Abstracts of Papers

Presented at the

20th European Conference on Cyber Warfare and Security

ECCWS 2021

A Virtual Conference

Hosted By

University of Chester

UK

24th-25th June 2021

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 DROPBOX **https://tinyurl.com/ECCWS21** Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.

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

E-Book ISBN: 978-1-912764-43-3
E-Book ISSN: 2048-8610
Book version ISBN: 978-1-912764-99-0
Book Version ISSN: 2048-8602

Published by Academic Conferences International Limited
Reading, UK
+44 (0) 118 324 6938
www.academic-conferences.org
info@academic-conferences.org

Contents

Paper Title	Author(s)	Page No	Guide No
Preface		v	x
Committee		vi	xi
Biographies		vii	xiv
Keynote Outlines			
Research papers			
The PUF Commitment: Evaluating the Stability of SRAM-Cells	Pascal Ahr, Christoph Lipps and Hans Dieter Schotten	1	1
Asylum Seekers From Russia to Finland: A Hybrid Operation by Chance?	Kari Alenius	11	2
Antarctica and Cyber-Security: Useful Analogy or Exposing Limitations?	Shadi Alshdaifat, Brett van Niekerk and Trishana Ramluckan	18	3
Evasion of Port Scan Detection in Zeek and Snort and its Mitigation	Graham Barbour, André McDonald and Nenekazi Mkuzangwe	25	4
The Manifestation of Chinese Strategies Into Offensive Cyberspace Operations Targeting Sweden	Johnny Bengtsson and Gazmend Huskaj	35	5
The Evolution of Cyber Fraud in the Past Decade	George-Daniel Bobric	44	6
AI-Powered Defend Forward Strategy	Jim Chen	52	7
Global Military Machine Learning Technology Development Tracking and Evaluation	Long Chen and Jianguo Chen	61	8

Paper Title	Author(s)	Page No	Guide No
Global Social Network Warfare on Public Opinion	Long Chen and Jianguo Chen	71	9
Serious Games for Cyber Security: Elicitation and Analysis of End-User Preferences and Organisational Needs	Sabarathinam Chockalingam, Coralie Esnoul, John Eidar Simensen and Fabien Sechi	80	10
Effectiveness of Covert Communication Channel Mitigation Across the OSI Model	Tristan Creek, Mark Reith and Barry Mullins	90	11
Deepfake Video Detection	Shankar Bhawani Dayal and Brett van Niekerk	100	12
A Shoestring Digital Forensic Cyber Range for a Developing Country	Jaco du Toit and Sebastian von Solms	110	13
A Strategy for Implementing an Incident Response Plan	Alexandre Fernandes, Adaíl Oliveira, Leonel Santos and Carlos Rabadão	120	14
Are Encypted Protocols Really a Guarantee of Privacy?	Jan Fesl, Michal Konopa, Jiří Jelínek, Yelena Trofimova, Jan Janeček, Marie Feslová, Viktor Černý and Ivo Bukovsky	130	15
Targeting in All-Domain Operations: Choosing Between Cyber and Kinetic Action	Tim Grant and Harry Kantola	139	16
Computer Aided Diagnostics of Digital Evidence Tampering (CADDET)	Babak Habibnia, Pavel Gladyshev and Marco Simioni	149	17

Paper Title	Author(s)	Page No	Guide No
Weaknesses of IoT Devices in the Access Networks Used by People in Their Homes	Aarne Hummelholm	159	18
Cyber Security Analysis for Ships in Remote Pilotage Environment	Aarne Hummelholm, Jouni Pöyhönen, Tiina Kovanen and Martti Lehto	169	19
A Review of National Cyber Security Strategies (NCSS) Using the ENISA Evaluation Framework	Angela Jackson-Summers	178	20
Some Cybersecurity Governance Imperatives in Securing the Fourth Industrial Revolution	Victor Jaquire, Petrus Duvenage and Sebastian von Solms	187	21
Critical Infrastructure Protection: Employer Expectations for Cyber Security Education in Finland	Janne Jaurimaa, Karo Saharinen and Sampo Kotikoski	195	22
Digital Forensic Readiness Implementation in SDN: Issues and Challenges	Nickson Karie and Craig Valli	203	23
Cyber Wargaming on the Strategic/Political Level: Exploring Cyber Warfare in a Matrix Wargame	Thorsten Kodalle	212	24
Cyber-Threat Analysis in the Remote Pilotage System	Tiina Kovanen, Jouni Pöyhönen and Martti Lehto	221	25
Impact of AI Regulations on Cybersecurity Practitioners	Louise Leenen, Trishana Ramluckan and Brett van Niekerk	230	26
Is Hacking Back Ever Worth it?	Antoine Lemay and Sylvain Leblanc	239	27

Paper Title	Author(s)	Page No	Guide No
EU Digital Sovereignty: A Regulatory Power Searching for its Strategic Autonomy in the Digital Domain	Andrew Liaropoulos	246	28
Mandatory Cybersecurity Training for all Space Force Guardians	Banks Lin, Mark Reith and Wayne Henry	253	29
The Challenges to Cybersecurity Education in Developing Countries: A Case Study of Kosovo	Arianit Maraj, Cynthia Sutherland and William Butler	260	30
Studying the Challenges and Factors Encouraging Girls in Cybersecurity: A Case Study	Arianit Maraj, Cynthia Sutherland and William Butler	269	31
IoT Security and Forensics: A Case Study	Erik David Martin, Iain Sutherland and Joakim Kargaard	278	32
Cybersecurity and local Government: Imperative, Challenges and Priorities	Mmalerato Masombuka, Marthie Grobler and Petrus Duvenage	285	33
KSA for Digital Forensic First Responder: A job Analysis Approach	Ruhama Mohammed Zain, Zahri Yunos, Nur Farhana Hazwani, Lee Hwee Hsiung and Mustaffa Ahmad	294	34
The Unrehearsed Boom in Education Automation, Amid COVID-19 Flouts, a Potential Academic Integrity Cyber Risks (AICR)!	Fredrick Ochieng Omogah	303	35
How Penetration Testers View Themselves: A Qualitative Study	Olav Opedal	314	36

Paper Title	Author(s)	Page No	Guide No
Cyber Range: Preparing for Crisis or Something Just for Technical People?	Jani Päijänen, Karo Saharinen, Jarno Salonen, Tuomo Sipola, Jan Vykopal and Tero Kokkonen	322	37
Multiple-Extortion Ransomware: The Case for Active Cyber Threat Intelligence	Bryson Payne and Edward Mienie	331	38
Resilience Management Concept for Railways and Metro Cyber-Physical Systems	Jyri Rajamäki	337	39
Digital Evidence in Disciplinary Hearings: Perspectives From South Africa	Trishana Ramluckan, Brett van Niekerk and Harold Patrick	346	40
Security and Safety of Unmanned Air Vehicles: An Overview	Sérgio Ramos, Tiago Cruz and Paulo Simões	357	40
The Rising Power of Cyber Proxies	Janine Schmoldt	369	41
Connected, Continual Conflict: Towards a Cybernetic Model of Warfare	Keith Scott	375	42
Emergency Response Model as a Part of the Smart Society	Jussi Simola, Martti Lehto and Jyri Rajamäki	382	43
Joint All-Domain Command and Control and Information Warfare: A Conceptual Model of Warfighting	Joshua Sipper	392	44
Defensive Cyber Deception: A Game Theoretic Approach	Abderrahmane Sokri	401	45
Using Semantic-Web Technologies for Situation Assessments of Ethical Hacking High-Value Targets	Sanjana Suresh, Rachel Fisher, Radha Patole, Andrew Zeyher and Thomas Heverin	407	46

Paper Title	Author(s)	Page No	Guide No
Educating the Examiner: Digital Forensics in an IoT and Embedded Environment	Iain Sutherland, Huw Read and Konstantinos Xynos	416	47
Interdependence of Internal and External Security	Ilkka Tikanmäki and Harri Ruoslahti	425	48
The Host Nation Support for the International Cyber Operations	Maija Turunen	433	49
A GDPR Compliant SIEM Solution	Ana Vazão, Leonel Santos, Adaíl Oliveira and Carlos Rabadão	440	50
The Threat of Juice Jacking	Namosha Veerasamy	449	51
Status Detector for Fuzzing-Based Vulnerability Mining of IEC 61850 Protocol	Gábor Visky, Arturs Lavrenovs and Olaf Maennel	454	52
Mobile Phone Surveillance: An Overview of Privacy and Security Legal Risks	Murdoch Watney	462	53
PHD Papers		471	55
The Impact of GDPR Infringement Fines on the Market Value of Firms	Adrian Ford, Ameer Al-Nemrat, Seyed Ali Ghorashi and Julia Davidson	473	57
Side Channel Attacks and Mitigations 2015-2020: A Taxonomy of Published Work	Andrew Johnson	482	58
Sanctions and Cyberspace: The Case of the EU's Cyber Sanctions Regime	Eleni Kapsokoli	492	59
How the Civilian Sector in Sweden Perceive Threats From Offensive Cyberspace Operations	Joakim Kävrestad and Gazmend Huskaj	499	60

Paper Title	Author(s)	Page No	Guide No
Aviation Sector Computer Security Incident Response Teams: Guidelines and Best Practice	Faith Lekota and Marijke Coetzee	507	61
Biocyberwarfare and Crime: A Juncture of Rethought	Xavier-Lewis Palmer, Ernestine Powell and Lucas Potter	517	62
Matters of Biocybersecurity With Consideration to Propaganda Outlets and Biological Agents	Xavier-Lewis Palmer, Ernestine Powell and Lucas Potter	525	63
Bio-Cyber Operations Inspired by the Human Immune System	Seyedali Pourmoafi and Stilianos Vidalis	534	64
Space Cyber Threats and Need for Enhanced Resilience of Space Assets	Jakub Pražák	542	64
e-Health as a Target in Cyberwar: Expecting the Worst	Samuel Wairimu	549	65
Talos: A Prototype Intrusion Detection and Prevention System for Profiling Ransomware Behaviour	Ashley Charles Wood, Thaddeus Eze and Lee Speakman	558	66
Masters Research Papers		569	67
The use of Neural Networks to Classify Malware Families	Theodore Drewes and Joel Coffman	571	69
Employing Machine Learning Paradigms for Detecting DNS Tunnelling	Jitesh Miglani and Christina Thorpe	580	69
Analysis of API Driven Application to Detect Smishing Attacks	Pranav Phadke and Christina Thorpe	588	70

