

**Proceedings of the**

**22<sup>nd</sup> European Conference on Cyber Warfare  
and Security**

**ECCWS 2023**

**A Conference Hosted By**

**Hellenic Air Force Academy (HAFA)**  
**and**  
**the University of Piraeus, Greece**

**22-23 June 2023**

Copyright the authors, 2023. All Rights Reserved.

No reproduction, copy or transmission may be made without written permission from the individual authors.

### **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**

ACIL 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-academic-conferences-and-publishing-international-limited/>

### **Self-Archiving and Paper Repositories**

We actively encourage authors of papers in ACIL conference proceedings and journals to upload their published papers to university repositories and research bodies such as ResearchGate and Academic.edu. Full reference to the original publication should be provided.

### **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.

The Electronic version of the Conference Proceedings is available to download from <https://papers.academic-conferences.org/>

The Conference Proceedings for this year and previous years can be purchased from <http://academic-bookshop.com>

E-Book ISBN: 978-1-914587-70-2

E-Book ISSN: 2048-8610

Book version ISBN: 978-1-914587-69-6

Book Version ISSN: 2048-8602

Published by Academic Conferences International Limited

Reading, UK

+44 (0) 118 324 6938

[www.academic-conferences.org](http://www.academic-conferences.org)

[info@academic-conferences.org](mailto:info@academic-conferences.org)

## 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 Warfare1</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, Agnė 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 Biocybersecurity/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

### **Masters Papers**

<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

### **Non-Academic Papers**

<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**

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

## **Late Submission**

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



## Preface

These proceedings represent the work of contributors to the 22<sup>nd</sup> European Conference on Cyber Warfare and Security (ECCWS 2023), which is held in Athens, Greece on 22 and 23 June 2023. ECCWS 2023 has been supported by the Hellenic Air Force Academy and the University of Piraeus. The Conference Chair is Professor Antonios Andreatos from the Hellenic Air Force Academy, Greece and the Programme Chair is Professor Christos Douligeris from the University of Piraeus, Greece.

ECCWS is a well-established event on the academic research calendar and now in its 22<sup>nd</sup> year its key aim remains the opportunity for participants to network and share ideas. The scope of the papers ensure an interesting conference. The subjects covered illustrate the wide range of topics that fall into this important and ever-growing area of research.

The opening keynote presentation is given by Prof. Dr. Kai Rannenberg, from Goethe University Frankfurt, Germany on the topic of *Multilateral Security: Defending one's assets without destroying one's values*. The second day of the conference will open with an address by Prof. Nineta Polemi, University of Piraeus, Greece speaking on *CyberSecPro: An agile and collaborative approach to cybersecurity practical trainings*.

With an initial submission of 132 abstracts, after the double blind peer review process 64 academic research papers, 12 PhD research papers, 2 Masters research papers 2 Non-Academic research papers and 5 work-in-progress papers are published in the Conference Proceedings. These papers represent research from Australia, Austria, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Lithuania, Malaysia, Mozambique, Netherlands, Nigeria, Norway, Portugal, Republic of Korea, Romania, Slovenia, South Africa, Sweden, Switzerland, Taiwan, UK, United Arab Emirates and the USA.

We hope that you will enjoy the conference and that you will find the opportunity to renew past collaborations and friendships and to engage in fruitful discussions leading to new advancements in research and development.

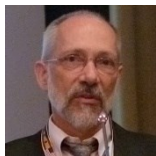
Professor Antonios Andreatos  
Hellenic Air Force Academy  
Professor Christos Douligeris  
University of Piraeus  
Greece  
June 2023

