19th International Conference on Cyber Warfare and Security (ICCWS 2024)

Johannesburg, South Africa
26 – 27 March 2024

Editors:

Jaco du Toit
Brett van Niekerk

ISBN: 978-1-7138-9506-0

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, (2024). 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. (2024)

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

Preface v

Committee vi

Biographies vii

Academic Papers

Cybersecurity Implications of Virtual Currency Reward Systems in the Metaverse
Hamza Allimia, Stacey Baror, Hein Venter *1-9*

On The Zero-Trust Intranet Certification Problem
Danielle Botha-Badenhorst, André Martin McDonald, Graham David Barbour, Ethan Buckinjohn, Wian Gertenbach 10-18

Social Media as a Strategic Advantage during Cyberwarfare: A Systematic Literature Review
Errol Baloyi, Oyena Mahlasela, Nokuthaba Siphambili, Mayan Stegmann 19-25

The Role of Industry-Academia Partnerships Can Play in Cybersecurity: Exploring Collaborative Approaches to Address Cybercrime
Benjamin Yankson, Emmanuel Berkoh, Mubarak Hussein, Yvonne Dadson 26-33

Cryptocurrency-crime Investigation: Fraudulent use of Bitcoin in a Divorce Case
Johannes George Botha, Louise Leenen 34-42

Capture the Flag with ChatGPT: Security Testing with AI ChatBots
David Chamberlain, Ellis Casey 43-54

Teenagers: A Social Media Threat Vector
Henry Collier, Charlotte Morton 55-61

Past and Present Russian Information Operations in Ukraine: Competition into Conflict
Stephen Defibaugh 62-65

Ransomware Detection Using Portable Executable Imports
Tanatswa Ruramai Dendere, Avinash Singh 66-74

A Proposed High-Level Methodology on How OSINT is applied in Blockchain Investigations
Wian Gertenbach, Johnny Botha, Louise Leenen 75-83

An Ontology of Cyberspace as a Basis for Decision-making in Cyberoperations
Alexander Grandin 84-94

Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model
Tapiwa Gundu 95-102

Anomaly Detection for the MIL-STD-1553B Multiplex Data Bus Using an LSTM Autoencoder
Brian Lachine, Alec Harlow, Vincent Roberge 103-111

Authentication in a Hyperconnected World: Challenges, Opportunities and Approaches
Christoph Lipps, Jan Herbst, Rekha Reddy, Matthias Rüb, Hans D. Schotten 112-120

Human-Centered AI in Military Cyber Operations
Clara Maathuis 121-128

Towards Trustworthy AI-based Military Cyber Operations
Clara Maathuis 129-136

Ukrainian Thoughts and Feelings based on One Year War Content Analysis
Clara Maathuis, Iddo Kerkhof 137-148

Can You Give Me a Lift?
William Mahoney, Adam Spanier 149-155

Cybercrime Classification: A Victimology-based approach
Sayonnha Mandal 156-167

Chain of Custody and Evidence Integrity Verification Using Blockchain Technology
Adir Miller, Avinash Singh 168-176

Cyber Resilience, Dependability and Security
Gareth Davies, Angela Mison, Peter Eden 177-184

Cross-disciplinary AI supply chain risk assessment
Gareth Davies, Angela Mison, Dr. Richard Ward 185-190

Proof of Concept of a Digital Forensic Readiness Cybercrime Language as a Service
Maryam Mohamad Al Mahdi, Stacey Baror 191-199

An Analysis of Cybersecurity Architectures
Noluntu Mpekoa 200-207

Bibliometric Analysis of Cyber Warfare Research in Africa: Landscape and Trends
Jabu Mtsweni, Mphahlela Thaba 208-218

Systematic Review to Propose a Blockchain-based Digital Forensic Ready Internet Voting System
Edmore Muyambo, Stacey Omeleze Baror 219-230

Theory-Guided Feature Selection in Cybercrime Data Science
Shiven Naidoo, Rennie Naidoo 231-239

Infusing Morabaraba game design to develop a cybersecurity awareness game (CyberMoraba)
Mike Wa Nkongolo 240-250

Bahrun Naim's Hacking Manifesto: How A Historical Model of Cyber Threat Mischaracterization Helps Us Diffuse a Dead Cyberterrorist Influencer
Tim Pappa 251-261

Typology of State Actors' Behavior in Cyber Space
Ada Peter, Ujunwa Ohakpougwu 262-267

Friend or Foe – The Impact of ChatGPT on Capture the Flag Competitions
Heloise Pieterse 268-276

Reverse-Engineering of Disinformation Campaigns During the War in Ukraine
Lora Pitman, Ava Baratz, Kelly Morgan, Marcy Alvarado 277-281

Deepfakes: The Legal Implications
Trishana Ramluckan 282-288

Metaverse: Virtual Currencies as a Mechanism for Employee Engagement and Retention
Shelley Robertson, Stacey Baror, Hein Venter 289-298

Cybersafe: Gamifying Cybersecurity Training with a Training App
Carlos Roque, Gareth Moodley, Sayonnha Mandal 299-307

Analysis of Media Influence on Military Decision-Making
Bonnie Rushing 308-316

Building Cybersecurity Capacities in Zambia's Business Sector: Guideline for SMEs
Goni Saar, Rabelani Dagada 317-326

Coming Back Down to Earth: A Grounded Look at Space Cybersecurity in Southeast Asia
Shantanu Sharma 327-337