Paper Title	Author(s)	Page No	Guide No
Evolving Satellite Control Challenges: The Arrival of Mega-Constellations and Potential Complications for Operational Cybersecurity	Carl Poole, Mark Reith and Robert Bettinger	597	71
Work In Progress Papers		603	73
Inter-Process CFI for Peer/Reciprocal Monitoring in RISC-V-Based Binaries	Toyosi Oyinloye, Lee Speakman and Thaddeus Eze	605	75
Use of Blockchain Technologies Within the Creative Industry to Combat Fraud in the Production and (Re)Sale of Collectibles	Alexander Pfeiffer, Stephen Bezzina and Thomas Wernbacher[1]	611	76
Peer2Peer Communication via Testnet Systems of Blockchain Networks: A new Playground for Cyberterrorists?	Alexander Pfeiffer, Thomas Wernbacher and Stephen Bezzina	615	77
Ethics of Cybersecurity in Digital Healthcare and Well-Being of Elderly at Home	Jyri Rajamäki	619	78
ECHO Federated Cyber Range as a Tool for Validating SHAPES Services	Jyri Rajamäki and Harri Ruoslahti	623	79
Abstracts Only			81
Establishing Real-Time Security for Levels 1 and 0 in SCADA Networks	Mark Baggett		83
Situational Awareness Dark Web	Micki Boland		84
Are Endpoint Users Willing to Secure Themselves? A Cyber-Physical Comparison	Jan Kleiner		84

Paper Title	Author(s)	Page No	Guide No
ICT Uses in Peace and War	Brett van Niekerk		85
Defund the Police, Domestic Terrorism and Information Warfare: An Anticipatory Ethical Analysis	Richard Wilson		**86**
Media Ecology, Twitter and Information Warfare: Ethical and Anticipated ethical issues	Richard Wilson		**87**
QAnon, Social Media Warfare, and Conspiracy Theories: An Ethical and Anticipatory Ethical Analysis	Richard Wilson		89
'Soft' Warfare, State Sponsored Information Deception, and Social Media: Ethical and Anticipated Ethical Issues	Richard Wilson		**90**
White Rage, Information Warfare and Bodily Performance: Ethical and Anticipated Ethical Issues	Richard Wilson		**91**
Additional Materials			**93**
Participant List			**95**
Google Scholar	The Importance of Paper citations and Google Scholar		**101**
About ACI			**103**

Preface

These proceedings represent the work of contributors to the 20th European Conference on Cyber Warfare and Security (ECCWS 2021), supported by University of Chester, UK on 24-25 June 2021. The Conference Co-chairs are Dr Thaddeus Eze University of Chester and Dr Lee Speakman, University of Salford and the Programme Chair is Dr Cyril Onwubiko from IEEE and Director, Cyber Security Intelligence at Research Series Limited.

ECCWS is a well-established event on the academic research calendar and now in its 20th year the key aim remains the opportunity for participants to share ideas and meet. The conference was due to be held at University of Chester, UK, but due to the global Covid-19 pandemic it was moved online to be held as a virtual event. The scope of papers will 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 *Detective Inspector David Turner, and Detective Constable Michael Roberts* on the topic of *Policing the UK Cyber Space*. There will be a second keynote at 12:45 on Thursday presented by: Detective Constable Will Farrell, and Police Constable Phil Byrom on CyberChoices – Helping young people choose the right and legal path. The second day of the conference will open with an address by of the *Keith Terrill, and Louisa Murphy* speaking on *Current Cyber Crime Patterns and Trends - Covering the Traditional and Dark Webs*.

With an initial submission of 116 abstracts, after the double blind, peer review process there are 54 Academic research papers, 11 PhD research papers, 4 Masters research paper and 5 work-in-progress papers published in these Conference Proceedings. These papers represent research from Australia, Austria, Canada, China, Czech Republic, Estonia, Finland, Germany, Greece, India, Ireland, KENYA, Kosovo, Malaysia, Netherlands, Norway, Pakistan, Portugal, Romania, South Africa, Sweden, UK and USA.

We hope you enjoy the conference.

Dr Thaddeus Eze
University of Chester
UK
June 2021

ECCWS Conference Committee

Dr. Mohd Faizal Abdollah, University Technical Malaysia Melaka, Malaysia; Dr William ("Joe") Adams, Univ of Michigan/Merit Network, USA; Dr. Tariq Ahamad, Prince Sattam Bin Abdulaziz University, Saudi Arabia; 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; Faculty John Anohar, Full time academic, Higher Education dept; Dr. Leigh Armistead, Edith Cowan University, Australia; Johnnes Arreymbi, University of East London, UK; Dr. Hayretdin Bahsi, Tallinn University of Technology, Estonia; Prof Jorge Barbosa, Full time academic, Coimbra Polytechnic - ISEC; Dr. Darya Bazarkina, Sholokhov Moscow State Humanitarian University, Russia; Mr Robert Bird, Coventry University, UK; Prof. Matt Bishop, University of California at Davis, USA; Dr Radomir Bolgov, Saint Petersburg State University, Russia; Dr. Svet Braynov, University of Illinois at Springfield, USA; Prof. Larisa Breton, FullCircle Communications, LLC, USA; Dr Jim Chen, DoD National Defense University, USA; Dr Sabarathinam Chockalingam, , Institute for Energy Technology,; Bruce Christianson, University of Hertfordshire, UK; 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; Geoffrey Darnton, Bournemouth University, UK; Josef Demergis, University of Macedonia, Greece; Prof Patricio Domingues, Full time academic, Polytechnic Institute of Leiria; 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; Prof. Dr. Alptekin Erkollar, ETCOP, Austria; Dr Thaddeus Eze, University of Chester, UK; John Fawcett, University of Cambridge, UK; Prof. Eric Filiol, ENSIBS, Vannes, France & CNAM, Paris, France; Dr. Chris Flaherty, University of New South Wales, Australia; Prof. Steve Furnell, University of Nottingham, UK; Mr. Tushar Gokhale, Hewlett Packard Enterprise, USA; Dr. Michael Grimaila, Air Force Institute of Technology, USA; Prof. Stefanos Gritzalis, University of the Aegean, Greece; Dr. Mils Hills, Northampton Business School, Uk; Dr Ulrike Hugl, University of Innsbruck, Austria; Aki Huhtinen, National Defence College, Finland; Bill Hutchinson, Edith Cowan University, Australia; Dr. Abhaya Induruwa, Canterbury Christ Church University, UK; Hamid Jahankhani, University of East London, UK; Nor Badrul Anuar Jumaat, University of Malaya, Malaysia; Maria Karyda, University of the Aegean, Greece; Ass. Prof. Vasilis Katos , Democritus University of Thrace, Greece; Dr. Anthony Keane, Technological University Dublin, Ireland; Jyri Kivimaa, Cooperative Cyber Defence and Centre of Excellence, Tallinn, Estonia; Prof. Ahmet Koltuksuz, Yasar University, Dept. of Comp. Eng, Turkey; Dr Maximiliano Korstanje, Full time academic, University of Palermo, Buenos Aires, Argentina; Prashant Krishnamurthy,

University of Pittsburgh, USA; Mr. Peter Kunz, DoctorBox, Germany; Takakazu Kurokawa, National Defence Acadamy, Japan; Rauno Kuusisto, Finnish Defence Force, Finland; Martti Lehto, National Defence University, Finland; Mr Trupil Limbasiya, NIIT University, Neemrana, Rajasthan, India; Dr Efstratios Livanis, University of Macedonia, Greece; Dr Leandros Maglaras, Full time academic, De Montfort University; James Malcolm, University of Hertfordshire, UK; Dr Mary Manjikian, Regent University, USA; Dr Arianit Maraj, Lecturer, AAB College-Faculty of Computer Sciences; Mario Marques Freire, University of Beira Interior, Covilhã, Portugal; Ioannis Mavridis , University of Macedonia, Greece; Rob McCusker, Teeside University, Middlesborough, UK; Dr Imran Memon, zhejiang university, china; Dr Shahzad Memon, University of Sindh, Pakistan; Jean-Pierre Molton Michel, Ministry of Agriculture, Haiti; Dr. Yonathan Mizrachi, University of Haifa, Israel; Dr Pardis Moslemzadeh Tehrani, University of Malaya, Malaysia; Evangelos Moustakas, Middlesex University, London, UK; Antonio Muñoz, University of Málaga , Spain; Daniel Ng, C-PISA/HTCIA, China; Dr. Funminiyi Olajide, Nottingham Trent University, UK; Dr Cyril Onwubiko, Cyber Security Intelligence at Research Series Limited,, UK; Rain Ottis, Tallinn University of Technology, Estonia; Dr Mahmut Ozcan, Webster University, USA; Prof Teresa Pereira, Instituto Politécnico de Viana do Castelo, Portugal; Michael Pilgermann, University of Glamorgan, UK; Dr Bernardi Pranggono, Sheffield Hallam University, UK; Prof Carlos Rabadão, Politechnic of Leiria, Portugal; Dr. Muttukrishnan Rajarajan, City University London, UK; Prof Saripalli Ramanamurthy, Pragati Engineering College, India; Dr Trishana Ramluckan, University of KwaZulu-Nata, South Africa; Dr Aunshul Rege, Temple University, United States; 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, Full time academic, Polytechnic of Leiria; Dr Keith Scott, De Montfort University, UK; Prof. Dr. Richard Sethmann, University of Applied Sciences Bremen, Germany; Dr. Yilun Shang, Northumbria University, UK; Prof. Paulo Simoes, University of Coimbra, Portugal; Dr Umesh Kumar Singh, Vikram University, Ujjain, India; Prof. Jill Slay, University of South Australia, Australia; Dr Lee Speakman, University of Chester, UK; Dr Joseph Spring, University of Hertfordshire, UK; 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; Prof Tuna USLU, Istanbul Gedik University, Occupational Health and Safety Program, Türkiye; Craig Valli, Edith Cowan UniversitY, Australia; Dr Brett van Niekerk, University of KwaZulu-Natal & Transnet, South Africa; Richard Vaughan, General Dynamics UK Ltd, UK; Dr Namosha Veerasamy, Council for Scientific and Industrial Research, South Africa; Dr Sangapu Venkata Appaji, KKR & KSR Institute of Technology and Sciences, India; Stilianos

Vidalis, School of Computer Science, University of Hertfordshire, UK; Dr. Natarajan Vijayarangan, Tata Consultancy Services Ltd, India; Dr Khan Ferdous Wahid, Airbus Group, Germany; Dr. Santoso Wibowo, Central Queensland University, Australia; Prof. Trish Williams, Flinders University, Australia; Prof Richard Wilson, Towson University, USA; Simos Xenitellis, Royal Holloway University, London, UK.

