

21st International Conference on Cyber Warfare and Security (ICCWS 2026)

Wilmington, North Carolina, USA
5-6 March 2026

ISBN: 979-8-3313-3334-8

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, (2026). 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. (2026)

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

The papers in these proceedings were presented at the conference in sessions organised by topics at the conference but are presented here by type of paper and then alphabetically by lead author.

About the Proceedings of the 21st International Conference on Cyber Warfare and Security, 2026	vii
Preface	ix
Biographies of Chairs and Keynote Speakers	x
Reviewer Committee	xiii

Academic Papers

<i>SLMs Meet GraphRAG: A Structured Approach to Context-Aware Cybersecurity Hint Generation</i> Ishan Abraham, Jens Mache, Taylor Wolff, Jack Cook, Richard Weiss, Justin Wang	1-8
<i>Systematic Literature Review: Challenges And Issues in the Adoption of SOAR Technology in Cybersecurity</i> Turki Alshammari, Talal Al-Balawi	9-17
<i>The Cyber-Physical Immune System: A Self-Healing V2X Framework for Global Defense and Healthcare</i> Babajide J. Asaju, Almustapha A. Wakili, Saugat Guni, Woosub Jung	18-26
<i>The Evolution of Penetration Testing in the Era of AI</i> Errol Baloyi, Mpho Letshwenyo, Mamello Mtshali, Alex Ramantswana	27-35
<i>Bridging the Cyber Gap: Mapping Misalignment Between Digital Adoption and Cybersecurity Capacity</i> Zakariya Belkhamza	36-44
<i>Evaluating an Investigative Process for Cryptocurrency-Related Crimes</i> Johnny Botha, Kreaan Singh, Louise Leenen	45-56
<i>Social Media's Role in Cyber Warfare: Attack Vectors, Space Ecosystem Integration, and Impacts</i> Gregory Broomfield	57-65
<i>Secure Cross-Domain Data Validation with Field Programmable Gate Arrays</i> Abigail Cliche, James Brock, Ryan Longwell, Jason Dahlstrom, Stephen Taylor	66-74
<i>Malinformation, Deepfakes, and Cyber Warfare: Ethical and Anticipated Ethical Issues</i> Noah Donnelly, Richard Wilson	75-82
<i>The Efficacy of WPA3 in Enhancing Human-Centered Privacy in Wireless Networks</i> Godisang Abigail Duma, Khutso Lebea	83-88
<i>LLM-Assisted CPSTRIDE Threat Modeling for Critical Water Infrastructure</i> Dallas Elleman, Amorita A. Christian, John Hale	89-98
<i>New Naval Strategy, Not Cyberwar: China's State-Sponsored Maritime Cyber Operations</i> Francesco Ferazza, Konsantinos Mersinas	99-105
<i>Implementing Countermeasures for Evasive VPN Clients in Educational Institutions</i> Jason Folker	106-113

