

Cyberspionage

Wie Nachrichtendienste um Informationen
und Kontrolle kämpfen

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhalt

Geleitwort	13
1 Von Spionen und Hackern	15
1.1 Das Geheimnis dieses Buchs	16
1.2 Worüber reden wir eigentlich?	17
1.2.1 Begriffe und Definitionen	17
1.2.2 Nachrichtendienste und Geheimdienste	24
1.2.3 Cyberspionage vs. Cyberkriminalität	30
1.3 Der Geheimdienstzyklus	33
1.4 Deutschland, deine Nachrichtendienste	35
1.4.1 Bundesnachrichtendienst (BND)	36
1.4.2 Bundesamt für Verfassungsschutz (BfV)	38
1.4.3 Bundesamt für den Militärischen Abschirmdienst (MAD)	40
1.5 Wie wird man (in Deutschland) Spion bzw. Spionin?	41
1.5.1 Personal und Bewerbungsprozess	42
1.5.2 Der Karrierepfad	43
1.5.3 Eine Frage des Geldes	43
1.5.4 Low-Level-Agenten	50
1.6 Geheimdienste weltweit	55
1.7 Die Abhängigkeit deutscher Nachrichtendienste	58
1.7.1 Digitale Souveränität der Sicherheitsarchitektur	59
1.7.2 Abfluss von Daten durch Cloud-Nutzung und KI-Modelle	61
1.8 Spionagetechniken	63
2 Die Rechte der Spione	65
2.1 Geheimhaltungsgrade	65
2.2 Achtung, Sicherheitsüberprüfung!	66
2.2.1 Einfache Sicherheitsüberprüfung (Ü1) nach § 8 SÜG	67
2.2.2 Erweiterte Sicherheitsüberprüfung (Ü2) nach § 9 SÜG	68
2.2.3 Erweiterte Sicherheitsüberprüfung mit Sicherheits- ermittlungen (Ü3) nach § 10 SÜG	69
2.2.4 Die Staatenliste	69

2.3	Deutschlands Cybersicherheitsarchitektur	71
2.3.1	Bundesamt für Sicherheit in der Informationstechnik (BSI)	72
2.3.2	Bundesministerium des Innern	72
2.3.3	Bundesministerium der Verteidigung	72
2.3.4	Bundeskanzleramt	73
2.3.5	Bundeskriminalamt	73
2.3.6	ZITis	73
2.3.7	Der Nationale Sicherheitsrat (NSR)	73
2.4	Das Traffic Light Protocol (TLP)	74
2.5	Das Artikel 10-Gesetz	75
2.6	Whistleblowing	78
2.6.1	Transparenz erzwingen und Missstände aufdecken	79
2.6.2	Geheimnisverrat	82
2.6.3	Das Hinweisgeberschutzgesetz (HinSchG)	83
2.6.4	Helden oder Verbrecher?	85
2.7	Das nachrichtendienstliche Informationssystem (NADIS)	88
2.7.1	Kritik an NADIS	89
2.7.2	Auskunftsrecht	90
2.8	Was droht einem Spion?	91
2.8.1	Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht (§ 353b StGB)	92
2.8.2	Landesverrat (§ 94 StGB)	93
2.8.3	Geheimdienstliche Agententätigkeit (§ 99 StGB)	93
2.8.4	Agententätigkeit zu Sabotagezwecken (§ 87 StGB)	94
2.8.5	Preisgabe von Staatsgeheimnissen (§§ 97 StGB)	95
3	Sicherheit vs. Freiheit	97
3.1	Der gläserne Bürger, der nichts zu verbergen hat	98
3.1.1	Der Wert von Informationen	100
3.1.2	Informationen monetarisieren	101
3.1.3	Palantir: Datenanalyse für Nachrichtendienste	103
3.2	Informationelle Selbstbestimmung und ihre Einschränkung	106
3.2.1	Ein kurzer Ausflug in die Kryptografie	107
3.2.2	Klarnamenpflicht: Anonym im Internet?	110
3.2.3	Vorratsdatenspeicherung: Analyse von Metadaten	113
3.2.4	Chatkontrolle: Inhalte über die Hintertür auswerten	117
3.2.5	Hacking durch Geheimdienste	121
3.2.6	Digitales Zentralbankgeld (CBDC)	129