Biographies

Conference and Programme Chairs

Dr Thaddeus Eze is a Senior Lecturer in Cyber Security at the University of Chester. He is the founder and convener of the IEEE UK & Ireland YP Postgraduate STEM Research Symposium, Vice Chair, IEEE UK & Ireland Young Professionals, a technical committee member for a number of international conferences (e.g., ICAS, CYBERWORLDS, EMERGING etc.), and currently runs the Computer Science departmental research seminar series. His research interests include Trustworthy Autonomics, MANET and Cyber Security (specifically, Return Oriented Programming, Policing the Cyber Threat and Cyber Education) and he has a number of publications in these areas.

Dr Lee Speakman is a Senior Lecturer and Programme Lead for Cybersecurity at the University of Chester. Lee has worked in Defence since 1999. He has gained experience in Intelligence, Strategy, Electronic Warfare, Communications, and Networking. He gained his PhD in MANETs from Niigata University, Japan, in 2009, and returned to Defence to work in Cyber and Information Security, and related areas. He joined the University of Chester in 2015 as the Programme Leader to develop and deliver Cybersecurity courses. His research interests are in software and system security.

Dr Cyril Onwubiko is the Secretary, IEEE UK & Ireland, Chair, IEEE UK & Ireland Blockchain Group, and Director, Cyber Security Intelligence at Research Series Limited, where he is responsible for directing strategy, IA governance and cyber security. Prior to Research Series, he had worked in the Financial Services, Telecommunication, Health sector and Government and Public services Sectors. He is a leading scholar in Cyber Situational Awareness (Cyber SA), Cyber Security, Security Information and Event Management (SIEM), Data Fusion & SOC; and interests in Blockchain and Machine Learning. He is the founder of the Centre for Multidisciplinary Research, Innovation & Collaboration (C-MRiC) https://www.c-mric.com. Detailed profile for Cyril can be found on https://www.c-mric.com/cyril

Keynote Speakers

Phil Byrom is a Merseyside Police Officer with 19 years' service. Phil is currently seconded to the North West Regional Organised Crime Unit as a Cyber Crime Prevent Officer and is responsible for delivering cybercrime prevention work across 6 North West Police forces. He also works to identify individuals who are on the verge of moving into cybercrime or have committed low level cybercrime and prevent them from either moving into cybercrime or divert them onto positive pathways and use their computer skills in more positive ways.

Will Farrell is a Police Detective with 12 years' experience, currently working with Cyber Crime Prevent at the North West Regional Organised Crime Unit in the UK. Will is responsible for delivery cybercrime prevention work across the 6 police forces in North West England. Will works to identify individuals on the cusp of committing cybercrime, and once identified, Will seeks to deter and divert them towards more positive pathways. Before joining the police, Will spent fourteen years in the commercial radio industry, managing the programme output of five radio stations. He was also a successful radio DJ for many popular radio stations.

Louisa Murphy is a Regional Cyber Protect Officer in the Cyber Crime Unit at the North West Regional Organised Crime Unit. (A collaboration of 6 local police forces). As part of a national policing network, her role focusses on making the North West a safer place online. She links directly to both the National Cyber Security Centre (NCSC) and Action Fraud to obtain the latest cybercrime information and will help organisations to stay on top of the latest cyber security information. Louisa works with the different sectors promoting and encouraging cyber resilience within their organisations. She speaks at conferences and business events to raise awareness of current cyber threats and national advice and best practice so that businesses and individuals can best protect themselves and their information and assets. She also works with victims to understand how they were targeted and to help them become more cyber secure.

Keith Terrill is a Regional Cyber Protect Officer in the North West Regional Cyber Crime Unit. They're responsible for delivering the Protect strand of UK Cyber Policing in the North West in conjunction with local forces, Action Fraud and the National Cyber Security Centre. The goal of this is to raise awareness of the latest cyber crime threats impacting businesses and individuals, and highlighting the

many practical steps that can be taken to improve cyber resilience. Outside of his role in the NWRCCU Keith has served as a Special Constable (volunteer Police Officer) in Response and Neighbourhood policing for nearly three years and previously worked as Programmer specialising in Networking.

Detective Inspector David Turner has over twenty years of experience in investigating serious, major and organised crime including counter terrorism. David Turner is presently responsible for managing the North West Regional Cyber Crime Unit to deliver against the Serious Organised Crime Strategy 2018 and National Cyber Security Strategy 2016 – 2021. Their role involves managing all the staff within the Regional Cyber Crime Team including the Regional Coordinator, the Regional Crime Cyber Unit 4P capability as well as the Dark Web and Digital Forensics Team. They have oversight of all investigations in the RCCU along with Protect, Prevent and Prepare activity ensuring collaboration across a range of sectors from law enforcement overseas to third sector organisations in the UK.

Mini Track Chairs

Dr. Sangapu Venkata Appaji is working as a Professor, at KKR and KSR Institute of Technology and Sciences, Guntur, India. He completed his doctorate in Computer science and Engineering in the area of Cryptography and Network Security from Jawaharlal Nehru Technological University Hyderabad, INDIA. He has more than 10 years of teaching experience in Computer Science and engineering and Information Technology department for graduate and post graduate students. He supervised IOT, Security related projects for graduate and postgraduate students.

Dr. Shahzad Memon is working as a Professor, at department of Electronics, 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 and Cyber Physical systems security. He also granted funding for research from Higher Education commission and ICT Research and Development, Ministry of Information Technology, Pakistan..

Dr Brett van Niekerk is a senior lecturer in computer science at the University of KwaZulu-Natal. 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.

Dr Trishana Ramluckan is a Postdoctoral Researcher in the School of Law and an Adjunct Lecturer in the Graduate School of Business at the University of KwaZulu-Natal. 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.

Workshop Facilitator

Dr Edwin "Leigh" Armistead is the President of Peregrine Technical Solutions, a certified 8(a) small business that specializes in Cyber Security. A retired United States Naval Officer, he 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

Kari Alenius is Professor in General History and Head of Department at the University of Oulu (Finland). He also worked as a Visiting Professor at Lakehead University, Canada, in 2019–2020. He has specialized on the history of Eastern Europe, history of ethnic relations, and history of information warfare.

Mark Baggett Vice President, Industrial Control Systems (ICS), Mission Secure, Mark's an industry veteran and ICS expert. He's designed, engineered, and implemented control systems internationally for energy's most prominent players. Mark leverages his expertise to help operations assess and mitigate cyber risks and implement a secure architecture, managing OT cybersecurity projects for rigs, refineries, pipelines, manufacturing plants, and chemical facilities.

Johnny Bengtsson is a forensic expert in hardware forensics at Swedish National Forensic Centre (NFC), and part-time industrial PhD student in IoT forensics at Linköping University, Sweden. He holds a Master of Science degree in Electrical Engineering from Linköping University, and also a University Diploma in Chemical Engineering from Chalmers University of Technology, Sweden.

George-Daniel Bobric is a PhD candidate within the "Carol I" National Defence University, Romania. His main areas of interest are mathematical and computer sciences, cyber security and information warfare.

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

Long Chen is currently pursuing the Ph.D. degree with the Beihang University, under the supervision of Prof. C. Xia. He has participated in several National Natural Science Foundations and other research projects as a Director and Contributor. His research interests include Network and Information Security, Intrusion Detection Technology.

Dr. Jim Q. Chen, Ph.D: Professor of Cyber Studies, College of Information and Cyberspace (U.S. National Defense University) Expertise in cyber warfare, cyber deterrence, cyber strategy, cybersecurity technology, artificial intelligence, and machine learning. Authored and published numerous peer-reviewed papers, articles, and book chapters on these topics. Has also been teaching graduate

courses on these topics. A recognized expert in cyber studies and artificial intelligence.

Dr. Sabarathinam Chockalingam is a Research Scientist 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 and serious games.

Joel Coffman is an Associate Professor in the Department of Computer and Cyber Sciences at the US Air Force Academy. He received his BS in computer science from Furman University, and his MS and PhD in computer science from the University of Virginia. Joel's research interests include automated software diversity, cloud security, and keyword search in databases.

2d Lieutenant **Tristan Creek** is completing his Masters degree in Cyber Operations at the Air Force Institute of Technology, Wright-Patterson AFB, OH, USA. Research interests include covert communication channels, long range WiFi exploitation, and Bluetooth Low Energy exploitation.

Tiago Cruz: Ph.D. degree in informatics engineering (University of Coimbra, 2012), where he has been an Auxiliary Professor with the Department of Informatics Engineering, since 2013. Research interests cover 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.

