18th International Conference on Cyber Warfare and Security (ICCWS 2023)

Towson, Maryland, USA
9 – 10 March 2023

Editors:

Richard L. Wilson
Brendan Curran

ISBN: 978-1-7138-7105-7
Review Process
Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy
ACPI adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:

Conference Proceedings
The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

Published by Academic Conferences and Publishing International Ltd.
33 Wood Lane
Sonning Common RG4 9SJ UK

Phone: 44 189 724 148
Fax: 44 189 724 691
info@academic-conferences.org

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
Email: curran@proceedings.com
Web: www.proceedings.com
ICCS 2023 Contents Page

Preface v
Committee vi
Biographies vii

Academic Papers

Secure Cloud Migration Strategy (SCMS): A Safe Journey to the Cloud
Dalal Alharthi 1-6

Cyber-Physical Attack Using High Power RF in Havana, Cuba
Allyffazzkamn Argudo, Ghislaine Nasibu 7-18

Cybersecurity in Digital Transformation applications: Analysis of Past Research and Future Directions
Zakariya Belkhamza 19-24

An Automated Post-Exploitation Model for Cyber Red Teaming
Ryan Benito, Alan Shaffer, Gurminder Singh 25-34

Review of End-to-End Encryption for Social Media
Vijay Bhuse 35-37

An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022
Johannes George Botha, Danielle Botha, Louise Leenen 39-48

Case Study: Conducting a Risk Assessment for an Electrical Utility
Edwin Covert 49-56

On the Use and Strategic Implications of Cyber Ranges in Military Contexts: A Dual Typology
Mischa Hansel, Andrew Dwyer, Kathrin Moog, Jantje Silomon 57-66

Evaluation of Quantum Key Distribution for Secure Satellite-integrated IoT Networks
Andrew Edwards, Yee Wei Law, Ronald Mulinde, Jill Slay 67-76

Commentary on Healthcare and Disruptive Innovation
Hilary Finch, Abasi-Amefon Affia, Woosub Jung, Lucas Potter, Xavier-Lewis Palmer 77-84

Courtney Fleming, Mark Reith, Wayne Henry 85-92

Predictors of Human Efficiency in Radar Detection Tasks
Elizabeth Fox, Arielle Stephenson, Christopher Stevens, Gregory Bowers 93-102

Nuclear Cyber Attacks: A Study of Sabotage and Regulation of Critical Infrastructure
Virginia Greiman 103-110

Brandon Griffin, Keitavius Alexander, Xavier-Lewis Palmer, Lucas Potter 111-118

Search and CompAre Reverse (SCAR): A Bioinformatics-Inspired Methodology for Detecting File Remnants in Digital Forensics
George Grispos, William Mahoney, Sayonnha Mandal 119-127

Development and Analysis of a Reconnaissance-Technique Knowledge Graph
Thomas Heverin, Elsa Deitz, Eve Cohen, Jordana Wilkes 128-136

Zero Trust is Not Enough: Mitigating Data Repository Breaches
JS Hurley 137-144
Managing Large-Scale Heterogeneous Deployments for Cybersecurity
JS Hurley ................................. 145-151

Digital Geopolitics: A Review of the Current State
Gazmend Huskaj .......................... 152-161

Managing Variable Cyber Environments with Organizational Foresight and Resilience Thinking
Eveliina Hytönen, Jyri Rajamäki, Harri Ruoslahti .................. 162-170

Fingerprinting Network Sessions for the Discovery of Cyber Threats
Christiaan Klopper, Jan .................... 171-180

S-400s, Disinformation, and Anti-American Sentiment in Turkey

Detecting and tracking hypersonic glide vehicles: A cybersecurity-engineering analysis of academic literature
Yee Wei Law, John Joshua Gliponeo, Dilpreet Singh, John McGuire, Jiajun Liang, Sook-Ying Ho, and Jill Slay .......... 189-198

Cyber security training in Finnish basic and general upper secondary education
Martti Lehto, Pekka Neittaanmäki ...................... 199-208

Russian Influence Operations during the Invasion of Ukraine
Joseph Littell, Nicolas Starck .................. 209-217

Modelling the Influential Factors Embedded in the Proportionality Assessment in Military Operations
Clara Maathuis, Sabarathinam Chockalingam ...................... 218-226

Social Media Manipulation Awareness through Deep Learning based Disinformation Generation
Clara Maathuis, Iddo Kerkhof .......................... 227-236

Social Media Manipulation Deep Learning based Disinformation Detection
Clara Maathuis, Rik Godschalk ......................... 237-245

Improvements on Hiding x86-64 Instructions by Interleaving
William Mahoney, Todd McDonald, George Grispos, Sayonnha Mandal ......................... 246-255

Developing Privacy Incident Responses to Combat Information Warfare
Sean McElroy, Lisa McKee ......................... 256-263

Use of Intrusion Detection Systems in Vehicular Controller Area Networks to Preclude Remote Attacks
Anthony Monge, Todd Andel ......................... 264-272

Digital Insanity: Exploring the Flexibility of NIST Digital Identity Assurance Levels
Kenneth Myers ................................. 273-278