4	Malware als digitale Waffe	135
4.1	Eine kurze Geschichte der Malware	136
4.2	Malware als Kriegswaffe? Das Kriegswaffenkontrollgesetz	142
4.3	Trojaner	144
4.3.1	Ablauf einer Trojaner-Infektion	145
4.3.2	Was leistet ein Trojaner?	146
4.3.3	Geld, Sabotage oder Spionage?	148
4.3.4	Staatstrojaner	150
4.3.5	Pegasus	153
4.4	Wie kommt man auf solche Namen?	155
5	Staatliche Akteure	159
5.1	Hybride Bedrohungen	160
5.2	Der Cyber- und Informationskrieg	164
5.3	Advanced Persistent Threats (APTs)	165
5.4	China	168
5.4.1	Operation »Titan Rain«	168
5.4.2	Comment Panda (APT1)	169
5.4.3	Gothic Panda (APT3)	170
5.4.4	Stone Panda (APT10)	170
5.4.5	Deep Panda (APT19)	171
5.4.6	Wicked Panda (APT41)	171
5.4.7	Angriff auf Tiefseekabel	171
5.5	Russland	174
5.5.1	Fancy Bear (APT28)	174
5.5.2	Cozy Bear (APT29)	175
5.5.3	Sandworm (APT44)	176
5.5.4	NoName057(16)	177
5.5.5	Cyberangriff auf Estland	180
5.5.6	Cyberangriff auf die Ukraine	180
5.5.7	Gegenangriffe der Ukraine auf Russland	181
5.5.8	Moonlight Maze	183
5.5.9	Jan Marsalek – ein russischer Spion?	184
5.6	Iran	187
5.6.1	Elfin/Refined Kitten (APT33)	187
5.6.2	Shamoon	187
5.6.3	OilRig (APT34)	188

5.7	Nordkorea	189
5.7.1	Büro 121	189
5.7.2	ScarCruft (APT37)	191
5.7.3	Lazarus Group (APT38)	192
5.7.4	Kimsuky (APT43)	193
5.7.5	Infiltration durch nordkoreanische Remote-Worker	195
5.7.6	Cyberkriminalität als staatliches Geschäftsmodell	197
5.8	USA	198
5.8.1	Crypto AG	199
5.8.2	Stuxnet	200
5.8.3	Equation Group	201
5.8.4	XKeyscore	202
5.8.5	Flame	203
5.8.6	Vault 7	204
5.9	Israel	206
5.9.1	IDF, Mossad und Shin Bet	206
5.9.2	Predatory Sparrow	208
5.10	APT-Gruppen, die Deutschland angreifen	209
5.11	Wahlmanipulation durch Influence Operations (IO)	211
5.11.1	Die Cyber-Kill-Chain	211
5.11.2	Die Cyber-Kill-Chain für Influence Operations	213
6	Attribution – wer war es wirklich?	217
6.1	Attributionstechniken und Attributionsebenen	218
6.1.1	Attributionsverfahren – der Ablauf	218
6.1.2	Attributionstechniken und -ebenen	220
6.1.3	Das Angriffsziel gibt Hinweise auf den Angreifer	221
6.2	Klassifizierung von Angreifern	223
6.3	Der Attributionsprozess	224
6.4	Indicators of Compromise (IoC)	227
6.5	MITRE ATT&CK	230
6.6	Zeitonenanalyse	234
6.7	Technische Attributionsfehler	240
6.7.1	Hinweise, aber noch keine Beweise	242
6.7.2	Vorsicht vor allzu schnellen Schlüssen	243
6.8	Das Attributionsparadoxon	244

7	OSINT – Die Macht der frei zugänglichen Informationen	247
7.1	Was ist OSINT?	248
7.2	Wer nutzt OSINT?	250
7.3	OpSec – oder wie man durch Werbung und Postsendungen Agenten enttarnt	251
7.3.1	Was Sie alles unbewusst von sich preisgeben	254
7.3.2	Dokumente richtig schwärzen	256
7.3.3	Metadaten entfernen	258
7.4	Informationen und Daten finden	260
7.4.1	So googeln Sie richtig!	260
7.4.2	Google-Alerts	265
7.4.3	Auf Job-Portalen findet man nicht nur Jobs	268
7.4.4	Mit der Wayback-Machine in die Vergangenheit reisen	270
7.5	Auslandsaufklärung	271
7.5.1	Mit Shodan die Welt durchsuchen	271
7.5.2	Die Stimme Nordkoreas	279
7.5.3	Wardriving mit WiGLE	282
7.5.4	Flugzeuge und Schiffe tracken	285
7.5.5	Spionage aus der Vogelperspektive	290
7.6	Personen aufspüren	293
7.6.1	Personen-Suchmaschinen	296
7.6.2	Strafverfolgung und Überwachungssysteme	298
7.7	Operation Searchlight	299
7.8	Operation TWILIGHT	314
8	HUMINT – Menschliche Quellen im digitalen Raum	315
8.1	Insider-Bedrohungen	315
8.1.1	Agenten und Spione: Ein kurzer Blick in die Geschichte	316
8.1.2	Wie schützt man sich vor sich selbst?	318
8.1.3	»Identity is the new perimeter«	319
8.1.4	Sicherheitsrisiken ohne böse Absichten	320
8.2	Techniken, Taktiken und Angriffsvektoren im Social Engineering	321
8.2.1	Angriff auf die menschliche Psyche	322
8.2.2	Manipulationstechniken bei Cyberangriffen	326