## **ECCWS Conference Committee**

*Dr Mohd Faizal Abdollah, University Technical Malaysia Melaka, Malaysia; Dr William ("Joe") Adams, University of Michigan/Merit Network, USA; Prof Hamid Alasadi, Basra University, Iraq; Dr Kari Alenius, University of Oulu, Finland; Prof Antonios Andreatos, Hellenic Air Force Academy, Greece; Dr Olga Angelopoulou, University of Warwick, UK; John Anohar, Higher Education dept, India; Dr Leigh Armistead, Edith Cowan University, Australia; Dr Sajad Bagheri Baba Ahmadi, , Iran; Dr Hayretdin Bahsi, Tallinn University of Technology, Estonia; Dr Dragos Barbieru, CAROL I National Defence University, Romania; Prof Jorge Barbosa, Coimbra Polytechnic - ISEC, Portugal; Stacey Baror, University of Pretoria, South Africa; Prof Matt Bishop, University of California at Davis, USA; Dr Jim Chen, DoD National Defense University, USA; Dr Sabarathinam Chockalingam, Institute for Energy Technology, Norway; Dr Maura Conway, Dublin City University, Ireland; Dr Paul Crocker, Universidade de Beira Interior, Portugal; Prof Tiago Cruz, University of Coimbra, Portugal; Dr Christian Czosseck, CERT Bundeswehr (German Armed Forces CERT), Germany; Josef Demergis, University of Macedonia, Greece; Prof Patricio Domingues, Polytechnic Institute of Leiria, Portugal; Paul Dowland, Edith Cowan University, Australia; Marios Efthymiopoulos, Political Science Department University of Cyprus, Cyprus; Dr Colin Egan, University of Hertfordshire, Hatfield, UK; Dr Ruben Elamiryan, Public Administration Academy of the Republic of Armenia, Armenia; Dr Thaddeus Eze, University of Chester, UK; Prof Eric Filiol, ENSIBS, Vannes, France & CNAM, Paris, France; Prof Steve Furnell, University of Nottingham, UK; Dr Dimitra Georgiou, University of Piraeus, Greece; Dr Michael Grimaila, Air Force Institute of Technology, USA; Bill Hutchinson, Edith Cowan University, Australia; Hamid Jahankhani, University of East London, UK; Nor Badrul Anuar Jumaat, University of Malaya, Malaysia; Dr Connie Justice, Purdue School of Engineering and Technology, IUPUI, USA; Maria Karyda, University of the Aegean, Greece; Anthony Keane, Technological University Dublin, Ireland; Jyri Kivimaa, Cooperative Cyber Defence and Centre of Excellence, Tallinn, Estonia; Prof Mortaza Kokabi, Shaheed Chamran Univ., Iran; Prof Ahmet Koltuksuz, Yasar University, Dept. of Comp. Eng, Turkey; Peter Kunz, Hexagon Geosystems, Germany; Martti Lehto, National Defence University, Finland; Christoph Lipps, German Research Center for Artificial Intelligence, Germany; Dr Efstratios Livanis, University of Macedonia, Greece; Dr Leandros Maglaras, De Montfort University, UK; Assc Manmeet Mahinderjit Singh , University Sains Malaysia, Malaysia; James Malcolm, University of Hertfordshire, UK; Dr Arianit Maraj, AAB College-Faculty of Computer Sciences, Kosovo; Ioannis Mavridis , University of Macedonia, Greece; Rob McCusker, Charles Sturt University, UK; Dr Yonathan Mizrahi, University of Haifa, Israel; Antonio Muñoz, University of Málaga, Spain; Daniel Ng, C-PISA/HTCIA, China; Dr Cyril Onwubiko, Cyber Security Intelligence at Research Series Limited, UK; Rain Ottis, Tallinn University of Technology, Estonia; Prof Teresa Pereira, Instituto Politécnico de Viana do Castelo, Portugal; Michael Pilgermann, Technische Hochschule Brandenburg - University of Applied Sciences, Germany; Prof Pedro Pinto, Instituto Politécnico de Viana do Castelo, Portugal; Dr Ajeet Singh Poonia, Full time academic, Bikaner Technical University, Rajasthan; Prof Maria-Magdalena Popescu, Carol I National Defence University , Romania; Dr Bernardi Pranggono, Sheffield Hallam University, UK; Prof Carlos Rabadão, Politechnic of Leiria, Portugal; Dr Trishana Ramluckan, University of KwaZulu-Nata, South Africa; Dr Mark Reith, Full time academic, Air Force Institute of Technology; Dr Neil Rowe, US Naval Postgraduate School, Monterey, USA; Prof Vitor Sa, Catholic University of Portugal, Portugal; Dr Char Sample, Carnegie Mellon University/CERT, USA; Prof Henrique Santos, University of Minho, Portugal; Prof Leonel Santos, Polytechnic of Leiria, Portugal; Dr Keith Scott, De Montfort University, UK; Prof Dr Richard Sethmann, University of Applied Sciences Bremen, Germany; Dr Yilun Shang, Northumbria University, UK; Prof Jill Slay, University of South Australia, Australia; Dr Lee Speakman, University of Chester, UK; Dr Joseph Spring, University of Hertfordshire, UK; Prof Iain Sutherland, Noroff University College , Norway; Dr Hamed Taherdoost, Hamta Group, Hamta Business Corp, Vancouver, Canada; Unal Tatar, University at Albany - SUNY, USA; Dr Selma Tekir, Izmir Institute of Technology, Turkey; Prof Dr Peter Trommler, Georg Simon Ohm University Nuremberg, Germany; Mr Paul Underhill, University of Chester, UK; Dr Brett van Niekerk, Durban University of Technology, South Africa; Richard Vaughan, General Dynamics UK Ltd, UK; Dr Namosha Veerasamy, Council for Scientific and Industrial Research, South Africa; Prof Trish Williams, Flinders University, Australia; Prof Richard Wilson, Towson University, USA; Dr Allison Wylde, Glasgow Caledonian University , UK; Dr Justyna Żywiołek, Czestochowa University of Technology, Poland.*

## Biographies

### Conference and Programme Chairs



**Antonios Andreatos** is a professor at the Computer Engineering Division of the Hellenic Air Force Academy. He serves as a scientific committee member for a number of international conferences, as well as a reviewer in several journals. He has published papers in various international journals and conference proceedings, book chapters and three books. His research interests include (among other topics) cyber security, cryptography, steganography, image processing, educational technology, IoT, etc.



**Christos Douligeris**, currently a professor at the Department of Informatics, University of Piraeus, Greece, held positions with the Department of Electrical and Computer Engineering at the University of Miami. He was an associate member of the Hellenic Authority for Information and Communication Assurance and Privacy and the President and CEO Hellenic Electronic Governance for Social Security SA. Dr. Douligeris has published extensively in the networking scientific literature and he has participated in many research and development projects. His main research interests lie in the areas of computer networking, communications, network security, cyber security, web science, data analytics, new technologies in education and emergency response operations.

