Contents

I. Introduction

The project team 1

1 Background 2

2 Project objectives and research questions 3

3 Definitions 4

4 Methodology 7
4.1 Literature review 9
4.2 Empirical data collection 10
4.3 Common checklist 11
4.4 Common analysing system 12

II. Cyber-OC in the Netherlands

G. Odinot, M.A. Verhoeven, R.L.D. Pool, C.J. de Poot 15

1 Organisation of investigation and prosecution in the Netherlands . 16
1.1 Criminal investigation of cybercrime in the Netherlands . . . 18
1.2 Legal framework on cybercrime in the Netherlands 23

2 Methodology 33
2.1 Selection of Dutch cases 33
2.2 Information available in police files 34
2.3 Interviews with experts 34

3 General description of the Dutch sample 35

4 Empirical findings 38
4.1 Suspect characteristics 38
4.2 Activities and modi operandi in the field of Cyber-OC 45
4.3 Collaboration and organisation 57
4.4 Damage of Cyber-OC 63
4.5 Criminal investigation of Cyber-OC 64

5 Concluding remarks for the Netherlands 88

6 References 95

III. Cyber-OC in Sweden

Y. Werner, L. Korsell 101

1 Context information 103
- 1.1 The character of cybercrime in Sweden 103
- 1.2 Development over time 103
- 1.3 Swedish penal legislation 104
- 1.4 Statistics 105
- 1.5 Political agenda 107
- 1.6 The police organisation 108
- 1.7 Measures by the police 109

2 Methodology 110
- 2.1 Selection of cases 110
- 2.2 Information available in police or prosecution files 110
- 2.3 Expert interviews 111
- 2.4 The cases 111

3 General description of the Swedish sample 112
- 3.1 Visible characteristics 112
- 3.2 Invisible characteristics 114
- 3.3 Typology 115

4 Empirical findings 118
- 4.1 Characteristics of suspects and groups in Cyber-OC 119
- 4.2 Activities and modi operandi in the field of Cyber-OC 127
- 4.3 External cooperation in the field of Cyber-OC 134
- 4.4 Summary suspects, groups, modi operandi and cooperation . 137
- 4.5 Damage of Cyber-OC 138
- 4.6 Criminal investigation of Cyber-OC 140

5 Concluding remarks for Sweden 155
- 5.1 Involvement of OC in cybercrime 155
- 5.2 Using the internet to commit offline OC 157
- 5.3 Windows of opportunity for OC groups 157
- 5.4 Structural changes in OC 159
- 5.5 The organisation of cybercrime 160
- 5.6 Recommendations 160

6 References 162

IV. Cyber-OC in Germany

G. Bulanova-Hristova, K. Kasper 165

1 Context information 167

2 Methodology 169
- 2.1 First inquiry – focus on criminal groups 170
- 2.2 Second inquiry – focus on cybercrime 171
- 2.3 Sampling 172

3 General description of the reported criminal investigations 173
- 3.1 Activity fields 174
- 3.2 Suspects and damage 175

4 Empirical findings 177
- 4.1 Overview of the sample 177
- 4.2 Group categorisation 178
- 4.3 Determination of the group membership 180
- 4.4 Summary of the analysed investigations 181
- 4.5 Characteristics of Cyber-OC suspects 185
- 4.6 Characteristics of Cyber-OC groups 195
- 4.7 Activities and modi operandi in the field of Cyber-OC 205
- 4.8 Damage of Cyber-OC 206
- 4.9 Investigative measures in the analysed Cyber-OC cases 212

5 Concluding remarks for Germany 213
- 5.1 Answers to the research questions 213
- 5.2 Key findings of the German case study 216

6 References 217

V. Concluding remarks from the three case studies

The project team 221

Theme 1: Organised crime groups entering cyberspace 223

Theme 2: Structure and organisation 224

Theme 3: Trust 226

Theme 4: Cyberspace and cyber logistics 228

Theme 5: Initiation of crimes and crime groups 229

Theme 6: New windows of opportunity 231
Theme 7: Long-term activities 232
Theme 8: The term ‘organised crime’ 234
Final remark 236

VI. Appendix – Literature review

Dorothee Dietrich, Karsten Kasper, Gergana Bulanova-Hristova . . . 239

Figures and Tables

Figure 1: Suspects by primary role 38
Figure 2: Suspects by age 40
Figure 3: Suspects with criminal history 41
Figure 4: Criminal history of suspects 42
Figure 5: Reported crimes 106
Figure 6: Hierarchic group structure 121
Figure 7: Network of clusters 125
Figure 8: Division of criminal investigations into cybercrime in a narrow/broad sense (N = 128) 174
Figure 9: Distribution of the criminal investigations to different crime areas (N = 128) 175
Figure 10: Distribution of criminal investigations according to area of crime (N = 18) 177
Figure 11: Matrix of group categories in Cyber-OC 178
Figure 12: All identified suspects per group 185
Figure 13: Number of core group members in comparison with total suspects (categories 1 and 2) 186
Figure 14: Distribution of gender (all identified suspects) 187
Figure 15: All identified suspects by age 188
Figure 16: Average age of suspect categories 189

Figure 17: Distribution of suspects according to age classes 190
Figure 18: Average age per group 191
Figure 19: Cyber-OC groups with a homogeneous core group (n = 9) 193
Figure 20: Formation process of cyber-entering groups 197
Figure 21: Formation process of offlineborn groups 198
Figure 22: Formation process of cyberborn groups 199
Figure 23: composition of core groups and peripheries of selected groups 201
Figure 24: Example of hierarchic group structure 202
Figure 25: Financial damage in the analysed Cyber-OC cases 208

Table 1: Public Security Agenda objectives 20
Table 2: Reported crimes 105
Table 3: Law enforcement and related authorities in Sweden 107
Table 4: Analysed cases 111
Table 5: Summary of group characteristics 137
Table 6: Offline groups entering cybercrime 181
Table 7: Offlineborn groups 182
Table 8: Cyberborn groups 184
Table 9: Characteristics of Cyber-OC groups – summary 204
Table 10: Immaterial damage caused by Cyber-OC groups 209