

# **Proceedings of the**

## **18<sup>th</sup> International Conference on Cyber Warfare and Security ICCWS 2023**

**A Conference**

**Hosted By**

**Towson University, Baltimore County  
Maryland, USA**

**9-10 March 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 ISI Web of Science and Elsevier Scopus. Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

From 2022 these proceedings are open access and freely available for all to read. The Conference Proceedings for previous years can be purchased from <http://academic-bookshop.com>

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

E-Book ISBN: 978-1-914587-62-7

E-Book ISSN: 2048-9889

Print ISBN: 978-1-914587-61-0

Book Version ISSN: 2048-9870

Published by Academic Conferences International Limited

Reading, UK

+44118 324 6938

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

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

## **ICCWS 2023 Contents Page**

|  |            |
|--|------------|
| <b><u>Preface</u></b>  | <b>v</b>   |
| <b><u>Committee</u></b>  | <b>vi</b>  |
| <b><u>Biographies</u></b>  | <b>vii</b> |
| <b><u>Academic Papers</u></b>  |            |
| <i>Secure Cloud Migration Strategy (SCMS): A Safe Journey to the Cloud</i><br>Dalal Alharthi   | 1-6        |
| <i>Cyber-Physical Attack Using High Power RF in Havana, Cuba</i><br>Allyfazzkkamn Argudo, Ghislaine Nasibu   | 7-18       |
| <i>Cybersecurity in Digital Transformation applications: Analysis of Past Research and Future Directions</i><br>Zakariya Belkhamza   | 19-24      |
| <i>An Automated Post-Exploitation Model for Cyber Red Teaming</i><br>Ryan Benito, Alan Shaffer, Gurminder Singh  | 25-34      |
| <i>Review of End-to-End Encryption for Social Media</i><br>Vijay Bhuse   | 35-37      |
| <i>An Analysis of Crypto Scams during the Covid-19 Pandemic: 2020-2022</i><br>Johannes George Botha, Danielle Botha, Louise Leenen   | 36-48      |
| <i>Case Study: Conducting a Risk Assessment for an Electrical Utility</i><br>Edwin Covert  | 49-56      |
| <i>On the Use and Strategic Implications of Cyber Ranges in Military Contexts: A Dual Typology</i><br>Mischa Hansel, Andrew Dwyer, Kathrin Moog, Jantje Silomon                      | 57-66      |
| <i>Evaluation of Quantum Key Distribution for Secure Satellite-integrated IoT Networks</i><br>Andrew Edwards, Yee Wei Law, Ronald Mulinde, Jill Slay                                 | 67-76      |
| <i>Commentary on Healthcare and Disruptive Innovation</i><br>Hilary Finch, Abasi-Amefon Affia, Woosub Jung, Lucas Potter, Xavier-Lewis Palmer  | 77-84      |
| <i>Securing Commercial Satellites for Military Operations: A Cybersecurity Supply Chain Framework</i><br>Courtney Fleming, Mark Reith, Wayne Henry                                   | 85-92      |
| <i>Predictors of Human Efficiency in Radar Detection Tasks</i><br>Elizabeth Fox, Arielle Stephenson, Christopher Stevens, Gregory Bowers   | 93-102     |
| <i>Nuclear Cyber Attacks: A Study of Sabotage and Regulation of Critical Infrastructure</i><br>Virginia Greiman  | 103-110    |
| <i>Social-Engineering, Bio-economies, and Nation-State Ontological Security: A Commentary</i><br>Brandon Griffin, Keitavius Alexander, Xavier-Lewis Palmer, Lucas Potter             | 111-118    |
| <i>Search and CompAre Reverse (SCAR): A Bioinformatics–Inspired Methodology for Detecting File Remnants in Digital Forensics</i><br>George Grispos, William Mahoney, Sayonaha Mandal | 119-127    |
| <i>Development and Analysis of a Reconnaissance-Technique Knowledge Graph</i><br>Thomas Heverin, Elsa Deitz, Eve Cohen, Jordana Wilkes   | 128-136    |
| <i>Zero Trust is Not Enough: Mitigating Data Repository Breaches</i><br>JS Hurley  | 137-144    |

