2014 6th International Conference in Cyber Conflict Proceedings

(CyCon 2014)

Tallinn, Estonia
3 – 6 June 2014

IEEE Catalog Number: CFP1426N-POD
ISBN: 978-1-4799-5113-0

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 7
Robert S. Dewar

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

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

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

Chapter 2. Models of Active Cyber Defense 69

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

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

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

Chapter 3. Cyber Situational Awareness 119

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

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

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

Operational Data Classes for Establishing Situational Awareness in Cyberspace 175
Judson Dressler, Calvert L. Bowen, III, William Moody, Jason Koepke

Chapter 4. Detection and Deception 189

Towards Multi-layered Intrusion Detection in High-Speed Backbone Networks 191
Mario Golling, Rick Hofstede and Robert Koch

Detecting and Defeating Advanced Man-In-The-Middle Attacks against TLS 209
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 223
Matthias Wübbeling, Till Elsner and Michael Meier

Elastic Deep Packet Inspection 241
Bruce W. Watson

An Automated Bot Detection System through Honeypots for Large-Scale 255
Fatih Haltaş, Erkam Uzun, Necati Şişeci, Abdulkadir Poşul and Bâkır Emre

Botnet over Tor: The Illusion of Hiding 273
Matteo Casenove and Armando Miraglia

Chapter 5. Cyber Operational Activities 285

Key Terrain in Cyberspace: Seeking the High Ground 287
David Raymond, Tom Cross, Gregory Conti, Michael Nowatkowski

Fighting Power, Targeting and Cyber Operations 303
Paul Ducheine and Jelle van Haaster

Cyber Fratricide 329
Samuel Liles and Jacob Kambic

Biographies 341