

14th International Conference on Cyber Warfare and Security (ICCWS 2019)

Stellenbosch, South Africa
28 February – 1 March 2019

Editors:

**Noelle van der Waag-Cowling
Louise Leenen**

ISBN: 978-1-5108-8292-8

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, (2019). All Rights Reserved. No reproduction, copy or transmission may be made without written permission from the individual authors.

Printed by Curran Associates, Inc. (2019)

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

Contents

Paper Title	Author(s)	Page No
Preface		v
Committee		vi
Biographies		viii
Research papers		
Effective Policing Apparatus in Nigeria: The Place of Forensic Soundness	John Alhassan, Adamu Muhammed, N. Iwokhagh, Musa Aibinu, Joseph Ojeniyi and A. Uduimoh	1
Distributed IDS Using Agents: An Agent-Based Detection System to Detect Passive and Active Threats to a Network	Abdullahi Arabo	11
Advanced Technologies Combating Terrorism in the EU: The Psychological Warfare Aspect	Darya Bazarkina	23
System for Detecting Data Protection Violations	Peter Chan and Lauren Hankel	30
AI-Based Deterrence in the Cyber Domain	Jim Chen	38
A Survey of APT Defence Techniques	Mercy Chitauro, Hippolyte Muyingi, Samuel John and Shadreck Chitauro	46
Implementing SCADA Scenarios and Introducing Attacks to Obtain Training Data for Intrusion Detection Methods	Simon Duque Antón, Michael Gundall, Daniel Fraunholz and Hans Dieter Schotten	56
A Digital Economy Technology Intergration Model Incorporating the Cyber Security Layer	Attlee Gamundani, Fungai Bhunu-Shava and Mercy Bere	65
Building an Ontology for Planning Attacks That Minimize Collateral Damage: Literature Survey	Tim Grant	78
Navigating the Cyber Sea: Dangerous Atolls Ahead	Virginia Greiman	87
Acknowledging and Reducing the Knowing and Doing gap in Employee Cybersecurity Compliance	Tapiwa Gundu	94
The Terrorist/Jihadi use of 3D-Printing Technologies: Operational Realities, Technical Capabilities, Intentions and the Risk of Psychological Operations	Ferdinand Haberl and Florian Huemer	103
Preserving Privacy and Integrity in Automotive Tire Sensors	Kenneth Hacker and Scott Graham	110
Database Security: Ensuring That the Database Course can Serve Cybersecurity Students as Well as Traditional Computer Science Students	Douglas Hawley	116
Online Security Behaviour: Factors Influencing Intention to Adopt Two-Factor Authentication	Mitch Holmes and Jacques Ophoff	123
Testing the Fault Tolerance of a Backup Protection System Using SPIN	Kenneth James and Kenneth Hopkinson	133

Paper Title	Author(s)	Page No
Fake Narratives, Dominant Discourses: The Role and Influence of Algorithms on the Online South African Land Reform Debate	Anna-Marie Jansen van Vuuren and Turgay Celik	142
Exploring Interactive Narrative and Ideology in War Games	Anna-Marie Jansen van Vuuren and Tristan Jacobs	148
Framework for the Development and Implementation of a Cybercrime Strategy in Africa	Joey Jansen van Vuuren, Louise Leenen and Piet Pieterse	156
Evolution of US Cybersecurity Strategy	Saltuk Karahan, Hongyi Wu and Leigh Armistead	168
Managing Classified Records in Inter-Governmental Organizations	Shadrack Katuu	177
Categorising Cyber Security Threats for Standardisation	Zubeida Casmod Khan	189
Enriching Behavioural Biometrics Experiments With an Ontology	Zubeida Casmod Khan	197
Token-Based Lightweight Image Cryptography Method for Internet of Things	Shih-Hsiung Lee and Chu-Sing Yang	207
Framework for the Cultivation of a Military Cybersecurity Culture	Louise Leenen and J.C Jansen van Vuuren	212
Data Poisoning: Achilles Heel of Cyber Threat Intelligence Systems	Thabo Mahlangu, Sinethemba January, Thulani Mashiane, Moses Dlamini, Siphon Ngo-beni and Nkqubela Ruxwana	221
Ethics of Trust in Man-Machine AI Interactions	Mary Manjikian	231
The Cybercrime Combating Platform	Fikile Mapimele and Bokang Mangoale	237
A Rollout Strategy for Cybersecurity Awareness Campaigns	Thulani Mashiane, Zama Dlamini and Thabo Mahlangu	243
Positioning South Africa in the BRICS Cybersecurity Context: A Strategic Perspective	Zoran Mitrovic and Colin Thakur	251
A Validated Lightweight Authentication Protocol Towards Commercial Low-Cost RFID Tags	Kealeboga Mpalane, Zothile Singano and Samuel Lefophane	260
Digital Forensic Readiness Approach for Potential Evidence Preservation in Software-Defined Networks	Howard Munkhondya, Adeyemi Ikuesan and Hein Venter	268
A Mathematical Model of Hacking the 2016 US Presidential Election	Dennis Nilsson Sjöström	277
Enhancing the Security of a Gateway Through Steganography	Docas Nwanebu	287
Cybersecurity Awareness Among Rural Communities in Sango Ota, Ogun State, Nigeria	Patrick Okon, Tolulope Kayode-Adedeji, Tayo-Adigboluja Afolayan and Charles Iruonagbe	294
Cyber Security Investment Cost-Benefit Investigation Using System Dynamics Modelling	Rudolph Oosthuizen, Leon Pretorius, Francois Mouton and Mirriam Molekoa	304
Countering Terrorist Propaganda in Asia: Towards a Better Communications Strategy in Cyberspace	Konstantin Pantserov and Konstantin Golubev	315

