
Contents

Introduction	ix
Chapter 1. History and Repertoire of Communication	
Interception Practices	1
1.1. Military interceptions during the war	7
1.1.1. The interception of telegraphic communications.	7
1.1.2. The interception of radio communications	13
1.1.3. Telephone interception	16
1.1.4. The use of SIGINT capabilities	18
1.1.5. Wartime interceptions in cyberspace	21
1.1.6. Drones and interceptions	23
1.2. The interception of international communications: espionage, surveillance, war	23
1.2.1. The interception of telegrams	23
1.2.2. Espionage during the Cold War: satellite, radio, telephone interceptions	24
1.2.3. The interception of international communications: the Echelon program.	25
1.2.4. Bulk cyber surveillance.	27
1.2.5. Foreign companies in national telecommunication infrastructures	28
1.2.6. Actions over undersea Internet cables.	29
1.2.7. Interceptions in planes and airports	30
1.2.8. International interceptions as a product of secret alliances	30
1.3. Interception of diplomatic correspondence	31
1.4. Political surveillance: targeted and bulk interceptions	33
1.4.1. Interception of correspondence	33
1.4.2. Bulk domestic surveillance in East Germany.	36
1.4.3. Cyber surveillance in Russia: the SORM system	36
1.4.4. Fixed and mobile telephone tapping.	37

1.4.5. The interception of electronic communications in the political sphere. . .	40
1.5. Criminal interceptions.	42
1.6. Police, justice: the fight against crime, lawful interceptions	44
1.7. On the usefulness and effectiveness of interceptions	45
Chapter 2. The Central Issue of Encryption	55
2.1. The capabilities required for interceptions.	55
2.1.1. Material, technological capabilities	56
2.1.2. Human resources	79
2.2. Protecting yourself against the threat of interceptions: encryption	87
2.2.1. The public key revolution	88
2.2.2. Advances in factorization	89
2.2.3. Shor's quantum algorithm	91
2.2.4. The evolution of computing capabilities	93
2.2.5. The evolution of etching precision	94
2.3. Attacking encrypted communications, circumventing the hurdle of encryption	94
2.3.1. Interceptions on encrypted messaging	95
2.3.2. The attacks against keys and PKIs.	104
2.3.3. The use of backdoors	108
Chapter 3. Power Struggles.	131
3.1. State pressure on the industry: cooperation or coercion logics?	131
3.2. The accounts of whistleblowers and their analyses of the balance of power between the state, the citizen and companies.	136
3.2.1. The account of Herbert O. Yardley	136
3.2.2. The account of Perry Fellwock (also known as Winslow Peck)	137
3.2.3. The account of Mark Klein.	138
3.2.4. The account of James Bamford	142
3.2.5. The account of Babak Pasdar	145
3.2.6. The account of Joseph Nacchio	146
3.2.7. The account of Edward Snowden	146
3.2.8. The account of Julian Assange.	148
3.3. Limits imposed on the state's power to control technology	149
3.3.1. The difficult and fragile international regulation of technologies.	149
3.3.2. Illicit markets and the circumvention of laws	154
3.4. Trust	162
3.4.1. How much confidence in encryption?.	163
3.4.2. The acceleration of calculations as a factor of confidence	164
3.4.3. Abandoning secret methods	165
3.4.4. Provable security	167
3.4.5. The worlds of Impagliazzo.	169

3.4.6. The contribution of quantum computing	172
3.5. Conclusion	173
3.5.1. Technologies	173
3.5.2. Actors	174
3.5.3. Interactions or relationships	175
Appendices	179
References	201
Index	217