Theodore Drewes is a senior at the United States Air Force Academy with a major in computer science. He plans on graduating in May 2021 and continue his career as a RPA pilot. While at the Academy, he took an interest in Artificial Intelligence, malware development, and computer graphics.

Jaco Du Toit is a lecturer at the Academy of Computer Science and Software Engineering at the University of Johannesburg. His areas of research include Cyber Security, with a focus on privacy and mobile operating environments. A specific interest to him is research in increasing the protection of private information using decentralised data and access control models.

Dr. Jan Fesl obtained his Ph.D. diploma in 2018 at Czech Technical University in Prague. His areas of research are computer networks, distributed systems, cyber-

security. Dr. Fesl is the leader of the Networking research group from the Faculty of Information Technology at Czech Technical University in Prague.

Adrian Ford is an information technology manager with over 25 years' experience and a doctoral research student of information security at the University of East London. He holds an MBA from Lancaster University Management School (2009), professional membership of the British Computer Society (MBCS) and is a Freeman of the Worshipful Company of Information Technologists.

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 and on Command & Control and Emergency Management systems. More details can be found at https://www.linkedin.com/in/tim-grant-r-bar/.

Dr Babak Habibnia PhD in Computer Science with a specialization in Digital Forensics and Cybercrime Investigation. His academic research focuses on redesigning digital forensics as a computer-assisted human activity. Dr Babak Habibnia presents for the first time a new scientific semi-automated approach based on visualization of relevant data properties to help investigators detect digital evidence tampering and anomaly.

Dr. 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.

Angela G. Jackson-Summers is an Assistant Professor of Information Systems in the Management Department at the U. S. Coast Guard Academy. She received her Ph.D. in Business Administration (Information Systems) from Kennesaw State University. Her research interests include IT/IS risk management, and data/information security and assurance.

Dr Victor J Jaquire has been within the field of cyber security for over 20 years within Government and the Private sector. He holds an Honours Degree in Management from Henley University and a Master's and PhD in Informatics from the University of Johannesburg. He has published various academic papers on cyber strategies and cyber counterintelligence maturity.

Andrew Johnson is a 3rd year PhD student within the Cyber Security Department of the University of South Wales, UK. His research field is predominantly in the modelling of Side Channel Attacks. Andrew continued his research study at the University after completing his MSc in Computer Systems Security in 2018. He has previously published two conference papers with the IEEE during his PhD study.

Thorsten Kodalle LTC (General Staff) lectures on security policy at the Command and Staff College of the German Armed Forces with a particular focus on NATO, Critical Infrastructure and Cyber. He is a member of the NATO research task group "Gamification of Cyber Defense/Resilience", an experienced facilitator of manual wargaming on the operational level for courses of action analysis, for operational analysis, operations research, serious gaming and especially for matrix wargaming."

Eleni Kapsokoli is a Ph.D. candidate at the University of Piraeus, Department of International and European Studies, Greece and Ph.D. Fellow of the European Doctoral School. She holds a bachelor's degree in Political Science and Public Administration and a master's degree in International Relations and Strategic Studies. Her main research interests are international security, terrorism, cybersecurity and cyberterrorism.

Nickson M. Karie received his PhD degree in computer science from the University of Pretoria, South Africa. Currently, he is a cybersecurity research fellow at Edith Cowan University, Perth, Australia. He has over 10 years of experience in academic teaching, research, and consultancy. His research interests include network security and forensics, intrusion detection and prevention, cloud and IoT security

Joakim Kävrestad is a doctoral student, at the University of Skövde, focusing on human aspects of cybersecurity. He is a prior forensic expert who is coordinating a master's program in Privacy, Information and Cybersecurity and teaching classes in digital forensics and technical cybersecurity.

Jan Kleiner is a PhD student of Political Science at Masaryk University in the Czech Republic. He focuses primarily on cybersecurity, the relationship between a state and citizens in cyberspace (e.g., how states secure their citizens in cyberspace), and propaganda and information warfare. He mainly employs quantitative (statistical) and mixed methods research designs.

MSc. Tiina Kovanen, MSc Tiina Kovanen is a PhD student at the university of Jyväskylä. She is interested in various cyber security topics for different cyber-physical systems. Currently she is working towards her degree by studying

possibilities and challenges related to ships remote pilotage environment, ePilotage.

Dr. Sylvain (Sly) Leblanc is a Professor in Computer Engineering at the Royal Military College of Canada, also serving as Chair for Cybersecurity and Primary Investigator of the Computer Security Laboratory. His research interests are in the Cyber Security of Vehicular Systems, Network Counter-Surveillance Operations, Vulnerability & Security Assessments and Cyber Education.

Louise Leenen's areas of specialisation are Artificial Intelligence applications in cybersecurity and mathematical modelling. She is currently an Associate Professor in the Computer Science Department at the University of the Western Cape in South Africa and a member of the Centre for Artificial Intelligence (CAIR).

Faith Lekota is an Independent IT Consultant. She is a PhD candidate at the University of Johannsesburg. Her research interest include cybersecurity frameworks, and information security best practise standards.

Dr. Andrew N. Liaropoulos is Assistant Professor in University of Piraeus, Department of International and European Studies, Greece. He is also a senior analyst in the Research Institute for European and American Studies (RIEAS) and a member of the editorial board of the Journal of European and American Intelligence Studies (JEAIS).

Capt Banks Lin, USAF (BS, San Jose State University) previously served as cybersecurity test lead at the Air Force Operational Test & Evaluation Center, conducting operational-realistic cyber assessments on space and missile weapon systems. He is currently a student at Air Force Institute of Technology studying for a Master of Science in Cyber Operations.

Christoph Lipps, M.Sc. graduated in Electrical and Computer Engineering at the University of Kaiserslautern where he meanwhile lectures as well. He is a Researcher and Ph.D. candidate at the German Research Center for Artificial Intelligence (DFKI) in Kaiserslautern. His research focuses on Physical Layer Security (PhySec), Physically Unclonable Functions (PUFs), Artificial Intelligence (AI), entity authentication and all aspects of network and cyber security.

Dr. Arianit Maraj, is a professor of Engineering Informatics and is also in Telecom of Kosovo. He received PhD from Polytechnic University of Tirana, in 2013. His research interest lay in Data security, Wireless communications and Ad-Hoc

networking. He has published a considerable number of scientific papers on international journals and conferences.

Erik David Martin BSc is currently working as an Infrastructure and Security Engineer at Sopra Steria in Stavanger, Norway. He has submitted several entries in the Exploit Database and has been active in the security research community throughout the last years. He has also published a series of articles regarding IoT and SCADA security. His research interests lie in the area of computer security and computer forensics.

Dr. Edward Mienie is the Executive Director of the Strategic & Security Studies program at the University of North Georgia. In addition, as associate professor he teaches national intelligence courses within his degree program. He has most recently helped introduce national intelligence education as an elective course to Georgia high schools, one of the first in the nation.

Jitesh Miglani B. Tech, M.Sc. graduated with a B.Tech in Computer Science Engineering from The NorthCap University, India in 2017 and a MSc in Applied Cyber Security from Technological University Dublin. He is currently working as a cyber security consultant in Deloitte Ireland.

Masombuka Mmalerato is cybersecurity specialist and currently working on her PhD with the main focus on Artificial Intelligence and cybersecurity. She has co-authored and peer-reviewed several articles on these disciplines. Her other research interests include blockchain, quantum computing and data analytics.

Haya Yusuf Mohamed Gulf Air Company, and MBA Student. College of Business and Finance, Ahlia University, Manama, Bahrain

Fredrick Ochieng' Omogah is a lecturer of I.T & Medical Informatics at Uzima University, Kenya. He is currently finalising Msc. I.T Security and Audit from Jaramogi Oginga Odinga University, Kenya. Received Bachelor of I.T from Australia, 2009. His main research areas are in I.T and cyber security in electronic healthcare

Dr Olav Opedal is an independent psychologist and data scientist in Ellensburg, WA, US. He received his PhD in General Psychology from Capella University in 2019. His main research areas are personality and behavior associated with computer use, and the applied use of big data analytics, machine learning and AI as an independent ML/AI practitioner.

Jani Päijänen (B.Eng) works as a Project Manager at the Institute of Information Technology of JAMK University of Applied Sciences. He has experience from delivering consultancy for clients in Project Management, Information Technology, and Software Development. Jani is currently doing his M.Eng in Cyber Security.

Dr. Bryson Payne is a nationally-recognized cyber coach, author, TEDx speaker, and the founding Director of the Center for Cyber Operations Education at the University of North Georgia, an NSA-DHS Center for Academic Excellence in Cyber Defense. He has coached programming and cyber competition teams at UNG since 2005, including UNG's #1 in the nation NSA Codebreaker Challenge 2019 and 2020 cyber operations teams.

Alexander Pfeiffer: recipient of a Max Kade Fellowship awarded by the Austrian Academy of Science to work at the Massachusetts Institute of Technology (MIT), Department for Comparative Media Studies / Writing in 2019 and 2020. In 2021 he returned to Donau-Universität Krems. Currently approaching his second PhD at the department of AI at the University of Malta. https://www.alexpfeiffer.at

Pranav Phadke, B.Sc, M.Sc. Pranav Phadke graduated with a B.Sc. in Information Technology and Masters In Computer Application from the University of Mumbai in 2015 and an M.Sc in Applied Cyber Security in 2019 from the Technological University of Dublin. He is currently working as a Software Engineer with a firm based in Dublin.

Captain Carl Poole received a master's degree in space systems with specialties in space vehicle design and space control modelling and simulation from the Air Force Institute of Technology March 2021. His research topics include the examination of space-based ballistic missile defense architectures for employed kinetic weapon concepts.