### Keynote Speakers



**Nineta Polemi** is a cybersecurity Professor in the University of Piraeus-UNIPi- ([Cyber Security Lab](#), Dept. of Informatics) and CTO/ Co-Founder of [trustilio](#). She established and acted as director of the UNIPi cybersecurity lab. She served (2017-2020) as Programme Manager and Policy Officer in the European Commission DG (CONNECT H1 Unit entitled 'Cybersecurity Technologies and Capabilities'). Her cybersecurity expertise is on: operational risk/conformity assessment, security management, incident management, supply chain security, threat intelligence. She has obtained her Ph.D. in Applied Mathematics (Coding Theory) from The City University of New York (Graduate Center). She held teaching and research positions in The City University of New York (Queens & Baruch Colleges), State University of New York (Farmingdale), Université Libre de Bruxelles (ULB)-Solvay Brussels School-. She has over 150 publications in security has organised numerous scientific and policy international cybersecurity scientific events and trainings e.g. [cyberhot](#). She has received many research grants (NATO, IEEE) and awards (NSA, MSI Army Research Office IEEE, CUNY, Hellenic Ministry of Maritime, Hellenic National Defense General) and has participated as Project and Technical Manager in more than 60 cybersecurity international, EU and national R&D and commercial projects. She serves as external expert/reviewer/consultant in EC, [ENISA](#), [FORTH](#), [Focal Point](#), [CodeWeTrust](#). She is a member of [ETSI](#) in the working groups of Cyber and AI.



**Kai Rannenberg**, Chair of Mobile Business & Multilateral Security ([www.m-chair.de](http://www.m-chair.de)) at [Goethe University Frankfurt](#) since 2002. Visiting Professor [National Institute for Informatics](#) (NII) (Tokyo, Japan) since 2012. Chair CEPIS ([www.cepis.org](http://www.cepis.org)) Legal & Security Issues Special Interest Network since 2003. Since 2007 Convenor ISO/IEC JTC 1/SC 27/WG 5 "Identity management & privacy technologies". 2004-2013 academic expert in the Management Board of [ENISA](#); 2013-2020 member ENISA's [Advisory Group](#) (until 2019 [Permanent Stakeholder Group](#)). Since 2021 Honorary Treasurer [International Federation for Information Processing](#), 1999-2002 Microsoft Research Cambridge (UK). Kai has been coordinating several leading EU research projects, e.g. the Network of Excellence "[Future of Identity in the Information Society \(FIDIS\)](#)" and the IP "[Attribute based Credentials for Trust](#)" ([ABC4Trust](#)).

Currently he is coordinating [CyberSec4Europe](#), a pilot for the Cybersecurity Competence Network the EU is aiming for, and [CyberSecPro](#) aiming for improved cybersecurity education and training.

### **Mini Track Chairs**



**Olga Angelopoulou** is an Assistant Professor in Cyber Security at the University of Warwick. Olga completed her doctorate in digital forensics in 2010 at the University of South Wales (Glamorgan) and is an active researcher in the field. She previously held academic posts at the University of Derby and the University of Hertfordshire. Olga is also the Editor-in-Chief for Information Security Journal: A global Perspective. Her research interests include digital investigations, cybercrimes, incident response and online fraud. She has several publications and presentations in the field and is involved in numerous scholarly activities.



**Sabarathinam Chockalingam** is a Research Scientist I at the Institute for Energy Technology in Halden, Norway. Saba has a PhD in Cyber Security and Artificial Intelligence from the Delft University of Technology and MSc in Cyber Security and Management from the University of Warwick. His research interests include cyber security, risk management and safety.



**Tiago Cruz** received his Ph.D. degree in informatics engineering from the University of Coimbra (Coimbra, Portugal), in 2012. He is an Assistant Professor in the Department of Informatics Engineering, University of Coimbra. His research interests include areas such as management systems for communications infrastructures and services, critical infrastructure security, broadband access network device and service management, Internet of Things.



**Christoph Lipps**, graduated in Electrical and Computer Engineering at the University of Kaiserslautern, where he meanwhile lectures as well. He is a Senior Researcher and Ph.D. candidate at the German Research Center for Artificial Intelligence (DFKI) in Kaiserslautern, Germany, heading the *Cyber Resilience & Security* Team of the Intelligent Networks Research Department. He is not only a member of the committee of the ICCWS and ECCWS, but also scientific committee member of various international conferences, and reviewer of several journals. His research focuses on Physical Layer Security (PhySec), Physically Unclonable Functions (PUFs), Artificial Intelligence (AI), entity authentication, Security in the Sixth Generation (6G) Wireless Systems and all aspects of network and cyber security.



**Clara Maathuis** is an Assistant Professor in AI and Cyber Security at Open University in the Netherlands. With a PhD in AI and Military Cyber Operations from the Delft University of Technology, she is involved in teaching different AI and cyber security courses and conducts research in AI, cyber/information operations, military technologies, and social manipulation.



**Shahzad Ahmed Memon** is currently working as senior researcher at department of computer Engineering, Faculty of Engineering and architecture in Beykoz University, Istanbul, Turkey. He also worked as Professor, at department of Electronics Engineering, Faculty of Engineering and Technology at University of Sindh, Pakistan. He completed his Doctorate PhD in Biometrics security from Brunel University, London, UK. He published his research in several national and international research journals. Dr. Memon attended and presented his research in national and international conferences organized in USA, UK, and Europe. Dr. Memon supervised MS and PhD students in the field of Biometrics, Cyber Security and Privacy, Smarts systems security, Cyber Physical systems security, Applications of Artificial

Intelligence. He also granted funding for research from Higher Education commission and ICT Research and Development, Ministry of Information Technology, Pakistan



**Brett van Niekerk** is a senior lecturer in information technology at the Durban University of Technology. He serves as chair for the International Federation of Information Processing Working Group on ICT in Peace and War, and the co-Editor-in-Chief of the International Journal of Cyber Warfare and Terrorism. He has numerous years of information/cyber-security experience in both academia and industry, and has contributed to the ISO/IEC information security standards. In 2012 he graduated with his PhD focusing on information operations and critical infrastructure protection. He is also holds a MSC in electronic engineering and is CISM certified.



