

# **2013 5th International Conference on Cyber Conflict**

**(CYCON 2013)**

**Tallinn, Estonia  
4 – 7 June 2013**



**IEEE Catalog Number: CFP1326N-POD  
ISBN: 978-1-4799-0450-1**

# Contents

Introduction

## **Chapter 1. Cyber Space – Automatic Information Sharing and Access**

Towards Improved Cyber Security Information Sharing	1
<i>Luc Dandurand, Oscar Serrano Serrano</i>	
Deriving Behavior Primitives from Aggregate Network Features using Support Vector Machines	17
<i>Owen McCusker, Scott Brunza, Dipankar Dasgupta</i>	
Context-based Access Control Model for Smart Space	35
<i>Alexander Smirnov, Alexey Kashevnik, Nikolay Shilov, Nikolay Teslya</i>	
Information Sharing Models for Cooperative Cyber Defence	50
<i>Jorge L. Hernandez-Ardieta, Juan E. Tapiador, Guillermo Suarez-Tangil</i>	

## **Chapter 2. Attack Modeling – Washing Away the Borders between Cyber and Kinetic Attacks**

The Vulnerability of UAVs to Cyber Attacks - An Approach to the Risk Assessment	78
<i>Kim Hartmann, Christoph Steup</i>	
A Cyber Attack Modeling and Impact Assessment Framework	101
<i>Igor Kotenko, Andrey Chechulin</i>	
Exploring the Prudent Limits of Automated Cyber Attack	125
<i>Jeffrey L. Caton</i>	
The Dawn of Kinetic Cyber	141
<i>Scott D. Applegate</i>	

## **Chapter 3. Cyber Attack Threat Assessment and Impact Propagation**

A Control Measure Framework to Limit Collateral Damage and Propagation of Cyber Weapons	156
<i>David Raymond, Gregory Conti, Tom Cross, Robert Fanelli</i>	
A Baseline Study of Potentially Malicious Activity Across Five Network Telescopes	172
<i>Barry Irwin</i>	
Illicit Network Structures in Cyberspace	189
<i>Kaarel Kalm</i>	
Threat Implications of the Internet of Things	202
<i>Michael J. Covington, Rush Carskadden</i>	

Cyber Deception and Autonomous Attack – Is There a Legal Problem? <i>William Boothby</i>	214
Legal Aspects of a Cyber Immune System <i>Janine S. Hiller</i>	231
Towards a Cyber Common Operating Picture <i>Gregory Conti, John Nelson, David Raymond</i>	246

#### **Chapter 4. Cyber Command – Towards Automatic Operations**

Complexity and Emergence in Ultra-Tactical Cyberspace Operations <i>Jeffrey L. Caton</i>	263
Patterns of a Cooperative Malware Analysis Workflow <i>Daniel Plohmann, Sebastian Eschweiler, Elmar Gerhards-Padilla</i>	277
Architecture for Evaluating and Correlating NIDS in Real - World Networks <i>Robert Koch, Mario Golling</i>	295
Mission-Centricity in Cyber Security: Architecting Cyber Attack Resilient Missions <i>Gabriel Jakobson</i>	315
Autonomous Intelligent Agents in Cyber Offence <i>Alessandro Guarino</i>	333
Autonomous Decision-Making Processes and the Responsible Cyber Commander <i>Jody M. Prescott</i>	345

#### **Chapter 5. Cyber Conflict – Politics, Semantics, Ethics and Moral**

Divided by a Common Language: Cyber Definitions in Chinese, Russian and English <i>Keir Giles, William Hagestad II</i>	363
Towards a Cyber Conflict Taxonomy <i>Scott D. Applegate, Angelos Stavrou</i>	380
Cyber Attack: A Dull Tool to Shape Foreign Policy <i>Emilio Iasiello</i>	398
The Future of Military Virtue: Autonomous Systems and the Moral Deskillling of the Military <i>Shannon Vallor</i>	416
An Ethical Analysis of the Case for Robotic Weapons Arms Control <i>John P. Sullins</i>	