

# **22nd European Conference on Cyber Warfare and Security (ECCWS 2023)**

Piraeus, Greece  
22-23 June 2023

**Editors:**

**Antonios Andreatos  
Christos Douligeris**

ISBN: 978-1-7138-7544-4

**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, (2023). 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. (2023)

**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](mailto: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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

## Contents

<b><u>Preface</u></b>	<b>ix</b>
<b><u>Committee</u></b>	<b>x</b>
<b><u>Biographies</u></b>	<b>xi</b>
<b><u>Academic Papers</u></b>	
<i>A Survey on National Cyber Emergency Plans</i> Konstantinos Adamos, Ioannis Filippopoulos, George Stergiopoulos, Dimitris Gritzalis	1-11
<i>Digital Forensic in A Virtual World; A Case of Metaverse and VR</i> tayba al ali, Sara Al Fulaiti, Manal Abuzour, Sheikha Almaqahami, Richard Ikuesan	12-21
<i>Attention-Based Deep Learning Modelling for Intrusion Detection</i> Ban AlOmar, Dr. Zouheir Trabelsi, Dr. Firas Saidi	22-32
<i>Towards the Development of Indicators of Fake Websites for Digital Investigation</i> Aysha Alkuwaiti, Mera Alremeithi, Haya Alobeidli, Richard Ikuesan	33-43
<i>An Educational Scenario for Teaching Cyber Security Using low-cost Equipment and Open Source Software</i> Antonios Andreatos	44-53
<i>A Methodical Framework for Conducting Reconnaissance and Enumeration in the Ethical Hacking Lifecycle</i> Fouz Barman, Nora Alkaabi, Hamda Almenhali, Mahra Alshedi, Richard Ikuesan	54-64
<i>A Commentary and Exploration of Maritime Applications of Biosecurity and Cybersecurity Intersections</i> Michaela Barnett, Issah Samori, Brandon Griffin, Xavier-Lewis Palmer, Lucas Potter	65-72
<i>Functional Architectural Design of a Digital Forensic Readiness Cybercrime Language as a Service</i> Stacey O Baror, Richard Adeyemi, I, Hein. S Venter	73-82
<i>Teaching Social Science Aspects of Information Security</i> Igor Bernik	83-88
<i>An Analysis of the MTI Crypto Investment Scam: User Case</i> Johnny Botha, Thor Pederson, Louise Leenen	89-99
<i>How to safely communicate with a phishing attacker by email?</i> Ladislav Buřita, Aneta Coufalikova, Kamil Halouzka	100-107
<i>Agile Methods For Improved Cyber Operations Planning</i> Jami Carroll	108-115
<i>A New Interpretation of Integrated Deterrence: Physical and Virtual Strategies</i> Jim Chen	116-123

<i>Influence Diagrams in Cyber Security: Conceptualization and Potential Applications</i> Sabarathinam Chockalingam, Clara Maathuis	124-131
<i>Permission-Based Classification of Android Malware Applications Using Random Forest</i> Nikolaos Chrysikos, Panagiotis Karampelas, Konstantinos Xylogiannopoulos	132-142
<i>Cultural Influences on Information Security</i> Henry Collier, Charlotte Morton, Dalal Alharthi, Jan Kleiner	143-150
<i>Designing a high-fidelity testbed for 5G-based Industrial IoT</i> Diogo Cruz, Tiago Cruz, Vasco Pereira, Paulo Simões	151-160
<i>Cognitive Security: Facing Cognitive Operations in Hybrid Warfare<sup>1</sup></i> Didier Danet	161-168
<i>JTF-ARES as a Model of a Persistent, Joint Cyber Task Force</i> Charlotte Donnelly, Marcel Stolz	169-176
<i>Cyber power in the African context: an exploratory analysis and proposition</i> Petrus Duvenage, Wilhelm Bernhardt, Sebastian von Solms	177-186
<i>DPIA for Cloud-based Health Organizations in the context of GDPR</i> Dimitra Georgiou, Costas Lambrinouidakis	187-198
<i>Radiograph Manufacturer and Model Identification Using Deep-RSI</i> Farid Ghareh Mohammadi, Ronnie Sebro	199-206
<i>Cyberspace Geography and Cyber Terrain: Challenges Producing a Universal map of Cyberspace</i> Alexander Grandin	207-213
<i>Detect, Deny, Degrade, Disrupt, Destroy, Deceive: which is the greatest in OCO?</i> Tim Grant	214-222
<i>Known Unknowns: The Inevitability of Cyber Attacks</i> Virginia Greiman	223-231
<i>Complicity in Unlawful Offensive Cyber Operations Under International Law on State Responsibility</i> Samuli Haataja	232-238
<i>Semiotics of Strategic Narratives of "Antichrist" in Russia's War in Ukraine</i> Michael Hotchkiss	239-247
<i>Processing Model and Classification of Cybercognitive Attacks: Based on Cognitive Psychology</i> Ki Beom Kim, Eugene Lim, Hun Yeong Kwon	248-256
<i>Designing an Email Attack by Analysing the Victim's Profile. An Alternative Anti-Phishing Training Method</i> Dimitrios Lappas, Panagiotis Karampelas	257-266
<i>Designing Security for the Sixth Generation: About Necessity, Concepts and Opportunities</i> Christoph Lipps, Annika Tjabben, Matthias Rüb, Jan Herbst, Sogo Pierre Sanon, Rekha Reddy, Yorman Munoz, Hans D. Schotten	267-275

