Informationstechnologische Täuschungen“ im Rahmen der Überwachung lokaler Funknetzwerke	320
a)	Erläuterung der Ermittlungsmaßnahme	320
b)	Verfassungsrechtliche Vorgaben	321
aa)	Telekommunikationsgeheimnis, Art. 10 I GG	322
bb)	Recht auf informationelle Selbstbestimmung, Art. 2 I i.V.m. Art. 1 I GG	324
(1)	Staatliche Identitätstäuschungen	324
(2)	Übertragung auf „informationstechnologische Täuschungen“ im Rahmen der Überwachung lokaler Funknetzwerke	325
cc)	Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Art. 2 I i.V.m. Art. 1 I GG	327
dd)	Konkurrenzverhältnis von GVIiS und Recht auf infor- mationelle Selbstbestimmung	329
ee)	Schlussfolgerung	331
c)	Strafprozessuale Zulässigkeit	332
aa)	Anwendbarkeit von § 100b I StPO?	333
(1)	„Eingreifen in ein informationstechnisches System“	333
(2)	„Erheben von Daten aus dem informationstechni- schen System“	334
(3)	Weitere Merkmale	334
(4)	Sonstige Anordnungsvoraussetzungen von § 100b StPO	335
d)	Zusammenfassung: Sekundärmaßnahmen III: „Informations- technologische Täuschungen“ im Rahmen der Überwachung lokaler Funknetzwerke	336
4.	Zusammenfassung: Sekundärmaßnahmen	336

Vierter Teil

Ergebnisse und Zusammenfassung

K.	Kernaussagen des Buches	339
L.	Ergebnisse der informationstechnologischen Analyse	341
M.	Zusammenfassung der rechtlichen Analyse	345

I.	Zulässigkeit der Primärmaßnahme	346
1.	Verfassungsrechtliche Vorgaben	346
2.	Strafprozessuale Zulässigkeit	347
II.	Zulässigkeit der Sekundärmaßnahmen I	348
III.	Zulässigkeit der Sekundärmaßnahmen II	349
IV.	Zulässigkeit der Sekundärmaßnahmen III	350
N.	Schlussfolgerung und theseartiger Überblick	352
I.	Schlussfolgerung für durchgeführte Maßnahmen des „WLAN-Catchings“ vor dem 24.08.2017	352
II.	Theseartiger Überblick	353
Anhang A	Einzelheiten zu der informationstechnologischen Untersuchung und Umsetzung	355
I.	Der Zugriff auf den Datenverkehr eines (fremden) lokalen Netzwerks	355
1.	Lokalisieren und Zuordnen des Access Points	355
a)	Abbildung eines Beacon-Frames und Probe-Response-Frames	355
b)	Beacon- und Probe-Response-Frame bei einem Hidden Network	355
2.	Der Zugang zum (fremden) Wireless LAN	356
a)	WEP-verschlüsseltes WLAN	356
aa)	Versendeter Datenteil bei WEP mit unverschlüsseltem Initialisierungsvektor	356
bb)	Einzelheiten zu den Angriffen auf WEP	356
(1)	<i>Fluhrer/Mantin/Shamir</i>	356
(2)	<i>KoreK</i>	359
(3)	Umsetzung einer WEP-Attack	359
b)	WPA/WPA2 (PSK)-verschlüsseltes WLAN	361
aa)	WPA mit Temporary Key Integrity Protocol	361
(1)	RC4-Schlüsselgenerierung (per Frame) in TKIP	361
(2)	(Weitere) Auswirkungen der neuen Schlüsselgene- rierung	361
bb)	WPA2 mit AES-CCMP	361
(1)	AES-Counter Mode	361
(2)	CBC-MAC	362
cc)	Einzelheiten zum Schlüsselmanagement	362
dd)	Einzelheiten zur Authentifizierung und Assoziierung bei WPA/WPA2	363
ee)	Attacks on WPA/WPA2	364
(1)	Brute-Force-Attack	364
(a)	Funktionsweise der Brute-Force-Attack	364
(b)	Erstellen eigener Dictionary Files und Rainbow Tables	365
(c)	Umsetzung der Brute-Force-Attack	365
(2)	Realisierung einer Evil-Twin-Attack	368
II.	(Inhaltliche) Untersuchung des Netzwerkverkehrs	371
1.	Auswerten der Daten und Herausfiltern der Kommunikationsinhalte	371
a)	Tools	371
aa)	Wireshark	371

