

1. Record Nr.	UNINA9910830906003321
Autore	Ventre Daniel
Titolo	Electronic communication interception technologies and issues of power / / Daniel Ventre and Philippe Guillot
Pubbl/distr/stampa	London, England ; Hoboken, NJ : , : ISTE Ltd : , : John Wiley & Sons, Inc., , [2023] ©2023
ISBN	1-394-23672-7 1-394-23670-0
Edizione	[1st ed.]
Descrizione fisica	1 online resource (259 pages)
Disciplina	929.605
Soggetti	Computers
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover -- Title Page -- Copyright Page -- Contents -- Introduction -- Chapter 1. History and Repertoire of Communication Interception Practices -- 1.1. Military interceptions during the war -- 1.1.1. The interception of telegraphic communications -- 1.1.2. The interception of radio communications -- 1.1.3. Telephone interception -- 1.1.4. The use of SIGINT capabilities -- 1.1.5. Wartime interceptions in cyberspace -- 1.1.6. Drones and interceptions -- 1.2. The interception of international communications: espionage, surveillance, war -- 1.2.1. The interception of telegrams -- 1.2.2. Espionage during the Cold War: satellite, radio, telephone interceptions -- 1.2.3. The interception of international communications: the Echelon program -- 1.2.4. Bulk cyber surveillance -- 1.2.5. Foreign companies in national telecommunication infrastructures -- 1.2.6. Actions over undersea Internet cables -- 1.2.7. Interceptions in planes and airports -- 1.2.8. International interceptions as a product of secret alliances -- 1.3. Interception of diplomatic correspondence -- 1.4. Political surveillance: targeted and bulk interceptions -- 1.4.1. Interception of correspondence -- 1.4.2. Bulk domestic surveillance in East Germany -- 1.4.3. Cyber surveillance in Russia: the SORM system -- 1.4.4. Fixed and mobile telephone tapping -- 1.4.5. The interception of electronic communications in the political sphere -- 1.5. Criminal interceptions

-- 1.6. Police, justice: the fight against crime, lawful interceptions --
1.7. On the usefulness and effectiveness of interceptions -- Chapter 2.
The Central Issue of Encryption -- 2.1. The capabilities required for
interceptions -- 2.1.1. Material, technological capabilities -- 2.1.2.
Human resources -- 2.2. Protecting yourself against the threat of
interceptions: encryption -- 2.2.1. The public key revolution.
2.2.2. Advances in factorization -- 2.2.3. Shor's quantum algorithm --
2.2.4. The evolution of computing capabilities -- 2.2.5. The evolution
of etching precision -- 2.3. Attacking encrypted communications,
circumventing the hurdle of encryption -- 2.3.1. Interceptions on
encrypted messaging -- 2.3.2. The attacks against keys and PKIs --
2.3.3. The use of backdoors -- Chapter 3. Power Struggles -- 3.1.
State pressure on the industry: cooperation or coercion logics? -- 3.2.
The accounts of whistleblowers and their analyses of the balance of
power between the state, the citizen and companies -- 3.2.1. The
account of Herbert O. Yardley -- 3.2.2. The account of Perry Fellwock
(also known as Winslow Peck) -- 3.2.3. The account of Mark Klein --
3.2.4. The account of James Bamford -- 3.2.5. The account of Babak
Pasdar -- 3.2.6. The account of Joseph Nacchio -- 3.2.7. The account
of Edward Snowden -- 3.2.8. The account of Julian Assange -- 3.3.
Limits imposed on the state's power to control technology -- 3.3.1.
The difficult and fragile international regulation of technologies --
3.3.2. Illicit markets and the circumvention of laws -- 3.4. Trust --
3.4.1. How much confidence in encryption? -- 3.4.2. The acceleration
of calculations as a factor of confidence -- 3.4.3. Abandoning secret
methods -- 3.4.4. Provable security -- 3.4.5. The worlds of
Impagliazzo -- 3.4.6. The contribution of quantum computing -- 3.5.
Conclusion -- 3.5.1. Technologies -- 3.5.2. Actors -- 3.5.3.
Interactions or relationships -- Appendices -- References -- Index --
EULA.