|   |         |
|---|---------|
| <i>Managing Large-Scale Heterogeneous Deployments for Cybersecurity</i><br>JS Hurley  | 145-151 |
| <i>Digital Geopolitics: A Review of the Current State</i><br>Gazmend Huskaj   | 152-161 |
| <i>Managing Variable Cyber Environments with Organizational Foresight and Resilience Thinking</i><br>Eveliina Hytönen, Jyri Rajamäki, Harri Ruoslahti   | 162-170 |
| <i>Fingerprinting Network Sessions for the Discovery of Cyber Threats</i><br>Christiaan Klopper, Jan  | 171-180 |
| <i>S-400s, Disinformation, and Anti-American Sentiment in Turkey</i><br>Russell Korb, Saltuk Karahan, Gowri Prathap, Ekrem Kaya, Luke Palmieri, Hamdi Kavak   | 181-188 |
| <i>Detecting and tracking hypersonic glide vehicles: A cybersecurity-engineering analysis of academic literature</i><br>Yee Wei Law, John Joshua Gliponeo, Dilpreet Singh, John McGuire, Jiajun Liang, Sook-Ying Ho,<br>and Jill Slay | 189-198 |
| <i>Cyber security training in Finnish basic and general upper secondary education</i><br>Martti Lehto, Pekka Neittaanmäki   | 199-208 |
| <i>Russian Influence Operations during the Invasion of Ukraine</i><br>Joseph Littell, Nicolas Starck  | 209-217 |
| <i>Modelling the Influential Factors Embedded in the Proportionality Assessment in Military Operations</i><br>Clara Maathuis, Sabarathinam Chockalingam   | 218-226 |
| <i>Social Media Manipulation Awareness through Deep Learning based Disinformation Generation</i><br>Clara Maathuis, Iddo Kerkhof  | 227-236 |
| <i>Social Media Manipulation Deep Learning based Disinformation Detection</i><br>Clara Maathuis, Rik Godschalk  | 237-245 |
| <i>Improvements on Hiding x86-64 Instructions by Interleaving</i><br>William Mahoney, Todd McDonald, George Grispos, Sayonha Mandal   | 246-255 |
| <i>Developing Privacy Incident Responses to Combat Information Warfare</i><br>Sean McElroy, Lisa McKee  | 256-263 |
| <i>Use of Intrusion Detection Systems in Vehicular Controller Area Networks to Preclude Remote Attacks</i><br>Anthony Monge, Todd Andel   | 264-272 |
| <i>Digital Insanity: Exploring the Flexibility of NIST Digital Identity Assurance Levels</i><br>Kenneth Myers   | 273-278 |
| <i>Risk likelihood of planned and unplanned cyber-attacks in small business sectors: A cybersecurity concern</i><br>Tabisa Ncubekezi  | 279-290 |
| <i>Ret-gadgets in RISC-V-based Binaries Resulting in Traps for Hijackers</i><br>Toyosi Oyinloye, Lee Speakman, Thaddeus Eze   | 291-299 |
| <i>Basic Elements of Cyber Security for a Smart Terminal Process</i><br>Jouni Pöyhönen, Jussi Simola, Martti Lehto  | 300-308 |
| <i>Anti-American Stance in Turkey: A Twitter Case Study</i><br>Gowri Prathap, Hamdi Kavak, Ekrem Kaya, Luke Palmieri, Saltuk Karahan, Alex Korb   | 309-317 |
| <i>Gaps in Asset Management Systems to Integrate Railway Companies' Resilience</i><br>Jyri Rajamäki, Jari Savolainen, Rauno Pirinen, Villamor   | 318-326 |

|   |         |
|---|---------|
| <i>LoRaWAN &amp; The Helium Blockchain: A Study on Military IoT Deployment</i><br>Michael A. Reyneke, Barry E. Mullins , Mark G. Reith  | 327-337 |
| <i>Blockchain Forensics: A Modern Approach to Investigating Cybercrime in the Age of Decentralisation</i><br>Saminu Salisu, Velitchko Filipov   | 338-347 |
| <i>Biocybersecurity and Deterrence: Hypothetical Rwandan Considerations</i><br>Issah Samori, Gbadebo Odularu, Lucas Potter, Xavier-Lewis Palmer   | 348-354 |
| <i>Lesson Plan: An Interdisciplinary Approach to Teaching Cyber Warfare Concepts</i><br>Donna Schaeffer, Patrick Olson  | 355-359 |
| <i>The Impact of Edge Computing on the Industrial Internet of Things</i><br>Nkata Sekonya, Siphesihle Sithungu  | 360-368 |
| <i>Cyber Threat Analysis in Smart Terminal Systems</i><br>Jussi Simola, Jouni Pöyhönen, Lehto Martti  | 369-378 |
| <i>Towards a Scientific Definition of Cyber Resilience</i><br>Sidney Smith  | 379-386 |
| <i>Implications of Cyberbiosecurity in Advanced Agriculture</i><br>Simone Stephen, Keitavius Alexander, Lucas Potter, Xavier-Lewis Palmer   | 387-393 |
| <i>Organizational Cybersecurity Post The Pandemic: An Exploration of Remote Working Risks and Mitigation Strategies</i><br>Stephen Treacy, Anoop Sabu, Thomas Bond, Joseph O'Sullivan, Jack Sullivan, Peter Sylvester | 394-401 |
| <i>A Quantitative Risk Assessment Framework for the Cybersecurity of Networked Medical Devices</i><br>Maureen Van Devender, Jeffrey Todd McDonald   | 402-411 |
| <i>Towards the Usefulness of Learning Factories in the Cybersecurity Domain</i><br>Namosha Veerasamy, Thuli Mkhwanazi, Zubeida Dawood   | 412-419 |
| <i>Naïve Bayes Supervised Learning based Physical Layer Authentication: Anti-Spoofing techniques for Industrial Radio Systems</i><br>Andreas Weinand, Christoph Lipps, Michael Karrenbauer, Hans Dieter Schotten      | 420-430 |
| <i>How the Russian Influence Operation on Twitter Weaponized Military Narratives</i><br>Dana Weinberg, Jessica Dawson, April Edwards  | 431-439 |
| <i>Nuclear Weapons, Cyber Warfare, and Cyber Security: Ethical and Anticipated Ethical Issues</i><br>Richard Wilson, Alexia Fitz  | 440-448 |
| <i>Robots Security Assessment and Analysis Using Open-Source Tools</i><br>Benjamin Yankson, Tyler Loucks, Andrea Sampson, Chelsea Lojano  | 449-456 |
| <i>Social Robots Privacy Enhancement Using Colored Petri Net (CPN) for Behavior Modeling: A Case Study of Asus Zenbo Robot</i><br>Benjamin Yankson, Farkhund Iqbal, Fadya AlMaeeni                                    | 457-464 |
| <b><u>PhD Papers</u></b>  |         |
| <i>A Unified Forensics Analysis Approach to Digital Investigation</i><br>Ali Alshumrani, Nathan Clarke, Bogdan Ghita  | 466-475 |
| <i>Offensive Cyberspace Operations for Cyber Security</i><br>Gazmend Huskaj   | 476-479 |