	bb) Dsniff	371
	b) E-Mails	372
	aa) E-Mails versenden per Simple Mail Transfer Protocol	372
	bb) E-Mails empfangen: POP3/IMAP	372
	cc) Verschlüsseltes World Wide Web	372
	(1) Einzelheiten zur Funktionsweise von SSL/TLS	372
Anhang B	Detailinformationen zur Arbeitsweise des Internet-Netzwerks	378
I.	Details zu den einzelnen Schichten des TCP/IP-Referenzmodells	378
1.	Anwendungsschicht	378
a)	SMTP als Beispielprotokoll	378
aa)	Grundlegendes	378
bb)	Kontaktaufnahme	378
2.	Transportschicht	380
a)	TCP als Beispielprotokoll	380
aa)	Grundlegendes	380
bb)	Verbindungsorientierung	380
3.	Internetschicht	382
a)	IP(v4) als Beispielprotokoll	382
aa)	Grundlegendes	382
bb)	Adressierung	382
	(1) IP-Adressen	383
	(2) Network Address Translation	384
cc)	Routing und Weiterleitung	385
dd)	Fragmentierung	386
4.	Netzzugangsschicht (Sicherungs-/Bitübertragungsschicht)	386
a)	Ethernet als Beispielprotokoll der Netzzugangsschicht	386
aa)	Grundlegendes	387
bb)	Adressierung	387
b)	IEEE 802.11 (WLAN) als Beispielprotokoll der Netzzugangsschicht	388
aa)	Die IEEE 802.11-Protokollfamilie	388
bb)	Medienzugriff	388
cc)	WPA2-Personal (PSK) vs. WPA2-Enterprise (802.1X)	389
	(1) Authentifizierung	389
	(2) Verschlüsselung	390
II.	Aufbau einzelner Protokolldateneinheiten	390
1.	Überblick	390
2.	Aufbau einer Nachricht am Beispiel von SMTP	391
3.	Aufbau eines Segments am Beispiel von TCP	393
4.	Aufbau eines Datagramms am Beispiel von IPv4	394
5.	Aufbau eines Frames am Beispiel von Ethernet	396
6.	Aufbau eines Frames am Beispiel des 802.11-Protokolls	398
Anhang C	Kryptologischer Hintergrund	400
I.	Kryptographische Algorithmen	400
1.	Symmetrische Algorithmen	400

a) Einführung	400
aa) Permutation und Substitution	400
bb) Blockchiffren vs. Stromchiffren	401
cc) Produktchiffren/Substitutions-Permutationschiffren	402
dd) Vernam-Chiffre/One-Time-Pad	402
b) Ausgewählte Blockchiffren	403
aa) Feistel-Chiffre	403
bb) Data Encryption Standard (DES)	405
(1) Überblick über die Funktionsweise von DES	405
(2) Die Erzeugung der Rundenschlüssel	407
(3) Eine Runde des DES-Algorithmus	408
(a) Die Rundenfunktion f	408
(aa) Expansionspermutation und XOR-Verknüpfung	408
(bb) S-Box-Substitution	410
(cc) P-Box-Permutation	412
(b) Verbindung von linker und rechter Hälfte	412
(4) Die weiteren Teilschritte	412
(a) Anfangspermutation	412
(b) Schlusspermutation	413
(5) Entschlüsselung mit DES	413
(6) Sicherheit von DES	413
(7) Triple-DES	414
cc) Advanced Encryption Standard (AES)	415
(1) Einordnung von AES	415
(2) Überblick über die Funktionsweise von AES	415
(3) Eine Runde des AES-Algorithmus	416
(a) Die Rundenfunktion f	418
(aa) Der endliche Körper $GF(2^8)$	418
(bb) Polynome	419
(cc) Byte-Substitution (SubBytes-Operation)	420
(dd) Zeilenverschiebung (ShiftRows-Operation)	421
(ee) Spaltentransformation (MixColumns-Op.)	422
(b) XOR-Verknüpfung mit Rundenschlüssel (Key-Addition)	423
(4) Erzeugung der Rundenschlüssel (Schlüssellexpansion)	423
(5) Entschlüsselung mit AES	424
(6) Sicherheit von AES	425
dd) International Data Encryption Algorithm (IDEA)	425
c) Betriebsmodi der Blockchiffren	426
aa) ECB-Mode	426
bb) CBC-Mode	427
cc) CTR-Mode	427
dd) CFB-Mode	428
ee) OFB-Mode	428
d) Ausgewählte Stromchiffren	429
aa) Allgemeines Prinzip von Stromchiffren	429
bb) RC4/Arcfour	430
(1) Überblick über die Funktionsweise von RC4	431