Risk likelihood of planned and unplanned cyber-attacks in small business sectors: A cybersecurity concern
Tabisa Ncubukezi .............................. 279-290

Ret-gadgets in RISC-V-based Binaries Resulting in Traps for Hijackers
Toyosi Oyinloye, Lee Speakman, Thaddeus Eze ....................... 291-299

Basic Elements of Cyber Security for a Smart Terminal Process
Jouni Pöyhönen, Jussi Simola, Martti Lehto ......................... 300-308

Anti-American Stance in Turkey: A Twitter Case Study

Gaps in Asset Management Systems to Integrate Railway Companies’ Resilience
Jyri Rajamäki, Jari Savolainen, Rauno Pirinen, Villamor ....................... 318-326
LoRaWAN & The Helium Blockchain: A Study on Military IoT Deployment
Michael A. Reyneke, Barry E. Mullins, Mark G. Reith 327-337

Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation
Saminu Salisu, Velitchko Filipov 338-347

Biocytbersecurity and Deterrence: Hypothetical Rwandan Considerations
Issah Samori, Gbadebo Odularu, Lucas Potter, Xavier-Lewis Palmer 348-354

Lesson Plan: An Interdisciplinary Approach to Teaching Cyber Warfare Concepts
Donna Schaeffer, Patrick Olson 355-359

The Impact of Edge Computing on the Industrial Internet of Things
Nkata Sekonya, Siphesihle Sithungu 360-368

Cyber Threat Analysis in Smart Terminal Systems
Jussi Simola, Jouni Pöyhönen, Lehto Martti 369-378

Towards a Scientific Definition of Cyber Resilience
Sidney Smith 379-386

Implications of Cyberbiosecurity in Advanced Agriculture
Simone Stephen, Keitavius Alexander, Lucas Potter, Xavier-Lewis Palmer 387-393

Organizational Cybersecurity Post The Pandemic: An Exploration of Remote Working Risks and Mitigation Strategies
Stephen Treacy, Anoop Sabu, Thomas Bond, Joseph O'Sullivan, Jack Sullivan, Peter Sylvester 394-401

A Quantitative Risk Assessment Framework for the Cybersecurity of Networked Medical Devices
Maureen Van Devender, Jeffrey Todd McDonald 402-411

Towards the Usefulness of Learning Factories in the Cybersecurity Domain
Namosha Veerasamy, Thuli Mkhwanazi, Zubeida Dawood 412-419

Naïve Bayes Supervised Learning based Physical Layer Authentication: Anti-Spoofing techniques for Industrial Radio Systems
Andreas Weinand, Christoph Lipps, Michael Karrenbauer, Hans Dieter Schotten 420-430

How the Russian Influence Operation on Twitter Weaponized Military Narratives
Dana Weinberg, Jessica Dawson, April Edwards 431-439

Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues
Richard Wilson, Alexia Fitz 440-448

Robots Security Assessment and Analysis Using Open-Source Tools
Benjamin Yankson, Tyler Loucks, Andrea Sampson, Chelsea Lojano 449-456

Social Robots Privacy Enhancement Using Colored Petri Net (CPN) for Behavior Modeling: A Case Study of Asus Zenbo Robot
Benjamin Yankson, Farkhund Iqbal, Fadya AlMaenei 457-464

PhD Papers

A Unified Forensics Analysis Approach to Digital Investigation
Ali Alshumrani, Nathan Clarke, Bogdan Ghita 466-475

Offensive Cyberspace Operations for Cyber Security
Gazmend Huskaj 476-479
Categorizing Cyber Activity Through an Information-psychological and Information-technological Perspective, Case Ukraine.
Harry Kantola 480-488

Using Military Cyber Operations as a Deterrent
Maria Keinonen 489-496

Identifying Commonalities of Cyberattacks Against the Maritime Transportation System
Rebecca Rohan 497-503

Evaluating a Non-platform-specific OCR/NLP system to detect Online Grooming
Jake Street, Funminiyi Olajide 504-511

Masters Papers

Demonstrating Redundancy Advantages of a Three-Channel Communication Protocol
Scott Culbreth, Scott Graham 513-522

UAV Payload Identification with Acoustic Emissions and Cell Phones
Hunter Doster, Barry Mullins 523-533

Just Warfare: Is a Nuclear Attack an appropriate Response to a Cyber Attack?
Alexia Fitz, Richard Wilson 534-541

A Review and Testing of Fault Tolerance Levels of Anti-Poaching Cybersecurity System
Isabelle Heyl, Julia Stone, Takudzwa Vincent Banda, Vian Smit, Dewald Blaauw 542-549

DACA: Automated Attack Scenarios and Dataset Generation
Frank Korving, Risto Vaarandi 550-559

Towards a Critical Review of Cybersecurity Risks in Anti-Poaching Systems
Christelle Steyn, Dewald Neville Blaauw 560-568

Work in Progress Papers

Locality-based electromagnetic leakage assessment using CNN
Ian Heffron, James Dean 570-576

Using Deep Reinforcement Learning for Assessing the Consequences of Cyber Mitigation Techniques on Industrial Control Systems
Terry Merz, Romarie Morales Rosado 577-580