Paper Title	Author(s)	Page No
Destabilization of Unstable Dynamic Social Equilibriums Through High-Tech Strategic Psychological Warfare	Evgeny Pashentsev	322
Design and Implementation of an Availability Scoring System for Cyber Defence Exercises	Mauno Pihelgas	329
IIoT Security: Do I Really Need a Firewall for my Train?	Barend Pretorius and Brett van Niekerk	338
The Applicability of the Tallinn Manuals to South Africa	Trishana Ramluckan	348
Social Media as a Declaration of war?	Trishana Ramluckan	356
How the United States Constructs Cyber-Threat Scenarios	Janine Schmoltd	361
A Socio-Technical Systems Analysis of Privacy Issues in Social Media Sites	Nobubele Angel Shoji and Jabu Mtsweni	369
A Bayesian Network Approach to the Proliferation of Software as a Weapon	Jantje Silomon	377
Artificial Intelligence: Playing the Imitation Game	Jantje Silomon and Monica Kaminska	388
Eating the Elephant: A Structural Outline of Cyber Counterintelligence Awareness and Training	Thenjiwe Sithole, Petrus Duvenage, Victor Jaquire and Sebastian von Solms	396
The Limitations of National Cyber Security Sensor Networks Debunked: Why the Human Factor Matters	Florian Skopik	405
Developing Military Cyber Workforce in a Conscript Armed Forces: Recruitment, Challenges and Options	Tiia Sömer, Rain Ottis and Birgy Lorenz	413
Applying Game Elements to Cyber eLearning: An Experimental Design	Landon Tomcho, Alan Lin, David Long, Mark Coggins and Mark Reith	422
Artificial Intelligence in the Cyber Security Environment	Petri Vähäkainu and Martti Lehto	431
The Cyber Security Dilemma: A South African Perspective	Brett van Niekerk	441
Economic Information Warfare: Classifying Cyber-Attacks Against Commodity Value Chains	Brett van Niekerk	448
Develop and Maintain a Cybersecurity Organisational Culture	Carien Van't Wout	457
Contextualising Cybersecurity Readiness in South Africa	Namosha Veerasamy, Thulani Mashiane and Kiru Pillay	467
Africa's Contribution to Academic Research in Cybersecurity: Review of Scientific Publication Contributions and Trends From 1998 to 2018	Sune von Solms	476
Analysing Different Approaches to Cross-Border Electronic Evidence Data-Sharing in Criminal Matters	Murdoch Watney	484
South African Android Applications, Their Security Permissions and Compliance With the Protection of Personal Information Act	Quintin White and Wynand van Staden	492

Paper Title	Author(s)	Page No
PhD Research Papers		503
A Taxonomy for Cybercrime Attack in the Public Cloud	Stacey Omeleze Baror and Hein Venter	505
Encryption Methodologies Based on Floating Point Algorithms	Weston Govere and Jonathan Blackledge	516
Strategic Culture Theory as a Tool for Explaining Russian Cyber Threat Perception	Martti Kari	528
Cybersecurity Incident Response for the Sub-Saharan African Aviation Industry	Faith Lekota and Marijke Coetzee	536
Securing the Internet of Battlefield Things While Maintaining Value to the Warfighter	Kasey Miller, Bryan O'Halloran, Anthony Pollman and Megan Feeley	546
An Analysis of Small and Medium-Sized Enterprises' Perceptions of Security Evaluation in Cloud Business Intelligence	Moses Moyo and Marriane Look	554
Masters Research Papers		563
Distributed-Ledger Based Event Attestation for Intelligent Transportation Systems	Luis Cintron, Scott Graham, Douglas Hodson and Barry Mullins	565
Comparison Analysis of AODV and DSR Under Attack by Black Hole Nodes in a NS3 Simulation	Thomas Edward Fogwell and Elisha Oketch Ochola	574
State of the art in Digital Forensics for the Internet of Things	Jaco-Louis Kruger and Hein Venter	588
Rethinking USAF Cyber Education and Training	Seth Martin and Mark Reith	597
A Novel Perspective on Cyber Attribution	Ronald Morgan and Douglas Kelly	609
Quantifying Cyber Vulnerability and Risk in Acquisitions	Aaron Pendleton and Mark Reith	618
Building Irrefutable Trust Throughout Computer Networks Using Blockchains	Dillon Pettit and Mark Reith	625
A Context-Aware Trigger Mechanism for Ransomware Forensics	Avinash Singh, Adeyemi Ikuesan and Hein Venter	629
Towards Understanding the Value of Ethical Hacking	Jason Wallingford, Mihika Peshwa and Douglas Kelly	639
Non Academic Paper		651
Constructing Large Scale Cyber Wargames	Kimo Bumanglag, David Law, Adam Welle and Peter Barrett	653
Work In Progress Papers		661
Enabling Trust in IIoT: An Physec Based Approach	Christoph Lipps, Simon Duque Antón and Hans Dieter Schotten	663
Towards the Development of a Neo4j Tool for Client Forensics	Rosemary Shumba and Joram Ngwenya	673