|  |         |
|--|---------|
| <i>Categorizing Cyber Activity Through an Information-psychological and Information-technological Perspective, Case Ukraine.</i>     | 480-488 |
| Harry Kantola  |         |
| <i>Using Military Cyber Operations as a Deterrent</i>  | 489-496 |
| Maria Keinonen   |         |
| <i>Identifying Commonalities of Cyberattacks Against the Maritime Transportation System</i>  | 497-503 |
| Rebecca Rohan  |         |
| <i>Evaluating a Non-platform-specific OCR/NLP system to detect Online Grooming</i>   | 504-511 |
| Jake Street, Funminiyi Olajide   |         |
| <b><u>Masters Papers</u></b>   |         |
| <i>Demonstrating Redundancy Advantages of a Three-Channel Communication Protocol</i>   | 513-522 |
| Scott Culbreth, Scott Graham   |         |
| <i>UAV Payload Identification with Acoustic Emissions and Cell Phones</i>  | 523-533 |
| Hunter Doster, Barry Mullins   |         |
| <i>Just Warfare: Is a Nuclear Attack an appropriate Response to a Cyber Attack?</i>  | 534-541 |
| Alexia Fitz, Richard Wilson  |         |
| <i>A Review and Testing of Fault Tolerance Levels of Anti-Poaching Cybersecurity System</i>  | 542-549 |
| Isabelle Heyl, Julia Stone, Takudzwa Vincent Banda, Vian Smit, Dewald Blaauw   |         |
| <i>DACA: Automated Attack Scenarios and Dataset Generation</i>   | 550-559 |
| Frank Korving, Risto Vaarandi  |         |
| <i>Towards a Critical Review of Cybersecurity Risks in Anti-Poaching Systems</i>   | 560-568 |
| Christelle Steyn, Dewald Neville Blaauw  |         |
| <b><u>Work in Progress Papers</u></b>  |         |
| <i>Locality-based electromagnetic leakage assessment using CNN</i>   | 570-576 |
| Ian Heffron, James Dean  |         |
| <i>Using Deep Reinforcement Learning for Assessing the Consequences of Cyber Mitigation Techniques on Industrial Control Systems</i> | 577-580 |
| Terry Merz, Romarie Morales Rosado   |         |

## ICCWS Preface

These proceedings represent the work of contributors to the 18th International Conference on Cyber Warfare and Security (ICCWS 2023), hosted Towson University, Baltimore County, Maryland, USA on 9-10 March 2023. The Conference co-Chairs are Richard Wilson, Towson University, Baltimore County, Maryland, USA, and Major Brendan Curran, from National Security Agency's Space Cybersecurity Office in Fort Meade, Maryland.

ICCWS is a well-established event on the academic research calendar and now in its 18th year, the key aim remains the opportunity for participants to share ideas and meet the people who hold them. The scope of papers will ensure an interesting two days. 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 Justin Fanelli, Technical Director, Dept of Navy PEO Digital, on the topic of *Can Zero Trust Restore Our Ailing Trust?* The second day of the conference will open with an address by Dr. George R. Lucas, Stockdale Center at the U.S. Naval Academy. His talk is titled *Military Ethics & Algorithmic Warfare: from the Battlefield to the Cyber Domain*

With an initial submission of 136 abstracts, after the double blind, peer review process there are 53 Academic research papers, 6 PhD research papers, 12 Masters Research papers and 1 work-in-progress paper published in these Conference Proceedings. These papers represent research from Brazil, Austria, China, Estonia, Finland, Germany, Israel, Italy, Kenya, Nigeria, Pakistan, Russia, Saudi Arabia, Slovakia, South Africa, Sweden, Switzerland, Taiwan, UAE, Uganda and the United Kingdom.

We hope you enjoy the conference.

Richard L. Wilson  
Towson University, Baltimore County  
Maryland, USA  
March 2023

