

Contents

1	Opening Remarks: Hacking and Digital Dissidence.....	1
1.1	Using Computers for the Pursuit of Political and Social Changes and for the Benefit of All Mankind	1
1.2	From Early Hackers to Digital Resistance Activities	5
1.3	The So-Called <i>Twitter Revolutions</i>	7
1.4	The Worldwide Scenario, and Some Preliminary Interpretative Questions	9
	References.....	22
2	Digital Resistance, Digital Liberties and Digital Transparency	27
2.1	A Preliminary Definition of <i>Digital Resistance</i> and <i>Digital Liberties</i>	27
2.1.1	Some Focal Aspects of Digital Dissidence	27
2.1.2	Preliminary Legal and Political Remarks	28
2.1.3	The Power of Technology in Critical Contexts and the New Public Sphere	30
2.2	The Fundamental Role of a Secure (and Peer-Reviewed) Liberation Technology: The <i>Haystack</i> Case-History.....	32
2.3	Two Key Aspects of Digital Resistance Activities, and Several Case Studies	36
2.3.1	The Key Aspects of Dissident Activities	36
2.3.2	Digital Resistance Case-Studies.....	41
2.4	Open Government, Collaborative Transparency and Civic Hacking as a Form of Digital Resistance	47
2.4.1	The Idea of Government as a Platform for Transparency.....	47
2.4.2	The Metaphor of Government 2.0 and the Idea of Collaborative Transparency	49

2.4.3	Citizen Engagement for the Oversight of Political Activity	51
2.4.4	Collaborative Mapping and Digital Resistance.....	59
	References.....	68
3	Hacking and Digital Dissidence Activities	73
3.1	The Role of Hackers in the Landscape of Digital Resistance.....	73
3.2	A First Analysis of Common Threats to Digital Freedom and to Hacker Activities	74
3.3	Being a Hacker in This Framework	76
3.3.1	Thinking Like a Hacker	76
3.3.2	State Antagonism, Fear and Violence.....	79
3.4	A Brand New Playground.....	81
3.4.1	Liberation Technologies.....	81
3.4.2	Anonymity and Bloggers' Rights	84
3.4.3	Innovation	86
3.4.4	Intellectual Property and Privacy	86
3.4.5	EPIC Activities in the Field of Privacy	88
3.4.6	Transparency	89
3.5	A New Perspective on Hacking	90
3.5.1	The Essence of hacking	90
3.5.2	The Hacker Spirit and Some Lessons from the Ushahidi Project.....	91
3.5.3	A New Breed of Hackers	94
3.6	The <i>Do-It-Yourself</i> Approach.....	97
3.7	The Hacker Ethic	99
3.8	Hacking and Crime	101
3.9	Threats to Hackers	105
3.9.1	The EFF Report Unintended Consequences	105
3.9.2	Some Significant Recent Legal Cases: Cease-and-Desist Actions	106
3.10	Hacking Electronic Voting Machines for the Purpose of Transparency	117
	References.....	122
4	Digital Resistance, Digital Liberties and Human Rights.....	125
4.1	Internet and Human Rights	125
4.2	Internet and the <i>Universal Declaration of Human Rights</i>	130
4.3	The Council of Europe and the Human Rights Guidelines for Internet Service Providers: The Role of ISPs in Human Rights Environments and Protection.....	133
4.4	The WSIS Declaration of Principles.....	134
4.5	The 2011 United Nations Report on the Promotion and Protection of the Right to Freedom of Opinion and Expression	137
4.6	A Charter of Human Rights and Principles for the Internet	144

4.7	The “Bill of Rights” Projects	152
4.7.1	The Internet Bill of Rights Drafted within the IGF Works.....	152
4.7.2	The Internet Rights and Principles Dynamic Coalition Bill of Rights.....	154
4.7.3	A Bill of Rights in Cyberspace	155
4.7.4	The EFF Bill of Privacy Rights for <i>Social Network Users</i>	156
4.8	A Human Rights Approach to the Mobile Internet.....	157
4.9	The Relationship Between Human Rights and Technology Sales to Oppressive Regimes	159
	References.....	159
5	The Use of Liberation Technology	161
5.1	Technical Resistance Tactics.....	161
5.2	Surveillance Self-Defense or Self-Defense Against Surveillance and Monitoring.....	167
5.3	A Recent Circumvention Tool Usage Report	169
5.4	Tools and Guides.....	171
5.4.1	Leaping Over the Firewall: A Review of Censorship Circumvention Tools by <i>Freedom House</i>	171
5.4.2	Ten Fundamental Aspects of a Typical Liberation Technology Tool	176
5.4.3	An Interesting (Comparative) Article on Real Anonymity of VPN Systems Users	180
	References.....	184
6	Digital Activism, Internet Control, Transparency, Censorship, Surveillance and Human Rights: An International Perspective	187
6.1	An Introductory Overview	187
6.1.1	The Global OpenNet Initiative Analysis.....	187
6.1.2	Techniques and Tools Commonly Used to Censor	201
6.2	An Analysis of Several Countries with Critical Human Rights Issues.....	203
6.2.1	Burma: Internet and Human Rights in a Particular Technological, Political and Legal Framework	203
6.2.2	Cuba: Internet Control, User Restrictions, Legal and Regulatory Frameworks, Blogosphere, Digital Dissidents and Civil Society	214
6.2.3	South Korea: Digital Resistance Issues	227
6.2.4	Saudi Arabia: The Digital Liberties Landscape.....	230
6.2.5	Syria: Digital Liberties Issues	233
6.2.6	Iran: Internet and Digital Liberties Issues.....	239
6.2.7	China: The Internet and Types and Levels of Chinese Internet Censorship.....	247

6.2.8	Turkmenistan: Censorship and Control	259
6.2.9	Uzbekistan: Internet, Censorship and Surveillance	262
6.2.10	Vietnam: Digital Resistance and Censorship	269
6.2.11	Australia: Internet Filtering Policies, Digital Liberties and Circumvention Tools	273
6.2.12	Iceland: Digital Resistance Issues and Freedom of Information	279
6.2.13	India: Freedom of Speech, Freedom of Information and Electronic Censorship	283
6.2.14	Russia. Internet and Human Rights: Political and Technological Frameworks	290
6.2.15	North Korea: The Main Digital Liberties Issues.....	295
6.3	Revolts and Digital Dissidence in Egypt and Tunisia: Where It All Began	301
6.3.1	A Brief Summary of Digital Dissidence in Egypt	301
6.3.2	A Brief Summary of Digital Dissidence in Tunisia.....	303
	References.....	304
7	Conclusions: The Landscape of Digital Liberties and the Future.....	309
7.1	Human Rights in the Digital Era and the Role of Law	309
7.2	Technology as an <i>Antibody</i>	311
7.3	The Technological Scenario.....	313
7.4	The Relationships Between Hacking and Digital Resistance.....	314
	References.....	315
	Author Index.....	317
	Subject Index.....	321