

OSINT

Wie Sie Informationen finden, verifizieren und verknüpfen

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Auf einen Blick

1	Einführung	13
2	Anwendungsgebiete von OSINT	21
3	Persönliche und technische Voraussetzungen	31
4	Operational Security	39
5	Geschichte und Theorie	95
6	Planung	115
7	Sammlung	139
8	Verarbeitung	381
9	Analyse	395
10	Verbreitung	425
11	Feedbackschleife: Ausgangspunkt für weitere Recherchen	433
12	Am Ball bleiben	435
13	Fazit und Ausblick	439

Inhalt

1	Einführung	13
1.1	Was ist Open Source Intelligence?	13
1.2	Was Sie in diesem Buch lernen werden	16
1.3	Aus- und Fortbildung	17
1.4	Über den Autor	18
2	Anwendungsgebiete von OSINT	21
2.1	Behörden und Organisationen mit Sicherheitsaufgaben	22
2.1.1	OSINT in der AAO	22
2.1.2	OSINT im Rahmen von Sofort- und Zeitlagen	23
2.1.3	OSINT für die Strafverfolgung	23
2.1.4	OSINT im Bevölkerungsschutz	24
2.2	Unternehmen	26
2.3	Journalismus	27
2.4	Wissenschaft	28
2.5	Zusammenfassung der Anwendungsgebiete	29
3	Persönliche und technische Voraussetzungen	31
3.1	Moralische und ethische Grundsätze	31
3.2	Neugier und das richtige Mindset	35
3.3	Psychische Gesundheit	35
3.3.1	Praktische Tipps für belastende Recherchen	37
3.4	IT- und Programmierkenntnisse	37

4	Operational Security	39
<hr/>		
4.1	Gefahren im Internet	39
4.1.1	Akteure	40
4.1.2	Motive	42
4.1.3	Angriffsarten	42
4.2	OPSEC-Workflow	44
4.3	Tipps für sensible Recherchen	47
4.4	Die Arbeitsumgebung einrichten	49
4.4.1	Smartphone	49
4.4.2	Wahl des Betriebssystems	49
4.4.3	Virtualisierung	52
4.4.4	Verschleierungsarten	57
4.4.5	Browser	62
4.4.6	Plug-ins	76
4.4.7	Best Practices für sichere Recherchen	83
4.4.8	Überprüfung von OSINT-Tools	90
4.4.9	Tool-Auswahl mit System	91
4.5	Zusammenfassung: OPSEC	93
5	Geschichte und Theorie	95
<hr/>		
5.1	OSINT: Die (kurze) Geschichte	95
5.2	Rechtliche Rahmenbedingungen	97
5.2.1	Rechtliche Bewertung polizeilicher Anwendungsfelder	99
5.2.2	Eingriffsintensität	100
5.2.3	Strafprozessrecht	103
5.2.4	Verwendung digitaler Beweismittel	103
5.2.5	Strafrecht	105
5.2.6	Informationszugangsrecht	106
5.2.7	Vertrags- und AGB-Recht	107
5.2.8	Fazit rechtlicher Rahmenbedingungen	107
5.3	Arten und Zweck der Informationsgewinnung	107
5.4	Von Daten über Informationen zu Intelligence	109
5.5	Der Intelligence Cycle	111