A Privacy-Compliant Process for Digital Forensics Readiness
Gabriel Shoderu, Stacey Baror, Hein Venter 337-347

Impact of Cyber Security Operations on Hardware Requirements for Stable and Workable Industrial Environments
Jussi Simola, Arttu Takala, Riku Lehkonen, Tapio Frantti, Reijo Savola 348-357

Hardware Sequence Combinators
Stephen Taylor, Gunnar Pope 358-365

A Strategic Path for Digital Transformation in Cyber Warfare for African Militaries
Mphahlela James Thaba, Jabu Mtsweni 366-373

Adversarial Camera Patch: An Effective and Robust Physical-World Attack on Object Detectors
Kalibinuer Tiliwalidi, Bei Hui, Chengyin Hu, Jingjing Ge 374-384

A Case Study on Multi-Countries Money Laundering Scheme and A Proposed Automatic Detection System
Xiao Tan, Tsz-Fung Tony Tse, Siu Ming Yiu, Hiu-Man Human Lam 385-394

Cyber Operations in Peace and War: A Framework for Persistent Engagement
Brett van Niekerk 395-404

Unpacking AI Security Considerations
Namosha Veerasamy, Danielle Badenhorst, Mazwi Ntshangase, Errol Baloyi; Noku Siphambili;
Oyena Mahlasela 405-413

Recognising Cyber Blockades as Crimes Against Humanity: Can International Criminal Law Keep Up?
Dora Vanda Velenczei 414-420

Covert Subversive Agents and Consensus Disruption on Large Projects
Johannes Vorster, Louise Leenen 421-429

Exploring South Africa's Cybersecurity Legal Framework regulating Information Confidentiality, Integrity, and Availability
Murdoch Watney 430-437

PhD Papers

Managing Cyber Security Debt: Strategies for Identification, Prioritisation, and Mitigation
Christo Coetzer, Louise Leenen 439-446

An AI Model for Digital Forensic Readiness in the Cloud using Secure Access Service Edge
taurai Hungwe, Prof Hein Venter 447-454

On the Benefits of Vulnerability Data Consolidation in Application Security
Santanam Kasturi, Xiaolong Li, Peng Li, John Pickard 455-462

Options for Signalling Cyber Deterrence Using Cyber Capabilities
Maria Keinonen, Kimmo Halunen 463-471

A Federated Distributed Digital Forensic Readiness Model for the Cloud
Renico Koen, Hein Venter 472-480

Strengthening Aviation Cybersecurity with Security Operations Centres
Wesley Murisa, Marijke Coetzee 481-489

Quantum-Secure Signalling Model for L1/L2 Next-Gen Interconnect and Roaming Networks Over IPX for NB-IoT Traffic: A Review
Themba Ngobeni, Boniface Kabaso 490-500

Integrating Enterprise Architecture into Cybersecurity Risk Management in Higher Education
Mafika Nkambule, Joey Jansen van Vuuren 501-510

A Study into Privacy and Legal Issues in Cloud Computing: The Mozambican Context
ambrosio Patricio Vumo 511-517

Masters Papers

Using Blockchain to Secure Digital Identity and Privacy Across Digital Sectors
Jaynill Gopal, Stacey Omeleze-Baror 519-526

Defining the "Cyber-Pearl Harbor" - Validation of the DSLP-framework in "Offensive Cyberspace Operations Targeting Ukraine: A Cyber Pearl-Harbor"
Jonathan Lilja, Eleshwa Eishayea, Gazmend Huskaj 527-534

Assessing the Effectiveness of ADS-B Mitigations
Heinke Lubbe, Rudi Serfontein, Marijke Coetzee 535-544

Identifying the Scope of Cybersecurity Research Conducted in the Maritime Industry: 2003 – 2023
Tshepo Mawer, Sune von Solms, Johan Meyer 545-554

National Critical Information Infrastructure Protection through Cybersecurity: A National Government Perspective
Thulisile Dephney Mkhwanazi, Lynn Futcher 555-564

Intelligence Agencies' move to the Cloud: Challenges and Opportunities
Karin Säberg, Gazmend Huskaj 565-573

Enhancing Privacy and Security in Large-Language Models: A Zero-Knowledge Proof Approach
Shridhar Singh 574-582

Securi-Chain: Enhancing Smart Contract Security in Blockchain Systems Through Optimized Access Control
Keanu Swart, Stacey Omeleze Baror, Hein Venter 583-591

Work in Progress Papers

Using Digital Forensics for Android Smartphone Devices to aid Criminal Investigations
Stephanie Agenbag, Andre Henney, Heloise Pieterse 593-596

Deep Learning-based Framework for Detecting Malicious Insider-Inspired Cyberattacks Activities in Organisations
Gibson Chengetanai, Teandai R. Chandigere, Pepukai Chengetanai, Rachna Verma 597-601

Active Gait System for Real-Time Surveillance Against Cyber-Physical Attacks
Glen Moepi, Topside Mathonsi 602-606

Utilization and Sharing of Cyber Threat Intelligence Produced by Open-Source Intelligence
Jyri Rajamäki, Stephen McMenamin 607-611

Implementation of OSINT for Improving an International Finance Sector Organization's Cybersecurity
Jyri Rajamäki, Krista Tiitta 612-616

Art Crime Does not pay: Multiplexed Social Network Analysis in Cultural Heritage Trafficking Forensics
Jarno Salonen, Alessandro Guarino 617-620