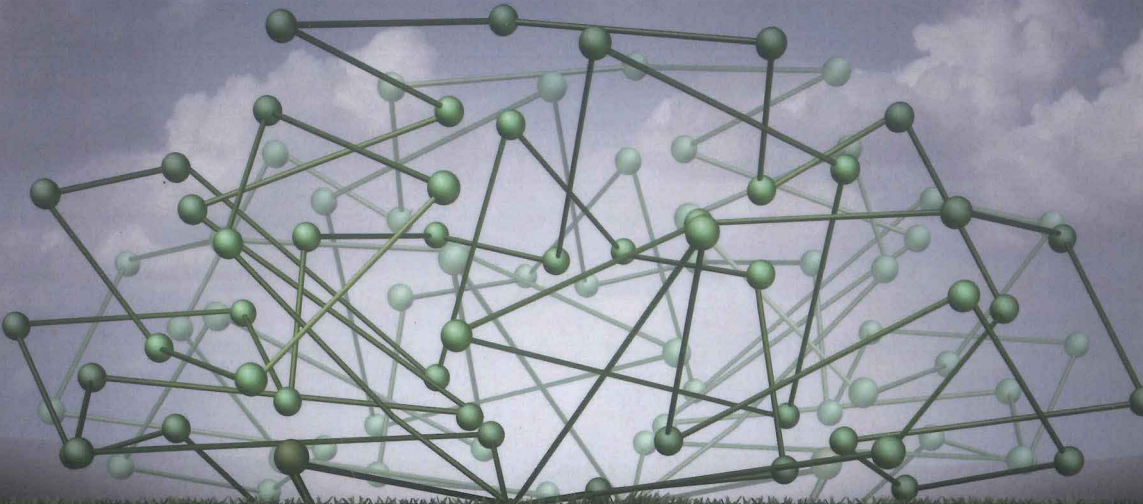


Rutger Leukfeldt



Cybercriminal networks

Origin, growth and criminal capabilities



eleven
international publishing

สำนักหอสมุดมหาวิทยาลัยเชียงใหม่

pbk
2,101.50
.b 164769.79
o 1242401
i 22685459

CYBERCRIMINAL NETWORKS

ORIGIN, GROWTH AND CRIMINAL CAPABILITIES

E.R. LEUKFELDT



eleven
international publishing

Contents

1. Introduction.....	1
1.1 Background	1
1.2 Research questions	2
1.3 Data and methods	3
1.4 Outline for dissertation.....	7

PART I: THEORY

2. Cybercrime, social opportunity structures and routine activity theory ..	11
2.1 Introduction	11
2.2 Cybercrime and social opportunity structures	12
2.3 Cybercrime and routine activity theory	20
2.4 Theoretical model of social opportunity structures and routine activities	29

PART II: CYBERCRIMINAL NETWORKS

3. Cybercrime and social ties	37
3.1 Introduction	37
3.2 Data and methods	39
3.3 Phishing: the Amsterdam case	40
3.4 Similarities and differences between the case reported by Soudijn and Zegers and the Amsterdam case.....	48
3.5 Opportunities for situational crime prevention.....	50
3.6 Conclusion and discussion	53
4. Social ties versus digital ties within cybercriminal networks.....	57
4.1 Introduction	57
4.2 (Cyber)criminal networks and social opportunity structures	58
4.3 Data and methods.....	61
4.4 Empirical results.....	63
4.5 Discussion and conclusion	73

5. A taxonomy of cybercriminal networks.....	77
5.1 Introduction.....	77
5.2 Social opportunity structures.....	78
5.3 Data and methods.....	79
5.4 Criminal opportunities.....	81
5.5 Mapping the networks.....	85
5.6 Taxonomy.....	90
5.7 Conclusion and discussion.....	92
6. Origin, growth and criminal capabilities of cybercriminal networks	95
6.1 Introduction.....	95
6.2 Prior empirical research in the Netherlands.....	96
6.3 Data and methods.....	99
6.4 Results.....	100
6.5 Conclusion and discussion.....	106
7. Money mules.....	111
7.1 Introduction.....	111
7.2 Prior empirical research on cybercriminal networks and money mules.....	112
7.3 Data and methods.....	115
7.4 Results.....	116
7.5 Conclusion and discussion.....	120

PART III: SUITABLE TARGETS

8. Suitable targets for phishing.....	127
8.1 Introduction.....	127
8.2 Suitable targets: expectations based on routine activity theory.....	128
8.3 Data and methods.....	131
8.4 Suitable targets: risk factors.....	131
8.5 Discussion: opportunities for crime prevention.....	134
9. Suitable targets for phishing and malware compared.....	137
9.1 Introduction.....	137
9.2 Suitable targets: expectations based on routine activity theory.....	139

9.3 Data and methods.....	141
9.4 Suitable targets: risk factors compared.....	142
9.5 Conclusion and discussion	146
10. An in-depth analysis of suitable targets	149
10.1 Introduction.....	149
10.2 Theoretical background.....	150
10.3 Methods.....	152
10.4 Results	153
10.5 Conclusion and discussion	158

PART IV: CONCLUSION AND DISCUSSION

11. Conclusion and discussion.....	165
11.1 Introduction	165
11.2 What are the processes of origin and growth of the cybercriminal networks?	166
11.3 What is the structure of cybercriminal networks?	167
11.4 What is the modus operandi of cybercriminal networks?	169
11.5 Who are suitable targets for cybercriminal networks?	173
11.6 Theoretical implications	175
11.7 Practical implications: possibilities for situational crime prevention..	178
11.8 Research limitations and future research directions.....	183
Summary	187
Samenvatting.....	193
References.....	201
Appendix 1: Definitions.....	213
Appendix 2: Analytical framework cybercriminal networks	217
Appendix 3: Informed consent study into cybercriminal networks	223
Acknowledgements	225
Curriculum vitae.....	227
Publications	229