

# Contents

<b>Botnets, Cybercrime and National Security</b> . . . . .	<b>1</b>
<i>Heli Tiirmaa-Klaar</i>	
1 Introduction . . . . .	1
2 Botnets as a Global Challenge for Industry, Governments and Individual Computer Users . . . . .	3
2.1 Botnets as an Awareness Issue . . . . .	4
2.2 Botnets as a Legal and Organisational Issue . . . . .	5
2.3 Botnets as a Side-Effect of Fast-Growing Internet Economy . . . . .	5
2.4 Botnets as a Global Cooperation Issue. . . . .	6
3 Botnets and Cybercrime . . . . .	8
3.1 Botnets Attacking Financial Services. . . . .	8
3.2 Spam Providing Botnets. . . . .	9
3.3 Extortion DDOS Attacks Against E-commerce and Critical Companies . . . . .	10
3.4 Conficker . . . . .	10
3.5 Patterns of Botnet Activity Moving Outside Europe and the U.S. . . . .	11
3.6 Botnets in Mobile Devices . . . . .	11
4 Botnets and National Security . . . . .	12
4.1 Cyber Espionage Against Governments and Companies . . . .	13
4.2 Botnets Used in Active Political Campaigns or in Conflicts . . . . .	15
4.3 Case Study of Estonia: Botnets Facilitating Digital Siege of a Country . . . . .	16
4.4 Georgia 2008: Cyber Attacks Facilitating Strategic Goals in Kinetic War . . . . .	20
4.5 Strategic Implications of Using Botnets in Modern Conflicts . . . . .	21
5 National Policies and Organisational Measures to Address Cyber Threats . . . . .	22
5.1 Strategic Vision and a Balanced Regulatory Approach for National Cyber Resilience . . . . .	23

5.2	National and International Requirements for Investigation of Cybercrime . . . . .	26
5.3	Focus on Internet Service Providers . . . . .	27
5.4	Examples of Existing Anti-Botnet Initiatives . . . . .	29
6	International Cooperation and Capacity Building as Cornerstone for Better Global Cybersecurity . . . . .	30
6.1	The Overview of International Initiatives to Address Cyber Threats and Cybercrime . . . . .	30
6.2	International Capacity Building to Address Cyber Threats and Cybercrime . . . . .	34
6.3	Conclusion . . . . .	37
	References . . . . .	38
	<b>Botnets: How to Fight the Ever-Growing Threat on a Technical Level . . .</b>	<b>41</b>
	<i>Jan Gassen, Elmar Gerhards-Padilla and Peter Martini</i>	
1	Introduction . . . . .	41
2	Fundamentals . . . . .	45
2.1	Malware . . . . .	46
2.2	Botnets . . . . .	48
3	Botnets: The Current Situation . . . . .	57
4	Analyzing the Threat . . . . .	59
4.1	Detecting . . . . .	60
4.2	Analyzing . . . . .	68
4.3	Tracking . . . . .	72
4.4	Measuring . . . . .	74
5	Fighting Botnets . . . . .	79
5.1	Prevent New Infections . . . . .	79
5.2	Mitigate Existing Botnets . . . . .	83
5.3	Minimizing Profit . . . . .	88
6	Botnets: The Way Ahead . . . . .	91
6.1	Future Trends . . . . .	92
6.2	Conclusion . . . . .	94
	References . . . . .	95

Botnets

Tiirmaa-Klaar, H.; Gassen, J.; Gerhards-Padilla, E.;  
Martini, P.

2013, VIII, 97 p. 5 illus., Softcover

ISBN: 978-1-4471-5215-6