## ICCWS Conference Committee

*Prof Azween Abdullah, Taylors University, Malaysia; Dr Bulent Acma, Anadolu University, Eskisehir, Turkey; Dr William ("Joe") Adams, Univ of Michigan/Merit Network, USA; Prof Hamid Alasadi, Iraq University college, Iraq; Dr Elie Alhajar, USMA, USA; Prof Todd Andel, University of South Alabama, USA; Prof Antonios Andreatos, Hellenic Air Force Academy, Greece; Leigh Armistead, Oak Ridge National Laboratory, USA; Researcher Jawad Awan, Institute of Information & Communication Technology, Pakistan; Prof Richard Baskerville, Georgia State University, USA; Dr Zakariya Belkhamza, Ahmed Bin Mohammed Military College, Qatar; Prof Vijay Bhuse, Grand Valley State University, USA; Dr Mustafa Canan, Naval Postgraduate School, USA; Dr Kevin Matthe Caramancion, Mercyhurst University, Erie, PA, USA; Dr Jim Chen, U.S. National Defense University, USA; Dr Sabarathinam Chockalingam, Institute for Energy Technology, Norway; Dr Nathan Clarke, University of Plymouth, UK; Dr Ronen Cohen, Ariel University Centre, Israel; Mr Edwin Covert, WarnerMedia, USA; Dr Paul Crocker, University of Beira Interior, Portugal; Dr Michael Dahan, Sapir College, Israel; Evan Dembskey, UNISA, South Africa; Prokopios Drogkaris, University of the Aegean, Greece; Prof Mariki Eloff, University of South Africa, South Africa; Prof Eric Filiol, ENSIBS, Vannes, France & CNAM, Paris, France; Larry Fleurantin, Fleurantin, Francois & Antonin, P.A., North Miami Beach, USA; Dr Jonathan Fuller, United States Military Academy, USA; Dr Ahmad Ghafarian, University of North Georgia, USA; Dr Scott Graham, Air Force Institute of Technology, USA; Prof Dr Tim Grant, Retired But Active Researcher, The Netherlands; Dr John Gray, Nova Southeastern University, USA; Virginia Greiman, Boston University, USA; Dr Michael Grimaila, Air Force Institute of Technology, USA; Dr George Grispos, University of Nebraska at Omaha, USA; Prof Bill Hutchinson, Edith Cowan University, Australia; Dr Berg Hyacinthe, State University of Haiti, Haiti; Ramkumar Jaganathan, VLB Janakiammal College of Arts and Science (affiliated to Bharathiar University), India; Dr Ezhil Kalaimannan, University of West Florida, USA; Dr Bilge Karabacak, Franklin University, USA; Dr Saltuk Karahan, Old Dominion University, USA; Prof Jesuk Ko, Universidad Mayor de San Andres, Bolivia; Dr Ahmet Koltuksuz, Yasar University, Turkey; Mr Peter Kunz, Hexagon Geosystems, Germany; Dr Gregory Laidlaw, University of Detroit Mercy, USA; Dr Sylvain (Sly) Leblanc, Royal Military College of Canada, Canada; Louise Leenen, CSIR, Pretoria, South Africa; Prof Martti Lehto, University of Jyväskylä, Finland; Dr Antoine Lemay, CYDEF, Canada; Dr Andrew Liaropoulos, University of Piraeus, Greece; Christoph Lipps, German Research Center for Artificial Intelligence, Germany; Volodymyr Lysenko, University of Washington, USA; Dr Bill Mahoney, University of Nebraska, Omaha, USA; ASSI Haribabu Maruturi, qiscet, india; Dr Paul Maxwell, Army Cyber Institute, USA; Dr Todd McDonald, Air Force Institute of Technology, USA; Dr Terry Merz, State University of New York College of Emergency Preparedness, Homeland Security and Cybersecurity, United States; Dr Robert Mills, Air Force Institute of Technology, USA; Assc Pardis Moslemzadeh Tehrani, Faculty of Law. University of Malaya, Malaysia; Dr Barry Mullins, Air Force Institute of Technology, USA; Prof Antonio Muñoz, University of Málaga, Spain; Dr Asoke Nath, St. Xavier's College(Autonomous), India; Dr Funminiyi Olajide, Nottingham Trent University, UK; Prof Abdelnaser Omran, School of Economics, Finance and Banking, Universiti Utara Malaysia, Malaysia; Rain Ottis, Tallinn University of Technology, Estonia; Dr Jaydeep Patil, D.Y.Patil Agriculture and Technical University Talsande, India; Dr*



*Gilbert Peterson, Air Force Institute of Technology, Dayton, Ohio, USA; Andy Pettigrew, George Washington University, USA; Dr Jackie Phahlamohlaka, Council for Scientific and Industrial Research, Pretoria, South Africa; Ms Heloise Pieterse, CSIR, South Africa; Dr Ajeet Singh Poonia, Bikaner Technical University, India; 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, Air Force Institute of Technology, USA; Lt Col Ernest Robinson, U.S. Marine Corps / Air War College, USA; Dr Neil Rowe, US Naval Postgraduate School, Monterey, USA; Prof Lili Saghafi, Canadian International College, Montreal, Canada; Dr Char Sample, US Army Research Laboratory, USA; Prof Leonel Santos, Politechnic of Leiria, Portugal; Ramanamurthy Saripalli, Pragati Engineering College, India; Dr Yilun Shang, Singapore University of Technology and Design, Singapore; Dr D. Cragin Shelton, Capitol Technology University, USA; Dr Dan Shoemaker, Centre for Assurance Studies, USA; Mr Avinash Singh, University of Pretoria, South Africa; Prof Jill Slay, University of South Australia, Australia; Dr William Spring, University of Hertfordshire, UK; Dr Kevin Streff, Dakota State University, USA; Ms sneha sudhakaran, Louisiana State University, USA; Dr Arwin Sumari, State Polytechnic of Malang, Java, Indonesia; Dr James Sweeney, Capella University, USA; Mr Unal Tatar, University at Albany - SUNY, USA; Dr Le Thi-Thu-Huong, Pusan National University, Korea; Mr Patrick Tobin, University College Dublin, Ireland; Dr Antonio Jorge Tomeu-Hardasmal, University of Cadiz, Spain; Dr Vu Tran, Naval Air Warfare Center - Weapons Division, USA; Dr Eric Trias, Air Force Institute of Technology, USA; Dr Chia-Wen Tsai, Ming Chuan University, Taiwan; Brett van Niekerk, Durban University of Technology., South Africa; Dr Namosha Veerasamy, Council for Scientific and Industrial Research, South Africa; Prof Murdoch Watney, University of Johannesburg, South Africa; Richard Wilson, Towson University, USA; Hongyi Wu, Old Dominion University, Virginia, USA; Enes Yurtoglu, Turkish Air War College, Turkey; Dr Zehai Zhou, University of Houston-Downtown, USA.*