<i>Tackling Uncertainty Through Probabilistic Modelling of Proportionality in Military Operations</i> Clara Maathuis, Sabarathinam Chockalingam	276-284
<i>Design Lessons from Building Deep Learning Disinformation Generation and Detection Solutions</i> Clara Maathuis, Iddo Kerkhof, Rik Godschalk, Harrie Passier	285-293
<i>Teaching pentesting to social sciences students using experiential learning techniques to improve attitudes towards possible cybersecurity careers</i> Aleksandras Melnikovas, Ricardo G. Lugo, Kaie Maennel, Agnè Brilingaitė, Stefan Sütterlin, Aušrius Juozapavičius	294-302
<i>Spam Email Detection Using Machine Learning Techniques</i> Mr, Antonios Andreatos, Prof	303-310
<i>Cyber Warfare and Cyber Terrorism Threats Targeting Critical Infrastructure: A HCPS-based Threat Modelling Intelligence Framework</i> Rennie Naidoo, Carla Jacobs	311-318
<i>Determination of the end device risk likelihood using the Bayesian network tools</i> Tabisa Ncubekezi	319-331
<i>Enabling fine-grained access control in information sharing with structured data formats</i> Tatu Niskanen, Jarno Salonen	332-340
<i>Towards an active cyber defence framework for SMMEs in developing countries</i> Nombeko Ntingi, Prof Sebastian von Solms, Dr Jaco du Toit	341-348
<i>Participants Prefer Technical Hands-on Cyber Exercises Instead of Organisational and Societal Ones</i> Jani Päijänen, Jarno Salonen, Anni Karinsalo, Tuomo Sipola, Tero Kokkonen	349-357
<i>A Reflection on Typology and Verification Flaws in consideration of Biocycbersecurity/Cyberbiosecurity: Just Another Gap in the Wall</i> Luke Potter, Kim Mossberg, Xavier Palmer	358-365
<i>Assessment of Cyber Security risks: A Smart Terminal Process</i> Jouni Pöyhönen	366-373
<i>Governance and management information system for cybersecurity centres and competence hubs</i> Jyri Rajamäki, Janne Lahdenperä	374-383
<i>Students' Application of the MITRE ATT&amp;CK® Framework via a real-time Cybersecurity Exercise</i> Aunshul Rege, Jamie Williams, Rachel Bleiman, Katorah Williams	384-394
<i>Role of Techno-Economic Coalitions in Future Cyberspace Governance: 'Backcasting' as a Method for Strategic Foresight</i> Mari Ristolainen	395-402
<i>Digital Streets of Rage: Identifying Rhizomatic Extremist Messages During a Hybrid Media Event using Natural Language Processing</i> Teija Sederholm, Petri Jääskeläinen, Milla Lonka, Aki-Mauri Huhtinen	403-409
<i>An Analysis of Critical Cybersecurity Controls for Industrial Control Systems</i> Nkata Sekonya, Siphesihle Sithungu	410-419

