

Inhaltsverzeichnis

Teil I Der Siegeszug der Informationskrieger

1	Der Fall Hazim Nada	3
1.1	Der „Alp“-Traum wird wahr	4
1.2	Der Desinformator wird gehackt	5
	Literatur	6
2	Die Einschlüge kommen näher	7
2.1	Die Söldner der Desinformation	9
	Literatur	11
3	Wie Worte die Welt entzünden können	13
3.1	Desinformation in der Geschichte	13
3.2	Trump, Johnson, Orban und die Spin Dictators – Die modernen politischen Gesichter der Desinformation	18
	Literatur	22
4	Begrifflichkeiten – Wie definieren wir die Definitionen?	25
4.1	Ziele der Desinformationskampagnen	32
	Literatur	35

5	Warum wirkt Desinformation?	37
5.1	Falschinformationen reisen schneller	46
5.2	Warum die Lüge „sexy“ ist	47
5.3	Polarisierung pays	48
5.4	In den Fängen der „alternativen Fakten“	51
5.5	„Flood the Zone with Shit“	52
5.6	Desinformation: Einmal im Kopf, immer im Kopf?	54
	Literatur	55
6	Vertrauenskrise in die traditionellen Medien – Brandbeschleuniger der Desinformation	59
6.1	Der große Vertrauensverlust	66
6.2	Zunehmende Polarisierung bedroht unsere Gesellschaft	69
6.3	Fazit	71
	Literatur	72
7	Medien-Prankster Joey Skaggs: Der Mann der Journalisten fing	75
7.1	Mainstream-Medien als Malerleinwand	76
7.2	Der Haifischmann – Art of the prank	79
7.3	Ein Element des Möglichen	82
	Literatur	91
 Teil II Desinformation – aus dem politischen Raum in die Wirtschaft		
8	Desinformationsangriffe auf Unternehmen – „A clear and present danger“	95
8.1	Söldner der Desinformation	97
8.2	Angreifer rüsten soziale Medien auf	100
8.3	Corporate Raiders im Kriegsgebiet	103
8.4	Journalisten als Werkzeug der Desinformatoren	105

	Inhaltsverzeichnis	XIX
8.5	Desinformationsangriffe von Aktivisten	107
8.6	Staatliche Desinformationsangriffe auf Impfstoffhersteller	110
	Literatur	114
9	Die Täter und ihre Motive	117
9.1	Staatlich geförderte Akteure	126
9.2	Ehemalige Mitarbeiter oder Kunden	127
9.3	Konkurrenten	128
9.4	Investoren, Corporate Raiders, Shortsellers	130
9.5	Hackivistische Gruppen	132
9.6	NGOs und Aktivisten	132
9.7	Erpresser	134
9.8	Anlegerschutzanwälte	134
	Literatur	135
10	Gefährdete Unternehmensbereiche	137
10.1	Angriff via Verdachtsberichterstattung	139
10.2	Angriffe zum richtigen Zeitpunkt	140
10.3	Angriffsfläche Produktionsprozesse	142
10.4	Angriffsflächen Produktqualität, Image und Dienstleistungen	143
10.5	Angriffsflächen Belegschaft, Recruitment und Soziales	145
10.6	Angriffsflächen Unternehmensführung und Finanzen	147
10.7	Angriffsflächen Lieferanten und Zulieferer	148
	Literatur	149
11	Tools und Taktiken – Mechaniken der Angriffe	151
11.1	Die Tools	156
11.2	Die Taktiken	162
	Literatur	170

Teil III Abwehr und Aufarbeitung

12	Verteidigung – Die hastige Suche nach Zeit und Raum	173
12.1	Der Faktor Zeit – Warum es so wichtig ist, schnell zu reagieren	175
12.2	Wenn die Welle rollt, ist es schon zu spät	176
	Literatur	188
13	Vorbereitung, Gegenmaßnahmen, Abwehrstrategien	189
	Literatur	202
14	Wohin bewegen wir uns? – Von DeepFakes zu Bio-Bots	203
14.1	Warnung an die Medien	212
14.2	Recht muss sich anpassen	213
	Literatur	215