2014 6th International Conference in Cyber Conflict Proceedings

(CyCon 2014)

Tallinn, Estonia
3 – 6 June 2014
# TABLE OF CONTENTS

Introduction 1

**Chapter 1. Active Cyber Defense: Concepts, Policy, and Legal Implications** 5

The “Triptych of Cyber Security”: A Classification of Active Cyber Defence  
*Robert S. Dewar* 7

Socio-Political Effects of Active Cyber Defence Measures  
*Keir Giles and Kim Hartmann* 23

The Drawbacks and Dangers of Active Defense  
*Oona A. Hathaway* 39

Artificial (Intelligent) Agents and Active Cyber Defence: Policy Implications  
*Caitríona H. Heinl* 53

**Chapter 2. Models of Active Cyber Defense** 69

Malware is called malicious for a reason: The risks of weaponizing code  
*Stephen Cobb and Andrew Lee* 71

Changing the game: The art of deceiving sophisticated attackers  
*Oscar Serrano Serrano, Bart Vanautgaerden and Nikolaos Virvilis-Kollitiris* 87

The Deployment of Attribution Agnostic Cyberdefense Constructs  
and Internally Based Cyberthreat Countermeasures  
*Jason Rivera and Forrest Hare* 99

**Chapter 3. Cyber Situational Awareness** 119

Dynamic Cyber-Incident Response  
*Kevin Mepham, Panos Louvieris, Gheorghita Ghinea and Natalie Clewley* 121

Beyond technical data - a more comprehensive  
Situational Awareness fed by available Intelligence Information  
*Andreas Kornmaier and Fabrice Jaouën* 139

Situational awareness and information collection from critical infrastructure  
*Jussi Timonen, Lauri Lääperi, Lauri Rummukainen, Samir Puuska and Jouko Vankka* 157

Operational Data Classes for Establishing Situational Awareness in Cyberspace  
*Judson Dressler, Calvert L. Bowen, III, William Moody, Jason Koepke* 175
Chapter 4. Detection and Deception

Towards Multi-layered Intrusion Detection in High-Speed Backbone Networks
Mario Golling, Rick Hofstede and Robert Koch

Detecting and Defeating Advanced Man-In-The-Middle Attacks against TLS
Enrique de La Hoz, Rafael Paez-Reyes, Gary Cochrane, Iván Marsa-Maestre, Jose Manuel Moreira-Lemus and Bernardo Alarcos

Inter-AS Routing Anomalies: Improved Detection and Classification
Matthias Wübbeling, Till Elsner and Michael Meier

Elastic Deep Packet Inspection
Bruce W. Watson

An Automated Bot Detection System through Honeypots for Large-Scale
Fatih Haltaş, Erkam Uzun, Necati Şişeci, Abdulkadir Poşul and Bâkır Emre

Botnet over Tor: The Illusion of Hiding
Matteo Casenove and Armando Miraglia

Chapter 5. Cyber Operational Activities

Key Terrain in Cyberspace: Seeking the High Ground
David Raymond, Tom Cross, Gregory Conti, Michael Nowatkowski

Fighting Power, Targeting and Cyber Operations
Paul Ducheine and Jelle van Haaster

Cyber Fratricide
Samuel Liles and Jacob Kambic

Biographies