(2) KSA-Algorithmus	431
(a) Die einzelnen Schritte des Algorithmus	431
(b) Beispielrechnung (KSA)	432
(3) PRGA-Algorithmus	433
(a) Die einzelnen Schritte des Algorithmus	433
(b) Beispielrechnung	434
(4) Entschlüsselung	435
(5) Sicherheit von RC4	436
cc) Weitere Stromchiffren	436
2. Asymmetrische Algorithmen	437
a) Einführung in die Public-Key-Kryptographie	437
aa) Einwegfunktion	437
bb) Trapdoor-Einwegfunktion	438
cc) Mathematische Umsetzung	438
(1) Faktorisierung (großer Zahlen)	438
(2) Diskreter Logarithmus	439
b) Der RSA-Algorithmus	439
aa) Das zugrunde liegende Prinzip	440
bb) Mathematische Umsetzung des Prinzips	441
cc) Vorüberlegungen	443
(1) Größenordnung der Zahlen	443
(2) Voraussetzungen	444
(3) Vorbereitung und Umwandlung des Klartextes	444
(4) Ausgabe des Geheimtextes als darstellbarer Text	446
(5) „Berechnung“ der Primzahlen	447
dd) Die einzelnen Schritte des Algorithmus	448
ee) Beispiel eines RSA-Verschlüsselungsvorganges	450
ff) Sicherheitsprinzip von RSA	457
(1) Berechnen des geheimen Schüssels	457
(2) Entschlüsseln ohne geheimen Schlüssel durch In-	
vertieren	458
(3) Randomisierung	459
c) Diffie-Hellman-Schlüsselvereinbarung	459
aa) Das zugrunde liegende Prinzip	459
bb) Parameterauswahl	461
(1) Primzahl p	461
(2) Basis g	461
(3) Geheimer Exponent x	462
cc) Die einzelnen Schritte des Algorithmus	462
dd) Beispielrechnung	463
ee) Mathematische Umsetzung des Prinzips	464
ff) Sicherheitsprinzip von Diffie-Hellman	465
(1) Diskreter Logarithmus	465
(2) Rückschluss auf den Schlüssel direkt	466
gg) Mehrpersonen	466
d) Elgamal-Algorithmus	467
aa) Das zugrunde liegende Prinzip	467
bb) Die einzelnen Schritte des Algorithmus	468
cc) Beispielrechnung	469

	dd) Mathematische Umsetzung des Prinzips	473
	ee) Sicherheitsprinzip von Elgamal	474
II.	Public-Key-Infrastrukturen	474
	1. Elemente einer PKI	474
	a) Digitale Zertifikate	474
	b) Certification Authority (CA)	474
	c) Root-CA	475
	d) Registration Authority (RA)	475
	e) Directory Service	475
	f) Certificate Revocation List	476
	2. Vertrauensmodelle	476
	a) Direct Trust	476
	b) Web of Trust	476
	c) Hierarchical Trust	477
	aa) Einstufige Hierarchie	477
	bb) Mehrstufige Hierarchie	477
	cc) Cross-Zertifizierung	478
	3. Lösung des Man-in-the-Middle-Problems durch eine PKI?	480
III.	Digitale Signaturen	480
	1. RSA als Signaturverfahren	482
	2. Elgamal-Signaturverfahren	482
	a) Die einzelnen Schritte des Signaturverfahrens	483
	b) Sicherheit des Elgamal-Signaturverfahrens	484
	3. Digital Signature Algorithm (DSA)	484
	a) Die einzelnen Schritte von DSA	486
	b) Sicherheit des Elgamal-Signaturverfahrens	486
IV.	Kryptologische Hashfunktionen	486
	1. Überblick über die Funktionsweise von Hashfunktionen	487
	2. Allgemeine Sicherheitsaspekte von Hashfunktionen	488
	3. Wichtige (eigenständige) Hashfunktionen	488
	a) MD5	488
	b) SHA-Familie	489
	c) RIPEMD-160	489
	4. Message Authentication Codes (MAC)	489
Anhang D	Mathematische Grundlagen und Zeichenkodierung	491
I.	Mathematische Grundlagen	491
	1. Natürliche und ganze Zahlen	492
	2. Gruppen und Körper	492
	a) Gruppen	493
	b) Ringe	493
	c) Körper	494
	3. Die multiplikative Inverse	494
	4. Teilbarkeit und Primzahlen	494
	a) Teiler	495
	b) Größter gemeinsamer Teiler	495
	c) Die Euler'sche ϕ -Funktion	495
	d) Primzahlen	495

e) Die Euler'sche ϕ -Funktion und Primzahlen	496
f) Primfaktorzerlegung	496
5. Modulare Arithmetik	497
a) Division mit Rest	497
b) Kongruenzen	498
c) Restklassen, Restklassengruppe, Restklassenring	499
d) Euklidischer Algorithmus	500
e) Vielfachsummandarstellung	501
aa) Erweiterter euklidischer Algorithmus	502
bb) Die multiplikative Inverse modulo einer Zahl	502
6. Der kleine Fermat und der Satz von Euler-Fermat	504
a) Der kleine Satz von Fermat	504
b) Der Satz von Euler-Fermat	504
7. Berechnung großer Potenzen	505
a) Square-and-Multiply-Algorithmus	505
aa) Allgemein	505
bb) Modulo-Rechnung	505
b) Binäre Modulo-Exponentiation	506
8. Exklusives Oder bzw. XOR-Verknüpfung	507
II. Zeichenkodierung	508
Quellen im World Wide Web	510
Zitierte Entscheidungen	523
Literaturverzeichnis	525
Stichwortregister	537