<i>NCSS: A global census of national positions on conflict, neutrality and cooperation</i> Radu Antonio Serrano Iova, Tomoe Watashiba	420-428
<i>Developing Cybersecurity in an Industrial Environment by Using a Testbed Environment</i> Jussi Simola, Reijo Savola, Tapio Frantti, Arttu Takala, Riku Lehtonen	429-438
<i>Smart Terminal System of Systems' Cyber Threat Impact Evaluation</i> Jussi Simola, Jouni Pöyhönen, Martti Lehto	439-449
<i>A Cyber Counterintelligence Competence Framework: Developing the Job Roles</i> Thenjiwe Sithole, Jaco Du Toit, Sebastian von Solms	450-457
<i>Static Vulnerability Analysis Using Intermediate Representations: A Literature Review</i> Adam Spanier, William Mahoney	458-465
<i>Legal and ethical issues of pre-incident forensic analysis.</i> Dr Iain Sutherland, Dr Matthew Bovee, Dr Konstantinos Xynos, Dr Huw O. L. Read	466-473
<i>Developing Robust Cyber Warfare Capabilities for the African Battlespace</i> Jabu Mtsweni, Mphahlela	474-483
<i>Cybersecurity Through Thesis in Laurea University of Applied Sciences</i> Ilona Frisk, Harri Ruoslahti, Ilkka Tikanmäki	484-492
<i>On the software architectures for fog-based secure IOT deployments</i> christos tselikis	493-499
<i>Towards Norms for State Responsibilities regarding Online Disinformation and Influence Operations</i> Brett van Niekerk, Trishana Ramluckan	500-509
<i>The Identification of Cybersecurity Work Roles for the Water Sector in South Africa</i> Sune von Solms	510-516
<i>Cyber Lessons that the World Can Learn from Lithuania</i> Matthew Warren, Darius Šttilis, Marius Laurinaitis	517-524
<i>Legal Response to Social Media Disinformation on National Level</i> Murdoch Watney	525-532
<i>On Benchmarking and Validation in Wargames</i> Adam Wilden, Mehwish Nasim, Peter Williams, Tim Legrand, Benjamin Peter Turnbull, Patricia A. H. Williams	533-543
<i>The UN Global Digital Compact (GDC), Achieving a trusted, free, open, and Secure Internet: Trust- building</i> Allison Wylde	544-551
<b><u>PhD Papers</u></b>	
<i>Cybersecurity in Mozambique: Status and Challenges</i> Martina De Barros	553-558

<i>Spreading Lies Through the Cyber Domain</i> Thomas Dempsey	559-566
<i>The Concept of Comprehensive Security as a Tool for Cyber Deterrence</i> Maria Keinonen	567-574
<i>Building Situational Awareness of GDPR</i> Pauliina Hirvonen, Martti J. Kari	575-583
<i>Organisational GDPR Investments and Impacts</i> Pauliina Hirvonen	584-591
<i>A Whole-of-Society Approach to Organise for Offensive Cyberspace Operations: The Case of the Smart State Sweden</i> Gazmend Huskaj, Stefan Axelsson	592-602
<i>A State-of-the-art of Scientific Research on Disinformation</i> Gazmend Huskaj, Stefan Axelsson	602-609
<i>Fake news as a distortion of media reality: tell-truth strategy in the post-truth era</i> Anastasiia Iufereva	610-615
<i>Hybrid threats-possible consequences in societal contexts</i> Georgiana Daniela Lupulescu	616-622
<i>Target Audiences' Characteristics and Prospective in Countering Information Warfare</i> Daniel Ionel Andrei Nistor	623-630
<i>Technology-Oriented Innovations and Cyber Security Challenges in the Healthcare Delivery System: A perspective from Developing Economy</i> Victor Kwarteng Owusu, Professor Gregar	631-638
<i>Deep-learning-based Intrusion Detection for Software-defined Networking Space Systems</i> Uakomba Uhongora, Ronald, Law, Jill	639-647
<b><u>Masters Papers</u></b>	
<i>How Does the Tallinn Manual 2.0 Shed Light on the Threat of Cyber Attacks against Taiwan?</i> Chih-Hsiang Chang	649-656
<i>Digital Forensic Readiness Model for Internet Voting</i> Edmore Muyambo, Stacey O. Baror	657-667
<b><u>Non-Academic Papers</u></b>	
<i>We see what we want to see: Pitfalls of Perception and Decision-making in Security Management</i> Helvi Salminen	669-677
<i>Zero Trust: The Magic Bullet or Devil's Advocate?</i> Helvi Salminen	678-686

## **Work in Progress Papers**

<i>Reconnaissance Techniques and Industrial Control System Tactics Knowledge Graph</i> Thomas Heverin	688-695
<i>AI-based quantum-safe cybersecurity automation and orchestration for edge intelligence in future networks</i> Aarne Hummelholm	696-702
<i>Security Issues of GPUs and FPGAs for AI-powered near &amp; far Edge Services</i> Stylianos Koumoutzelis, Ioannis Giannoulakis, Titos Georgoulakis, George Avdikos, Emmanouil Kafetzakis	703-706
<i>Hybrid Threat and Information Influence in Connection with Security of Supply</i> Jyri Rajamäki, Tehi Palletvuori	707-710
<i>Demand Analysis of the Cybersecurity Knowledge Areas and Skills for the Nurses: Preliminary Findings</i> Jyri Rajamäki, Paresh Rathod, Kitty Kioskli	711-716
<i>Hidden Permissions on Android: A Permission-Based Android Mobile Privacy Risk Model</i> Saliha Yilmaz, Mastaneh Davis	717-724

## **Late Submission**

<i>From Provoking Emotions to fake Images: The Recurring Signs of fake news and Phishing Scams Spreading on Social Media in Hungary, Romania and Slovakia</i> Kenyeres Attila Zoltán and Lauren Weigand	726-732
--	---------