Lucas Potter is a Biomedical Engineering PhD Student and member of the SAMPE (Systems Analysis of Metabolic Physiology) Lab at Old Dominion University. His doctoral research is focused on cellular respiration in those with compromised metabolism. Past research endeavors include human factors research, specifically human factors analysis of performance in virtual reality, modeling of physiology, and materials engineering.

Seyedali Pourmoafi I have spent most of my time learning and build up my knowledge around Computer Science subject ever since I lay hands on my first self-build computer at my early childhood self-studying desire and researching on the internet led me to learn very fast in childhood. I am extremely curious about

Astronomy and Computer science. I decided to study Mathematics in high school and Computer Science at the university. I had my first degree in Computer Science software engineering before I moved to the UK. Then I decided to start with an Undergraduate degree and choosing an entirely new degree and specialism which leads to being graduated in information technology with a Web specialism degree. Then after having a short discussion with a member of the faculty, I decided to follow the new direction by choosing M.Sc. in networking, now I am finishing up my Ph.D. study in Cybersecurity.

Jakub Pražák is a Ph.D. candidate of International Relations at the Charles University's Faculty of Social Studies and a project assistant at the Prague Security Studies Institute. His main research areas are weaponization of outer space and dual-use technology.

Carlos Rabadão is Coordinator Professor at Polytechnic Institute of Leiria. He received his PhD degree in Computer Engineering from University of Coimbra in 2007. He has published more than 50 papers at conference proceedings and refereed journals. His major research interests include Cybersecurity, Information Security Management Systems and Intrusion Detection Systems for IoT.

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 Helsinki University of Technology, and a PhD in mathematical information technology from University of Jyväskylä.

Dr Trishana Ramluckan is the group research manager for Educor Holdings. In 2020 she completed post- doctoral research in International Cyber Law at the School of Law, UKZN. Her areas of research include the intersections of IT with law and governance. She is a member of the IFIP working group on ICT Uses in Peace and War and is an Academic Advocate for ISACA.

Dr Harri Ruoslahti is a Senior lecturer of Security and risk management at Laurea University of Applied Sciences, a researcher in related projects, and Laurea's point of contact in ECHO (the European network of Cybersecurity centres and competence Hub for innovation and Operations).

Karo Saharinen (M.Eng) is working as a Senior Lecturer in IT and handling the responsibility of degree programme coordinator of the master's degree programme in IT, Cyber Security at JAMK University of Applied Sciences. He is currently working on his PhD related to Cyber Security Education.

Leonel Santos is Assistant Professor at Polytechnic Institute of Leiria. He received his PhD degree in Computer Science from University of Trás-os-Montes e Alto Douro in 2020 and is a researcher at Computer Science and Communication Research Centre. His major research interests include Cybersecurity, Information and Networks Security, IoT, Intrusion Detection Systems and Computer Forensics.

Janine Schmoldt studied International Relations at the University of Erfurt, Germany. Afterwards, she completed her Master at the Vrije Universiteit Amsterdam where she studied Law and Politics of International Security. She is currently a PhD student at the University of Erfurt.

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.

Jussi Simola is a doctoral candidate of cyber security at University of Jyväskylä. He received his master degree in Information Systems from the Laurea University of Applied Sciences in 2015. He has worked as a cybersecurity specialist and he has participated in the development of a common Early Warning System for the EU member countries.

Dr. Joshua Alton Sipper is a Professor of Cyberwarfare Studies at the Air Force Cyber College. He completed his Doctoral work at Trident University in September of 2012, earning a Ph.D. in Educational Leadership (emphasis, E-Learning Leadership). Dr. Sipper's research interests include cyber ISR, policy, strategy, and warfare.

Abderrahmane Sokri has a Ph.D. in administration from HEC-Montreal. He is currently serving as economist for the Canadian Department of National Defence. His current research interest includes game theory applied to military operations. He has published in good international journals such as the European Journal of Operational Research.

Sanjana Suresh is a freshman at the LeBow College of Business within Drexel University, majoring in Finance and Business Analytics. She is actively involved in a variety of activities at Drexel, including Drexel's Undergraduate Student Government Association, Drexel Women in Business, and Undergraduate Research. In her free time, Sanjana enjoys spending time with her friends and family, reading, writing, and playing lacrosse.

Professor Iain Sutherland BSc MSc PhD MBCS is currently Professor of Digital Forensics at Noroff University College in Kristiansand, Norway. He is a recognised expert in the area of computer forensics. He has authored articles ranging from forensics practice and procedure to network security. His current research interests lie in the areas of computer forensics and computer security.

Christina Thorpe, B.Sc, Ph.D. Christina Thorpe graduated with a B.Sc. (Hons) in Computer Science from University College Dublin in 2005 and a Ph.D. in Computer Science in 2011. She was a postdoctoral research fellow in the Performance Engineering Lab in UCD from 2011 - 2018. She is currently a Lecturer in Cyber Security in the Technological University Dublin.

Mr. Ilkka Tikanmäki is a researcher at Laurea University of Applied Sciences and a doctoral student of Operational art and tactics at the Finnish National Defence University. He holds an MBA degree in Information Systems and BSc degree in Information Technology.

Maija Turunen is a postgraduate student in military sciences at the Finnish National Defense University. Her main research areas consist of cyber warfare and Russia. Maija Turunen works as a legal counsel at the Finnish Transport Infrastructure Agency.

Brett van Niekerk is a senior lecturer at the University of KwaZulu-Natal. He serves as chair for the IFIP Working Group on ICT in Peace and War, and co-Editor-in-Chief of the International Journal of Cyber Warfare and Terrorism. He holds a PhD focusing on information operations and critical infrastructure protection.

Namosha Veerasamy: BSc: IT Computer Science Degree, BSc: Computer Science (Honours Degree), MSc: Computer Science with distinction (University of Pretoria) and a PhD (University of Johannesburg). Currently senior researcher (Council for Scientific and Industrial Research in, Pretoria). Qualified as a Certified Information System Security Professional and Certified Information Security Manager. Has been involved in cyber security research and governance for over 15 years.

Gábor Visky is a researcher at NATO CCDCOE, his main field of expertise is industrial control systems. Gábor's previous assignments include 15 years of designing hardware and software for embedded control systems and researching their vulnerabilities through reverse engineering. Gábor holds an MSc degree in Information Engineering with a specialty in Industrial Measurement.

Samuel Wairimu is a PhD student in Computer Science in the Department of Mathematics and Computer Science at Karlstad University, Sweden. He received his Master's in Cybersecurity from the University of Chester, UK in the year 2018. His main research areas are cybersecurity, cyberwarfare, information security and privacy, and security and privacy in e-Health.

Richard L. Wilson is a Professor of Philosophy at Towson University in Towson, MD. Teaching Ethics in the Philosophy and Computer and Information Sciences departments and Senior Research Fellow in the Hoffberger Center for Professional Ethics at the University of Baltimore. Professor Wilson specializes in Applied Ethics teaching a wide variety of Applied Ethics Classes.

Ashley Wood is a Visiting Lecturer and current PhD student at the University of Chester, with a First class BSc(Hons) degree in Cybersecurity and an MSc in Advanced Computer Science with Distinction. Ashley has keen interests in digital forensics, cybercrime investigation, systems/network security and malware analysis.

Keynote Outlines

xxx

Keynote Outlines

The following are outlines for the Keynote Speeches which will take place at ECCWS 2021.

Current Cyber Crime Patterns and Trends, and Staying Cyber Aware

Every year nearly 30,000 cyber crimes are reported to UK Law Enforcement with victims reporting financial losses in the millions. Raising awareness of cyber crime and cybersecurity issues amongst businesses and individuals, and encouraging the reporting of these crimes is therefore a critical element of Law Enforcement's efforts to combat cyber crime, a role fulfilled by the Cyber PROTECT Network.

In this session, Regional Cyber PROTECT Officers Louisa Murphy and Keith Terrill will be discussing current patterns and trends being seen in reports to police and during investigations of Computer Misuse offences, and some of the often simple steps businesses and individuals can take to significantly strengthen their cyber resilience.

What you will take away from this session:

- Identify common cyber crimes and how they're committed
- Understanding what makes businesses and individuals vulnerable to cyber crime
- How the Cyber PROTECT Network can help businesses protect themselves
- Reporting cyber crime to Law Enforcement

Cyber Choices – Helping Young People Choose the Right and Legal Path

The average age of arrest for all crime is 35 – for cybercrime it's just 17. Cybercrime prevention is a key part of the UK's National Cyber Security Strategy. In this session, DC Will Farrell and PC Phil Byrom will explain how police are preventing cybercrime from happening in the first place. Find out how individuals on the cusp of committing cybercrime are identified and how police help them make informed Cyber Choices, diverting individuals away from crime to do positive things with their computer skills instead.

- What you will take away from this session:
- Overview of types of cybercrime
- Understand what police are doing to Prevent cybercrime
- Identify common pathways into cybercrime
- Awareness of positive diversions for young people

Research Paper Abstracts

The PUF Commitment: Evaluating the Stability of SRAM-Cells

Pascal Ahr[1], Christoph Lipps[1] and Hans Dieter Schotten[1,2]

[1]German Research Center for Artificial Intelligence, Kaiserslautern, Germany

[2]University of Kaiserslautern, Division of Wireless Communication and Radio Positioning, Kaiserslautern, Germany

Pasacal.Ahr@dfki.de
Christoph.Lipps@dfki.de
Hans_Dieter.Schotten@dfki.de
DOI: 10.34190/ECW.21.031

Abstract: Static Random Access Memory (SRAM) based Physical Unclonable Functions (PUFs) are a dedicated sub-area of silicon PUFs in the research area of Physical Layer Security (PhySec). Due to their high Shannon Entropy, low energy consumption and availability they are particularly suitable for Industrial Internet of Things (IIoT) security applications. SRAMs are volatile memories, bistable systems which always adopt one of two values: zero or one. During the startup process - powering up the cells-, the cells take one of these states, the so called Startup-Value. This "hardware fingerprint" is depending due to physical features, fluctuations and deviation occurring during the manufacturing process of the semiconductors and the devices, and can thus be different at each restart. For a function in a mathematical meaning, and particularly for cryptographic applications, it is necessary that every element of the definition area is only mapped to one element of the codomain. For this purpose the startup-values of the SRAM have to be (mostly) stable for every restart. To verify the suitability, and appropriateness for cryptographic applications, the paper examines the stability of the startup-values; how often does the same but still individual bit-patterns occur and how many and which bits are flipping. To provide comparable results, 30 SRAMs are evaluated with 500 startup procedures each. For automated testing a Printed Circuit Board (PCB) is implemented, controlled by a Microcontroller Unit (MCU). In order to monitor the temperature and humidity –as external influencing factors of the startup behaviour- corresponding sensors are integrated as well. The evaluation provides a high resolution of the course of stability over the various measures, and thus enables a detailed analysis. As a part, the mapping of functions to data-points is done by using regression tools. Thereby it is not only possible to determine the stability in total, but the course over all restarts as well. The results of the work contribute to PUF research in general and prove the applicability of

SRAM-PUFs in IIoT and other application areas, especially for resource constrained devices, by evaluating and proofing the stability of SRAM cells.

