15th International Conference on Cyber Warfare and Security (ICCWS 2020)

Norfolk, Virginia, USA
12 – 13 March 2020

Editors:

Brian K. Payne
Hongyi Wu

ISBN: 978-1-7138-0880-0

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, (2020). 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. (2020)

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		vii
Research papers		
Prey-Predator Model for Countering Internet-assisted Radicalization and Recruitment	Naresh Adhikari, Naila Bushra and Amrita Ghimire	1
Blockchain-based Redistricting Evaluation Protocol	Naresh Adhikari, Naila Bushra and Mahalingam Ramkumar	9
A Layered Network Collapse Method in Cyber Terrorism	Elie Alhajjar and Steve Morse	18
Resilient Cybersecurity Architecture	Wasim A AlHamdani	23
Cyber Alliances and Proxy Cyber Warfare	Jorge Barbosa	33
Cyber Warfare: Can there be Small Cyber Military Powers?	Jorge Barbosa	39
An Examination in Social Engineering: The Susceptibility of Disclosing Private Security Information in College Students	Rachel Bleiman and Aunshul Rege	47
Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security	Jonny Botha and Heloise Pieterse	57
Electronic Healthcare Record and Cyber Security Threats: A Development of an Agile Framework	Sarah Bouazzaoui and Charles Daniels	67
Scalable Verification of NP Problems in Blockchain	Naila Bushra, Naresh Adhikari and Mahalingam Ramkumar	72
A Warfare Domain Approach to the Disinformation Problem	Mustafa Canan and Anthony Akil	82
Countering Disinformation Propaganda: Reverse Engineering the Experimental Implicit Learning Paradigm	Mustafa Canan and Daphne Canan	92
The Strategy of Persistent Engagement: From Single Domain to Cross-Domains	Jim Q. Chen	102
Fingerprinting Vehicles With CAN Bus Data Samples	David R. Crow, Scott R. Graham and Brett J. Borghetti	110
Mathematically Modelling Cyber-Attacks Utilizing Engineering Techniques	Chuck Easttom	119
Applying Systems Engineering Principles to Penetration Testing	Chuck Easttom and William Butler	127
From Simple Scoring Towards a Meaningful Interpretation of Learning in Cybersecurity Exercises	Margus Ernits, Kaie Maennel, Sten Mäses, Toomas Lepik and Olaf Maennel	135
Intelligent based Framework for Detection of Fake News in the Social Network Platforms	Olusanjo Fasola, Joseph Ojeniyi and Samuel Oyeniyi	144

Paper Title	Author(s)	Page No
Leveraging Serious Games in Air Force Multi-Domain Operations Education: A Pilot Study	Nathaniel Flack, Christopher Voltz, Richard Dill, Alan Lin and Mark Reith	155
Cyber Resilience through Machine Learning: Data Exfiltration	Kieran Fletcher and H. Anthony Smith	165
Connected Vehicle Security	Guillermo A. Francia, III	173
Cyberwar as a New Type of War?	Petr Frantis	182
A Strategic Roadmap for Cybersecurity Capability Engineering across Different Environments	Noluxolo Gcaza and Jabu Mtsweni	187
An Analysis of Connected Cars Technology and Security	Ahmad Ghafarian and Saman Sardari	195
Artificially Intelligent Systems and Human Rights: A Global Perspective	Virginia A. Greiman	204
Information Policy Security Compliance in Dutch Local Government: Results from a Vignette Survey	Vincent Homburg and Jeroen Kokje	211
Notre Dame Fire Conspiracism as Reflective of Russian Ideological Competition with the West	Michael Bennett Hotchkiss	219
The Critical Need for Tool Validation before Using Malware Scanners in Digital Forensics	Nicolas Hughes and Cihan Varol	228
Avoiding the Pitfalls of an Artificial Reality (Is A.I. Real Enough)	John S. Hurley and Dorothy O. Potter	236
Toward an Ambidextrous Framework for Offensive Cyberspace Operations: A Theory, Policy and Practice Perspective	Gazmend Huskaj and Ion A. Iftimie	243
Anticipatory Ethics for Vulnerability Disclosure	Gazmend Huskaj and Richard L. Wilson	254
The Use of Signals Intelligence in Offensive Cyberspace Operations: An Anticipatory Ethical Analysis	Ion A. Iftimie and Richard L. Wilson	262
Customers' Perception of Cybersecurity Threats Toward e-Banking Adoption and Retention: A Conceptual Study	Abdul Bashiru Jibril, Michael Adu Kwarteng, Miloslava Chovancova and Richard Denanyoh	270
A Fast Alert Correlation Method with Bayesian Feature Constraints	Minchul Kim, Youngwoo Park, Insung Han and Sungyoung Cho	277
Crown in the Clouds: A Canadian Data Sovereignty Crisis	Neal Kushwaha and Bruce W. Watson	286
Digital Forensic Readiness Framework for Software-Defined Networks Using a Trigger-Based Collection Mechanism	Maxime Lagrasse, Avinash Singh, Howard Munkhondya, Adeyemi Ikuesan and Hein Venter	296
Representing Strategic Cyber and Information Warfare in Matrix Games	Hyong Lee and James DeMuth	306
Non-Kinetic Warfare: The New Game Changer in the Battle Space	Martti Lehto and Gerhard Henselmann	316
Mini-Drones Swarms and Their Potential in Conflict Situations	Martti Lehto and Bill Hutchinson	326

