2012 4th International Conference on Cyber Conflict

(CYCON 2012)

Tallinn, Estonia
5 – 8 June 2012

IEEE Catalog Number: CFP1226N-PRT
ISBN: 978-1-4673-1270-7

TABLE OF CONTENTS

Introduction

Chapter 1: Cyberspace – The Role of States in the Global Structure

Legal Implications of Territorial Sovereignty in Cyberspace 1
Wolff Heintschel von Heinegg

When "Not My Problem" Isn't Enough: Political Neutrality and National Responsibility in Cyber Conflict 14
Jason Healey

Neutrality in Cyberspace 27
Wolff Heintschel von Heinegg

Impact of Cyberspace on Human Rights and Democracy 39
Vittorio Fanchiotti / Jean Paul Pierini

Chapter 2: Cyber Policy & Strategic Options

Russia's Public Stance on Cyber/Information Warfare 51
Keir Giles

French Cyberdefense Policy 64
Patrice Tromparent

A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations 76
Louise Arimatsu

Internet as a Critical Infrastructure – A Framework for the Measurement of Maturity and Awareness in the Cyber Sphere 95
Assaf Y. Keren, Keren Elazari

The Significance of Attribution to Cyberspace Coercion: A Political Perspective 108
Forrest Hare

The Militarisation of Cyberspace: Why Less May Be Better 123
Myriam Dunn Cavelty

Chapter 3: Cyber Conflict – Theory & Principles

Beyond Domains, Beyond Commons: 136
The Context and Theory of Conflict in Cyberspace
Jeffrey L. Caton

Applying Traditional Military Principles to Cyber Warfare 147
Samuel Liles, J. Eric Dietz, Marcus Rogers, Dean Larson

The Principle of Maneuver in Cyber Operations 159
Scott D. Applegate

Countering the Offensive Advantage in Cyberspace: N/A
An Integrated Defensive Strategy
David T. Fahrenkrug

An Analysis For A Just Cyber Warfare 172
Mariarosaria Taddeo

Chapter 4: Cyber Conflict – Actors

Socially Engineered Commoners as Cyber Warriors - Estonian Future or Present? 182
Birgy Lorenz, Kaido Kikkas

The Notion of Combatancy in Cyber Warfare 194
Sean Watts

Direct Participation in Cyber Hostilities: 209
Terms of Reference for Like-Minded States?
Jody Prescott

Chapter 5: "Cyber-Attacks" – Trends, Methods & Legal Classification

Attack Trends in Present Computer Networks 225
Robert Koch, Björn Stelte, Mario Golling

"Attack" as a Term of Art in International Law: 237
The Cyber Operations Context
Michael N. Schmitt

Ius ad bellum in Cyberspace – Some Thoughts on N/A
the "Schmitt-Criteria" for Use of Force
Katharina Ziolkowski

The "Use of Force" in Cyberspace: A Reply to Dr Ziolkowski 248
Michael N. Schmitt

A Methodology for Cyber Operations Targeting and 255
Control of Collateral Damage in the Context of Lawful Armed Conflict
Robert Fanelli, Gregory Conti

Command and Control of Cyber Weapons 268
Enn Tyugu

A Case Study on the Miner Botnet 279
Daniel Plohmann, Elmar Gerhards-Padilla

Chapter 6: Cyber Defence – Methods & Tools

Natural Privacy Preservation Protocol for Electronic Mail 295
Kim Hartmann, Christoph Steup

Paradigm Change of Vehicle Cyber-Security 312
Hiro Onishi

Sensing for Suspicion at Scale: A Bayesian Approach 323
for Cyber Conflict Attribution and Reasoning
Harsha K. Kalutarage, Siraj A. Shaikh, Qin Zhou, Anne E. James

The Role of COTS Products for High Security Systems 342
Robert Koch, Gabi Dreo Rodosek

Conceptual Framework for Cyber Defense 356
Information Sharing within Trust Relationships
Diego Fernández Vázquez, Oscar Pastor Acosta,
Christopher Spirito, Sarah Brown, Emily Reid