

Table des matières

Introduction	1
Chapitre 1. Histoire et répertoire des pratiques d'interception des communications	21
1.1. Les interceptions militaires dans la guerre.	27
1.1.1. L'interception des communications télégraphiques	27
1.1.1.1. La guerre civile américaine	28
1.1.1.2. La guerre civile au Chili.	31
1.1.1.3. La guerre hispano-américaine de 1898	32
1.1.1.4. L'interception du télégraphe au début du XX ^e siècle	32
1.1.2. L'interception des communications radio.	33
1.1.3. L'interception du téléphone	37
1.1.4. L'utilisation des capacités de SIGINT.	38
1.1.5. Les interceptions dans le cyberspace en temps de guerre	42
1.1.6. Drones et interceptions.	44
1.2. L'interception des communications internationales : espionnage, surveillance, guerre	44
1.2.1. Les interceptions des télégrammes	44
1.2.2. L'espionnage durant la Guerre froide : interceptions satellitaires, radio, téléphonie	45
1.2.3. Les interceptions de communications internationales : le programme Echelon	46
1.2.4. Cybersurveillance massive	48
1.2.5. Les entreprises étrangères dans des infrastructures nationales de télécommunication	50
1.2.6. Actions sur les câbles internet sous-marins.	50

1.2.7. Les interceptions dans les avions et aéroports	52
1.2.8. Les interceptions internationales grâce aux alliances secrètes . . .	52
1.3. Les interceptions des correspondances diplomatiques	52
1.4. La surveillance politique : interceptions ciblées et massives	54
1.4.1. L'interception des correspondances	54
1.4.1.1. Les cabinets noirs	56
1.4.1.2. L'État nazi et les interceptions de télégrammes et de la téléphonie	57
1.4.2. La surveillance domestique de masse en Allemagne de l'Est . . .	58
1.4.3. La cybersurveillance en Russie : le système SORM	58
1.4.4. Écoutes de la téléphonie fixe et mobile	58
1.4.4.1. Les écoutes dans la vie politique américaine	58
1.4.4.2. L'affaire des écoutes de l'Élysée	60
1.4.4.3. Le scandale des écoutes téléphoniques en Argentine	60
1.4.4.4. Le cas du Chili : les opérations W et Topografo	61
1.4.4.5. Scandales au Pérou	61
1.4.5. L'interception des communications électroniques dans la sphère politique	62
1.4.5.1. Les scandales des interceptions sauvages en Colombie . . .	62
1.4.5.2. L'espionnage au Togo	63
1.5. Les interceptions criminelles	64
1.6. Police, justice : la lutte contre le crime, les interceptions légales . . .	66
1.7. De l'utilité et de l'efficacité des interceptions	67

Chapitre 2. La question centrale du chiffrement 77

2.1. Les capacités nécessaires aux interceptions	77
2.1.1. Les capacités matérielles, technologiques	78
2.1.1.1. L'attaque de type MITM	80
2.1.1.2. De l'analyse de trafic à l'exploitation des métadonnées . . .	81
2.1.1.3. Le DPI (<i>Deep Packet Inspection</i>)	81
2.1.1.4. Intégrer les équipements d'interception à la source dans les infrastructures de télécommunication	84
2.1.1.5. Les collectes <i>downstream</i> et <i>upstream</i>	86
2.1.1.6. Les IMSI-Catcher	88
2.1.1.7. L'interception des communications satellitaires	90
2.1.1.8. L'interception et le stockage des données collectées	93
2.1.1.9. L'interception des courriers électroniques	94
2.1.1.10. De l'intérêt d'avoir la mainmise sur les infrastructures . . .	96
2.1.2. Les moyens humains	102

2.2. Se protéger de la menace des interceptions : le chiffrement	110
2.2.1. La révolution des clés publiques	111
2.2.2. Les progrès de la factorisation	113
2.2.3. L’algorithme quantique de Shor	114
2.2.4. L’évolution des capacités de calcul	117
2.2.5. L’évolution de la finesse de gravure	118
2.3. Attaquer les communications chiffrées, contourner l’obstacle du chiffrement	118
2.3.1. Interceptions sur les messageries chiffrées	119
2.3.2. Attaques contre les clés et les PKI	128
2.3.2.1. Les clés, cibles des attaques	129
2.3.2.2. Attaquer les PKI	130
2.3.2.3. Synthèse des méthodes visant à affaiblir la sécurité des communications ou en exploiter les vulnérabilités, afin d’en rendre possible l’interception	132
2.3.3. Du recours aux <i>backdoors</i>	133
2.3.3.1. Le contournement du chiffre	134
2.3.3.2. La réduction de l’entropie des clés	135
2.3.3.3. Le contrôle de la cryptologie	137
2.3.3.4. Les <i>backdoors</i> et leur dimension politique	143
2.3.3.5. Des exemples concrets d’introduction de <i>backdoors</i> par les États et le crime	148
2.3.3.6. Une « alliance » d’États en faveur des <i>backdoors</i> cryptographiques	152
Chapitre 3. Enjeux de pouvoir	157
3.1. Pressions de l’État sur l’industrie : logique de coopération ou de contrainte ?	157
3.2. Les récits des lanceurs d’alerte et leur analyse des rapports de force entre l’État, le citoyen, l’entreprise	162
3.2.1. Le récit d’Herbert O. Yardley	162
3.2.2. Le récit de Perry Fellwock (<i>aka</i> Winslow Peck)	164
3.2.3. Le récit de Mark Klein	165
3.2.4. Le récit de James Bamford	168
3.2.5. Le récit de Babak Pasdar	172
3.2.6. Le récit de Joseph Nacchio	173
3.2.7. Le récit d’Edward Snowden	173
3.2.8. Le récit de Julian Assange	175
3.3. Les limites au pouvoir de contrôle de la technologie par l’État	176

3.3.1. La difficile et fragile régulation internationale des technologies . . .	176
3.3.2. Les marchés illicites et le contournement des lois	181
3.3.2.1. La multiplication des acteurs et des moyens de l’interception	181
3.3.2.2. Les producteurs de technologies d’interception du secteur privé	182
3.3.2.3. Le marché des logiciels espions	183
3.3.2.4. La vente de systèmes de surveillance à des régimes autoritaires	184
3.3.2.5. Pegasus : interception ciblée de la téléphonie mobile	185
3.4. La confiance	190
3.4.1. Quelle confiance dans le chiffrement ?	191
3.4.2. L’accélération des calculs comme facteur de confiance	192
3.4.3. Abandonner les méthodes secrètes	193
3.4.4. Les preuves de sécurité.	195
3.4.5. Les mondes d’Impagliazzo	198
3.4.6. L’apport du calcul quantique	201
3.5. Conclusion	201
3.5.1. Les technologies.	201
3.5.2. Les acteurs	202
3.5.3. Les interactions ou relations.	204
Annexe	207
Bibliographie	231
Index	249