

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

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright The Authors, (2023). All Rights Reserved. No reproduction, copy or transmission may be made without written permission from the individual authors.

Printed with permission by Curran Associates, Inc. (2023)

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

ACPIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:

<http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academicconferences-and-publishing-international-limited/>

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: 441 189 724 148
Fax: 441 189 724 691
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

ICCWS 2023 Contents Page

<u>Preface</u>	v
<u>Committee</u>	vi
<u>Biographies</u>	viii
<u>Academic Papers</u>	
<i>Secure Cloud Migration Strategy (SCMS): A Safe Journey to the Cloud</i> Dalal Alharthi	1-6
<i>Cyber-Physical Attack Using High Power RF in Havana, Cuba</i> Allyfazzkkamn Argudo, Ghislaine Nasibu	7-18
<i>Cybersecurity in Digital Transformation applications: Analysis of Past Research and Future Directions</i> Zakariya Belkhamza	19-24
<i>An Automated Post-Exploitation Model for Cyber Red Teaming</i> Ryan Benito, Alan Shaffer, Gurminder Singh	25-34
<i>Review of End-to-End Encryption for Social Media</i> Vijay Bhuse	35-37
<i>An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022</i> Johannes George Botha, Danielle Botha, Louise Leenen	39-48
<i>Case Study: Conducting a Risk Assessment for an Electrical Utility</i> Edwin Covert	49-56
<i>On the Use and Strategic Implications of Cyber Ranges in Military Contexts: A Dual Typology</i> Mischa Hansel, Andrew Dwyer, Kathrin Moog, Jantje Silomon	57-66
<i>Evaluation of Quantum Key Distribution for Secure Satellite-integrated IoT Networks</i> Andrew Edwards, Yee Wei Law, Ronald Mulinde, Jill Slay	67-76
<i>Commentary on Healthcare and Disruptive Innovation</i> Hilary Finch, Abasi-Amefon Affia, Woosub Jung, Lucas Potter, Xavier-Lewis Palmer	77-84
<i>Securing Commercial Satellites for Military Operations: A Cybersecurity Supply Chain Framework</i> Courtney Fleming, Mark Reith, Wayne Henry	85-92
<i>Predictors of Human Efficiency in Radar Detection Tasks</i> Elizabeth Fox, Arielle Stephenson, Christopher Stevens, Gregory Bowers	93-102
<i>Nuclear Cyber Attacks: A Study of Sabotage and Regulation of Critical Infrastructure</i> Virginia Greiman	103-110
<i>Social-Engineering, Bio-economies, and Nation-State Ontological Security: A Commentary</i> Brandon Griffin, Keitavius Alexander, Xavier-Lewis Palmer, Lucas Potter	111-118
<i>Search and CompAre Reverse (SCAR): A Bioinformatics-Inspired Methodology for Detecting File Remnants in Digital Forensics</i> George Grispos, William Mahoney, Sayonna Mandal	119-127
<i>Development and Analysis of a Reconnaissance-Technique Knowledge Graph</i> Thomas Heverin, Elsa Deitz, Eve Cohen, Jordana Wilkes	128-136
<i>Zero Trust is Not Enough: Mitigating Data Repository Breaches</i> JS Hurley	137-144

<i>Managing Large-Scale Heterogeneous Deployments for Cybersecurity</i> JS Hurley	145-151
<i>Digital Geopolitics: A Review of the Current State</i> Gazmend Huskaj	152-161
<i>Managing Variable Cyber Environments with Organizational Foresight and Resilience Thinking</i> Eveliina Hytönen, Jyri Rajamäki, Harri Ruoslahti	162-170
<i>Fingerprinting Network Sessions for the Discovery of Cyber Threats</i> Christiaan Klopper, Jan	171-180
<i>S-400s, Disinformation, and Anti-American Sentiment in Turkey</i> Russell Korb, Saltuk Karahan, Gowri Prathap, Ekrem Kaya, Luke Palmieri, Hamdi Kavak	181-188
<i>Detecting and tracking hypersonic glide vehicles: A cybersecurity-engineering analysis of academic literature</i> Yee Wei Law, John Joshua Gliponeo, Dilpreet Singh, John McGuire, Jiajun Liang, Sook-Ying Ho, and Jill Slay	189-198
<i>Cyber security training in Finnish basic and general upper secondary education</i> Martti Lehto, Pekka Neittaanmäki	199-208
<i>Russian Influence Operations during the Invasion of Ukraine</i> Joseph Littell, Nicolas Starck	209-217
<i>Modelling the Influential Factors Embedded in the Proportionality Assessment in Military Operations</i> Clara Maathuis, Sabarathinam Chockalingam	218-226
<i>Social Media Manipulation Awareness through Deep Learning based Disinformation Generation</i> Clara Maathuis, Iddo Kerkhof	227-236
<i>Social Media Manipulation Deep Learning based Disinformation Detection</i> Clara Maathuis, Rik Godschalk	237-245
<i>Improvements on Hiding x86-64 Instructions by Interleaving</i> William Mahoney, Todd McDonald, George Grispos, Sayonhha Mandal	246-255
<i>Developing Privacy Incident Responses to Combat Information Warfare</i> Sean McElroy, Lisa McKee	256-263
<i>Use of Intrusion Detection Systems in Vehicular Controller Area Networks to Preclude Remote Attacks</i> Anthony Monge, Todd Andel	264-272
<i>Digital Insanity: Exploring the Flexibility of NIST Digital Identity Assurance Levels</i> Kenneth Myers	273-278
<i>Risk likelihood of planned and unplanned cyber-attacks in small business sectors: A cybersecurity concern</i> Tabisa Ncubekezi	279-290
<i>Ret-gadgets in RISC-V-based Binaries Resulting in Traps for Hijackers</i> Toyosi Oyinloye, Lee Speakman, Thaddeus Eze	291-299
<i>Basic Elements of Cyber Security for a Smart Terminal Process</i> Jouni Pöyhönen, Jussi Simola, Martti Lehto	300-308
<i>Anti-American Stance in Turkey: A Twitter Case Study</i> Gowri Prathap, Hamdi Kavak, Ekrem Kaya, Luke Palmieri, Saltuk Karahan, Alex Korb	309-317
<i>Gaps in Asset Management Systems to Integrate Railway Companies' Resilience</i> Jyri Rajamäki, Jari Savolainen, Rauno Pirinen, Villamor	318-326