## Biographies

### Conference and Programme Chairs



**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.



**Major Brendan Curran** currently serves as a strategist for the National Security Agency's Space Cybersecurity Office in Fort Meade, Maryland. Major Curran is an Army Space Operations Officer with over twenty years of experience as both an active duty U.S. Army Commissioned and Non-Commissioned Officer in the fields of engineering, intelligence, communications, and space operations. Over the course of his fourteen years in the space community Brendan has integrated space-based capabilities and emerging technologies in support of military activities throughout Europe, Southwest Asia, and Africa. Major Curran established the Space Operations & Integrated Joint Special Technical Operations programs at 10th Special Forces Group (Airborne), Mission Command Training Program, and the Army Space Officer position at U.S. Space Force Space Operations Command (then U.S. Air Force Space Command) where he co-chaired the initial planning team that led to the creation of the National Space Defense Center. His professional passions are operational design, unconventional warfare, and strategy. Brendan is Defense Advanced Research Projects Agency (DARPA) Service Chief Fellow, Horatio Alger Association Distinguished Military Scholar, recipient of the BG Sharp Distinguished Leadership Award, and alumni of the U.S. Army training with industry program at the Johns Hopkins University Applied Physics Laboratory. He attended Towson University, MD on an Army Green to Gold scholarship where he earned a BS in Philosophy. Major Curran later attended Norwich University where he earned a MA in Diplomacy with a concentration in international conflict resolution. Major Curran is married to Dr. Carrie Arnold. They have a seven-year-old daughter. When he's not gazing up at the stars, Brendan can be found immersed in gardening and herpetology.

### Keynote Speakers



**Mr. Justin Fanelli** is the Technical Director of Program Executive Office Digital & Enterprise Services (PEO Digital), chartered to provide strategic technical leadership for the rapid transformation of enterprise IT infrastructure within the Department of Navy. His portfolios include Cloud and Platforms, Cyber and Operations, Digital Workplace/Productivity, Infrastructure, End User Services, and several others. Mr. Fanelli also serves as Chief Architect of Defense Medical Intelligence Data and Advisor to The Advanced Research Projects Agency for Health (ARPA-H), the moonshot startup within US Department of Health and Human Services.



**Dr. George R. Lucas** is a specialist in applied ethics (military, professions, technology) and history of modern philosophy/philosophy of science. He is Distinguished Chair in Ethics Emeritus at, Stockdale Center for Ethical Leadership, U.S. Naval Academy (Annapolis MD), Emeritus status conferred by Secretary of the Navy in April 2014 for life. Lucas is widely published, most recently with the book, *Law, Ethics, and Emerging Military Technologies: Confronting Disruptive Innovations* (Oxford: Routledge, 2022). He is also the General Editor of a Collected Critical Edition of the Works of Alfred North Whitehead (Edinburgh University Press). Lucas' current areas of research interest are Cyber Ware Ethics and AI and Cyber Warfare.

### Mini Track Chairs



**Dr. Jawad Hussain Awan** is Assistant Professor, Department of Computer Science, Shaheed Zulfikar Ali Bhutto Institute of Science & Technology, Gharao Campus, Sindh, Pakistan. He is a member of IFIP WG 9.10: ICT Uses in Peace and War, and an active researcher with the Global Foundation for Cyber Studies and Research Group. His research interests are ICT, Data Science, Cyber security, Security challenges in Smart and Physical Systems. He has published his research in several national and international research journals. He is the member of Editorial Review Board of a number of journals including of IEEE Access, Egyptian Journal of Informatics and the Journal of Information Warfare. He performed his duties as Committee member in ICCWS & ECCWS 2019, 2020, 2021 and 2022. He is also Microsoft Certified Professional in Web Programming, and has won research awards with the collaboration of HEC, Pakistan and the British Council. He also worked as Lab Manager, Lecturer, and Research Fellow.



**Dr. Zakariya Belkhamza** is currently a member of faculty at the computer information Systems department, Ahmed Bin Mohammed Military College, Doha, Qatar. His area of expertise is information systems, strategic information systems, system design and architecture. Dr. Zakariya Belkhamza holds a Ph.D. in Information systems. He has published several papers in International journals and has authored and edited several books in the area of information systems.



**Dr. Jason C. Brown** is a research scientist and assistant professor at the Army Cyber Institute at West Point. He teaches risk management and organizational security, and as a futurist, he studies emerging threats, technological and social trends, and responses to those threats. A currently serving officer with the U.S. Army, Dr. Brown has worked within the intelligence, information operations, and cyber career fields. He has authored technical reports on the future of extremism, information warfare, cyber enabled financial crimes, and Chinese soft power.



**Dr. Jessica Dawson** is the Information Warfare Division Chief at the Army Cyber Institute at West Point. She holds a Ph.D. from Duke Sociology and teaches social inequality and social theory. Her research focuses on the digital disruption of social processes. She serves as a special advisor to Army senior leaders on social media threats and information warfare.



**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.



**Dr. Char Sample** is a researcher with ICF. Dr. Sample also teaches at Boise State University. She has given guest lectures at Bournemouth University, Rensselaer Polytechnic University and Royal Holloway University. Dr. Sample has over 20 years' experience in the information security industry. Dr. Sample's research focuses on deception, and the role of cultural values in cybersecurity events **Update**. More recently she has begun researching the relationship between human cognition and machines. Presently Dr. Sample is continuing research on modeling cyber behaviors by culture, other areas of research are data resilience, cyber-physical systems and industrial control systems.



**Dr. Pardis Moslemzadeh Tehrani**, is a Visiting Associate Professor at the Faculty of Law, the University of Malaya. She was a Senior Lecturer at the same university from 2015 to 2022. Her research interests span the area of Information Technology Law, International Humanitarian Law and legal research methodology. Pardis has made scholarly contributions in peer-reviewed journals and presented papers in several national and international conferences and served on many conferences and workshop program committees.



**Dr Stilianos Vidalis**, Head of the Networks, Security and Systems subject group at the Department of Computer Science of the University of Hertfordshire. Leading the development of an innovative technology that automates threat assessments. Experienced in all aspects of Information Operations (IO) with excellent understanding of the Information Security (IS) lifecycle. Acted as an instructor for the British Armed Forces Intelligence Personnel on penetration testing and digital forensics for a number of years. Acted as a cyber-expert for the Welsh Government and for the Wales University Officers' Training Corps (WUOTC).