<i>Agentic AI-Driven Social Engineering: An Elicitation Simulation for Cybersecurity Education</i> Audrey Fruean, Rose Zhao, Joshua Goldberg, Emily Flores, Ella Zou, Emma Trowbridge, Hsiao An Wang	114-121
<i>Cybersecurity Threats Targeting Remote Workers: A Review</i> Ngomani Fundiswa, Noluntu Mpekoa	122-128
<i>The Conceptualisation of a National Malware Intelligence Laboratory for South Africa</i> Wian Gertenbach, Andre McDonald, Mfundo Masango, Ele Mukondeleli, Ethan Buckinjohn, Rendani Mmbodi, Molebogeng Latakomo, Ndabe Hlongwane, Namosha Veerasamy	129-138
<i>Cyber–Space Governance: Securing Orbit through Resilient Global Traffic Management</i> Philippe Goffin, Gazmend Huskaj	139-147
<i>Ontological Security and Threat Mitigation in Healthcare: A Descriptive Exploration</i> Brandon Griffin, Michaela Barnett, Tom VanNorman, Nina Janine Medina, Lucas Potter, Xavier Palmer	148-156
<i>The APT Paradox: Sophisticated Simplicity in Nation-state Cyber Operations (2024–2025), Trends, Detection Provenance, and Practical Gaps</i> Raymond André Hagen	157-166
<i>Quantifying the Economic Impact of Ransomware: Cyber Risk Modeling with Gamma Regression</i> Li Huang, Kimberly A. Cornell	167-175
<i>First Steps, Lasting Impact: Platform-Aware Forensics for the Next Generation of Analysts</i> Vinayak Jain, Sneha Sudhakaran, Saranyan Senthivel	176-184
<i>Regulatory Challenges in Maritime Cybersecurity: Evidence from Expert Workshops</i> Bilge Karabacak, Kasey Miller, Ulku Clark, Jeff Cummings, Edwin Garces, Geoff Stoker	185-193
<i>Migrating Time and Security-Critical PKIs to Post-Quantum Cryptography: SWIM and C-ITS</i> Anni Karinsalo, Sara Nikula, Sami Lehtonen	194-201
<i>From Water Plants to Nuclear Reactors: Mapping SCADA Vulnerabilities in Small Modular Energy Systems</i> Shreyas Kumar, Aleksander Alvarez, Jashanjodh Bajwa, Shrutwik Muppa	202-211
<i>Cyber Security in the Subsea Telecommunication Cable Networks</i> Martti Lehto, Petro Julkunen, Hans Hartikainen	212-221
<i>On the Establishment of Trust: Challenges, Opportunities and Socio- Cultural Factors</i> Christoph Lipps, Denise Scharwatz, Henry Collier	222-231
<i>Q-Learning Model for Proportionality Assessment in Military Operations</i> Clara Maathuis	232-240
<i>Proportionality Assessment in Military Operations based on SARSA and PPO Models</i> Clara Maathuis	241-249
<i>Genetic Algorithms for Proportionality Assessment in Military Operations</i> Clara Maathuis	250-258

<i>Beyond Posters: A User-Centric Digital Twin Framework for Cybersecurity Awareness</i> Fhatuwani Makhamedzha, Errol Baloyi, Rendani Mmbodi, Ndabezinhle Hlongwane	259-267
<i>Architectural Framework for an Enhanced Multi-Party Fully Homomorphic Encryption Scheme</i> Joshua Edward Mamza, Idris Ismaila, Joseph Ojeniyi, Shafi'i Abdulhamid, Moses Noel, Olusanjo Fasola	268-278
<i>Blockchain Use in Disbursing Financial Aid at Higher Education Institutions</i> Livhuwani Mathintha, Noluntu Mpekoa, Tevin Moodley	279-288
<i>Human Cognition is a Tool in Warfare in the Cyber Domain</i> Niina Meriläinen	289-295
<i>A Hybrid Machine Learning Approach for Red Team Log Analysis</i> Nickolas Mohr, Alan Shaffer, Gurminder Singh, Armon Barton	296-303
<i>A Key Rotation Management System: Design and Implementation for Improved Data Security</i> Malibongwe Ntalali, Noluntu Mpekoa, Sheethal Tom	304-312
<i>Explainable AI in Insider Financial Fraud Detection Models: A Review of Transparency and Trust</i> Hillary Kwame Ofori, William Leslie Brown-Acquaye, Forgor Lempogo, Kwame Bell-Dzide, Israel Edem Agbehadji	313-322
<i>Cyber-Physical Incident Attribution in UAV/Rail Attacks</i> Isaac Ojeh, Xavier Palmer, Lucas Potter	323-330
<i>Zero Trust Architecture for UAV/Rail Logistics Ecosystem</i> Isaac Ojeh, Xavier Palmer, Lucas Potter	331-338
<i>Policing Vulnerability to Criminal Persuasive Technology Use on Futurist Moon Bases</i> Tim Pappa	339-345
<i>How Ends, Ways, and Means are Manifested in the Cyber Defense Strategies of Superpowers</i> Piia Perälä, Martti Lehto, Pekka Pirinen	346-354
<i>From Surveillance Monocultures to Agroecological Defense: A Sovereignty-centered Framework for Agricultural Cyberbiosecurity</i> Rolando Perez, Xavier Palmer, Lucas Potter, Dodzi Koku Hattoh, Salomey Afua Addo, Srdjan Lesaja	355-364
<i>From Hoax to Reality: Deepfake-Driven Misinformation and the Death of Ozzy Osbourne</i> Alexander Pfeiffer, Nanditha Krishna, Thomas Wernbacher, Walter Seböck	365-373
<i>How Did They get Aboard my Ship?: Analysing Vessel Cyber Incidents Using the Cyber Kill Chain</i> Jeroen Pijpker, Stephen McCombie	374-382
<i>A Governance Model for Cyber Threat Information Sharing in the Healthcare Sector</i> Jyri Rajamäki, Ilkka Tikanmäki	383-390