<i>LoRaWAN & The Helium Blockchain: A Study on Military IoT Deployment</i> Michael A. Reyneke, Barry E. Mullins , Mark G. Reith	327-337
<i>Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation</i> Saminu Salisu, Velitchko Filipov	338-347
<i>Biocybersecurity and Deterrence: Hypothetical Rwandan Considerations</i> Issah Samori, Gbadebo Odularu, Lucas Potter, Xavier-Lewis Palmer	348-354
<i>Lesson Plan: An Interdisciplinary Approach to Teaching Cyber Warfare Concepts</i> Donna Schaeffer, Patrick Olson	355-359
<i>The Impact of Edge Computing on the Industrial Internet of Things</i> Nkata Sekonya, Siphesihle Sithungu	360-368
<i>Cyber Threat Analysis in Smart Terminal Systems</i> Jussi Simola, Jouni Pöyhönen, Lehto Martti	369-378
<i>Towards a Scientific Definition of Cyber Resilience</i> Sidney Smith	379-386
<i>Implications of Cyberbiosecurity in Advanced Agriculture</i> Simone Stephen, Keitavius Alexander, Lucas Potter, Xavier-Lewis Palmer	387-393
<i>Organizational Cybersecurity Post The Pandemic: An Exploration of Remote Working Risks and Mitigation Strategies</i> Stephen Treacy, Anoop Sabu, Thomas Bond, Joseph O'Sullivan, Jack Sullivan, Peter Sylvester	394-401
<i>A Quantitative Risk Assessment Framework for the Cybersecurity of Networked Medical Devices</i> Maureen Van Devender, Jeffrey Todd McDonald	402-411
<i>Towards the Usefulness of Learning Factories in the Cybersecurity Domain</i> Namosha Veerasamy, Thuli Mkhwanazi, Zubeida Dawood	412-419
<i>Naïve Bayes Supervised Learning based Physical Layer Authentication: Anti-Spoofing techniques for Industrial Radio Systems</i> Andreas Weinand, Christoph Lipps, Michael Karrenbauer, Hans Dieter Schotten	420-430
<i>How the Russian Influence Operation on Twitter Weaponized Military Narratives</i> Dana Weinberg, Jessica Dawson, April Edwards	431-439
<i>Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues</i> Richard Wilson, Alexia Fitz	440-448
<i>Robots Security Assessment and Analysis Using Open-Source Tools</i> Benjamin Yankson, Tyler Loucks, Andrea Sampson, Chelsea Lojano	449-456
<i>Social Robots Privacy Enhancement Using Colored Petri Net (CPN) for Behavior Modeling: A Case Study of Asus Zenbo Robot</i> Benjamin Yankson, Farkhund Iqbal, Fadya AlMaeeni	457-464
PhD Papers	
<i>A Unified Forensics Analysis Approach to Digital Investigation</i> Ali Alshumrani, Nathan Clarke, Bogdan Ghita	466-475
<i>Offensive Cyberspace Operations for Cyber Security</i> Gazmend Huskaj	476-479

<i>Categorizing Cyber Activity Through an Information-psychological and Information-technological Perspective, Case Ukraine.</i>	
Harry Kantola	480-488
<i>Using Military Cyber Operations as a Deterrent</i>	
Maria Keinonen	489-496
<i>Identifying Commonalities of Cyberattacks Against the Maritime Transportation System</i>	
Rebecca Rohan	497-503
<i>Evaluating a Non-platform-specific OCR/NLP system to detect Online Grooming</i>	
Jake Street, Funminiyi Olajide	504-511
<u>Masters Papers</u>	
<i>Demonstrating Redundancy Advantages of a Three-Channel Communication Protocol</i>	
Scott Culbreth, Scott Graham	513-522
<i>UAV Payload Identification with Acoustic Emissions and Cell Phones</i>	
Hunter Doster, Barry Mullins	523-533
<i>Just Warfare: Is a Nuclear Attack an appropriate Response to a Cyber Attack?</i>	
Alexia Fitz, Richard Wilson	534-541
<i>A Review and Testing of Fault Tolerance Levels of Anti-Poaching Cybersecurity System</i>	
Isabelle Heyl, Julia Stone, Takudzwa Vincent Banda, Vian Smit, Dewald Blaauw	542-549
<i>DACA: Automated Attack Scenarios and Dataset Generation</i>	
Frank Korving, Risto Vaarandi	550-559
<i>Towards a Critical Review of Cybersecurity Risks in Anti-Poaching Systems</i>	
Christelle Steyn, Dewald Neville Blaauw	560-568
<u>Work in Progress Papers</u>	
<i>Locality-based electromagnetic leakage assessment using CNN</i>	
Ian Heffron, James Dean	570-576
<i>Using Deep Reinforcement Learning for Assessing the Consequences of Cyber Mitigation Techniques on Industrial Control Systems</i>	
Terry Merz, Romarie Morales Rosado	577-580