

Contents

Part I Digital Society

1	Cyber-Attacks Against Critical Infrastructure	3
	Martti Lehto	
1.1	Introduction	3
1.2	Cyber Security Threats Against Critical Infrastructure	6
1.3	Cyber-Attacks Against Critical Infrastructure	13
1.4	Critical Infrastructure Protection	34
1.5	Conclusion	35
	References	36
2	Key Elements of On-Line Cyber Security Exercise and Survey of Learning During the On-Line Cyber Security Exercise	43
	Mika Karjalainen, Tero Kokkonen, and Niko Taari	
2.1	Introduction	43
2.2	Pedagogical Framework for Learning in On-Line Cyber Security Exercises	45
2.3	Methods and Data	46
2.4	Results	50
2.5	Conclusion	54
	References	55
3	Cyber Law and Regulation	59
	Virginia A. Greiman	
3.1	Introduction	59
3.2	Governance of the Internet and Cyberspace	60
3.3	Cyber Operations	65
3.4	Computer Crime Law	67
3.5	Regulations in Cyber Space	69
3.6	Summary	75
	References	76

4	Understanding and Gaining Human Resilience Against Negative Effects of Digitalization	79
	Kirsi M. Helkala and Carsten F. Rønnfeldt	
4.1	Introduction	79
4.2	Human—Part of Information System	80
4.3	Types of Influence	81
4.4	Gaining Individual Resistance	85
4.5	Discussion and Conclusion	88
	References	89
5	Users' Psychopathologies: Impact on Cybercrime Vulnerabilities and Cybersecurity Behavior	93
	Naomi Woods	
5.1	Introduction	93
5.2	Psychopathology and Abnormal Psychology	95
5.3	Online Benefits, Risks, and Security Behavior	97
5.4	Understanding Users' Mental Disorders	102
5.5	Conclusion	129
	References	130
6	Process Ontology Approach to Military Influence Operations	135
	Miika Sartonen, Aki-Mauri Huhtinen, Monika Hanley, and Petteri Simola	
6.1	Introduction	136
6.2	Modern Influence Environment	136
6.3	Psychology of Modern Influence Practices	138
6.4	Influence in Warfare	140
6.5	Military Influence Operations	142
6.6	Process Ontology Approach	143
6.7	Conclusion	145
	References	145
 Part II Critical Infrastructure Protection		
7	Future Smart Societies' Infrastructures and Services in the Cyber Environments	151
	Aarne Hummelholm	
7.1	Introduction	151
7.2	Smart City Communication Infrastructures	157
7.3	Cyber Threats and Risks in the Future Network Environments of Smart Cities	163
7.4	Cyber Threat Risks and the QFD Model	170
7.5	Performing and Modelling Threat Analyses	175
7.6	Conclusions and Future Work	179
	References	181

8	Cyber Security in Healthcare Systems	183
	Martti Lehto, Pekka Neittaanmäki, Jouni Pöyhönen, and Aarne Hummelholm	
8.1	Introduction	183
8.2	Hospital as a Cyberspace	185
8.3	Cybersecurity Risks Related to Hospital Systems	192
8.4	Healthcare Cybersecurity	202
8.5	Conclusion	209
	References	212
9	Cyber Security of an Electric Power System in Critical Infrastructure	217
	Jouni Pöyhönen	
9.1	Introduction	217
9.2	Organization’s Cyber Structure	219
9.3	Main Cyber Security Threats in an Electricity Organization ...	222
9.4	Organization’s Decision-Making Levels and System View	224
9.5	Implementing Measures to Enhance Cyber Trust	228
9.6	Conclusion	237
	References	238
10	Maritime Cybersecurity: Meeting Threats to Globalization’s Great Conveyor	241
	Chris Bronk and Paula deWitte	
10.1	Introduction	241
10.2	Seaborne Commerce and Sea Control: Lessons from the Last Century	242
10.3	Cybersecurity and the Maritime System	243
10.4	Law, the Sea, and Cyberspace	248
10.5	Relevant Public Policy	249
10.6	Conclusion and Prescriptions	252
	References	253
11	Cyberattacks Against Critical Infrastructure Facilities and Corresponding Countermeasures	255
	Petri Vähäkainu, Martti Lehto, and Antti Kariluoto	
11.1	Introduction	255
11.2	Critical Infrastructure and Resilience	257
11.3	Cyber-Physical Systems	260
11.4	Cybersecurity	262
11.5	Artificial Intelligence and Machine Learning	264
11.6	Cyberattacks Against Critical Infrastructure Facilities	267
11.7	Defensive Mechanisms Against Cyberattacks	277
11.8	Conclusion	285
	References	286

