

Table of Contents

Introduction	xi
Chapter 1. Canada’s Cyber Security Policy: a Tortuous Path	
Toward a Cyber Security Strategy	1
Hugo LOISEAU and Lina LEMAY	
1.1. Introduction	1
1.2. Canada in North America: sovereign but subordinate?	4
1.3. Counter-terrorism for the improvement of national security	13
1.4. The long path to a national CI protection strategy and national cyber security strategy.	25
1.5. The adoption of the current strategies for CI protection and cyber security	31
1.6. Conclusion	37
1.7. Bibliography	38
1.7.1. Scientific and media articles	39
1.7.2. Primary Data	40
1.7.3. Websites	44
Chapter 2. Cuba: Towards an Active Cyber-defense	45
Daniel VENTRE	
2.1. Cyberspace: statistics and history	47
2.1.1. The marginalization of Cuba.	47
2.1.2. Cuban cyberspace as the target of attacks	50
2.2. Theoretical and practical considerations on information warfare and cyber-warfare	54
2.2.1. Development of capabilities	54
2.3. Cyber-warfare theories and practices	56
2.3.1. Fidel Castro’s discourse	57

2.3.2. The concept of active cyber-defense	59
2.4. Regulations and ways around them	60
2.4.1. The State's influence over cyberspace	61
2.4.2. Getting around the restrictions.	63
2.5. Capabilities of control, surveillance and interception	65
2.6. Enemies	66
2.7. Conclusion	70
2.8. Bibliography	73
Chapter 3. French Perspectives on Cyber-conflict	77
Daniel VENTRE	
3.1. Cyberspace.	79
3.2. Assessments, view on the world and awakening	88
3.2.1. Attacks.	88
3.2.2. The feeling of insecurity, the threat.	93
3.2.3. Potential vulnerabilities of States	98
3.2.4. Evolution of the international environment	99
3.3. Reaction, position of France and choice: theories, political strategies and military doctrines	100
3.3.1. Information: a powerful weapon for those controlling it	100
3.3.2. Media information: beneficial if controlled	101
3.3.3. Economic information as power, if controlled	101
3.3.4. Information warfare	102
3.3.5. Information warfare or information control	103
3.3.6. The ANSSI	104
3.3.7. Cyber-security and cyber-defense.	106
3.3.8. Army: Information operations, NEB (numérisation de l'espace de bataille/digitization of battlespace), info-development	108
3.3.9. Cyber-war and other modalities of the cyber-conflict	120
3.4. Conclusion	127
3.5. Bibliography	131
Chapter 4. Digital Sparta: Information Operations and Cyber-warfare in Greece	135
Joseph FITSANAKIS	
4.1. Geopolitical significance	136
4.2. Strategic concerns and internal balancing	139
4.3. Formative experiences in information operations: the Ergenekon conspiracy	141
4.4. Formative experiences in information operations: intensifying cyber-attacks.	142

4.5. Formative experiences in information operations: the Öcalan affair	143
4.6. Formative experiences in information operations: the Greek wiretapping case of 2004–2005.	145
4.7. Emerging civilian information operations strategies	148
4.8. Emerging military information operations strategies	152
4.9. The European Union dimension in Greek information operations	155
4.10. Conclusion	156
4.11. Bibliography	158
Chapter 5. Moving Toward an Italian Cyber Defense and Security Strategy	165
Stefania DUCCI	
5.1. Information warfare and cyber warfare: what are they?	165
5.2. Understanding the current Italian geopolitical context	168
5.3. The Italian legal and organizational framework	172
5.4. The need for a national cyber-defense and -security strategy	177
5.5. Conclusion	188
5.6. Bibliography	188
Chapter 6. Cyberspace in Japan’s New Defense Strategy.	193
Daniel VENTRE	
6.1. Japan’s defense policy	194
6.2. Cyberspace in Japan’s defense strategy.	197
6.2.1. The context	197
6.2.2. Cyberspace in security and defense policies	203
6.3. Conclusion	217
6.4. Bibliography	221
Chapter 7. Singapore’s Encounter with Information Warfare: Filtering Electronic Globalization and Military Enhancements	223
Alan CHONG	
7.1. Singapore: electronic globalization and its pitfalls	225
7.2. Cyberdefence in the private sector and society at large	228
7.3. The Singapore Armed Forces and the embrace of third-generation warfare	235
7.3.1. Force multiplication	237
7.3.2. Continually revitalizing existing conventional arms capabilities	239
7.3.3. Generating asymmetrical advantages in operational transparency	242

7.4. Conclusion	245
7.5. Bibliography	247
Chapter 8. A Slovenian Perspective on Cyber Warfare	251
Gorazd PRAPROTNIK, Iztok PODBREGAR, Igor BERNIK and Bojan TIČAR	
8.1. Introduction	251
8.2. Preparations for digital warfare	254
8.3. Specifics of technologically-advanced small countries.	256
8.4. Geostrategic, geopolitics and the economic position of the Republic of Slovenia.	258
8.5. Information and communication development in Slovenia	259
8.6. Cyber-threats in Slovenia	261
8.7. Slovenia in the field of information and communication security policy	264
8.8. Slovenia's information and communication security policy strategy	266
8.8.1. The EU information and communication security policy	266
8.8.2. NATO's information and communications security policy.	267
8.8.3. Slovenia's information and communication security policy	268
8.8.4. Analysis of key strategic documents regulating the field of information and communication security policy in the Republic of Slovenia	269
8.8.5. National bodies that govern the field of information and communication security policy in the Republic of Slovenia	270
8.8.6. Directorate for information society (Ministry of Higher Education, Science and Technology)	271
8.8.7. Slovenian Computer Emergency Response Team	271
8.8.8. Directorate of e-Government and Administrative Processes (Ministry of Public Administration)	272
8.8.9. Office of the Government of the Republic of Slovenia for the Protection of Classified Information	272
8.8.10. Slovenian Intelligence and Security Agency	273
8.8.11. National Center for Crisis Management	274
8.9. Conclusion	274
8.10. Bibliography	276
Chapter 9. A South African Perspective on Information Warfare and Cyber Warfare	279
Brett VAN NIEKERK and Manoj MAHARAJ	
9.1. The South African structure of information warfare	280
9.2. A South African perspective on cyber-warfare	283
9.3. The Southern African cyber-environment	284

9.4. Legislation	288
9.5. Cyber-security and information warfare organizations in South Africa	289
9.6. Estimated cyber-warfare capability in Africa	290
9.7. Conclusion	291
9.8. Bibliography	292
Chapter 10. Conclusion	297
Daniel VENTRE	
10.1. Cyberspace	301
10.2. Bibliography	306
List of Authors	307
Index	309