**Trishana Ramluckan** is a Honorary Researcher in the School of Law at the University of KwaZulu-Natal and Research Manager at Educor Holdings. She is a member of the IFIP working group on ICT Uses in Peace and War, the Institute of Information Technology Professionals South Africa and is an Academic Advocate for ISACA. In 2017 she graduated with a Doctor of Administration specialising in IT and Public Governance and in 2020 she was listed as in the Top 50 Women in Cybersecurity in Africa. Her current research areas include Cyber Law and Information Technology Governance.



**Dr Keith Scott** Is Programme Leader for English Language at De Montfort University in Leicester. His research operates at the intersection of communication, culture and cyber, with particular interests in influence, information warfare, and simulations and serious gaming as a training, teaching, and research tool. He is a member of the Prometheus Research group, supported by the UK Development, Concepts and Doctrine Centre, which investigates the application of cybernetics and systems thinking within the context of warfare, as well as more general considerations of AI and pervasive technology.



**Paulo Simões** received his Ph.D. degree in informatics engineering from the University of Coimbra (Coimbra, Portugal), in 2002. He is an Associate Professor in the Department of Informatics Engineering, University of Coimbra. His research interests include network and infrastructure management, security, critical infrastructure protection.

### **Workshop Facilitators**



**Dr Edwin “Leigh” Armistead** is the Principal of ArmisteadTec LLC, a Veteran-Owned Small Business (VOSB) that is certified by the Small Business Administration (SBA) as a Historically Underutilized Business Zone (HBZ), <https://www.armisteadtec.com/>. This company primarily focuses on the academic functions of Information Warfare (IW), to include curriculum development, teaching as well as other related tasks to include lecturing and writing. A retired United States Naval Officer, Dr Armistead has significant Information Operations academic credentials having written his PhD on the conduct of Cyber Warfare by the federal government and has published three books, in an unclassified format in 2004, 2007 and 2010, all focusing on full Information Warfare. He is also the Chief Editor of the Journal of Information Warfare (JIW) <https://www.jinfowar.com/>; the Program Director of the International Conference of Cyber Warfare and Security and the Vice-Chair Working Group 9.10, ICT Uses in Peace and War. Shown below are the books on full spectrum cyber warfare and the JIW:

## Biographies of Contributing Authors

**Konstantinos Adamos** (B.Sc., M.Sc.) Cybersecurity Researcher with the Information Security and Critical Infrastructure Protection Research Group (Athens University and Economics & Business, Greece). Also a Ph.D. candidate with the Dept. of Information and Communication Systems Engineering (University of the Aegean, Greece). His current research interests focus on cybersecurity, critical infrastructure protection, data protection, and risk assessment.

**Tayba Al Ali** is a graduate of Information technology with specialization in cyber security and networking at Zayed University. She's certified in Introduction to Networks and Switching, Routing, and Wireless Essentials, Tayba's constant appearance on the dean's list during her studies at the University is a testament to her academic prowess. Her passion for technology guarantees a successful career in IT.

**Nora AlKaabi** is an Information Technology graduate from Zayed University, specializing in Security and Network Technology. Her fascination with technology and cybersecurity fuels her drive to create innovative solutions for businesses to overcome security challenges. Nora is passionate about contributing to a secure and digitally-driven society, utilizing her skills and knowledge to make a positive impact on the world.

**Ban AlOmar** is currently pursuing her Ph.D. degree with the College of Information Technology, United Arab Emirates University. Her main research areas are Artificial Intelligence, machine learning, network security and intrusion detection and prevention.

**Antonios S. Andreatos** is Professor at the Hellenic Air Force Academy, Greece. He has published his research in international journals, conference proceedings and book chapters. He is involved in scientific committees of several conferences and reviewer in several journals. His current research interests focus on Cryptography, Image processing, CyberSecurity, IoT, Engineering Education, e-Assessment, CyberSecurity Education.

**Stacey Omeleze Baror** obtained her B.sc Hon and Master in Computer Sci., From the Computer Science Department, University of Pretoria. She is currently studying towards a PhD in Computer Science, at the University of Pretoria in research areas focusing on digital forensic, Software engineering, intelligent systems, Digital Forensics Application, Digital Forensic Readiness, and Information Security.

**Igor Bernik** is Professor of Information Sciences and vice dean for Quality and Development at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. His research fields are information systems, cybersecurity, and the growing requirement for cybersecurity awareness. He is an (co)author of several scientific books and articles published in recognized international journals.

**Micki Boland** is a global cybersecurity warrior and evangelist with Check Point Software Technologies Office of the CTO. A practitioner with 20 years in IT, cybersecurity, emerging technology innovation, Micki holds ISC2 CISSP, Master of Science in Technology Commercialization University of Texas at Austin and MBA Global Security Concentration from East Carolina University.

**Johnny Botha** enrolled for a PhD in Computer Science at the University of Western Cape. Topic: *“A process for Blockchain Crime Investigations Based on Open-source Intelligence”*. Project Manager & Researcher (CSIR). Masters degree in Information Technology, at University of South Africa (UNISA). NDip and BTech degree in Computer Systems Engineering at the Tshwane University of Technology (TUT).

**Ladislav Burita**, University of Defence, Brno, Czech Republic. PhD. from 1985 and professor from 2003. He worked in NATO/MIP team; was head of the faculty research program and defense project MENTAL. His area of interest is information and knowledge systems. He published a hundred papers at conferences and in journals.