12	Saving Lives in a Health Crisis Through the National Cyber Threat Prevention Mechanism Case COVID-19	293
	Jussi Simola	
12.1	Introduction	293
12.2	Problem Formulation	295
12.3	Challenges in the Decision-Making Process with COVID-19	297
12.4	Central Concepts	299
12.5	Previous Works	306
12.6	Findings	306
12.7	Discussion and Conclusions	307
	References	310
13	Information Security Governance in Civil Aviation	315
	Tomi Salmenpää	
13.1	Introduction	315
13.2	Information Security Management in Civil Aviation	320
13.3	Information Security Management Governance in Civil Aviation	323
13.4	Conclusions	334
	References	335
14	Smart Cities and Cyber Security Ethical and Anticipated Ethical Concerns	337
	Richard L. Wilson	
14.1	Introduction	337
14.2	Smart Cities and Cyber Security	339
14.3	Smart Cities and Ethics	340
14.4	Smart Cities, Technology, and Anticipatory Ethics	341
14.5	Technologies Essential to the Development of Smart Cities	342
14.6	Smart Cities and Anticipated Ethical Issues	343
14.7	Smart Cities and Anticipated Cyber Security Risks	344
14.8	Applied Anticipatory Ethics	346
14.9	Rules for Computing Applied Artifacts	346
14.10	Conclusion	350
	References	351
15	TrulyProtect—Virtualization-Based Protection Against Reverse Engineering	353
	Nezer Zaidenberg, Michael Kiperberg, and Amit Resh	
15.1	Introduction	354
15.2	Virtualization in x86 and ARM	354
15.3	Encrypted Code Execution	356
15.4	System Implementation	358
15.5	Related Work	363
15.6	Conclusions	364

References	364
Part III Computational Methods and Applications	
16 Refining Mosca’s Theorem: Risk Management Model for the Quantum Threat Applied to IoT Protocol Security	369
Mikko Kiviharju	
16.1 Introduction	369
16.2 Quantum Computation and C(I)IP	371
16.3 QC Threat Model	372
16.4 IoT Protocols	379
16.5 Cryptographic Primitives in IoT Protocols	382
16.6 QC Threat Assessment for IoT Protocols	388
16.7 Quantum Resilience in IoT	392
16.8 IoT Protocol Risk Assessment	394
16.9 Conclusions	395
References	397
17 Intelligent Solutions for Attack Mitigation in Zero-Trust Environments	403
Mikhail Zolotukhin, Timo Hämäläinen, and Pyry Kotilainen	
17.1 Introduction	403
17.2 Intrusion Detection with Deep Learning	405
17.3 Deep Reinforcement Learning	407
17.4 Traffic Generation	410
17.5 Software-Defined Networking and Network Function Virtualization	411
17.6 Prototype Environment	413
17.7 Conclusion and Future Work	415
References	416
18 Insecure Firmware and Wireless Technologies as “Achilles’ Heel” in Cybersecurity of Cyber-Physical Systems	419
Andrei Costin	
18.1 Introduction	419
18.2 ADS-B in Air Transport	420
18.3 Wireless Firing Systems for Remote Explosives and Robotic Weapons	425
18.4 CCTV for Physical Security	431
18.5 Conclusions	437
References	438
19 Physical Weaponization of a Smartphone by a Third Party	445
Juhani Rauhala	
19.1 Introduction	445
19.2 Remote Destruction of the Smartphone	446
19.3 Categorical Framework for Smartphone Dangers	449

19.4	Nation State as a Bad Actor	452
19.5	Counterfeit Smartphones	453
19.6	Discussion	454
19.7	Conclusion	455
19.8	Appendix: Threat Analysis	455
	References	458
20	Practical Evasion of Red Pill in Modern Computers	461
	Amit Resh, Nezer Zaidenberg, and Michael Kiperberg	
20.1	Introduction	461
20.2	Background	462
20.3	Local Red Pills	467
20.4	Conclusion	472
	References	473
21	Malware Analysis	475
	Michael Kiperberg, Amit Resh, and Nezer Zaidenberg	
21.1	Introduction	475
21.2	Static Analysis	476
21.3	Dynamic Analysis	478
21.4	Conclusion	482
	References	482