

Contents

1	Industrial Espionage	1
1.1	Introduction.....	1
1.2	Espionage in General	1
1.3	Industrial, Corporate, Commercial, or Economic Espionage	2
1.4	Business: Competitive Intelligence.....	2
1.5	The Problem.....	3
1.6	The Human Factor	4
1.7	Statistics	5
1.8	Some Actual Facts	8
1.9	Summary	10
2	Intercepting Ambient Conversations	11
2.1	Introduction.....	11
2.2	Interception Devices	11
2.3	Transmitting Setups	14
2.4	Microphones	15
2.5	Exotic Tools	17
2.6	Systems for Enforcing Secrecy of Communications	18
2.7	Summary	21
3	Interception of Computer Data	23
3.1	Introduction.....	23
3.2	Hardware for Intercepting Computer Data	23
3.3	Means of Data Transfer.....	24
3.4	Software	25
3.5	Wireless Networks	26
3.6	Man-in-the-Middle Attacks	29
3.7	Data Security.....	30
3.8	Data Traffic and Management.....	31
3.9	Advanced Persistent Threats.....	32

3.10	Teleworking and Industrial Espionage.....	33
3.11	Global Surveillance.....	35
3.12	Summary	35
4	Intercepting Fixed Line Telephony.....	37
4.1	Introduction.....	37
4.2	Fixed Line Telephony Interception Devices	37
4.3	Wiretaps	38
4.4	Structured Cabling	41
4.5	Digital Lines and Private Branch Exchanges.....	42
4.6	Call Detail Records Interception.....	45
4.7	Wireless Communications	46
4.8	VoIP Specifics	48
4.9	Telecommunications Security	49
5	Mobile Phones Interception	51
5.1	Introduction.....	51
5.2	Cellphone Data that Can Be Intercepted.....	51
5.3	Cellphone Theft and Data Exportation	52
5.3.1	In General.....	52
5.3.2	Files on the SIM Card	53
5.3.3	Device Data.....	55
5.3.4	Data Extraction	56
5.3.5	External Memory Cards and Computers.....	59
5.4	Interception Software.....	59
5.5	Network Security	61
5.6	Encryption and Cryptanalysis	62
5.7	Internal Fraud.....	63
5.8	Phone Call Interception.....	64
5.8.1	Introduction.....	64
5.8.2	Theory	64
5.8.3	Implementation	67
5.8.4	Configuration	70
5.9	Short Message Service.....	72
5.10	Bluetooth®	73
5.10.1	In General.....	73
5.10.2	Data Interception via Bluetooth®	73
5.10.3	Targeting Users	74
5.10.4	Integrity (Cellphone Control: Billing)	74
5.10.5	Bluetooth® and Social Engineering.....	75
5.10.6	Tools (Hardware-Software).....	77
5.11	Protection Measures.....	77
5.11.1	Protection Against Interceptions.....	77
5.11.2	Practical Advice for Cellphone Protection	80
5.12	Conclusions.....	81

6	An Example of a Malware that Can Be Used for Industrial Espionage or as a Personal Spyware and a Way to Protect from It	83
6.1	Introduction.....	83
6.2	The Tor Network.....	84
6.3	Current Threat Landscape.....	84
6.4	What Would Make Such a Malware Successful?	86
6.5	Technical Description of the Malware Operation	87
6.6	What Would Make Countermeasures Effective?	89
6.7	Technical Description of the Anti-malware Operation	91
6.8	Conclusions.....	92
7	Protection Against Industrial Espionage	95
7.1	Introduction.....	95
7.2	About Protection in General	95
7.3	Patents	96
7.4	Confidential Information, Know-How, and Trade Secrets.....	97
7.5	Equipment for Detection of Electronic Tapping	98
7.5.1	Frequency Receivers and Scanners.....	99
7.5.2	Spectrum Analyzers	101
7.5.3	Broadband Receivers	102
7.5.4	Field Meters	104
7.5.5	NLJD: Nonlinear Junction Detectors.....	104
7.5.6	Portable X-ray Device.....	107
7.5.7	Thermal Imaging Cameras.....	107
7.5.8	Infrared Detectors	108
7.5.9	Camera Lens Optical Detection Device.....	108
7.5.10	Detection of Telecommunications Interceptions.....	109
7.5.11	Conclusion	112
7.6	Methodology for Detection of Electronic Interception.....	113
7.6.1	Initial Contact.....	113
7.6.2	Follow-Up	113
7.6.3	Detection Planning and Choice of Areas	114
7.6.4	Identification of the Areas and Vulnerability Analysis.....	115
7.6.5	Transmission Detection.....	116
7.6.6	Electric and Electronic Checks	116
7.6.7	Simple Visual Check.....	117
7.6.8	Telecommunications Check	118
7.6.9	Computing and Network Infrastructure Check.....	119
7.6.10	Findings, Deliverables, and Next Steps	120
7.7	Preventive Measures and Area Protection	120
7.8	Choosing the Right Contractor	122
7.8.1	Introduction.....	122
7.8.2	Categories	123
7.8.3	What Should Be Avoided.....	125
7.8.4	Economic Background.....	125

Industrial Espionage and Technical Surveillance
Counter Measurers

Androulidakis, I.I.; Kioupakis, F.-E.

2016, XIII, 126 p. 74 illus., 65 illus. in color., Hardcover

ISBN: 978-3-319-28665-5