**Jami M. Carroll** retired from the Navy after 20 years. He later founded Prisdian Security Solutions in 2008. His research areas include offensive cyber operations, threat intelligence, denial/deception, and geopolitical instability. His degrees include: BBA, National University; MBA, Southern New Hampshire University; MS/DSc in in Cybersecurity, Capitol Technology University.

**Chih-Hsiang (‘Sharon’) Chang** is a Master student of Interdisciplinary Legal Studies at National Taiwan University. She is the co-author of The Best Memorial-Defendant of Red Cross International Humanitarian Law Moot 2021 Hong Kong. The main focus of her research is international law, law of armed conflict and cyber warfare.

**Jim Q. Chen, Ph.D.** is Professor and Associate Dean at the U.S. National Defense University College of Information and Cyberspace. His expertise is in cyber strategy, cyber deterrence, cyber warfare, cybersecurity technology, artificial intelligence, and machine learning. He has authored and published more than 90 peer-reviewed papers, articles, and book chapters on these topics. He has also been teaching graduate courses on these topics. He is a recognized expert in cyber studies and artificial intelligence.

**Sabarathinam Chockalingam** is a Research Scientist I at the Institute for Energy Technology in Halden, Norway. Saba has a PhD in Cyber Security from the Delft University of Technology and MSc in Cyber Security and Management from the University of Warwick. His research interests include cyber security, risk management, serious games.

**Nikolaos Chrysikos** is an electrical engineer in the Hellenic Air Force. He graduated from Hellenic Air Force Academy in 2022 . His diploma thesis was on malicious android applications analysis and classification. He is interested in data analysis and Cyber Security.

**Henry Collier** is an associate professor and the Director for the Technology Programs at Norwich University’s college of Graduate and Continuing Studies. He received his Ph.D. in engineering security from the University of Colorado Colorado Springs. His main research areas are human factors in cybersecurity and networking.

**Tiago Cruz** is an Associate Professor with the Department of Informatics Engineering of the University of Coimbra. His research interests cover areas such as management systems for communications infrastructures and services, critical infrastructure security, broadband access network device and service management, Internet of Things, software defined networking, and network function virtualization.

**Didier Danet** is a senior lecturer of Defense management at Saint-Cyr Military Academy, France. He holds a PhD in Management Sciences from Rennes 1 University. He is the Director of the Post-Master Training Program “Cyberdefense and Intangible Fields”. His main research areas are Cyber Crisis Management, Military Organisations and Irregular Warfare.

**Martina Jennifer Zucule de Barros** is a PhD student in cybersecurity. Her research explores cybersecurity education. She has a master degree in Distributed Systems Engineering from the Technical University of Dresden. She is currently working as a university teacher in Computer Science at Universidade Pedagógica de Maputo (UPM).

**Thomas Dempsey** is a second-year Doctoral student in Strategic Intelligence. Thomas has a Masters degree in Cybersecurity and multiple industry certifications. In addition to academics, Thomas is a Cybersecurity professional who has worked in cyber for over 14 years, including time on active duty in the United States Marine Corps conducting defensive cyber operations.

**Charlie Donnelly** is studying Computer Science and Economics at the University of Chicago. She has worked with the Securities and Exchange Commission and Morgan Stanley’s Technology Investment Banking Group. She is interested in studying military applications of cybersecurity.

**Petrus ('Beer') Duvenhage** has extensive experience in the field of information security. He holds a PhD from the University of Pretoria and a PhD from the University of Johannesburg.

**Bastian Fraune** is a computer-scientist and works as a researcher in industrial cyber security projects. His research interests include secure architectures for critical infrastructures, cyber-physical systems and digitization of systems. He holds a master’s degree in computer science and is working on secure power grid architectures in his PhD-project.

**Dimitra Georgiou:** Lecturer at the Computer Engineering Division of the Hellenic Air Force Academy and an Adjunct Lecturer (Department of Digital Systems, University of Piraeus). She received her PhD in Security Policies of Cloud Computing from the University of Piraeus in 2018. Research interests lie in the areas of information and communication Systems Security and Privacy.

**Farid Gharehmohammadi** is a Mayo Clinic postdoctoral researcher investigating deep learning in medical imaging. He earned his Ph.D. in computer science from University of Georgia. He has a decade of industrial and research experience. He published over 20 journal, conference papers and book chapters. He received the Outstanding Achievement Award for deep learning at CSCI’19.

**Alexander Grandin** has a Master’s degree in Science (2022) and Military science (2018) and works as a research officer at the Finnish National Defense University (FNDU). He has served in the Finnish Defense Forces from 2012.

**Tim Grant** is retired but an active researcher (Professor emeritus, Netherlands Defence Academy). Tim has a BSc in Aeronautical Engineering (Bristol University), a Masters-level Defence Fellowship (Brunel University), and a PhD in Artificial Intelligence (Maastricht University). Tim's research focuses on Offensive Cyber Operations, Command & Control, and Emergency Management. More details are at <https://www.linkedin.com/in/tim-grant-r-bar/>.



**Virginia A. Greiman.** Assistant Professor (Global Cyber Law, Governance, Megaprojects and Infrastructure Planning, Boston University). Was a diplomatic head of delegation (U.S. Department of State in Eastern and Central Europe, Asia and ). Held several high-level appointments with the U.S. Department of Justice. Conducts research and publishes in cyber resilience, cyber law and regulation, nuclear cyber security, and global infrastructure megaprojects.

