19th European Conference on Cyber Warfare and Security (ECCWS 2020)

Online
25 – 26 June 2020

Editors:

Thaddeus Eze
Lee Speakman
Cyril Onwubiko

ISBN: 978-1-7138-1445-0

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		vi
Committee		vii
Biographies		viii
Research papers		
On the Security of the EMV Authentication Methods of Contactless Cards	Ossama Al-Maliki and Hisham Al-Assam	1
Online Fraud & Money Laundry in E-Commerce	Hasan Alsaibai, Shooq Waheed, Fatima Alaali, and Rami Abu Wadi	13
Cyber Humanity in Cyber War	Jorge Barbosa	20
Detecting a Rogue Switch using Network Automation	Vijay Bhuse and Vineet James	26
An Investigation into Evidence (Digital) Artefacts Resulting from the use of Cryptocurrency Applications	Stephen Blenkin, Gareth Davies and Peter Eden	32
Information Sharing in Cyber Defence Exercises	Agnė Brilingaitė, Linas Bukauskas, Aušrius Juozapavičius and Eduardas Kutka	42
Analysis of Reports on Cyber Threats and Attacks Using Text-Analytical Software	Ladislav Burita	50
Tracking Botnets on Nation Research and Education Network	Ivan Daniel Burke and Alan Herbert	61
Fostering Cybersecurity Awareness Among Computing Science Undergraduate Students: Motivating by Example	Tiago Cruz and Paulo Simões	72
Cyber Crisis Management and Leadership	Didier Danet and Claude Weber	82
Water Distribution Network Leak Detection Management	Arno de Coning and Francois Mouton	89
Cyber as a Hybrid Threat to NATO's Operational Energy Security	Arnold Dupuy, Ion Iftimie, Daniel Nussbaum and Stefan Pickl	98
Cyber Counterintelligence: Some Contours towards the Academic Research Agenda	Petrus Duvenage, Victor Jaquire and Sebastian von Solms	107
An Ontology for Cyber ISTAR in Offensive Cyber Operations	Tim Grant, Carien van 't Wout and Brett van Niekerk	117
The Weapons of Choice: Terrorist Armament Culture and the Use of Firearms in Online Propaganda and Identity-Building through Cyberspace	Ferdinand J. Haberl	126
What LEGAD needs to know? Analysis of AARs from Locked Shields (2012-2018)	Jakub Harašta	136

Paper Title	Author(s)	Page no
Strengthening the Cybersecurity of Smart Grids: The Role of Artificial Intelligence in Resiliency of Substation Intelligent Electronic Devices	Ion A. Iftimie and Gazmend Huskaj	143
Online Polarization, Radicalization and Conspiracy	Petri Jääskeläinen and Aki-Mauri Huhtinen	151
An Ontology for the South African Protection of Personal Information Act	Y. Jafta, L. Leenen and P. Chan	158
Usefulness of Cyber Attribution Indicators	Henrik Karlzén	168
Turning the Asymmetry Around: Tactical Principles of Warfare in the Cyber Domain	Mikko Kiviharju and Mika Huttunen	177
Finnish View on the Combat Functions in the Cyber Domain	Mikko Kiviharju, Mika Huttunen and Harry Kantola	186
Cyber Wargaming on the Technical/Tactical Level: The Cyber Resilience Card Game (CRCG)	Thorsten Kodalle	195
Using Machine Learning for DNS over HTTPS Detection	Michal Konopa, Jan Fesl, Jiří Jelínek, Marie Feslová, Jiří Cehák, Jan Janeček and František Drdák	205
Towards Cyber Sensing: Venturing Beyond Traditional Security Events	Artūrs Lavrenovs, Kimmo Heinäaro and Erwin Orye	212
Cyber Security Capacity Building: Cyber Security Education in Finnish Universities	Martti Lehto	221
How to Secure the Communication and Authentication in the IIoT: A SRAM-based Hybrid Cryptosystem	Christoph Lipps, Pascal Ahr and Hans Dieter Schotten	232
Blockchain Based Voting Systems	Yash Soni, Leandros Maglaras and Mohamed Amine Ferrag	241
The Future Direction of Cybercrime and the Difficulties of Digital Investigations: A Rationale for a Review of Digital Investigation Specialist Education	Angela Mison, Gareth Davies and Peter Eden	249
Hybrid Warfare in Society's Information Environment: An Empirical Analysis Using the Grounded Theory	Erja Mustonen-Ollila, Martti J. Lehto and Jukka Heikkonen	258
Actors in Society's Hybrid Information Environment: Grounded Theory Analysis	Erja Mustonen-Ollila, Martti J. Lehto and Jukka Heikkonen	268
Young People and the Dark Side of Social Media: Possible Threats to National Security	Teija Norri-Sederholm, Reetta Riikone, Panu Moilanen and Aki-Mauri Huhtinen	278

