# 18th European Conference on Cyber Warfare and Security (ECCWS 2019)

Coimbra, Portugal
4 - 5 July 2019

**Editors:**

**Tiago Cruz**
**Paulo Simoes**

ISBN: 978-1-5108-9009-1

**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** | | vii |
| **Committee** | | viii |
| **Biographies** | | x |
| **Research papers** | | |
| Using Hypervisors to Overcome Structured Exception Handler Attacks | Asaf Algawi, Michael Kiperberg, Roee Leon and Nezer Zaidenberg | 1 |
| Creating Modern Blue Pills and Red Pills | Asaf Algawi, Michael Kiperberg, Roee Leon, Amit Resh and Nezer Zaidenberg | 6 |
| Information Technology Governance: The Role of Board of Directors in Cybersecurity Oversight | Abdalmuttaleb Al-Sartawi | 15 |
| Revisiting Cyber Definition | Riza Azmi and Kautsarina | 22 |
| Secure Application for Health Monitoring | Vijay Bhuse and Harsh Sinha | 31 |
| Crossed Swords: A Cyber Red Team Oriented Technical Exercise | Bernhards Blumbergs, Rain Ottis and Risto Vaarandi | 37 |
| The far Right of the UK and Ukraine’s Views About European Integration: An Analysis of Online Political Discourse | Radomir Bolgov and Olga Filatova | 45 |
| A Comparison of Chat Applications in Terms of Security and Privacy | Johnny Botha, Carien Van‘t Wout and Louise Leenen | 55 |
| Detection of Premeditated Security Vulnerabilities in Mobile Applications | Agnė Brilingaitė, Linas Bukauskas and Eduardas Kutka | 63 |
| Online Glossary of Cyber Security | Ladislav Burita | 72 |
| A Framework for Managing Cybersecurity Effectiveness in the Digital Context | Marian Carcary, Eileen Doherty and Gerry Conway | 78 |
| Personal Data Protection (PDP): A Conceptual Framework for Organisational Management of Personal Data in the Digital Context | Marian Carcary, Eileen Doherty and Gerry Conway | 87 |
| A Capability Approach to Managing Organisational Information Security | Marian Carcary, Eileen Doherty and Gerry Conway | 97 |
| Leveraging the OODA Loop with Digital Analytics to Counter Disinformation | Jami Carroll | 106 |
| A Framework for Improved Home Network Security | António Craveiro, Ana Oliveira, Jorge Proença, Tiago Cruz and Paulo Simões | 114 |
| Hackers and the Military: How to Recruit and Manage Hidden Talents? | Didier Danet | 124 |
| Artificial Intelligence Cybersecurity Framework: Preparing for the Here and now With AI | Emily Darraj, Char Sample and Connie Justice | 132 |
| A Performance Study of the Ethical Hacking Capabilities of Single Board Computers | Adolfo Jose Arias de la Vega and Christina Thorpe | 142 |