**Samuli Haataja** is a Senior Lecturer at Griffith Law School, Griffith University. He researches state-sponsored cyber-operations under public international law. He published his book 'Cyber Attacks and International Law on the Use of Force: The Turn to Information Ethics' with Routledge in 2019, and he has published in various international law and technology journals.

**Thomas Heverin** is the lead of Girls Learn Cyber, Inc., a training company for K-12 girls in cybersecurity. He holds a Ph.D. focused on cybersecurity, the CISSP, and years of cybersecurity experience. He led research and development projects for the U.S. Navy after serving as a Surface Warfare Officer."

**Pauliina Hirvonen** is a PhD student in the Information Technology Department of the University of Jyväskylä, in Finland. Her on-going dissertation of GDPR relates to Information Systems and especially on information and/or cyber security field. The research considers the overall impacts of privacy regulation and developing situational awareness from the organisational perspectives.

**Michael Bennett Hotchkiss** is an independent researcher with interests in the psychology of influence, criminology, and nation-state disinformation; especially in the context of Russian active measures. Michael earned a Master of Organization Development from Bowling Green State University; and a Bachelor of Arts in Psychology from the University of Connecticut, graduating Phi Beta Kappa.

**Aki-Mauri Huhtinen** (LTC (GS)) is a military professor at the Finnish National Defence University's Department of Leadership and Military Pedagogy. His areas of expertise are military leadership, command and control, information warfare, the philosophy of science in military organizational research.

**Aarne Hummelholm**, PhD in Information Technology (University of Jyväskylä, 2019). He has over 30 years' experience in the design, development of architectures` of authorities` telecommunications networks and information systems. Key themes in his work have been critical service availability, usability, cyber security and preparedness issues.

**Gazmend Huskaj:** Head of Cyber Security at GCSP. Was a doctoral student (Cyberspace Operations, Swedish Defence University.) Was Director of Intelligence on Cyber-related issues in the Swedish Armed Forces. A veteran with over five years of duty in conflict / post-conflict areas including two tours to the Balkans and one in Central Asia. Current work focuses on capacity-building, dialogue, and policy analysis.

**Anastasiia Iufereva** Ph.D. Student (IULM University, Milan, Italy). She has been awarded academic degrees: a bachelor's degree in journalism (2012), and a master's degree in management(2014). Her research interests oscillate between mass media and social

practices. In particular, she studies how journalists' professional cultures are shaped in the light of online platforms and media convergence.

**Panagiotis Karampelas** is an assistant professor at the Hellenic Air Force Academy, Greece. He received his PhD in electronic engineering from University of Kent in 2005. He participates in the advisory board of several scientific journals and conferences. His main research areas are Software Engineering, Data Mining, Cyber Security, Digital Forensics, Social Network Analysis

**Major Maria Keinonen** is a senior research officer and a PhD student for Military Sciences in the National Defence University in Finland. In her doctoral research, she focuses on the study of cyber deterrence from the perspective of a small state.

**Stylianos Koumoutzelis** is a graduate of the Electrical and Computer Engineering School of the National Technical University of Athens. With a focus on hardware design and development, he possesses expertise in the design and implementation of complex systems. He has also worked extensively in the fields of AI/ML, Telecommunications, and European research projects.

**Eugene Lim** is currently a master's student at Korea University's Graduate School of Cyber Security. Lim's bachelors degree is in International Studies and is currently interested in international cybersecurity and cyber policy. Her global research publications include 'Review of the Validity and Rationality of Artificial Intelligence Regulation' in the Florida Artificial Intelligence Research Society.

**Georgiana-Daniela Lupulescu** works at a public institution that offers specialization/improvement courses for military personnel. She is currently a PhD student at the National Defence University, conducting a research on the influence of hybrid threats in the realization of resilience policies in the national security field.

**Clara Maathuis** is Assistant Professor in AI and Cyber Security at Open University in the Netherlands. With a PhD in AI and Military Cyber Operations from Delft University of Technology, she is involved in teaching different AI and cyber security courses and conducts research in AI, cyber/information operations, military technologies, and social manipulation.

**Bill Mahoney** is the Charles and Margre Durham Distinguished Professor in Cybersecurity at the University of Nebraska at Omaha, where he teaches both undergraduate and graduate cybersecurity classes. His research areas include code obfuscation, reverse engineering and anti-reverse engineering techniques, and vulnerability analysis. An additional interest is in vulnerabilities with critical infrastructure equipment.

**Aleksandras Melnikovas**, Senior instructor at the Leadership and Methodology Development Centre, Military Academy of Lithuania. Obtained Masters degree in Education sciences in 2017, currently PhD student in Political sciences. Since 2021 works as a junior scientist within the project „Advancing Human Performance in Cybersecurity“.

**Jabu Mtsweni** is the Head of Information and Cyber Security Centre and Chief Researcher at the Council for Scientific and Industrial Research (CSIR), NRF-Rated Researcher (C2), and a Certified Cybersecurity Manager, Research Fellow at the Stellenbosch University. He has

published over 80 peer-reviewed conference and journal articles over the years in different forums.

**Edmore Muyambo** is a Master's Research Student at the University of Pretoria, South Africa. He received his Honours Degree in Computing from the University of South Africa in 2022. Edmore is a Data Engineer at the Standard Bank of South Africa. His main areas of focus are Data Integration, Data Transformation and partly Data Visualisation.