Paper Title	**Author(s)**	**Page No**
Enhanced Channel-PUFs: The Advantages of Artificial Intelligence for Channel Estimation	Christoph Lipps, Sachinkumar Bavikatti Mallikarjun, Mathias Strufe and Hans Dieter Schotten	335
Bring Your Own Device (BYOD) Information Security Risks: Case of Lesotho	Mamoqenelo Priscilla Morolong, Fungai Bhunu Shava and Attlee M. Gamundani	346
Complex Network Analysis for Evaluating Effects of Asymmetry Established by Closed National Networks	Juha-Pekka Nikkarila and Vesa Kuikka	355
Impact of Security and Trust as Factors that influence the Adoption and Use of Digital Technologies that Generate, Collect and Transmit User Data	Fortune Nwaiwu, Michael Adu Kwarteng, Abdul Bashiru Jibril, Ladislav Buřita and Michal Pilik	363
Defending Forward: An Exploration through the Lens of Biocybersecurity	Xavier-Lewis Palmer and Saltuk Karahan	373
Systemic Methodology for Cyber Offense and Defense	C. Ariel Pinto and Matthew Zurasky	380
Distributed Authority as a Guiding set of Principles for Transnational Cyber Security Governance	Karine Pontbriand	391
The New Role of the ‘Next Generation’ CFO	Dorothy O. Potter and John S. Hurley	398
Cyber-assets at Risk (CAR): The Cost of Personally Identifiable Information Data Breaches	Omer Ilker Poyraz, Sarah Bouazzaoui, Omer Keskin, Michael McShane and C.Ariel Pinto	402
Leveraging the Benefits of Big Data with Fast Data for Effective and Efficient Cybersecurity Analytics Systems: A Robust Optimisation Approach	Paresh Rathod and Timo Hämäläinen	411
International Information Power and Foreign Malign Influence in Cyberspace	Joseph H. Schafer	423
Bug Bounties: Bottom-up Initiatives as Forms of Cyber Arms Control?	Jantje A. M. Silomon	431
Modelling the Supply Chain: Trust but Verify in Complex Systems	Theresa Sobb, Char Sample, Cragin Shelton and Benjamin Turnbull	439
NetFlow Based Framework for Identifying Anomalous End User Nodes	Risto Vaarandi and Mauno Pihelgas	448
IoT –based Adversarial Attack‘s Effect on Cloud Data Platform Services in a Smart Building Context	Petri Vähäkainu, Martti Lehto and Antti Kariluoto	457
Cyber Probability of Kill: The Effectiveness of Malware in a Heterogeneous Software Environment	Brandon Webster, Matthew Stenger, Alix Valcin, Joel Coffman and Carlos Salazar	466
Who Hath Measured the (Proving) Ground: Variation in Offensive Capabilities Test and Evaluation	JD Work	471
A Method for Teaching Open Source Intelligence (OSINT) Using Personalised Cloud-based Exercises	Saber Yari, Sten Mäses and Olaf Maennel	480
PhD Research Papers		491
Examining the “Known Truths” in Cyber Threat Intelligence – The Case of STIX	Siri Bromander, Lilly Pijnenburg Muller, Martin Eian and Audun Jøsang	493
Career Development in Cyber Security: Bootcamp Training Programs	Emin Caliskan and Risto Vaarandi	503

Paper Title	Author(s)	Page No
An Anticipatory Ethical Analysis of Offensive Cyberspace Operations	Gazmend Huskaj and Richard L. Wilson	512
Rising to the Challenge of Insider Threats for Middle Powers	Jessemyn Modini, Mark Van Zomeren, Stuart Fowler, Keith Joiner and Tim Lynar	521
Psychometric Modelling of Cybersecurity Roles	Paul Wyatt Poteete	530
National Cyber Threat Prevention Mechanism as a part of the E-EWS	Jussi Simola and Martti J. Lehto	539
Beyond 2000: The Rise of Australian Cyber Warfare Capability	Andrew Williams	549
Masters Research Papers		557
Cybersecurity Knowledge Requirements for Strategic Level Decision Makers	Fernando Garcia-Granados and Hayretdin Bahsi	559
A Review of Security System Assessment Tools Suitable for eHealth in Namibia	Naemi Gerson and Fungai Bhunu Shava	569
An Analysis of Social Networking Threats	Jennyphar Kahimise and Fungai Bhunu Shava	576
A Case for a Dynamic Approach to Digital Forensic Readiness in an SDN Platform	Howard Munkhondya, Adeyemi R. Ikuesan and Hein S. Venter	584
Non Academic Paper		595
Cyber Attack Grammars for Risk/Cost Analysis	Terry Patten, Daniel Mitchell and Catherine Call	597
Work In Progress Paper		607
Alternate Coupling for Targeted Supply Chain Attacks	David M. Rohret and Abiud Jimenez	609
Late Submissions		615
A Defined Digital Forensic Criteria for Cybercrime Reporting	Stacey Omeleze Baror, Richard Adeyemi Ikuesan and Hein S. Venter	617
Digital Forensic Readiness Framework for Smart Homes	Sebastien Philomin, Avinash Singh, Adeyemi Ikuesan and Hein Venter	627