| Paper Title | Author(s) | Page No |
|---|---|---|
| Investigation and Surveillance on the Darknet: An Architecture to Reconcile Legal Aspects With Technology | Maxence Delong, Eric Filiol and Baptiste David | 151 |
| Cybersecurity Assessment of the Public Sector in Greece | George Drivas, Leandros Maglaras, Helge Janicke and Sotiris Ioannidis | 162 |
| Improving Phishing Awareness in the United States Department of Defense | Christopher Dukarm, Richard Dill and Mark Reith | 172 |
| Putting Together the Pieces: A Concept for Holistic Industrial Intrusion Detection | Simon Duque Antón and Hans Dieter Schotten | 178 |
| A Cyber Counterintelligence Matrix for Outsmarting Your Adversaries | Petrus Duvenage, Victor Jaquire and Sebastian von Solms | 187 |
| The Offensive Cyber Operations Playbook | Dennis Granåsen and Margarita Jaitner | 194 |
| Building a (French) National Priority: The Grammar of the French Cyber Defence Strategy | Saïd Haddad | 202 |
| Where Cyber Meets the Electromagnetic Spectrum | Gerhard Henselmann and Martti Lehto | 209 |
| Protection of Critical Infrastructure in National Cyber Security Strategies | Eduardo Izycki and Rodrigo Colli | 219 |
| Towards a Framework for the Selection and Prioritisation of National Cybersecurity Functions | Pierre Jacobs, Sebastiaan von Solms, Marthie Grobler and Brett van Niekerk | 229 |
| Information Security Management Scaffold for Mobile Money Systems in Uganda | Fredrick Kanobe, Margaret Patricia Alexander and Kelvin Joseph Bwalya | 239 |
| Optimal Sensor Placement in Network Topology From the Defence Point of View | Vesa Kuikka and Juha-Pekka Nikkarila | 248 |
| Operator Impressions of 3D Visualizations for Cybersecurity Analysts | Kaur Kullman, Noam Ben Asher and Char Sample | 257 |
| The Balanced Digitalization and Digital Security: Case of Regional Authorities | Tuija Kuusisto and Rauno Kuusisto | 267 |
| Operational Tempo in Cyber Operations | Antoine Lemay and Sylvain Leblanc | 275 |
| In Search of a Social Contract for Cybersecurity | Andrew Liaropoulos | 282 |
| The Importance of Strategic Leadership in Cyber Security: Case of Finland | Jarno Limnéll and Martti Lehto | 288 |
| PhySec in Cellular Networks: Enhancing Security in the IIoT | Christoph Lipps, Mathias Strufe, Sachinkumar Bavikatti Mallikarjun and Hans Dieter Schotten | 297 |
| Technical Guidelines for Evaluating and Selecting Data Sources for Cybersecurity Threat Intelligence | Jabu Mtsweni and Muyowa Mutemwa | 305 |
| Cyberpsychological Threat Intelligence | Julie Murphy and Anthony Keane | 314 |
| Strategic Foresight and Resilience Through Cyber-Wargaming | David Ormrod and Keith Scott | 319 |

| **Paper Title** | **Author(s)** | **Page No** |
|---|---|---|
| The Persuasion Game: Developing a Serious Game Based Model for Information Warfare and Influence Studies | David Ormrod, Keith Scott, Lynn Scheinman, Thorsten Kodalle, Char Sample and Benjamin Turnbull | 328 |
| Cyber Attribution 2.0: Capture the False Flag | Timea Pahi and Florian Skopik | 338 |
| Operational Risk Assessment on Internet of Things: Mitigating Inherent Vulnerabilities | Youngjun Park, Mark Reith and Barry Mullins | 346 |
| Cyber Security of Vehicle CAN bus | Jouni Pöyhönen, Pyry Kotilainen, Janne Poikolainen, Janne Kalmari and Pekka Neittaanmäki | 354 |
| How to Apply Privacy by Design in OSINT and big Data Analytics? | Jyri Rajamäki and Jussi Simola | 364 |
| Research Challenges for Cybersecurity and Cyberwarfare: A South African Perspective | Trishana Ramluckan, Brett van Niekerk and Louise Leenen | 372 |
| Cyber-Influence Operations: A Legal Perspective | Trishana Ramluckan, Alicia Wanless and Brett van Niekerk | 379 |
| Online Expression and Spending on Personal Cybersecurity | Juhani Rauhala, Pasi Tyrväinen and Nezer Zaidenberg | 387 |
| Does Time Spent on Device Security and Privacy Inhibit Online Expression? | Juhani Rauhala, Pasi Tyrväinen and Nezer Zaidenberg | 394 |
| The Need for More Sophisticated Cyber-Physical Systems war Gaming Exercises | Aunshul Rege and Joe Adams | 403 |
| Western World Order in the Crosshairs? A Theoretical Review and Application of the Russian 'Information Weapon' | Mari Ristolainen and Juha Kukkola | 412 |
| A Cross-Discipline Approach to Countering 4th Generation Espionage | Char Sample, Keith Scott and Emily Darraj | 420 |
| A Novel Intrusion Detection System Architecture for Internet of Things Networks | Leonel Santos, Ramiro Gonçalves and Carlos Rabadão | 428 |
| An Analysis of Security Features on Web Browsers | Siddhartha Sengupta and Joon Park | 436 |
| Alert Correlation Using Diamond Model for Cyber Threat Intelligence | Youngsup Shin, Changwan Lim, Mookyu Park, Sungyoung Cho, Insung Han, Haengrok Oh and Kyungho Lee | 444 |
| Digital Dematerialisation in the Portuguese tax System | Ana Paula Silva and Susana Aldeia | 451 |
| Information Security is More Than Just Policy; It is in Your Personality | Petteri Simola, Toni Virtanen and Miika Sartonen | 459 |
| Cyber Security Risk Modelling and Assessment: A Quantitative Approach | Abderrahmane Sokri | 466 |
| Taxonomies of Cybercrime: An Overview and Proposal to be Used in Mapping Cyber Criminal Journeys | Tiia Somer | 475 |
| On Neutrality and Cyber Defence | Marcel Stolz | 484 |