**Rennie Naidoo** is an Associate Professor of Informatics at the University of Pretoria, South Africa. His research focuses on the interplay between information systems, people and organizations. His papers have appeared in the Journal of Strategic Information Systems, the European Journal of Information Systems, Information Technology & People, and The Information Society Journal.

**Mehwish Nasim** is a Computer Science Lecturer at the University of Western Australia. She works in the emerging field of social cybersecurity. Informed by sociological theories on human interaction, she develops mathematical models of social influence to combat the dissemination of misinformation across social media platforms. She also models operations in information environment in wargames.

**Tabisa Ncubekezi** is an academic at the Cape Peninsula University of Technology. She has done her Ph.D. in the same institution. Her primary research areas are communication networks, cloud computing, cyber security, and e-Learning.

**Tatu Niskanen** is a researcher with a background in cybersecurity and information systems science. In addition to research work, he has experience in software development. He is working for the Applied cybersecurity team at VTT Technical Research Centre of Finland and finishing up his master's degree at the university of Jyväskylä.

**Daniel Nistor** is a Public Affairs specialist with more than a decade of experience in media operations for the Romanian Armed Forces and Ministry of Defence. He is currently a PhD student at the National Defence University, conducting a research on consolidating a society's security culture through better institutional strategic communication.

**Nombeko Ntingi** holds a BSc (Computer Science) from the University of Transkei, Master's degree in IT from Carnegie Mellon University, and a BCom (Financial Management) from the University of South Africa. She holds certificates in SAP ABAP, Cyber Security from UJ, CPUT and F'SAT; Managing Risk Harvard Online. She is currently pursuing PhD studies at the University of Johannesburg.

**Victor Kwarteng Owusu** is a Ph.D. candidate at the Faculty of Management and Economics, Tomas Bata University in Zlin, Czech Republic. He has two publications to his credit. He has also attended conferences across Europe and the United Kingdom including British Academy of management (BAM), hosted by Manchester business school. His main research area is organizational performance.

**Jani Päijänen** works as a Project Manager at the Institute of Information Technology of JAMK University of Applied Sciences. He has industry background in delivering consultancy for clients in Project Management, Information Technology, and Software Development.

**Tehi Palletvuori** is Security Management master's degree student at Laurea University of Applied Sciences. Palletvuori BBA (Finance), MBA (Entrepreneurship and Business Competence) has over 20 years of working experience in Banking, Corporate Treasury and IT. Since March 2020 she has worked at Finnish National Emergency Supply Agency and is responsible for financial sector preparedness.

**Nikolaos Papakonstantinou**, D.Sc.(Tech.), Docent, is an Electrical and Computer Engineer interested in system resilience and cybersecurity. He is the Research Team Leader of the Applied cybersecurity team at the VTT Technical Research Centre of Finland.

**Konstantina Papachristopoulou** is a senior Research ICT Project Manager for EU-funded projects in Eight Bells Ltd. She has a diverse background and R&D experience obtained from various initiatives across European and national programs. She has successfully delivered more than 25 multidisciplinary research projects, focusing on areas such as cybersecurity, IoT & CPSoS, health, and sustainable manufacturing.

**Ada Peter** is a Professor, Digital Infrastructure, and International Security. She produces comprehensive, policy-focused, nontechnical cybersecurity documents that emphasize and teach senior principal state officials how to make informed cyber policy planning decisions. Her current research focuses on how U.S. national cyber strategies undermine critical infrastructures' protection against previous and potential cyber weapons.

**Lucas Potter** earned his B.S. in Biomedical Engineering in 2015 from VCU and a PhD in Biomedical Engineering ODU. He has researched human factors for three federal organizations, biomedical engineering for three private companies and is an active contributor to the field of Biocybersecurity.

**Dr. Jouni Pöyhönen**, Col (ret.) is a postdoctoral researcher of cyber security programs in University of Jyväskylä. He received a Ph.D. in Information Technology from University of Jyväskylä. He has over 30 years' experience as developer and leader of C4ISR Systems in Finnish Air Forces. He has more than twenty cyber security research papers or articles.

**Jyri Rajamäki**, Principal Lecturer in Information Technology at Laurea University of Applied Sciences and Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä, Finland, holds D.Sc. degrees in electrical and communications engineering from the Helsinki University of Technology, and a PhD in mathematical information technology from the University of Jyväskylä.

**Trishana Ramluckan** is the research manager at Educor Holdings, an honorary research fellow for Law at the University of KwaZulu-Natal, a curator of the EU:CD's Cyber Diplomacy Atlas, a member of the IFIP working group on ICT Uses in Peace and War, and was listed in the Top 50 Women in Cybersecurity in Africa (2020).

**Huw O.L. Read** is Charles A. Dana Professor of Digital Forensics and the Director of the Centre of Cybersecurity and Forensics Education and Research (CyFER) at Norwich University, Vermont, USA. For over 15 years, he has taught in several countries, authored over 20 peer-reviewed publications in the field and has been awarded numerous competitive grants.

**Aunshul Rege** is an Associate Professor and Director of the Cybersecurity in Application, Research, and Education (CARE) Lab at Temple University. Her research focuses on the human and behavioral aspects of cyberattacks, surveillance, privacy, social engineering, and cybersecurity education, and has been funded by various National Science Foundation grants.

**Mari Ristolainen** is a Researcher at the Finnish Defence Research Agency. She has studied psychology at the Moscow State University and she earned a doctorate in Russian Language and Cultural Studies from the University of Joensuu in 2008. She has been conducting postdoctoral research in the field of Russian and Border Studies in several Academy of Finland- and EU-funded projects at the University of Eastern Finland and at the University of Tromsø, Norway. Her current research interests include cyber warfare as a phenomenon, Russian digital sovereignty, and the governance of cyber/information space.

