

Inhaltsverzeichnis

Vorwort von Brigadegeneral Karl H. Schreiner	11
Vorwort von Gerold Hübner	17
Einleitung	21
1 Evolution	25
1.1 Strategie	25
1.2 Technostrategie	28
1.3 Der Beginn der hochtechnisierten Kriege	35
1.3.1 Die neue technostrategische Situation	37
1.3.2 Cyberwarfare als nächster Schritt	43
2 Hacking	47
2.1 Hacker	49
2.2 Prinzipien des Hacking	51
2.3 Bugs und Sicherheitslücken	53
2.4 Reverse Engineering und Zero Days	56
3 Strukturen	59
3.1 Komplexität	60
3.1.1 Unvermeidbarkeit	60
3.1.2 Vernetzte Informationstechnik	61
3.1.3 Doppelte Vulnerabilität	62
3.1.4 Angriffsschichten und Redundanzen	63
3.1.5 Verwundbarkeiten und Unsicherheiten	65
3.2 Globalität	66
3.2.1 Interkonnektivität	66
3.2.2 Fehlende Regulierung	67
3.2.3 Strategisches Verständnis der Globalität	69

3.3	Vernetzungen und Interoperabilität	69
3.3.1	Angriffsmultiplikation	70
3.3.2	Angriffsmigration	71
3.3.3	Schadensabschätzungen	72
3.3.4	Systemweite Angriffe	72
3.4	IT-Sicherheit	74
3.4.1	COTS	75
3.4.2	Sicherheitsstufen und Angreifertypen	76
3.4.3	Entnetzung	80
3.5	Non-Attribution	80
3.5.1	Technischer und regulativer Hintergrund	81
3.5.2	Territoriale und personale Non-Attribution	84
3.5.3	Motivationale Non-Attribution	85
3.5.4	Kriege der Patrioten	87
3.5.5	Agitation	88
3.5.6	Konfliktunabhängige Operationen	89
3.5.7	Zeugnisse der Verzweiflung	89
3.5.8	Rechte	91
3.6	Kosten	91
4	Ziele	93
4.1	Vorbetrachtungen	93
4.1.1	Verwundbarkeiten von Informationsgesellschaften	93
4.1.2	Eine Heuristik	95
4.2	Informationen	97
4.2.1	Geschlossene Informationen	97
4.2.2	Offene Informationen	101
4.3	Identitäten	106
4.3.1	Falsche Identitäten	107
4.3.2	Transparente Identitäten	108
4.4	Infrastrukturen	108
4.4.1	Lokale Infrastrukturen	110
4.4.2	Nationale Infrastrukturen	114
4.4.3	KRITIS	118

5 Strategien	121
5.1 Strategien als sicherheitspolitische Heuristik	121
5.2 Grundlagen kriegesischen Hackens	123
5.2.1 Zielgerichteter und opportunistischer Zugriff	125
5.2.2 Optionen im Umgang mit Daten	125
5.2.3 ROM-Faktor	129
5.2.4 Anforderungen	131
5.2.5 Transportwege	133
5.3 Erkennen und Täuschen	137
5.3.1 Aufklärung	138
5.3.2 E-Spionage	139
5.3.3 Täuschung	141
5.4 Angriff	142
5.4.1 Eleganz	143
5.4.2 Streuung von Angriffen	145
5.4.3 Prinzipien der CNA	147
5.5 Abschreckung	149
5.6 Verteidigung	152
5.6.1 Das Konzept des Schutzes	153
5.6.2 Abwehr	154
5.6.3 Klassische Techniken und Konzepte des IT-Schutzes	155
5.6.4 Prinzipien der CND	167
6 Realitäten	169
6.1 Militärische Vorfälle	169
6.1.1 Cyberwar in Estland	169
6.1.2 Cyberwar in Georgien	171
6.1.3 Operation Orchard	173
6.1.4 Operation Buckshot Yankee	174
6.1.5 Conficker	174
6.1.6 Stuxnet	175
6.2 Pläne	180
6.2.1 Information Operations der USA	180
6.2.2 Xinxizhan	184

6.3	Kapazitäten	188
6.3.1	Das US-Cybercommand	188
6.3.2	Ressourcen	190
7	Ausblick	191
7.1	Die Zukunft des Cyberwar	191
7.1.1	Die nahe Zukunft des Krieges	192
7.1.2	Cyberwar und Cybercrime	195
7.2	Die Regulierung des Cyberwar	196
7.2.1	Cyberwar im internationalen Recht	196
7.2.2	Schutz von Infrastrukturen und Wirtschaft	200
7.2.3	Haftungsfragen	201
7.2.4	Freiheitsrechte	203
7.3	Entnetzung	206
7.3.1	Der Rückschritt als Fortschritt	206
7.3.2	Erste Trends zur Entnetzung	207
7.4	The End of Western Civilization as We Know It?	208
	Anhang	213
A	Hintergrund: Hacking	215
A.1	Footprinting	216
A.1.1	Nützliche Informationen	217
A.1.2	Verfahren des Footprinting	222
A.2	Exploitation	229
A.2.1	Grundlegende Techniken	230
A.2.2	Störungen	233
A.2.3	Identitätsdiebstahl & Anonymisierung	234
A.2.4	Exploitation Kits	237
A.3	Malware	238
A.3.1	Angriffsvektoren	239
A.3.2	Viren und Würmer	240
A.3.3	Trojaner	241
A.4	Social Engineering	242