Paper Title	Author(s)	Page no
Fault Tolerance: An Approach Toward a Hybrid Fault Tolerance Framework Within a Distributed Computer Architecture	Christopher O'Flaherty, Louis Hyman, Malcolm Hodgson and Dewald Blaauw	284
Mobile Forensics: Beyond Traditional Sources of Digital Evidence	Heloise Pieterse	295
Cyber Security: Trust Based Architecture in the Management of an Organization's Security	Jouni Pöyhönen and Martti Lehto	304
Cybersecurity Awareness in an Industrial Control Systems Company	Stefan Prins, Annlizé Marnewick and Suné von Solms	314
Ransomware Attacks Against Critical Infrastructure	Aunshul Rege and Rachel Bleiman	324
Cyber-Informed: Bridging Cybersecurity and Other Disciplines	Char Sample, Sin Ming Loo, Connie Justice, Eleanor Taylor and Clay Hampton	334
Towards a Methodology for the Classification of IoT Devices	Dimitrios Sarris, Konstantinos Xynos, Huw Read, and Iain Sutherland	342
Cyber Security System of FPGA Platform for Wireless Sensor Networks	Gulfarida Tulemissova and Olimzhon Baimuratov	351
Security of Systems on Chip	Eda Tumer and Leandros Maglaras	362
Influence of Attack Vectors on Generic Artificial Intelligence –assisted Smart Building Feedback Loop System	Petri Vähäkainu, Martti Lehto and Antti Kariluoto	371
Assessment of the French and Dutch Perspectives on International Law and Cyber-Operations	Brett van Niekerk, Trishana Ramluckan and Daniel Ventre	380
Signing Your Name Away: An Overview on the Risks of Electronic Signatures	Suné von Solms	390
Artificial Intelligence and its' Legal Risk to Cybersecurity	MM Watney	398
Smart City IoT: Co-Designing Trustworthy Public Safety Drones for Indoor Flight Missions	Harry Wingo	406
The Evolution of Ransomware Variants	Ashley Charles Wood and Thaddeus Eze	410
Vulnerabilities Analysis of Software Solutions for Critical Activity Sectors	Alin Zamfiroiu, Victor Emmanuell Badea and Paul Pocatilu	421
Small Network Telescope for Advanced Security Monitoring	Linda Zeghache and Hakimi Yacine	428
A Viewpoint on Management Practices for Cybersecurity in Industry 4.0 Environment	Najam Ul Zia and Victor Kwarteng Owusu	435
A Change Management Perspective to Implementing a Cyber Security Culture	Trishana Ramluckan, Brett van Niekerk and Isabel Martins	442

Paper Title	Author(s)	Page no
Phd Research Papers		449
Cyberattacks and the Prohibition of the Use of Force under Humanitarian Law with Reference to the Tallinn Manual	Khalil Akbariavaz, Pardis Moslemzadeh Tehrani and Johan Shamsuddin bin Haj Sabaruddin	451
A Study on Problems of Behaviour-based User Attribution in Computer Forensic Investigation	Francis Xavier Kofi Akotoye, Richard Ikuesan Adeyemi and Hein S. Venter	458
Defining the Workforce and Training Array for the Cyber Risk Management and Cyber Resilience Methodology of an Army	Lisa Davidson	466
Designing Attack Infrastructure for Offensive Cyberspace Operations	Gazmend Huskaj, Ion A. Iftimie and Richard L. Wilson	473
Applications of Epidemiology to Cybersecurity	Jessemyn Modini, Timothy Lynar, Elena Sitnikova and Keith Joiner	483
Computational Propaganda: Targeted Advertising and the Perception of Truth	Julie Murphy, Anthony Keane and Aurelia Power	491
Comparing Personality Traits Between Penetration Tester, Information Security and its Professionals from Two Cohorts	Olav Opedal	501
A Framework for a Foundational Cyber Counterintelligence Awareness and Skills Training Programme	Thenjiwe Sithole, Jaco du Toit, Victor Jaquire and Sebastian von Solms	510
The Three "Cyber Logics" and Their Implications to Cyber Conflicts: Germany, France, and the United Kingdom as Case Studies	Bruna Toso de Alcântara	518
Cyber Deterrence and Russia's Active Cyber Defense	Maija Turunen and Martti J Kari	526
The Roots of Restraint in Cyber Conflict	Federico Variola	533
Strategic Cyber Threat Intelligence: Building the Situational Picture with Emerging Technologies	Janne Voutilainen and Martti Kari	545
Event Tracing for Application Security Monitoring in Linux	Jack Whitter-Jones, Mark Griffiths and Ross Davies	554
Masters Papers		559
Enabling Rapid Response and Service Restoration with Machine Learning Techniques	Andre Lopes and Andrew Hutchison	561
Using Ethereum Smart Contracts for Botnet Command and Control	Alexandre Oliveira, Vinícius Gonçalves and Geraldo Rocha Filho	570
Towards Cyber-User Awareness: Design and Evaluation	Toyosi Oyinloye, Thaddeus Eze and Lee Speakman	577

Paper Title	Author(s)	Page no
OS Kernel Malware Detection through Data-Characterization of Memory Analysis	Harmi Armira Mohamad Har, Farihan Ghazali and Maslina Daud	589
Non-Academic Paper		597
Mitigating Insider Threats: A Case Study of Data Leak Prevention	Nurul Mohd and Zahri Yunos	599
Work in Progress Papers		607
Modern Techniques for Discovering Digital Steganography	Michael T. Hegarty and Anthony J. Keane	609
SHAPES Secure Cloud Platform for HealthCare Solutions and Services	Jyri Rajamäki and Aarne Hummelholm	614
Late Submission		619
Artificial Intelligence in Megaprojects: The Next Frontier	Virginia A. Greiman	621