Contents

Abstract

Preface

Acknowledgements

Chapter 1 Introduction and Objectives 1

1.1 Introduction *3*

1.2 Objectives of the thesis *4*

Chapter 2 State-of-the-art Technology 5

2.1 Cyber Defence Situation Awareness. *7*

2.1.1 Situation Awareness Assessment *8*

2.2 Research and Technology Challenges *13*

2.2.1 Human Factors *13*

Chapter 3 Description of technology modules and components 17

3.1 CySA Technology Demonstrators *19*

3.1.1 ARMOUR *19*

3.1.2 PANOPTESEC *20*

3.2 Visualisation *21*

3.2.1 A multi-aspect three-dimensional operational picture *22*

Chapter 4 Design and Implementation of a proposed Architecture 33

4.1. The Next Generation Cognitive Computing Security Operations Center *35*

4.1.1 Network Flow Forensics *36*

4.1.1.1 Configuration of the NF3 Ensemble model *43*

4.1.2 Adaptive Analytical λ-Architecture in support of cyberdefence *45*

4.1.2.1 Configuration of the λ-NF3 model *47*

Chapter 5 Architecture validation and experimentation 51

5.1 Architecture Validation *53*

5.1.1 Results of the NF3 Ensemble model and discussion *53*

5.1.2 Results of the λ-NF3 model and discussion *59*

5.2 Verification and Validation (V&V) Framework to evaluate CySA *64*

5.2.1 Hypothesis and Research Questions *66*

5.2.2 V&V Model *68*

5.2.3 Proposal´s and Research´s constraints *69*
5.2.4 Initial Risk Analysis of the research findings *70*
5.2.5 Support to Decision Making *70*
5.2.6 User acceptance *71*
5.3 Research on Datasets for operationalising a mission-centric CySA *73*
Chapter 6 Enabling techniques for Decision Support Systems 79
6.1 Autonomous Intelligence Cyber Defence Agents (AICA) *81*
6.1.1 Artificial intelligence and cyber defence *83*
6.1.2 Intelligent and autonomous agents in cyberspace *87*
Chapter 7 Conclusions and future work 93
7.1 Conclusions *95*
7.1.1 Conclusions of the NF3 machine learning models *96*
7.2 Future Work *97*
7.2.1 Discussion on future research initiatives with regards to NF3 models *97*
Table of Figures 100
Table List 101
References 102