<i>Designing Modular Cybersecurity Education for Healthcare: Integrating XiA and ManagiDiTH Frameworks with CyberSecPro Insights</i>	391-400
Jyri Rajamäki, Jussi Simola	
<i>Military Leadership in the Age of Cognitive Warfare</i>	401-407
Mikko Salminen	
<i>Evaluation of AI Agent Accelerated Cyber Operations Planning</i>	408-416
Pietari Sarjakivi, Panu Moilanen	
<i>VAOS: Vulnerability Attribute Ontology Score Framework for Evaluating Vulnerability Databases</i>	417-426
Johnny Shaieb, John Hale	
<i>Digital Forensic Readiness to Mitigate Insider Threats in the SaaS Cloud Environment</i>	427-438
Gabriel Shoderu, Stacey Baror, Abiodun Modupe, Sheunesu Makura	
<i>Social Media Misinformation in Europe and Africa: A Systematic Literature Review</i>	439-448
Nokuthaba Siphambili, Errol Baloyi, Elekanyani Mukondeleli, Molebogeng Latakomo	
<i>Revisiting Biometrics in Cybersecurity: Do AI Methods and Zero-Trust Architectures Drive Innovation?</i>	449-458
Siphehile Sithungu, Christoph Lipps	
<i>AI Agents vs. Human Investigators: Balancing Automation, Security, and Expertise in Cyber Forensic Analysis</i>	459-467
Sneha Sudhakaran, Naresh Kshetri	
<i>Advancements in Developer-Focused IDE-Integrated Mobile App Security Scanning and Testing Tools</i>	468-475
Franck Monga Tamala, Noluntu Mpekoa, Khutso Lebea	
<i>SentinelSphere: AI-Driven Cybersecurity Platform Combining Threat Detection with Security Awareness</i>	476-485
Nikolaos D. Tantaroudas, Ilias Karachalios, Andrew McCracken	
<i>Aligning DYNAMO Framework with the EU Cyber Resilience Act in the Energy Sector</i>	486-493
Ilkka Tikanmäki, Jarmo Maikkola, Joonas Nykopp, Sara Väisänen, Shakti Panta Khatri	
<i>The Life Cycle Approach to Effective Crisis Communications in Mitigating Cyber Threats and Attacks</i>	494-504
Jussi Toivanen, Vilma Luoma-aho	
<i>Hybrid Learning Techniques for Image Forensics and Privacy Protection in the Face of Deep Fake Threats</i>	505-510
Arif Ullah, Sidra Pervez, Muhammad Wajidullah Khan, Aina Hassan, Muazam Ali	
<i>VessiGuard: AI-Driven Anomaly Detection for Maritime Cyber Defence</i>	511-519
Ravi Varma Kanumuri, Laavanya Rachakonda, Hosam Alamleh, Bilge Karabacak, Ulku Clark Yaylacicegi	
<i>The Informed Fake News Advisor (IFNA): Toward Sociotechnical Solutions for Fake News Detection</i>	520-530
Namosha Veerasamy, Danielle Badenhorst	
<i>Rethinking the Human–Technical Split in Cybersecurity</i>	531-537
Jukka Vuorinen	