Keywords: physical layer security, physically unclonable functions, SRAM-stability, industrial internet of things, cyber security

Asylum Seekers From Russia to Finland: A Hybrid Operation by Chance?

Kari Alenius

University of Oulu, Finland

kari.alenius@oulu.fi
DOI: 10.34190/EWS.21.069

Abstract: This paper analyses interpretations made of the arrival of asylum seekers through Russia to Finland in the period from November 2015 to March 2016. Prior to that time, there were almost no asylum seekers at all from Russia to Finland, and their arrival ended just as abruptly in the spring of 2016. The news published in Finland's leading media during the above-mentioned period has been reviewed for the purposes of the study. Even as it was happening, different interpretations of the nature of the issue were presented in the media. The topic is important in three ways. First, the activities of the Finnish media in connection with this small-scale crisis have hardly been studied at all. It is therefore now possible to make a basic analysis of how Finnish media reacted to the surprising situation that had arisen on the border between Russia and Finland. Second, if it was a hybrid warfare operation, what Russia achieved through it should be evaluated. Third, the analysis can be used to assess the likelihood of a strong influx of refugees into the European Union via Russia. It is very well known that Russia, like other great powers, is interested in increasing its influence abroad. Russia is also ready to use a variety of means to achieve its goals. In particular, the conquest of Crimea and the outbreak of war in eastern Ukraine in 2014 have shown that Russia does not shy away from aggressive operations that combine traditional military means with modern unconventional practices where necessary. However, it cannot be concluded that whenever Russia seems to be carrying out operations planned by state leadership, they really are such. Each case deserves a separate analysis.

Keywords: hybrid operations, asylum seekers, refugees, Finland, Russia

Antarctica and Cyber-Security: Useful Analogy or Exposing Limitations?

Shadi Alshdaifat[1], Brett van Niekerk[2] and Trishana Ramluckan[2,3]

[1]University of Sharjah, UAE
[2]University of KwaZulu-Natal, South Africa
[3]Educor Holdings, South Africa

salshdaift@sharjah.ac.ae
vanniekerkb@ukzn.ac.za
ramluckant@ukzn.ac.za
DOI: 10.34190/EWS.21.013

Abstract: Antarctica is the last discovered continent, and is designated as a protected area for scientific research and peace and military operations are banned. Its status is governed by the 1959 Antarctic Treaty and subsequent agreements. These treaties related to Antarctica are cited as an example or a possible model for a treaty or international law for cyberspace. However, research facilities in Antarctica have fallen victim to cyber-attacks, and due to the environmental conditions, cyberattacks could potentially be devastating for the researchers who are affected. These cyber-incidents raise questions of how the current proposed application of international law for cyberspace will apply to such an area. The paper will assess the applicability of the Antarctica treaties to cybersecurity from two perspectives. The first perspective will discuss the existing proposals of adopting the treaties as a model for cyberspace, and the second will consider hypothetical scenarios based on previous cyber-security incidents in order to assess if the current proposals of international law are sufficient. These two perspectives will be contrasted to investigate the viability of the Antarctica Treaty system as a model for international treaties on cyberspace.

Keywords: area protection, cyber-attack, cyber-security, international humanitarian law, international security

Evasion of Port Scan Detection in Zeek and Snort and its Mitigation

Graham Barbour, André McDonald and Nenekazi Mkuzangwe

Information and Cybersecurity Centre, Defence and Security Cluster, Council for Scientific and Industrial Research, Pretoria, South Africa

gbarbour@csir.co.za
amcdonald@csir.co.za
nmkuzangwe@csir.co.za
DOI: 10.34190/EWS.21.033

Abstract*:* East-west cyberattacks typically scan for open TCP ports on local network hosts in order to identify vulnerable services for subsequent exploitation. Since TCP port scans do not appear in legitimate network traffic, widely used intrusion detection systems such as Zeek and Snort include an option to search for these scans in background traffic, with the objective of alerting a network operator to potential threats. These port scan detectors are designed to trigger when the running count of rejected TCP connection attempts in a specified time interval exceeds a predetermined threshold (the rejection approach), and in the case of the Snort *sfportscan* pre-processor, when observing a dramatic increase in TCP connections over a relatively short period of time (the connection approach). In this paper, we present a novel algorithm for generating fast port scans that remain undetected by Zeek, thereby revealing a flaw that east-west cyberattacks may exploit. The differentiating factor of the new port scan algorithm is its rapid transmission of a spoofed TCP connection request to the network switch immediately after scanning each port. Port scans were conducted on a physical test network with an enterprise grade switch, where a network security testing and assessment appliance was used to generate background traffic from different application profiles. Experimental data is presented which demonstrates that (i) the novel scans remain undetected by Zeek for a scan rate of up to 1 million ports per second, and that (ii) neither Zeek nor Snort can detect the novel scans if the scan rate is reduced to 0.86 ports per minute or fewer. A strategy that combines the connection approach with a modified rejection approach for detecting the newly proposed fast port scans is proposed. It is concluded that this combined strategy holds potential for more reliable detection of port scans than the individual approaches. We envisage that the new port scan algorithm, the proposed detection strategy and the experimental findings would empower network security practitioners and designers of intrusion detection systems to address the shortcomings of existing detectors and improve detection strategies in general, thereby leading to more reliable detection of east-west cyberattacks.

Keywords*:* *e*ast-west cyberattack, port scan, TCP scan, packet spoofing, reconnaissance, intrusion detection, port scan detection, anomaly detection, Zeek, Snort

The Manifestation of Chinese Strategies Into Offensive Cyberspace Operations Targeting Sweden

Johnny Bengtsson[1,2] and Gazmend Huskaj[3,4]

[1]Swedish National Forensic Centre (NFC), Swedish Police Authority, Linköping, Sweden
[2]Linköping University, Sweden
[3]Swedish Defence University, Stockholm, Sweden
[4]University of Skövde, Sweden

johnny.bengtsson@polisen.se
gazmend.huskaj@fhs.se
DOI: 10.34190/EWS.21.066

Abstract: The aim of this article is to present how Chinese strategies are manifested into offensive cyberspace operations targeting Sweden. It is commonly known that People's Republic of China (PRC, and in this definition the meaning of the government and its military), uses five-year plans (FYP) for social and economic steering strategy of their country. This has been going on since 1953 until today. In 2015, the national strategic plan Made in China 2025 (中国制造2025) was launched by Le Keqiang, the Premier of the State Council of PRC. The main goal with this plan is to strengthen the economic development. In addition, Chinese military strategists noted the importance of information warfare and intelligence during military operations. This article is based on open sources: the official English translated version of the 13th Five-year plan (FYP) and other reporting on cyberspace operations linked to the PRC. A number of cases are presented to highlight the link between the PRC FYP and their targets. Next, the current situation in Sweden is presented and how the country is targeted by PRC-linked activities, both in and through cyberspace, but also military infiltration on academia. The results show that Sweden has been, and is continuously the target of offensive cyberspace operations. In parallel, the country is also the target of military infiltration on the academia, and direct investment strategies such as Huawei attempting to compete for the 5G frequency actions arranged by the Swedish Post and Telecom Authority. In conclusion, Sweden will continue to experience cyberespionage from PRC on all levels and on all domains; science, technology, IP and privacy information theft. Previously unveiled cyberspace operations cases in

this article have proven to be a convenient strategy for the PRC to reduce its research and development gap in several ways; innovatively, financially and to shortening the time-to-market (TTM).

Keywords: Chinese strategies, cyberespionage, information warfare, offensive cyberspace operations, Sweden

The Evolution of Cyber Fraud in the Past Decade

George-Daniel Bobric

"Carol I" National Defense University, Bucharest, Romania

dbobric08@gmail.com
DOI: 10.34190/EWS.21.010

Abstract: Everyday reality faces an existential paradigm: the belligerent and puritanical visions characteristic to the beginning of the current century were projected from the physical space into the operational environment constituted by the cyberspace. Similarly, cyberspace is one of the "grounds" used for initiating illicit operations carried out by various individuals or groups to achieve personal or collective goals. The peculiarities of the cyber environment that favour the commission of online crimes under the auspices of the significant protection of the perpetrator's real identity materialize in a unitary whole that, in recent years, has been irrefutably consolidated and which represents a major threat to the states' national security. At the same time, the concoction of motives that constitute the starting point in the process of elaborating, initiating and executing cyber attacks revolves around ensuring the personal gains of their initiators, especially the financial ones. This paper is an empirical, qualitative research, its objective being to investigate the evolution of the actions performed within the cyberspace related to the cyber-enabled fraud, both in terms of cantitative and qualitative aspects. In order to achieve the proposed objective, an analysis of the literature relevant to the topic of the paper was performed. Also, significant data provided by institutions from different countries with a special role in the cyber security domain were collected, to have an overview on the current situation regarding the cyber fraud activities by analyzing the trends from the past decade. Nonetheless, a short presentation of the possible evolutive directions of the instruments specific to the cyber fraud in the future years will be performed. The results of the study show a vertiginous increase from year to year in the number of cyber-fraud actions, in the number of the victims' complaints and in the amount of financial losses registered as a result of these actions. Starting from these preliminary data, the profile organizations can elaborate future in-depth studies on this worrying phenomenon

represented by the exacerbation of the number of illicit actions carried out in the cyberspace categorized as cyber-fraud.