| **Paper Title** | **Author(s)** | **Page No** |
|---|---|---|
| Integrative Approach to Understand Vulnerabilities and Enhance the Security of Cyber-Bio-Cognitive-Physical Systems | Todor Tagarev, Nikolai Stoianov and George Sharkov | 492 |
| Cyber Resilience Strategy and Attribution in the Context of International law | Pardis Moslemzadeh Tehrani | 501 |
| A Biological Framework for Characterizing Mimicry in Cyber-Deception | Steven Templeton, Matt Bishop, Karl Levitt and Mark Heckman | 508 |
| Agile Technology Development to Improve Scenario-Based Learning Exercises | Benjamin Turnbull, David Ormrod, Nour Moustafa and Nicholas Micallef | 518 |
| The Possibilities of Cyber Methods as Part of Maritime Warfare: Baltic Sea | Maija Turunen | 527 |
| Grasping Cybersecurity: A set of Essential Mental Models | Jan van den Berg | 534 |
| A Legal Perspective of the Cyber Security Dilemma | Brett van Niekerk and Trishana Ramluckan | 544 |
| An Analysis of Selected Cyber Intelligence Texts | Brett van Niekerk, Trishana Ramluckan and Petrus Duvenage | 551 |
| A Legal Understanding of State-Linked Cyberattacks and Malicious Cyber Activities | Murdoch Watney | 560 |
| A Methodology for the Comparative Analysis of Strategic Culture and Cyber Warfare | Andrew Williams | 568 |
| Cyber Warfare, Terrorist Narratives and Counter Terrorist Narratives: An Anticipatory Ethical Analysis | Richard Wilson | 577 |
| Cambridge Analytica, Facebook, and Influence Operations: A Case Study and Anticipatory Ethical Analysis | Richard Wilson | 587 |
| Information Warfare: Fabrication, Distortion and Disinformation: A Case Study and Anticipatory Ethical Analysis | Richard Wilson | 596 |
| ARM Security Alternatives | Raz Ben Yehuda, Roee Leon and Nezer Zaidenberg | 604 |
| IoT Architectures for Critical Infrastructures Protection | Alin Zamfiroiu, Bogdan Iancu, Catalin Boja, Tiberiu Georgescu and Cosmin Cartas | 613 |
| **Phd Research Papers** | | 621 |
| A Conceptual Model for the Development of Cybersecurity Capacity in Mozambique | Martina Jennifer Zucule de Barros and Horst Lazarek | 623 |
| The Peculiarities of Securitising Cyberspace: A Multi-Actor Analysis of the Construction of Cyber Threats in the US (2003-2016) | Noran Shafik Fouad | 633 |
| E-Health Systems in Digital Environments | Aarne Hummelholm | 641 |
| Undersea Optical Cable Network and Cyber Threats | Aarne Hummelholm | 650 |

