
Contents

List of Figures	xi
List of Tables	xv
Preface	xvii
Acknowledgments	xix
Intro	1
Part 01 Quantum Technologies	23
1 Small Phenomena, Big Implications	25
1.1 Uncertainty	25
1.2 Entanglement	26
1.3 Superposition	27
1.4 Conclusion	29
2 Quantum Sensing and Metrology	31
2.1 First-Generation Quantum Sensing	36
2.2 Modern Quantum Sensing Approaches	39
2.3 Quantum Sensing Applications	47
2.3.1 Measuring Time	47
2.3.2 Sensing Location	51
2.3.3 Sensing Gravitational Fields	65
2.3.4 Quantum Illumination	68
2.3.5 Quantum Radar	71
2.4 From SIGINT to MASINT	74
2.5 Quantum Sensing: Conclusion	75
3 Understanding Computation	77
3.1 Mechanical Calculation	78
3.2 The Birth of Machine Computation	80
3.2.1 Combinatorial Problems	80

3.2.2	Numerical Analysis	82
3.3	Numeric Coding	83
3.3.1	Encoding Digital Information	86
3.3.2	Digital Computation	90
3.4	Computing, Computability and Turing Complete . . .	91
3.4.1	Introducing The Halting Problem	94
3.4.2	The Halting Problem Cannot Be Solved	96
3.4.3	Using The Halting Problem	97
3.5	Moore's Law, Exponential Growth, and Complexity Theory	98
3.5.1	Software Speedups	102
3.5.2	Polynomial Complexity (P)	106
3.5.3	Nondeterminism	107
3.5.4	NP-Complete and NP-Hard	110
3.5.5	NP-Complete Problems Are Solvable!	115
3.5.6	BQP, BPP, and Beyond	116
3.6	Computing Today	118
3.7	Conclusion	119
4	The Birth of Quantum Computing	121
4.1	Why Quantum Computers?	122
4.1.1	Richard Feynman and Quantum Computing . .	122
4.2	Reversibility	124
4.2.1	The Arrow of Time	125
4.2.2	The Second Law of Thermodynamics	126
4.2.3	Reversible Computation	130
4.2.4	The Landauer Limit	134
4.3	Cellular Automata and Conway's Life	136
4.3.1	Computing with CPUs, GPUs, and CA(s) . . .	136
4.3.2	Life (The Game)	140
4.4	Digital Physics	145
4.4.1	Edward Fredkin and Project MAC	146
4.5	Reversible Computing and Supercomputing	151
4.5.1	A Most Successful Term Paper	151
4.5.2	Reversible Computing Today	153
4.5.3	Defense Money	157
4.6	The Conference on The Physics of Computation (1981)	159
4.7	Russia and Quantum Computing	162
4.8	Aftermath: The Quantum Computing Baby	164
4.8.1	Growing Academic Interest	164

4.8.2	The First Quantum Computers	168
4.8.3	Coda	169
5	Quantum Computing Applications	173
5.1	Simulating Physical Chemistry	174
5.1.1	Nitrogen Fixation, without Simulation	181
5.1.2	Modeling Chemical Reactions	184
5.2	Quantum Factoring (Shor's Algorithm)	188
5.2.1	An Introduction to Cryptography	190
5.2.2	Forty Years of Public Key Cryptography	196
5.2.3	Cracking Public Key with Shor's Algorithm	199
5.2.4	Evaluating The Quantum Computer Threat to Public Key Cryptography	203
5.2.5	Post-Quantum Cryptography	208
5.3	Quantum Search (Grover's Algorithm)	210
5.3.1	Symmetric Ciphers: DES and AES	210
5.3.2	Brute-Force Key Search Attacks	214
5.3.3	Cracking AES-128 with Grover's Algorithm	218
5.3.4	Grover's Algorithm Today	223
5.4	Conclusion	226
6	Quantum Computing Today	229
6.1	How to Build a Quantum Computer	231
6.2	The Quantum Computer Landscape	235
6.2.1	Comparing Quantum Media	236
6.2.2	Five Kinds of Quantum Computers	237
6.3	Skeptics Present Quantum Computing's Challenges	242
6.3.1	Scientific Challenges	243
6.3.2	Engineering Challenges	245
6.3.3	Validation Challenges	248
6.3.4	Ecosystem Challenges	248
6.3.5	Quantum Supremacy and Quantum Advantage	249
6.4	The Outlook for Quantum Computing	253
7	Quantum Communications	257
7.1	Information-Theoretic Security	260
7.1.1	An Easy Math Problem	260
7.1.2	A Hard Math Problem	261
7.1.3	An Impossible Math Problem	262
7.2	Golden Ages: SIGINT and Encryption Adoption	264