## **Biographies of Contributing Authors**

**Azza M. AlGhamdi** is a Cybersecurity doctoral candidate at Marymount University. Her dissertation entitled "Establishing a Cybersecurity School to Close the Workforce Gap" explores how to make cybersecurity a more visible discipline and domain of study in universities and how to attract more college freshmen to pursue cybersecurity as a career to increase student enrollment.

**Allyfazzkkamn R. Argudo**, 19 years of active duty service (U.S. Army), working on satellite communications / cybersecurity. I'm working on my Doctor of Science, Cybersecurity. Research focuses on data transmission security thru multi-spectrum orchestration. I hold a masters in information assurance (Thomas Edison State University, 2020) and a bachelor's in electronics engineering (2017).

**Ali Alshumrani** is pursuing his Ph.D. in Digital Forensics at the Centre for Cyber Security, Communications and Network Research (CSCAN) at the University of Plymouth. His research is focused on developing a unified digital forensics tool to advance data analytics automation. His research interests reside in digital forensics, cyber security, data ontology and data graph.

**Vijay Bhuse** is an Associate Professor of Computer Science at the Grand Valley State University. He received his Ph.D. from Western Michigan University in 2007 and completed his postdoctoral fellowship from the Dartmouth College. He worked in industry before returning to academia. His research interests are Network Security, Wireless Sensor Networks, Malware Analysis and Secure Coding.

**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 at the CSIR. Masters degree in Information Technology, at University of South Africa (UNISA). NDip and BTech degree in Computer Systems Engineering at the Tswane University of Technology (TUT).

**Edwin Covert** is a cybersecurity director for a large media company. Previously, he was the Global Head of Security Architecture for a global bank. He has a Bachelor of Science in cybersecurity from the University of Maryland University College. He is currently a Master's candidate at Colorado State University studying the management of information technology.

**Scott Culbreth** is a Second Lieutenant in the United States Air Force. He graduated from the United States Air Force Academy in 2021 with a B.S. in Computer Science and the Air Force Institute of Technology in 2022 with a M.A.S. in Cyber Systems. Research Interests include Secure Networking and Defense focused technologies.

**Hunter Doster** is an Air Force Officer currently working at the Air Force Research Lab. He graduated from the United States Air Force Academy in 2020 with a B.S. in computer engineering and from the Air Force Institute of Technology in 2022 with a M.S. in Computer Engineering. His main research areas are digital signal processing for acoustic emissions and digital RF systems.

**Andrew Dwyer** is a Lecturer (Assistant Professor) in Information Security at Royal Holloway, University of London. His research spans computational decision-making, critical approaches to cybersecurity, as well as exploring the role of cyber operations in contemporary conflict. He completed his DPhil in Cyber Security at the University of Oxford in 2019.

**Andrew Edwards** is a student at the University of South Australia, currently undertaking a Master of Telecommunication Engineering. The focus of research for his minor thesis is in quantum cryptography as applied to satellite-integrated communication networks.

**Sulemana Bankuoru Egala** is a Doctoral researcher in Management Science and Engineering majoring in data mining and information management at the School of Management and Economics, University of Electronic Science and Technology of China (UESTC) and an Assistant lecturer at the Department of Informatics, SD Dumbo University of Business and Integrated Development Studies, Wa, Ghana.

**Hilary Finch** is a masters student at Old Dominion University at the School of Cybersecurity. As a former educator of almost 10 years, she brings a unique perspective to the importance of research in cybersecurity. She currently serves as the Educational Liaison for CySecSol, LLC, an organization that brings underrepresented communities into the field of cybersecurity.

**Alexia Fitz** is an undergraduate student at Towson University dual majoring in International Studies and Political Science with a minor in Human Rights and History. She has found a passion for researching laws of war and WMDs. She plans on continuing her academic career with a master's in security studies, followed by law school.

**Courtney Fleming** attends the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, OH studying for her Master's degree in Cyber Operations. She graduated from Mississippi State University with a Bachelor's degree in Mathematics in 2018. Her research interests include space cybersecurity, cyber attack tactics, and software vulnerability analysis.

**Elizabeth Fox** is a research psychologist at the Air Force Research Laboratory, Wright-Patterson Air Force base, Ohio. She received her PhD in Human Factors and Industrial-Organisational Psychology from Wright State University in 2019. She develops and applies models of performance and neural activity to assess cognitive processes and inform system design and automation.

**Virginia A. Greiman**, Assistant Professor (Global Cyber Law and Governance and Megaprojects / Infrastructure Planning, Boston University). Served as a U.S. Department of State delegation diplomatic head in Eastern/ Central Europe, Asia and Africa and held high level appointments with the U.S. Department of Justice. Researches and publishes: cyber resilience, cyber law/regulation, nuclear cyber security, and global infrastructure megaprojects.

**Brandon Griffin** is a current cybersecurity student with CySecSol. He has received a bachelor's degree in kinesiology from Old Dominion University in Norfolk, Virginia. Brandon is interested in cyberbiosecurity, informational warfare, social media and the relationship they have on national security.

**George Grispos** - Assistant Professor of Cybersecurity (School of Interdisciplinary Informatics, University of Nebraska, Omaha). Received a MSc. in Computer Forensics and E-Discovery and his Ph.D. in Computing Science (University of Glasgow). Research interests: digital forensics, cybersecurity, residual data, and incident response. Has conducted research with Fortune 500 Organizations (financial services and manufacturing sectors), and law enforcement agencies.