<i>Legal Protection against Digital Personal Identity Fraud in South Africa</i>	
Murdoch Watney	538-546
<i>Critical Infrastructure, Industrial Control Systems and Cyber Warfare: Ethical and Anticipated Ethical Issues</i>	
Richard Wilson, Noah Donnelly	547-553
<i>Smart Phones and Current Developments in Cyberwarfare: An Ethical and Anticipatory Ethical Analysis</i>	
Richard Wilson, Noah Donnelly	554-560
<i>Russia, Weaponized Social Media and Cyber Warfare: Ethical and Anticipated Ethical Issues</i>	
Richard Wilson, Noah Donnelly	561-568
<i>Echo Chambers, Filter Bubbles, and Cyber Warfare: An Ethical and Anticipatory Ethical Analysis</i>	
Richard Wilson, Noah Donnelly	569-577
<i>Cyber Operations and the Threshold for Cyber Warfare: Ethical and Anticipated Ethical Issues</i>	
Richard Wilson, Noah Donnelly	578-584
<i>Lessons Learned While Performing 'Hands On' Teaching in a Live Environment</i>	
Adam Yusuf, Justin Clevenger, Char Sample	585-592
PhD Papers	
<i>Cyber-Security in Cyber-Physical Systems and Critical Infrastructure: A Self-Healing Federated Learning Intrusion Detection Framework</i>	
Francisca Ezulike, Sheunesu Makura, Stacey Baror, Hein Venter	594-603
<i>PRISM-APT: A Model-First Synthesis for APT Defence</i>	
Raymond André Hagen	604-615
<i>Frequent Itemset Mining for Model Data Reduction</i>	
Blake Johns, Ryan Benton	616-623
<i>Sleeper Code in Protein Data Files as Cyber Adversarial Vectors</i>	
Tia Pope	624-632
Masters Papers	
<i>Applicability Of Industry 4.0 Technologies in Combating Fraud in the Financial System</i>	
Jennyfer da Conceição Fonseca Santos, Luciana Paula Reis, June Marques Fernandes	634-642
<i>Doctrine-to-Deployment: Role of Advanced Persistent Threats in Russia's "Information Confrontation" Doctrine</i>	
Elia Gelati, Luigi Martino	643-650
<i>Cybersecurity Issues and Solutions Within the South African Small and Medium-Sized Enterprises</i>	
Benediction Kitwa Kalombola, Tabisa Ncubukezi	651-658
<i>AI-Augmented Proactive Cyber-Detection and Mitigation of Cybersecurity Threats in the Banking Sector</i>	
Prince Rotondwa Mulea, Dewald Blaauw	659-667
<i>Analysis of Cybersecurity Strategies Across Continents</i>	
Pekka Pirinen, Piia Perälä, Martti Lehto	668-675

Wargaming Design for Cyber Warfare

Dong Wang 676-684

Non-Academic Papers

A Review of the Maritime Cybersecurity Regime Over the Last Decade

Leigh Armistead 686-693

Automated Threat Modeling using Artificial Intelligence on User Stories within the SDLC to Generate Security Tasks

Shantu Asif Hossain 694-704

SOC Puppets: How Whaley's Theory of Outs and 'Noisy' Sock Puppets Encouraging Discovery of Network Deception Could Enhance Security Operations Center Analysis

Tim Pappa, Keyur Rajyaguru 705-712

Work in Progress Papers

Exploring NIS2 Compliance in the Energy Sector Using AI-Driven Cyber Threat Intelligence

Jani Siivola, Rami Paronen, Uzair Tariq, Quyet Pham, Warren Villegas, Ilkka Tikanmäki, Jyri Rajamäki 714-717

ECHO Early Warning System for Water Infrastructure Protection

Ilkka Tikanmäki, Sara Jylhäkangas, Kitty Tapola, Jeni Awa 718-720

Automated Exploit Chain Modeling and Analysis

Thomas Wahl, Nicolas White, Guang Jin, Sukarno Mertoguno, Kevin Stevens, Froy Maldonado 721-724

Late Submissions

Cyberbiosecurity in Action: Securing the Biological Battlespace from Digital Subversion

Adya Daruka, Anusha Nigam, Shreyas Kumar 726-734

Cybersecurity Issues and Solutions Within the South African Small and Medium-Sized Enterprises

Benediction Kitwa Kalombola, Tabisa Ncubukezi 735-742

Biosecure-LLM Framework: Protecting LLMs from Cyberbiosecurity Threats and the Case for Independent AI Safety Governance

Xavier-Lewis Palmer, Lucas Potter, Srdjan Lesaja, Sotirios Karathanasis, Mohammad Ghasemigol 743-750

A Comprehensive Cyber Defense Framework for the Indonesian National Armed Forces: Bridging Governance Gaps for National and ASEAN Cyber Resilience

Timothy Shives, Fibriansyah Fatahillah 751-758