7.2.1	The Golden Age of SIGINT	264
7.2.2	The Golden Age of Encryption	270
7.3	Quantum Random Number Generation (QRNG) . . .	271
7.4	Quantum Key Distribution	276
7.4.1	BB84	277
7.4.2	How QKD Works	279
7.4.3	Why QKD Is Secure	283
7.4.4	QKD Gains Momentum	286
7.4.5	QKD Commercialized, Miniaturized	289
7.5	Quantum Internet	293
7.6	Conclusion	300
 Part 10 Shaping the Quantum Future		303
 8 Quantum Technologies and Possible Futures		305
8.1	Do Quantum Artifacts Have Politics?	305
8.1.1	Threat Modeling	307
8.1.2	Future Quantum Technology Scenarios	308
8.2	Scenario 1: Government Superior and Dominant . . .	309
8.2.1	Winner Take All	310
8.2.2	Strategic Surprise: Cryptanalysis	315
8.2.3	Forged Signatures and Our Legal Realities . . .	322
8.2.4	Attacks on Passwords and Other Authentica- tion Systems	325
8.2.5	Strategic Surprise: Nuclear Weapons	331
8.2.6	Quantum Strategic Surprise: Chemical, Biolog- ical, and Genetic Weapons	332
8.2.7	Strategic Surprise: Remote Sensing	335
8.2.8	Quantum Strategic Surprise: QKD and Quan- tum Internet	339
8.2.9	Quantum Strategic Surprise: Secrecy and Leak- age	341
8.2.10	Countermeasures in a Government-Dominant Scenario: Disruption, Denial, Degradation, De- struction, and Deception	344
8.3	Scenario 2: Public/Private Utopia	347
8.3.1	How Quantum Technologies Could Change Gov- ernance and Law	350
8.3.2	Implications for Human Primacy	355

8.4	Scenario 3: Public/Private, East/West Bloc	361
8.5	Scenario 4: Quantum winter	366
8.6	Conclusion	372
9	A Policy Landscape	375
9.1	Quantum Technology's Policy Impact	376
9.1.1	Game-Changers: Code-Breaking and Possibly Machine Learning	378
9.1.2	Quantum Technology Dominance	379
9.2	Industrial Policy	380
9.2.1	National Quantum Investments outside The US	380
9.2.2	US Quantum Technology Industrial Policy . . .	383
9.2.3	Industrial Policy: Options and Risks	385
9.2.4	Innovation and The Taxpayer	392
9.2.5	The Risk of Choosing Poorly	397
9.3	Education Policy	401
9.3.1	Graduate Training in QIS	401
9.3.2	The Human Capital Challenge	407
9.3.3	Faculty Research Incentives	408
9.4	National Security and Quantum Technologies	411
9.4.1	Export Controls	413
9.4.2	Quantum Technology and Space Law	422
9.4.3	Quantum Technology and Cybersecurity	424
9.5	Quantum Technology and Privacy	426
9.5.1	Secrets and Their Time Value	427
9.5.2	Regulation of Decryption	428
9.5.3	Challenges of Government Power	433
9.5.4	The European Approach to Privacy Rights . .	437
9.6	Quantum Prediction	440
9.6.1	Product development	441
9.6.2	Fairness	443
9.7	Measuring Quantum's Research Output	446
9.7.1	Academic Publications	446
9.7.2	Quantum Technology's Patent Output	451
9.8	Conclusion	454
10	The Quantum Age: Conclusions	457
10.1	Quantum Computing Winter Is a Probable Scenario for 2030	458
10.1.1	Public/Private Scenario	459

10.2	Assessing the Next Decade of Quantum Technologies .	460
10.2.1	Prospects for Quantum Sensing	460
10.2.2	Prospects for Quantum Computing	461
10.2.3	Prospects for Quantum Communications	462
10.3	Law and Policy Priorities for the Quantum Age	464
Appendices		469
A	Introduction to the Quantum Realm	471
A.1	The Quantum World: A Brief Introduction	472
A.2	Terminology, Size, and Frequency	473
A.2.1	The Atom	474
A.2.2	Quantum Sizes	475
A.2.3	Light	477
A.2.4	Quantum Speeds	479
B	Introduction to Quantum Effects	483
B.1	Wave Mechanics	483
B.1.1	Quantum Swirls	484
B.1.2	Light: Newton Thought It Was a Particle . . .	488
B.1.3	Light: It Acts Like a Wave	488
B.1.4	Light: How Can It Possibly Be a Wave?	492
B.2	Quantum Effects 1: Uncertainty	501
B.3	Quantum Effects 2: Polarization	505
B.3.1	Six Experiments with Quantum Polarization .	509
B.4	Quantum Effects 3: Entanglement	513
B.5	Quantum Effects 4: Superposition	517
B.6	The Cat State	522
	Bibliography	525
Index		567
Colophon		577