**Mischa Hansel** leads IFSH's "International Cybersecurity" (ICS) research focus. His research interests encompass cybersecurity strategies and military postures as well as multilateral efforts to regulate offensive cyber operations. He completed his PhD with a thesis on conflict and cooperation in the field of international cybersecurity at the University of Cologne.

**Ian Heffron** is a Captain in the United States Air Force and currently attends the Air Force Institute of Technology. He has a background in computer science and serves as a Cyberspace Operations Officer. He has served overseas in South Korea and in Germany.

**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.

**Isabelle Heyl**, is currently a student at the University of Stellenbosch. I grew up in Johannesburg and moved to Stellenbosch in 2019. I am 21 years old and passionate about my studies and my hobbies such as triathlon and guitar.

**J.S. Hurley** joined ODNI in December 2020 focusing on the use of advanced data science tools and techniques and cyber intelligence. Hurley previously served as Professor at NDU in CIC focused on data analytics and cyberspace strategies and formerly as Senior Manager, Distributed Computing, The Boeing Company, in the Network Systems Division.

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

**Harry Kantola** (LtCol) is currently appointed as Research Manager at Finnish Defence Research Agency. He holds a General staff officers' degree (Licentiate) from the Finnish National Defence University, a Master's degree in War studies from the Swedish National Defence University and a Post Graduate certificate in Cyber Defence and Information Assurance from Cranfield University, UK.

**Hamdi Kavak** is an Assistant Professor in the Computational and Data Sciences Department and co-director of the Center for Social Complexity at George Mason University. His research interests lie at the intersection of data science and modeling & simulation. His email and website addresses are [hkavak@gmu.edu](mailto:hkavak@gmu.edu) and <http://www.hamdikavak.com>.

**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.

**Christiaan Klopper** is a master's student in IT focusing on big data science at the University of Pretoria, SA. He received his BEng in electronic engineering from the University of Pretoria in 2010. His main research areas are data science, big data analytics and developing a self-learning cyber defence system that can discover undetectable threats.

**Alex Korb** is a PhD student and graduate research assistant at Old Dominion University, Virginia, USA. He received his Master's degree in International Studies in 2019. His primary research interests are cyber- and information warfare, globalization and internet culture, and disinformation.

**Frank Korving** obtained his Master's degree at Tallinn University of Technology, Estonia in 2022. He has been a security practitioner for a large Nordic financial institution for the last five years.

**Gentry Lane** is the CEO & Founder of ANOVA Intelligence, a cyber national security software company. She is a senior software executive, statistician and cyberpower military strategist. She holds a DoD-appointed position to NATO STO, is a Senior Fellow at the Potomac Institute & Fellow at the National Security Institute.

**Yee Wei Law** is a Senior Lecturer at UniSA STEM, University of South Australia. His research is currently focusing on space system security, adversarial machine learning and machine diagnostics.

**Martti Lehto**, PhD (Military Sciences), Col (GS) (ret.): Cyber security (University of Jyväskylä). Over 30 years of experience as developer and leader of C4ISR Systems in Finnish Defence Forces. He has over 200 publications, research reports and articles on the areas of C4ISR systems, cyber security and defence, information warfare, air power and defence policy.

**Joe Littell** ([joseph.littell@westpoint.edu](mailto:joseph.littell@westpoint.edu)): US Army psychological operations officer and research scientist at the Army Cyber Institute at the United States Military Academy. His research focus on information warfare and disinformation. He holds degrees a bachelor's degree in Computer Science from the University of South Florida and a master's degree in Data Science from Duke University.

**Rich Losier** is a high-energy, leader driving collaborative security innovation. He has a proven record of rapid prototyping for strong business results. He is a thought leader for DevOps in preparation for IP licensing or M&A activity. Through personal values of integrity, respect, courage and commitment, Rich is a perpetual learner, team-builder, and positive organizational force.

**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.

**Dwayne McDaniel** has been working as a Developer Relations professional since 2015 and has been involved in tech communities since 2005. He loves sharing his knowledge, and he has done so, by giving talks at over a hundred events worldwide. Dwayne currently lives in Chicago. Outside of tech, he loves karaoke, live music, and performing improv.

**Sean McElroy** has built financial services products throughout his 20-year career. He serves as the CSO of Lumin Digital, a digital banking fintech. Previously, he co-founded Alkami Technology. Sean is a Ph.D. student in Dakota State University's Cyber Defense program and earned a Masters of Science in Information Security Engineering from the SANS Technology Institute.

**Lisa McKee**, a highly regarded security and privacy expert, has 20 years of industry experience, and a regular featured speaker at conferences and events globally including RSAC. Her Ph.D. is in Cyber Defense and dissertation in Privacy from Dakota State University where she shares her passion for privacy and security as an associate professor.

**Anthony Monge** is a retired US Naval officer and currently a PhD candidate at the University of South Alabama in Mobile. His current research is in Controller Area Network (CAN) Bus security for vehicles and similar Cyber-Physical systems. He currently resides in the Dallas-Fort Worth area with his wife and children.

**Kenneth Myers** is a doctoral student in the cybersecurity program at Marymount University, Arlington, VA, USA. His main research areas are identity and access management, cybersecurity workforce planning, and digital identity.

**Ghislaine Nasibu Mwana**, I am currently working toward a Doctor of Science in Cybersecurity. My thesis dissertation topic is "Cybersecurity consideration when adopting blockchain technology in the accounting field". I have a Master of Accountancy degree from the George Washington University. My researches are oriented toward how technology can impact the financial sector and processes.

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

**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.

**Toyosi Oyinloye** is a lecturer at the University of Chester, UK. Her main research area is in software exploitation and software protection methods which she has been studying for the past three years in her doctorate. She has authored other related papers as outcomes of her study.