**Harri Ruoslahti**, PhD, works as a Principal lecturer at the Resilience Lab of Laurea University of Applied Sciences.

**Helvi Salminen** has worked in information security since June 1990 in a high security industrial environment. Before her security career she has 12 years of experience in systems development. She has 30+ years experience in cryptographic systems management and various security frameworks. She was awarded as CISO of the year in Finland 2014.

**Nkata Sekonya** is a postgraduate student in computer science at the University of Johannesburg, SA. He received his BSc in Information Technology from the University of Johannesburg in 2021. His main research interests are digital forensics, critical infrastructure protection, and the internet of things.

**Radu Serrano** is PhD student at the Ragnar Nurkse Department of Innovation and Governance of TalTech, Estonia. He also develops and manages cybersecurity, smart governance, e-democracy and technology projects at the e-Governance Academy. His main research areas include cybersecurity, internet voting and business administration.

**Jussi Simola**: post-doctoral researcher and has a PhD degree in cyber security from the University of Jyväskylä. Expertise includes decision-support technologies, situational awareness systems, information security, and continuity management. His current research work is focused on the development of maritime cyber security. Has been involved in developing a common early warning system for the EC.

**Ms Thenjiwe Sithole** is a PhD student at the University of Johannesburg. She holds a Masters in Information Technology (Information Systems) from the University of Pretoria and a Master of Engineering Sciences in Electronics (Telecommunications) from the University of Stellenbosch. She also has Certificate in Cyber Security from the University of Johannesburg.

**Siphesihle Sithungu** is from Johannesburg, South Africa and holds an MSc in Computer Science (University of Johannesburg). He is a lecturer at the University of Johannesburg, and his research interests are artificial intelligence and critical information infrastructure protection. Mr Sithungu is a technical committee member for the International Conference on Computational Intelligence and Intelligent Systems.

**Adam Spanier** is currently pursuing a PhD in IT Computing Systems from the University of Nebraska at Omaha. He has a BS in Computer Science and is pursuing his MS in Cybersecurity concurrently with his PhD. His research interests include intermediate representation analysis in cybersecurity, computational trust, and cybersecurity gamification.

**Iain Sutherland** is Professor of Digital Forensics and Head of Research at Noroff University College in Kristiansand, Norway, a university he helped to establish in 2012. A recognised expert in computer forensics, he has supervised several PhD students and provided evidence as an expert witness. He has authored articles ranging from forensics practice and procedure to network security.

**Pardis Moslemzadeh Tehrani** is the Associate Head of the Law School, at the Faculty of Business, Law and Tourism, University of Sunderland. Before joining the Sunderland University, she was a Senior Lecturer and Visiting Associate Professor at the Faculty of Law, University of Malaya. Her research spans the area of information technology law, international law and legal research methodology. She is the author and co-author of more than 70 research papers, books, book chapters and conference papers. She has served on many conferences, seminars, forums and workshop programme committees and delivered talks at various panels, NGOs, research centres and international bodies such as ICRC and other Human Rights organisations.

**Ranko Trišić.** I started my Master's degree, in Games Studies and Engineering, in 2020, in Klagenfurt, Austria. My research and thesis are about hacking and cheating in game industries. As a part of my thesis, I had to create game according to topic. So, I created board game under the name "*HACKER'S CYBER ATTACK*".

**Uakomba Uhongora** is a PhD candidate at the University of South Australia. Her PhD is on space systems cyber security with a focus on the integration of SDN and space systems. She is a lecturer at the Namibia University of Science and Technology. Her research interests are cyber security, deep learning, space systems and SDN.

**Brett van Niekerk** is a senior lecturer at the Durban University of Technology, chairs the International Federation of Information Processing Working Group on ICT in Peace and War, and is co-Editor-in-Chief of the *International Journal of Cyber Warfare and Terrorism*. He is CISM certified, with over 50 publications and 20 presentations.

**Basie von Solms** is a Research Professor in the Academy for Computer Science and Software Engineering at the University of Johannesburg. He specialises in Cyber Security. He is a Past President of the International Federation for Information Processing (IFIP). Professor Rossouw von Solms is an emeritus professor from the Nelson Mandela University. Rossouw has supervised 65 students successfully to a Master's and Doctoral degrees in the fields of information security and IT governance. He has published and presented in excess of 200 peer-reviewed research papers.

**Richard L. Wilson** is a Professor in Philosophy at Towson University in Towson, MD. Professor Wilson Teaches Applied Ethics in the Philosophy and Computer and Information Sciences departments at Towson while also serving as Senior Research Scholar in the Hoffberger Center for Professional Ethics at the University of Baltimore. Professor Wilson's interest's are

directed towards applying phenomenology to issues with emerging and innovative technologies.

**Allison Wylde** holds posts with Glasgow Caledonian University (London) as a Senior Lecturer, and with the Cardiff University Centre for Cyber Security Research: research includes- artificial intelligence (AI) intelligent virtual assistants (IVAs); trust and zero trust; and, work on cyber security norms and the Global Digital Compact with the United Nations Internet Governance Forum.

**Saliha Yilmaz** is currently pursuing a PhD in Cybersecurity at Kingston University London. Her research focuses on detecting privacy risk-prone mobile applications. Her previous research and studies focused on predictive policing and personal data legislation in government institutions. Cybersecurity, data privacy, threat intelligence, crime science, and data-driven policing are among her research interests.