6	Planung	115
<hr/>		
6.1	Strategische Planung	115
6.2	Anforderungen und Scope	116
6.2.1	Fragen an den Auftraggeber	116
6.2.2	Das Ende des Projekts	118
6.3	Die richtigen Quellen auswählen	119
6.3.1	Recherchestrategie	119
6.3.2	Annäherung an die Antwort	120
6.4	Dokumentation planen und erstellen	122
6.4.1	Grundlagen	123
6.4.2	Manuelle Dokumentation	123
6.4.3	Automatisierte Dokumentation	135
6.4.4	Sicherung digitaler Beweismittel	136
6.4.5	Zusammenfassung: Dokumentation	137
7	Sammlung	139
<hr/>		
7.1	Recherchen im Web: mehr als Google!	139
7.1.1	Arten von Suchmaschinen	139
7.1.2	Suchstrategie	142
7.2	Google	147
7.2.1	Wichtige Einstellungen vor der Recherche	148
7.2.2	Von der Suche zu den Ergebnissen	150
7.2.3	Suchoperatoren: Google Dorks	153
7.2.4	Erweiterte Suche	157
7.2.5	Die Google-Suche mit UDM-Parametern steuern	158
7.3	Bing	160
7.4	Yandex	162
7.5	Weitere Suchmaschinen	163
7.5.1	Private Suchmaschinen	165
7.5.2	Metasuchmaschinen	168
7.5.3	Gerichtsentscheidungen	171
7.5.4	Akademische Suchmaschinen	172
7.5.5	KI-gestützte Suchmöglichkeiten	172

7.6	Inverse Bildersuche	176
7.6.1	Mit Google nach Bildern suchen	176
7.6.2	Weitere Angebote	178
7.7	Recherchen zu Personen	178
7.7.1	Profiling	178
7.7.2	Die digitale Identität	180
7.7.3	Suche nach Nachnamen und Familien	181
7.7.4	Personensuchmaschinen	183
7.7.5	Biometrische Methoden	191
7.7.6	Telefonnummer	201
7.7.7	E-Mail-Adressen	205
7.7.8	Leaks & Breaches	208
7.8	Recherchen zu Orten	211
7.8.1	Grundlagen	211
7.8.2	Kartendienste	212
7.8.3	Ground-Level	223
7.8.4	Luft- und Drohnenbilder	233
7.8.5	Satellitenbilder	234
7.8.6	Webcams	240
7.8.7	Immobilien	242
7.8.8	Kartentools	243
7.9	Recherchen zu Verkehrsmitteln	247
7.9.1	Grundlagen	247
7.9.2	Land	249
7.9.3	Wasser	261
7.9.4	Luft	264
7.10	Recherchen in sozialen Netzwerken (SOCMINT)	269
7.10.1	Arten sozialer Netzwerke	270
7.10.2	Typische Elemente	271
7.10.3	Grundlegende Methoden	273
7.10.4	Metriken und Trends	274
7.10.5	Rechercheidentität	274
7.10.6	Personen in sozialen Netzwerken finden	278
7.10.7	Facebook	287
7.10.8	Instagram	300
7.10.9	X (Twitter)	304
7.10.10	TikTok	307
7.10.11	Snapchat	310

7.10.12 Bluesky	311
7.10.13 Mastodon	313
7.10.14 Truth Social	315
7.10.15 BeReal	317
7.10.16 Messenger	318
7.10.17 Video-Plattformen	322
7.10.18 Dating-Plattformen	329
7.10.19 Fitness-Apps: Strava	330
7.10.20 Gaming-Plattformen	333
7.10.21 GitHub	334
7.10.22 Business-Netzwerke	334
7.10.23 Weitere soziale Netzwerke	337
7.10.24 Soziale Netzwerkanalyse	338
7.11 Recherchen zu Webseiten (WEBINT)	340
7.11.1 Internetgrundlagen	340
7.11.2 Protokolle	340
7.11.3 Zentrale Web-Technologien	348
7.11.4 Ermittlungen zu URLs	350
7.11.5 Ermittlungen zu Webseiten	351
7.11.6 Webarchive	358
7.11.7 Drahtlose Netzwerke	361
7.11.8 Web Scraping	362
7.12 Recherchen zu Firmen und Organisationen	363
7.12.1 Kerninformationen	363
7.12.2 Suche über Anbieter	368
7.12.3 Digitale Präsenz(en)	372
7.12.4 Geschäftsaktivitäten	372
7.12.5 Sanktionslisten	373
7.13 Recherchen zu Finanzen	373
7.13.1 Bankverbindungen	373
7.13.2 Zahlungsdienstleister	376
7.14 Recherchen automatisieren	378
7.14.1 Monitoring von Inhalten	378
7.14.2 Veränderungen tracken	379