**Ada Peter** is a Professor, Digital Media, and International Security. She explores the processes of cyber weaponization, terrorism, and conflict to help governments make informed decisions about warfare in the fifth domain.

**Gowri Prathap** holds a bachelor of science degree in Computational and Data Sciences from George Mason University (GMU). She is currently a TECDP analyst working at Cigna. Before joining Cigna, she worked as a research and teaching assistant at GMU. Her research interests are Artificial Intelligence and Machine Learning.

**Jyri Rajamäki** is 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. He 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.

**Michael A. Reyneke** received his B.S. in Computer Engineering from Utah Valley University in 2017. He is currently a Cyber Operations masters' degree student at the Air Force Institute of Technology. His current research interests include the Internet of Things, wireless communications, critical infrastructure protection, cyber-physical systems security/sensing, national security, and reverse engineering.

**Rebecca Rohan** is a resident in the Doctorate of Science in Cybersecurity program at Marymount University, Arlington, Virginia, U.S. She received a MS in cybersecurity with concentrations in forensics and intelligence from Utica University, Utica, NY, in 2012. Her main research areas are maritime cybersecurity, cybersecurity education, cybersecurity intelligence, and diversity in cybersecurity.

**Saminu Salisu** is the CTO of Bilic.io, and a PhD student at Vienna University of Technology, Austria. His research interests are Information Visualisation, Visual Analytics, Uncertainty Visualisation and Spatio-Temporal Visualisation. He is also the co-founder of Bird on-chain analytics protocol.

**Issah Abubakari Samori** has a background in Biomedical Engineering and currently works as an Artificial Intelligence Engineer. He focuses on building AI solutions for challenges in biomedicine and healthcare. Outside of building these AI solutions, he is also interested in the implications these solutions have on cybersecurity and biocybersecurity

**Donna M. Schaeffer** is a Professor in the School of Technology and Innovation at Marymount University. Dr. Schaeffer has published more 100 articles and papers, book chapters, and encyclopedia entries. She serves as Co-Chair of Transform Learning Working Group at the National Institute of Cybersecurity Education, and held leadership positions in professional associations.

**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.

**Alan Shaffer** is a Senior Lecturer and Associate Chair of Academics for the Computer Science Department at the Naval Postgraduate School. His research interests include cyber operations and security, computer systems modelling and verification, and data science. He has been involved with the IEEE Symposium on Security and Privacy as Organizing Committee Treasurer.

**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.

**Dr Sidney Smith** graduated from Towson University with a BS in Computer Science in 1990, a MS from TU in 2013, and a D.Sc. in 2019. He began his career with the US Army in 1990 and is currently a Computer Scientist for the Army Research Laboratory. He holds these professional certifications: CISSP, CISA, and CAP.

**Simone Stephen** is affiliated with the Old Dominion University School of Cybersecurity. Her areas of research interest currently include cyberbiosecurity, bioeconomics, mechanical engineering, aerospace engineering, space systems, cybersecurity, security awareness, environmental management, digitalization, education, and artificial intelligence.

**Christelle Steyn**, a student nearing the end of my masters studies at the University of Stellenbosch. I have an interest in cybersecurity and information systems and combined these fields with my interest in nature and wildlife conservation for my research.

**Jake Street** is a PhD student and Academic Associate and Nottingham Trent University, UK. His research is focused on creating solutions for protecting children online from social engineering attacks e.g. Online Grooming, as well as observing the additional factors that make these attacks complex to mitigate.

**David Tileston** is a cybersecurity engineer and exercise developer at Carnegie Mellon University's Software Engineering Institute (SEI). His experience at the SEI over the past 7 years includes dynamic defense research, cybersecurity curriculum development, cyber

exercise ranges, and infrastructure automation. David previously worked as a tool developer for 2 years as an Army Civilian.

**Stephen Treacy**, Anoop Sabu, Thomas Bond, Joseph O’Sullivan, Jack Sullivan, and Peter Sylvester are research collaborators based out of Cork University Business School, Ireland. This project was the result of a Masters’ thesis developed from the MSc in Information Systems for Business Performance in conjunction with ForcePoint Cybersecurity.

**Maureen S. Van Devender** is currently pursuing a Ph.D. in Computing at the University of South Alabama with a research focus on cybersecurity risk assessment. Her publications include the topics of cybersecurity vulnerability of networked medical devices and privacy preserving techniques in data that contains personally identifiable information.

**Namosha Veerasamy** is a computer scientist in the field cyber security research and governance for over 15 years. She received her PhD from the University of Johannesburg. She is currently employed as a senior researcher at the Council for Scientific and Industrial Research (CSIR) in Pretoria. She also holds CISSP and CISM certifications.

**Andreas Weinand** received his Dipl.-Ing. degree (M.Sc) from the TU Kaiserslautern, Germany in 2015. He is currently pursuing the Dr.-Ing. degree (Ph.D) at the Institute for Wireless Communication and Navigation at the RPTU Kaiserslautern, Germany. His research interests are in the area of reliable and secure wireless systems for machine type communication (MTC).

**Dana Beth Weinberg**, PhD, is a Professor of Sociology and Data Analytic at Queens College-CUNY. She currently studies influence operations and the ways they leverage and weaponize narratives. She is the Director of the New War Research Consortium, a civil-military collaboration combining academic insights and practical solutions for national security policy.

**Benjamin Yankson** is an assistant professor and Cybersecurity practitioner with several years of experience in various technical leadership roles in information technology security within the healthcare and education industries. His research focuses on IoT Security, Privacy, Cybersecurity Threat and Risk Assessment, Security Auditing/Compliance, and Digital Forensics. In addition, he has served as a reviewer and TPC member of several conferences