8.2.3	Wenn die Venus-Falle zuschnappt	331
8.2.4	Elicitation: Lass die Zielperson reden	335
8.3	Virtual Human Intelligence (V-HUMINT)	340
8.3.1	Vom toten Briefkasten zum Dead Drop	342
8.3.2	Vertrauen, Kontrolle und Persistenz	349
8.4	Fazit	352
9	SIGINT – Signale abfangen	353
9.1	IMSI-Catcher	353
9.1.1	Wie funktioniert ein IMSI-Catcher?	354
9.1.2	Bestandteile eines IMSI-Catchers	355
9.1.3	Wer verwendet IMSI-Catcher?	356
9.1.4	IMSI-Catcher erkennen	356
9.2	Signaling System 7	357
9.2.1	Wie funktioniert SS7?	357
9.2.2	SS7 ausnutzen	358
9.2.3	Sicherheitsproblem und Reformbedarf	358
9.3	Zahlensender	359
9.3.1	Wie funktioniert ein Zahlensender?	359
9.3.2	Ein Beispiel: The Buzzer	360
9.3.3	Klassen von Zahlensendern	361
10	Game of Drones	365
10.1	Was leisten Drohnen?	365
10.2	Billige Flugzeuge oder teure Kugeln?	367
10.3	Drohnen als Aufklärungswerkzeug	369
10.4	Kamikaze-Drohnen vs. klassische Luftverteidigung	371
10.5	Abwehrmaßnahmen	372
10.6	Drohnenforensik	374
10.6.1	Drohnen analysieren und verstehen	374
10.6.2	Drohnenforensik im Ukraine-Krieg	376
10.7	Glasfaserdrohnen	376
10.8	Interview mit dem Drohnen-Experten Mikko Hyppönen	378

11	OpSec – Operative Sicherheit	381
11.1	Unerkannt unterwegs	383
11.1.1	Linux Tails – das Betriebssystem, das Edward Snowden empfeht	383
11.1.2	Burner Phones	387
11.1.3	Schutz vor Gesichtserkennung	388
11.2	Festplatten, Datenträger und Mails verschlüsseln	390
11.2.1	Festplattenverschlüsselung	390
11.2.2	USB-Stick-Verschlüsselung	397
11.2.3	E-Mail-Verschlüsselung	404
11.3	Passwörter und Authentifizierung	409
11.3.1	Passwortmanager	410
11.3.2	Zwei-Faktor-Authentifizierung (2FA)	413
11.4	Anonym und sicher kommunizieren	415
11.4.1	Lauschabwehr	416
11.4.2	Browser-Fingerprinting	420
11.4.3	Das Tor-Netzwerk	423
11.4.4	So melden Sie Missstände anonym und sicher	434
12	Künstliche Intelligenz in der Cyberspionage	443
12.1	Was ist KI?	444
12.2	KI-Agenten	447
12.2.1	Planen und handeln	448
12.2.2	Wissen erweitern	449
12.2.3	Wer entscheidet?	451
12.2.4	Rent A Human	453
12.2.5	Ein Blick in die Zukunft: Ist Sicherheit nur noch ein Mythos?	456
12.3	Sprachmodelle für den nachrichtendienstlichen Einsatz	458
12.4	Gefährliche Sprachmodelle	461
12.4.1	LLMs für Black Hats	461
12.4.2	LLMs für Geheimdienstoperationen	465
12.5	Deepfakes, synthetische Bilder und Stimmen als psychologische Waffe	466
12.5.1	Quid est veritas? Was ist überhaupt noch wahr?	466
12.5.2	Desinformationskampagnen und Einflussoperationen	469

12.5.3	Beeinflussung durch KI-Nutzung	471
12.5.4	Profile mithilfe von KI erstellen	474
12.5.5	Trusted Authorities	474
Index		477