

Inhaltsverzeichnis

1	Einleitung	1
2	Phänomenologie	3
2.1	Unterscheidung zwischen Wirtschaftsspionage und Konkurrenzausspähung	4
2.2	Verflechtung staatlicher und unternehmerischer Ausspähung	5
2.3	Der Innentäter	8
2.3.1	Innentäter im engeren Sinn	8
2.3.2	Innentäter im weiteren Sinn	9
2.3.3	Gefährdungspotential durch Innentäter	10
2.3.4	Motivationslage der Innentäter	11
2.3.5	Innentäter – korrupte Wirtschaftskriminelle?	13
2.4	Phänomenologische Einschätzung der Wirtschaftsspionage	13
2.4.1	Phänomenologische Erkenntnisse zur Spionage	13
2.4.2	Wirtschaftsspionage als Form der Wirtschaftskriminalität	14
2.4.3	Empirische Erkenntnisse	16
2.5	Zwischenfazit	26
3	Die Angriffsmethoden	29
3.1	Kategorisierung von Angriffsarten	29
3.2	Open Source Intelligence (OSINT)	31
3.3	Human Intelligence (HUMINT)	35
3.3.1	Social Engineering	37
3.3.2	Anfälligkeit für Social Engineering	39
3.3.3	Social Engineering – arglistige Täuschung?	40
3.3.4	Social Engineering durch Innentäter	42
3.4	Signal Intelligence (SIGINT)	43
3.5	Kriminalgeographie des Worldwide Web	43
3.5.1	APT Angriffe	44
3.5.2	IT Angriffe durch Innentäter	47
3.6	Zwischenfazit	48

4	Rechtliche Einordnung	49
4.1	Differenzierung nach Schutzbereichen	50
4.1.1	Schutzbereich der „Wirtschaftsspionage“	50
4.1.2	Schutzbereich der „Wirtschaftsausspähung“	51
4.1.3	Schutzbereich der „Computerdelikte“	51
4.2	Tatbestandliche Voraussetzungen der Wirtschaftsausspähung	53
4.2.1	Betriebs- und Geschäftsgeheimnisse	53
4.2.2	Täterkreis	56
4.2.3	Tathandlungen	57
4.2.4	Geheimnisverrat	58
4.2.5	Geheimnisausspähung	59
4.2.6	Geheimnisverwertung	61
4.3	Tatbestandliche Voraussetzungen der Wirtschaftsspionage	62
4.3.1	Geheimdienst einer fremden Macht	64
4.3.2	Ausüben geheimdienstlicher Tätigkeit	65
4.3.3	Zweckbindung der Handlung	66
4.3.4	Zielrichtung der Handlung	67
4.3.5	Funktionelle Eingliederung des Täters	68
4.4	Tatbestandliche Voraussetzungen der Computerdelikte	68
4.4.1	Datenbegriff	69
4.4.2	Ausspähen und Abfangen von Daten	71
4.4.3	Veränderungen von Daten	74
4.4.4	Computersabotage	75
4.4.5	Computerbetrug	76
4.5	Ausgewählte sonstige relevante Tatbestände	78
4.6	Zwischenfazit	80
5	Kriminologische Erklärungsansätze	81
5.1	Vor den Theorien	82
5.2	Anomietheorie nach Merton	82
5.3	Kontrolltheorie nach Hirschi	84
5.4	White Collar Crime Approach nach Sutherland	86
5.5	Subkulturtheorie 2.0	87
5.5.1	Ursprung	87
5.5.2	Anwendbarkeit im arbeitsplatzbezogenen Kontext	88
5.6	Neutralisationstechniken	90
5.7	Routine Aktivitäts Theorie nach Cohen und Felson	93
5.8	Situational Action Theorie nach Wikström	94
5.9	Leipziger Verlaufsmodell nach Schneider	97
5.10	Kriminologische Erkenntnisse zu Cyberkriminellen	100
5.10.1	Gruppendynamische Ansätze	100
5.10.2	Individuelle Ansätze	101
5.11	Zwischenfazit	103

6 Präventionsansätze	105
6.1 RADAR Ansatz	106
6.2 R – Risikobeurteilung	107
6.2.1 Geht es immer nur um „Kronjuwelen“?	107
6.2.2 Verantwortlichkeiten	108
6.2.3 Klassifizierungen	108
6.3 A – Auswahl von Mitarbeitern und Partnern	111
6.3.1 Auswahl von Mitarbeitern	111
6.3.2 Auswahl von Geschäfts- und Kooperationspartnern	118
6.4 D – Durchgängiges Sicherheitskonzept	120
6.4.1 Elemente im Einzelnen	121
6.4.2 Maßnahmenplanung	124
6.5 A – Awarenessbildung	126
6.5.1 Awareness und Capability	126
6.5.2 Organisatorische und personelle Awareness	127
6.6 R – Regelmäßige Auditierung	130
6.7 Zwischenfazit	134
7 Schlussbetrachtung	137
Literatur	139
Stichwortverzeichnis	145