8	Verarbeitung	381
<hr/>		
8.1	Datenbereinigung und -transformation	381
8.1.1	Filterung und Strukturierung	382
8.1.2	Wissensmanagement	384
8.1.3	Übersetzung	389
8.1.4	Decodierung	389
8.2	Künstliche Intelligenz in der OSINT-Auswertung	392
9	Analyse	395
<hr/>		
9.1	Kritisches Denken und Verifikation	395
9.1.1	Quellenanalyse	397
9.1.2	Faktencheck	397
9.1.3	Medienrecherche	398
9.2	Bewertungssysteme	399
9.3	Manipulationsarten	401
9.3.1	Deep Fakes und andere Techniken	402
9.3.2	Erkennung von Manipulationen	403
9.4	Grundlagen der Analyse	404
9.5	Kognitive Verzerrungen und Bias	405
9.6	Strukturierte Analysetechniken	408
9.7	Analyse von (Bild-)Dateien	411
9.7.1	Exkurs: File Carving	414
9.7.2	Lokalisierung des Aufnahmeortes	415
9.7.3	Bestimmung des Aufnahmezeitpunkts: Chronolokalisation	418
9.8	Visualisierung und grafische Analysetechniken	422
9.8.1	Grundlegende Techniken	422
9.8.2	Grafikerstellung	422
9.8.3	Werkzeuge zur Netzwerkanalyse	423

10	Verbreitung	425
<hr/>		
10.1	Arten von Intelligence-Produkten	426
10.1.1	Bericht	426
10.1.2	Vortrag und Präsentation	427
10.1.3	Visuelle und multimediale Produkte	428
10.1.4	Periodische Statusberichte und Dashboards	428
10.1.5	Ad-hoc-Briefing	428
10.2	Forensische Berichte erstellen	429
10.2.1	Struktur des Berichts	429
10.2.2	Sanitarisierung von sensiblen Daten	430
11	Feedbackschleife: Ausgangspunkt für weitere Recherchen	433
<hr/>		
11.1	Leistungsbewertung	433
11.2	Qualitätssicherung und Fehleranalyse	433
11.3	Kontinuierliche Optimierung und Wissensmanagement	434
12	Am Ball bleiben	435
<hr/>		
12.1	Trainingsmöglichkeiten	435
12.1.1	Praktische Übungen und Challenges	435
12.1.2	OSINT 4 Good	436
12.2	Austausch	437
12.3	Blogs	437
12.4	News	438
13	Fazit und Ausblick	439
<hr/>		
	Index	441

Index

220vk.com	338
3-2-1-Regel	89
4×4-System	399

A

Abbyy FineReader	384
ABCDE F/X-Schema	399
ActivityPub	313
ADAPT-Framework	92
Admiralty Code	399
Adresssuche	202
Ads Library (Facebook)	296
ADS-B Exchange	266
Advanced Persistent Threats (APTs)	41
Advanced Research Projects	
Agency (ARPA)	340
Agentic AI	141
airportcodes.aero	264
Akademische Suchmaschinen	172
Aleph	386
Allgemeine Aufbauorganisation (AAO)	22
Analysetechniken	408
Analysis of Competing Hypotheses (ACH)	410
Ancestry	182
Anforderungen	116
Anonymisierung	430
Anonymität	44
Anytype	388
Archive Webpage	136
ArchiveBox	134
Archivierung	381
Armchair Detectives	33
ARPANET	340
arXiv	172
Assumptions Log	409
Auto Archiver	135
Autogespot	253
Automatic Dependent Surveillance	
Broadcast (ADS-B)	265
Automatic Identification System (AIS)	262