| **Paper Title** | **Author(s)** | **Page No** |
|---|---|---|
| The Current State of Research in Offensive Cyberspace Operations | Gazmend Huskaj | 660 |
| Cyber Sanctions: The Embargo of Flagged Data in a Geo-Cultural Internet | Ion Iftimie | 668 |
| The Transformation of Islamic Terrorism Through Cyberspace: The Case of ISIS | Eleni Kapsokoli | 677 |
| Protecting the Besieged Cyber Fortress: Russia's Response to Cyber Threats | Martti Kari | 685 |
| Government Efforts Toward Promoting IoT Security Awareness for end Users: A Study of Existing Initiatives | Kautsarina and Bayu Anggorojati | 692 |
| Cyber Entanglement: A Framework for the Study of U.S.–China Relations | Karine Pontbriand | 702 |
| Effects of Cyber Domain in Crisis Management | Jussi Simola and Martti Lehto | 710 |
| A Data Security Framework for Cloud Computing Adoption: Mozambican Government Cloud Computing | Ambrósio Patricio Vumo, Josef Spillner and Stefan Köpsell | 720 |
| **Masters Research Papers** | | 731 |
| A Technical Overview on the Usage of Cloud Encryption Services | Daniel Carvalho, João Morais, João Almeida, Pedro Martins, Carlos Quental and Filipe Caldeira | 733 |
| Description Logics and Axiom Formation for a Digital Forensics Ontology | Dagney Ellison, Adeyemi Richard Ikuesan and Hein Venter | 742 |
| Self-Directed Learning Tools in USAF Multi-Domain Operations Education | Nathaniel Flack and Mark Reith | 752 |
| Detecting Advanced Persistent Threat Malware Using Machine Learning-Based Threat Hunting | Tien-Chih Lin, Cheng-Chung Guo and Chu-Sing Yang | 760 |
| A Standardization Guide for Homomorphic Encryption Applications for Digital Forensic Investigations | Nnana Mogano | 769 |
| Fake News Detection Using Ensemble Machine Learning | Potsane Mohale and Wai Sze Leung | 777 |
| Synthetic Data Generation With Machine Learning for Network Intrusion Detection Systems | Marvin Newlin, Mark Reith and Mark DeYoung | 785 |
| Human Factors of Cyber Operations: Decision Making Behind Advanced Persistence Threat Operations | Veikko Siukonen | 790 |
| **Non Academic Papers** | | 799 |
| Thoughts About a General Theory of Influence in a DIME/PMESII/ASCOP/IRC2 Model | Thorsten Kodalle, Char Sample, David Ormrod and Keith Scott | 801 |
| Success Factors and Pitfalls in Security Certifications | Helvi Salminen | 811 |

| **Paper Title** | **Author(s)** | **Page No** |
|---|---|---|
| Instilling Digital Citizenship Skills Through Education: A Malaysian Perspective | Ramona Susanty, Zahri Yunos, Mustaffa Ahmad and Norrizan Razali | 819 |
| Smart Citizens Wanted! How to act Responsibly With Data Security and Privacy? | Christine Ziske and Ulf Ziske | 828 |
| **Work In Progress Papers** | | 837 |
| Towards Automated Threat-Based Risk Assessment for Cyber Security in Smarthomes | Pankaj Pandey, Anastasija Collen, Niels Nijdam, Marios Anagnostopoulos, Sokratis Katsikasand Dimitri Konstantas | 839 |
| Applicability of Resilience Metrics in the Context of Telecommunications Services | Tarja Rusi | 845 |
| Mitigating Return Oriented Programming | Lee Speakman, Thaddeus Eze, David Baker and Samuel Wairimu | 852 |
| US-Russian Relations in Cybersecurity: The Constructivist Dimension | Ilona Stadnik | 858 |