Keywords: cyber-fraud, cyberspace, cyber attacks, cybercrime, cybersecurity

AI-Powered Defend Forward Strategy

Jim Chen

U.S. Department of Defense National Defense University, Fort McNair, Washington, USA

jim.chen@ndu.edu
DOI: 10.34190/EWS.21.505

Abstract: The goal of the defend forward strategy in the cyber domain is to thwart attacks at their sources or at least mitigate their impact before they reach their targets. To achieve this goal, specific capabilities must be built into the technology and the processes that support this mission. These capabilities include but are not limited to the following ones: robust intelligence collection, accurate decision-making, quick and accurate targeting, constantly changing to avoid being detected by adversaries, unexpected maneuvering to generate precise and surprising effect at the speed of light, and objective assessment of missions accomplished. It has to be acknowledged that the high demand for these unique capabilities cannot be satisfied without the employment of artificial intelligence (AI). This paper explores one way of building these unique capabilities utilizing AI in order to support the defend forward strategy. The proposed solution calls for the integrated architecture of capability, speed, and precision as well as the checks-and-balances architecture. The paper reveals how strategic advantages can be achieved via the use of these new capabilities supported by human-machine teaming. This exploration can provide guidance for developing new capabilities for commanders' toolkits. Consequently, it will help to nurture a cyber persistent force comprised of humans and machines.

Keywords: defend forward, persistent engagement, artificial intelligence, human-machine teaming, strategic advantages

Global Military Machine Learning Technology Development Tracking and Evaluation

Long Chen[1,2] and Jianguo Chen[3]

[1]Beijing Key Laboratory of Network Technology, Beihang University, Beijing, China

[2]Innovation Technology Research Institute, Beijing Topsec Network Security Technology Co Ltd, China

[3]Hebei Seismological Station, Earthquake Administration of Hebei Province, Shijiazhuang, China

zhuanjiatuijian@126.com

DOI: 10.34190/EWS.21.092

Abstract: We have carried out global military machine learning technology development tracking and evaluation research, summarized the global military machine learning technology development status, analyzed its main technology development path, studied its development trend, analyzed the global military machine learning technology typical military application cases and development prospects, and proposed Enlightenment suggestions. Related institutions are paying close attention to the development strategy of machine learning in the military field. Representative countries have formulated the technical route of machine learning in the military field. In particular, the U.S. military has seized the opportunity for Intelligence construction. During the past few years, it has been conducting theoretical preparations and technological evolution. The U.S. military's intelligent construction is speeding up in an all-round way, and the overall combat capability will make a sharp jump. In particular, the U.S. Department of Defense(DoD) has accelerated the militarization of artificial intelligence applications and specially established the Joint Artificial Intelligence Center (JAIC) to coordinate and advance military research on artificial intelligence. With regard to machine learning to strengthen the construction and operations of various services and arms, militaries have intensively deployed various military intelligence research projects, carried out research on machine learning intelligent algorithms and promoted the transformation of artificial intelligence technology to intelligence processing, unmanned platforms, command and control, and weapon equipment systems. Troops from different countries around the world are taking machine learning technology into their land-based, sea-based, air-based, space-based and network space platforms weapons, networks and other systems. Taking the US military as an example around machine learning, the US Army conducts research on distributed processing and applied machine learning systems in

autonomous networks and heterogeneous environments. The Navy develops unmanned naval information and response electronic attack projects. The Air Force's "quantum plan" and autonomous clusters resilient network, machine learning wingman, and six-generation machine developed so that it greatly increased combat power. Marines carry out the depth of reinforcement learning collaborative information warfare. Space army carries out analysis of the space-based data management. In particular, a series of planned network covered troops cyber threat defense, military IoT network defense, machine learning behavior detection, social network data analysis, and network electronic warfare, and other dimensions. In addition, we investigated the induction machine learning in future operations, intelligence, network, logistics, identification, health, trend data, and a plurality of key areas of current situation with development trend. We also put forward the suggestions.

Keywords: global military, machine learning, artificial intelligence, project tracking

Global Social Network Warfare on Public Opinion

Long Chen[1,2] and Jianguo Chen[3]

[1]Beijing Key Laboratory of Network Technology, Beihang University, Beijing, China

[2]Innovation Technology Research Institute, Beijing Topsec Network Security Technology Co Ltd, China

[3]Hebei Seismological Station, Earthquake Administration of Hebei Province, Shijiazhuang, China

zhuanjiatuijian@126.com

DOI: 10.34190/EWS.21.093

Abstract: Information warfare can be divided into two types: technical and psychological information warfare. The scope of cyberspace weapons is expanding from the physical network domain to the cognitive information domain. Technologies such as network penetration, public opinion guidance and attacks, cognitive intervention and control will become the main development directions. Controlling public opinion and controlling audiences will become the cyberspace cognitive domain. The development goal of the weapon. In recent years, emerging network media such as social networks and mobile communication networks have played an important organizational and planning role in a series of significant events, which are likely to cause severe threats to national security and even the international community's stability. We conclude that social public opinion

weapons are mainly divided into six categories: Bot, Botnet, Troll, Manipulate real people and events, Cyborg, and Hacked or stolen. Since social network warfare is a brand new war situation in the context of great powers, in social media, the confrontation of camps can be observed. States use social media platforms to penetrate and media war, and its Internet space monitor and build defenses. A digital wall has been placed horizontally on the boundary of the virtual space. In recent years, as the trend toward weaponization of social media has become increasingly apparent, military powers such as the United Kingdom, the United States, and Russia have taken the initiative to take the lead in the field of social media. All countries continue to strengthen the research on fundamental cognitive theories. Many basic research projects that integrate information, biology, network, and cognition have been launched one after another. The combat practice shows that the effectiveness of social media even exceeds some traditional combat methods. With the prominent role of social media in modern warfare, its combat use has become increasingly widespread and has gradually become a force multiplier in modern warfare. At present, the deployment of weapons directed by social network users in significant countries is mainly focused on incident and public opinion reconnaissance, sentiment analysis, and active intervention. In short, all countries are using social media to spread political propaganda and influence the digital information ecosystem. The technical means, scale, scope, and precision of social media weapons have been continuously improved. It is gaining momentum to reshape the cyberspace security pattern of various countries fundamentally.

Keywords: social network, global warfare, public opinion

Serious Games for Cyber Security: Elicitation and Analysis of End-User Preferences and Organisational Needs

Sabarathinam Chockalingam, Coralie Esnoul, John Eidar Simensen and Fabien Sechi

Institute for Energy Technology, Halden, Norway

Sabarathinam.Chockalingam@ife.no; Coralie.Esnoul@ife.no; John.Eidar.Simensen@ife.no; Fabien.Sechi@ife.no
DOI: 10.34190/EWS.21.043

Abstract: Digitalisation is more actual than ever and even forced by the Covid-19 pandemic for many. The evolution of technology enables everyone and everything to be connected. This is one of the reasons why cyber security is important to

society as it makes the large majority vulnerable to cyber-attacks. Cyber-attacks not only impact confidentiality, integrity and availability of information but also can cause physical damage like Stuxnet. Notably, humans are considered the weakest link in cyber security. Training plays an important role in strengthening the weakest link. A survey was conducted with the aim of developing a serious game for cyber security training where we found that current cyber security trainings are not effective in practice. The survey results showed that the conventional training method is both widely used and at the same time considered the least preferred training method. On the other hand, the game-based training method seems to be the least used training method, but this seems to be one of the most preferred training methods. Existing serious games in cyber security are "generic" as they do not seem to neither consider end-user preferences nor can be tailored to the specific and varying needs of an organisation. Therefore, a survey was conducted in an organisation to elicit end-user preferences. This was complemented with interviews of key management personnel to gather organisational needs. Based on the analysis of survey and interview results, a set of requirements are provided for developing a serious game for cyber security training in a specific organisation.

Keywords: cyber security, organisational needs, serious games, training, user requirements

Effectiveness of Covert Communication Channel Mitigation Across the OSI Model

Tristan Creek, Mark Reith and Barry Mullins

Air Force Institute of Technology, Wright-Patterson AFB, USA

Tristan.Creek@afit.edu
Mark.Reith.ctr@afit.edu
Barry.Mullins@afit.edu
DOI: 10.34190/EWS.21.108

Abstract: The Internet consists of various levels of communication technologies which are often categorized by a layered model called the OSI model. Among the technologies within the seven layers of the OSI model, covert communication channels allow attackers to subvert defenders and secretly transmit data by leveraging technologies beyond their specified standards. These covert communication channels impact security differently depending on which layer of the OSI model they exist. Although mitigating every channel is ideal, limited resources require the consideration of the effectiveness of mitigating covert communication channels. This paper presents the impact of covert communication

channels on each layer of the OSI model, how to mitigate them, and concludes with recommending the mitigation of covert communication channels on layers 1 through 4 of the OSI model. The final recommendation deliberates that an organization must decide their cost-to-risk ratio on an individual basis when considering solutions to mitigating covert communication channels.