B

Backlink Checker	351
Backup	89, 381
Baidu	164

Bangs	165
Bank Identifier Code (BIC)	376
Base64-Codierung	390
Basic Bank Account Number (BBAN)	373
BBC Monitoring	95
Beautiful Soup	362
Bellingcat	28
Bellingcat OpenStreetMap Search	247
BeReal	317
Besondere Aufbauorganisation (BAO)	22
Betriebssysteme	49
Beweissicherung	123
Bewertungssysteme	399
Bias	395, 405
Bildersuche	176
Bildschirmvideos	125
Bing	160
Biometrie	191
Bitwarden	85
Black Marble	236
Blackbird	285
Blind Spot	120, 408
Bluesky	311
Blur	77
Blurry	37
Bookmarklets	38, 350
Bottom Line Up Front	429
Brave	70
Browser	62
<i>Firefox</i>	125
<i>Vivaldi</i>	125
Browserling	62
Bundesweites amtliches Anwalts-	
verzeichnis	367

C

Capacities	387
Carbon14	358
CarNet.ai	249
Carrot2	168
CATMA (Computer Assisted Text	
Markup and Analysis)	383
CertStream	353
Cerulean	264
Changedetection.io	379
ChatGPT	140, 173

-
- Chatty 328
- Cheap Fakes 402
- chess.com 333
- Chrome 68
- Chromium 70
- Chronolokalisation 411, 418
- Classified Information 110
- Claude.ai 173
- Closed Source Information 110
- Cluster-Illusion 407
- Comet 75
- CompanyHouse 372
- Confirmation Bias 141, 406
- Container 54
- Copyfish 77
- Crawling 140
- CrewData 264
- Crime-as-a-Service (CaaS) 41
- Critical Thinking 395
- crt.sh 353
- Cruising 96
- Cryptomator 88
- CSS (Cascading Style Sheets) 349
- curl 345
- D**
-
- Dangerzone 88
- Dark Ships 263
- Data Science 339
- Datawrapper 423
- Datenbereinigung 382
- Datenhehlerei 106
- Datenschutz 273
- Datenschutz-Grundverordnung (DSGVO) ... 98
- Dating 329
- Datum 110
- dauerhaftes Monitoring 99
- deck.blue 312
- Decodierung 389
- Deep Fakes 402
- DeepL 389
- Defense Advanced Research Projects
 Agency (DARPA) 340
- Desinformation 401
- DEVONthink 387
- dig 345
- Digger.tools 353
- digiKam 200
- Digital Open Source Investigations 32
- Digital Rights Management 132
- DNSDumpster 353
- Document Object Model (DOM) 348, 350
- Dogpile 140
- Dokumentation 122, 383
- Domain Name System (DNS) 344
- Domain-Age-Checker 358
- Dorks 153
- DPMAreger 373
- Draw.io 422
- Drehscheibe Online 261
- Dronetag 269
- DuckDuckGo 165
- DuckDuckGo Maps 216
- Due Diligence 363
- E**
-
- Earth Copilot 239
- Easy Scraper 81
- Eingriffsintensität
 Dauer der Erhebung 101
 Heimlichkeit 100
 Kernbereich 101
 nachteilige Folgen 102
 öffentliche Daten 102
 Persönlichkeitsprofil 102
 pseudonymisierte oder anonymisierte
 Daten 102
 Streubreite 100
 Zugangssicherung 101
- E-Mail-Adressen 205
- Epieos 204, 206, 285–286
- Equasis 263
- Erlaubnisprinzip 98
- Ermittlungskreislauf 112
- eTools.ch 169
- Evaluation 433
- EXIF 412
- exiftool 413
- ExoneraTor 61
- Exploit Database 156
- Ezlinavis 423
- F**
-
- Face Swapping 402
- Face++ 195
- Facebook 287
 Graph Search 295
- Facebook Marketplace 299
- FaceCheck.ID 194