

2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon 2022)

**Tallinn, Estonia
31 May – 3 June 2022**



**IEEE Catalog Number: CFP2226N-POD
ISBN: 978-1-6654-8885-3**

**Copyright © 2022, NATO CCDCOE Publications
All Rights Reserved**

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP2226N-POD
ISBN (Print-On-Demand):	978-1-6654-8885-3
ISBN (Online):	978-9-9169-7891-7
ISSN:	2325-5366

Additional Copies of This Publication Are Available From:

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

Introduction	1
<i>The Role of Military Cyber Exercises: A Case Study of Locked Shields</i> Max Smeets	7
<i>Cyber Resilience versus Cybersecurity as Legal Aspiration</i> Lee A. Bygrave	24
<i>Public-Private Partnerships and Collective Cyber Defence</i> John Morgan Salomon	41
<i>Obnoxious Deterrence</i> Martin C. Libicki	60
<i>The Promise and Perils of Allied Offensive Cyber Operations</i> Erica D. Loneragan and Mark Montgomery	73
<i>'Releasing the Hounds?' Disruption of the Ransomware Ecosystem Through Offensive Cyber Operations</i> Michael Bátrla and Jakub Harašta	87
<i>Third-Party Countries in Cyber Conflict: Understanding the Dynamics of Public Opinion Following Offensive Cyber Operations</i> Miguel Alberto Gomez and Gregory Winger	110
<i>Machine Expertise in the Loop: Artificial Intelligence Decision-Making Inputs and Cyber Conflict</i> Christopher E. Whyte	128
<i>Subverting Skynet: The Strategic Promise of Lethal Autonomous Weapons and the Perils of Exploitation</i> Lennart Maschmeyer	148

<i>'Responsibility to Detect?': Autonomous Threat Detection and its Implications for Due Diligence in Cyberspace</i> Arun Mohan Sukumar	165
<i>Exploring Changing Battlefields: Autonomous Weapons, Unintended Engagements and the Law of Armed Conflict</i> Tsvetelina J. van Benthem	180
<i>Legal Aspects of Misattribution Caused by Cyber Deception</i> Petr Stejskal and Martin Faix	195
<i>Military Data and Information Sharing – a European Union Perspective</i> Sebastian Cymutta, Marten Zwanenburg and Paul Oling	209
<i>Cyber Threats Against and in the Space Domain: Legal Remedies</i> Seth W. Dilworth and D. Daniel Osborne	225
<i>Maritime Hacking Using Land-Based Skills</i> Michael L. Thomas	238
<i>A Cryptographic and Key Management Glance at Cybersecurity Challenges of the Future European Railway System</i> Mikko Kiviharju, Christina Lassfolk, Sanna Rikkonen and Hannu Kari	253
<i>Security and Privacy Issues of Satellite Communication in the Aviation Domain</i> Georg Baselt, Martin Strohmeier, James Pavur, Vincent Lenders and Ivan Martinovic	273
<i>Keep the Moving Vehicle Secure: Context-Aware Intrusion Detection System for In-Vehicle CAN Bus Security</i> Sampath Rajapaksha, Harsha Kalutarage, M. Omar Al-Kadri, Garikayi Madzudzo and Andrei V. Petrovski	296

<i>Towards a Digital Twin of a Complex Maritime Site for Multi-Objective Optimization</i> Joseph A. J. Ross, Kimberly Tam, David J. Walker and Kevin D. Jones	318
<i>The Design of Cyber-Physical Exercises (CPXs)</i> Siddhant Shrivastava, Francisco Furtado, Mark Goh and Aditya Mathur	333
<i>Data Quality Problem in AI-Based Network Intrusion Detection Systems Studies and a Solution Proposal</i> Emre Halisdemir, Hacer Karacan, Mauno Pihelgas, Toomas Lepik and Sungbaek Cho	352
<i>JARVIS: Phenotype Clone Search for Rapid Zero-Day Malware Triage and Functional Decomposition for Cyber Threat Intelligence</i> Christopher Molloy, Philippe Charland, Steven H. H. Ding and Benjamin C. M. Fung	369
<i>Emergence of 5G Networks and Implications for Cyber Conflict</i> Keir Giles and Kim Hartmann	388