Keywords: covert communication channels, OSI model, network technology

Deepfake Video Detection

Shankar Bhawani Dayal and Brett van Niekerk

University of KwaZulu-Natal, South Africa

sbdayal15@gmail.com
vanniekerkb@ukzn.ac.za
DOI: 10.34190/EWS.21.110

Abstract: Deepfakes pose a threat to many aspects of society, such as election manipulation, involuntary pornography and fraud by means of identity theft. This paper aims to determine if deepfake models which are pre-trained on older datasets are still able to accurately detect whether a video is real or a deepfake from a newer dataset. From a comprehensive literature review, two papers were selected to be tested. The first model tested was from Afchar et al. (2018), was unable to run due to an error involving Keras, to no fault of the code. The model that was successfully tested on a sub-dataset was the XceptionNet model from the FaceForensics++ paper by Rössler et al. (2019). It was shown that the XceptionNet model was not able to effectively detect deepfake videos, having a 51.31% classification accuracy on the subdataset, further analysis of the results showed that it only had a 13.16% accuracy when detecting deepfake videos and it had 89.47% accuracy when detecting real videos. As the methods which are used to create deepfake material improve, the previous work which has been done will need to be tested on the material created by the newer methods to determine if they are still effective at detecting deepfakes.

Keywords: deepfake, FaceForensics++, generative adversarial networks, Xceptionnet, deepfake detection challenge dataset

A Shoestring Digital Forensic Cyber Range for a Developing Country

Jaco du Toit and Sebastian von Solms

University of Johannesburg, South Africa

jacodt@uj.ac.za
basievs@uj.ac.za
DOI: 10.34190/EWS.21.008

Abstract: The 2020 Covid-19 lockdown forced many universities and other training institutions to rethink how training occurs. Training typically consists of theoretical aspects, but they may also contain practical elements. Practical computer training typically requires computer hardware and software of a certain standard, configuration, and setup. Such practicals then make use of dedicated lab equipment and/or virtual environments. The non-contact requirement in the Covid-19 lockdown shifted the focus towards totally online virtual environments. In some settings, such virtual environments are also known as cyber ranges. Many organisations provide access to pre-built cyber ranges, and individuals can quickly join a cyber range. Existing cyber ranges offer individuals access through free or pay accounts. Organisations can contract cyber range service providers to use their platforms for teaching and learning. The National Institute for Standards and Technology (NIST) also has a draft cyber range guide that organisations can use to plan and set up their cyber range. Setting up a cyber range for an organisation's purposes requires significant investment and skills. The research described in this paper flows from the problems during the Covid-19 pandemic to offer specific courses which need particular lab environments. Students had to have access to specialised software programs and large data sets to do their practicals. Lecturers spent a large amount of time helping students, having unreliable Internet connections and low-level hardware devices, to do the required practicals. The problem resulted in a decision to plan, implement, and maintain such a cyber range for a typical South African context. The resultant cyber range solution had to allow students with the limitations mentioned above to perform their practical work properly. The main limitation was a shoestring budget. The shoestring cyber range is also compared against more feature-rich environments to highlight the features that are not included in such a shoestring cyber range. The research concludes that providing basic cyber range functionality may be sufficient in specific circumstances.

Keywords: cyber security, cyber range, digital forensics, virtual

A Strategy for Implementing an Incident Response Plan

Alexandre Fernandes[1], Adaíl Oliveira[1,2], Leonel Santos[1,2] and Carlos Rabadão[1,2]

[1]School of Technology and Management, Polytechnic of Leiria, Portugal

[2]Computer Science and Communication Research Centre, Polytechnic of Leiria, Portugal

alexandre.fernandes@ipleiria.pt; adail.oliveira@ipleiria.pt; leonel.santos@ipleiria.pt; carlos.rabadao@ipleiria.pt

DOI: 10.34190/EWS.21.080

Abstract: With the exponential growth of the Internet, several challenges and security threats arise. Those threats are due to the lack of adequate security mechanisms, security policy flaws, increasing usage of mobile devices, mobility, and user's naivety. Although organisations try their best to deploy effective security solutions and practices, there will always be security incidents. Therefore, they must place detection methods to identify those threats and vulnerabilities. On the other hand, response activities must be established to deal with and respond to the detected incidents. An Incident Response Plan (IRP) aims to provide an organisation with an easy-to-follow guide that leads to a quick and effective incident response. The implementation of such a plan is not an easy task. To implement an IRP requires an organisation a lot of research and analysis of the existing frameworks and examples. Most frameworks explain how to set up a Computer Security Incident Response Team and how they should handle incidents, but only a few instruct how to implement a plan. The proposal of this paper is to present a practical strategy on how to implement an IRP, complementing the existing incident response frameworks, thus reducing the difficulty of creating an effective and useful plan. The study and proposal of this topic come from the research and experience developed during the implementation of an academic Security Operation Centre. The paper starts by presenting the most relevant incident response frameworks and related work. It then proposes a flexible strategy for creating an IRP that can be adjusted to any organisation's scope and objectives. During the strategy presentation, the various domains of incident response are presented. Finally, strategies for its implementation will be introduced. As the main contribution of this work, the reader will be able to understand the common structure and content of an IRP and to create their own plan.

Keywords: incident response, CSIRT, framework, cybersecurity, security operations centre

Are Encypted Protocols Really a Guarantee of Privacy?

Jan Fesl[1,2], Michal Konopa[1], Jiří Jelínek[1], Yelena Trofimova[2], Jan Janeček[1,2], Marie Feslová[1], Viktor Černý[2] and Ivo Bukovsky[1]

[1]University of South Bohemia, Branisovska 31, Ceske Budejovice, Czech Republic

[2]Czech Technical University in Prague, Faculty of Information Technology, Thákurova 9, Prague, Czech Republic

jfesl@prf.jcu.cz, konopm05@prf.jcu.cz, jjelinek@prf.jcu.cz, trofiyel@fit.cvut.cz, janecek@fit.cvut.cz, dolezm01@prf.jcu.cz, cernyvi2@fit.cvut.cz, ibuk@prf.jcu.cz

DOI: 10.34190/EWS.21.047

Abstract: Most internet traffic is being encrypted by application protocols that should guarantee users' privacy and anonymity of data during the transmission. Our team has developed a unique system that can create a specific pattern of traffic and further analyze it by using machine learning methods. We investigated the possibility of identifying the network video streams encrypted within the HTTPS protocol and explored that it is possible to identify a particular content with a certain probability. Our paper provides a methodology and results retrieved from the real measurements. As the testing data set, we used the streams coming from the popular platform Youtube. Our results confirm that it is possible to identify encrypted video streams via their specific traffic imprints, although it should not be possible due to the used encryption.

Keywords: internet traffic, encrypted video stream, identification, data traffic pattern, machine learning

Targeting in All-Domain Operations: Choosing Between Cyber and Kinetic Action

Tim Grant[1] and Harry Kantola[2]

[1]R-BAR, Benschop, The Netherlands
[2]Finnish National Defence University, Helsinki, Finland

tim.grant.work@gmail.com
harry.kantola@mil.fi
DOI: 10.34190/EWS.21.045

Abstract: Targeting is the process of selecting and prioritizing targets and matching the appropriate response to them. The process is the same whether the response is cyber, kinetic, or some combination, but there are major differences between cyberspace and the physical (i.e. land, sea, air, and space) domains. Cyber operations are often stealthy and can proceed much faster than kinetic operations. Cyber targets differ greatly from their physical counterparts, and can – if desired – be engaged with no permanent damage. Cyber effects can more easily cross geographical boundaries and jurisdictions, but with an increased risk of collateral damage. Western militaries are transitioning from joint operations to all-domain (or multi-domain) operations. Until now, targeting has been done separately by domain. In future, units will have capabilities in all five domains, constructing cross-domain kill-chains from sensor to shooter. A new targeting choice will then arise: do we engage this target in cyberspace or through a physical domain? Intuitively, it would seem that kinetic action is better suited to destroying assets and denying access to an area, while cyber action lends itself to deception. However, the combination of cyber and kinetic action may be better still. One example is Operation Orchard in which the Israeli Air Force bombed a suspected nuclear reactor at Al Kibar, Syria, in 2007. To hide the ongoing air raid, the Israelis took over the Syrian air defence system using network attack techniques, feeding it a false sky picture. This paper proposes an approach for choosing between cyber and/or kinetic action as part of the targeting process in all-domain operations, based on representing target elements and their dependencies as a network.

Keywords: targeting, all-domain operations, multi-domain operations, target selection, target-response matching, target engagement

Computer Aided Diagnostics of Digital Evidence Tampering (CADDET)

Babak Habibnia, Pavel Gladyshev and Marco Simioni

DFIRe, University College Dublin, Ireland

Babak.Habibnia@ucd.ie
Pavel.gladyshev@ucd.ie
marco.simioni@ucdconnect.ie
DOI: 10.34190/EWS.21.059

Abstract: The tampering of the digital crime scene has become more common. When tampering behaviour is successful, it does not leave a trace of either the incriminating evidence or the act of tampering and the digital evidence that digital investigators seek will be absent. The research into the automatic detection of digital evidence tampering has been ongoing for over 13 years. Many approaches had been proposed, but the practical tools for automatic or semi-automated detection of evidence tampering are still missing. Due to the complexity of real-world computers and the differences between software installed on different computers automatic analysis is hard. A similar problem exists in medical imaging. Despite the common grand design, every human is unique and complex, and it is hard to come up with the exact rules for detecting lesions in medical images. Visualization for forensic analysis of the data stored on a specific device has received much less attention, while the use of visualization for detection of digital evidence tampering is virtually unexplored. This paper proposes, for the first time, a semi-automated approach based on visualization of relevant data properties, helping human investigators to detect digital evidence tampering and anomaly. This is analogous to computer-aided processing of medical X-Ray images that enhance the visibility of lesions facilitating easier detection by a doctor. This paper aims to identify data tampered features on the digital devices, then find suitable visualization to display identified data tampered features for investigators. One of the outstanding features of the approach proposed in this paper for detecting digital evidence tampering is its malleability. It can easily apply to any specific or whole part of data in the digital devices, visualize, and reveal offender concealment behaviour concerning the detection of evidence tampering.

Keywords: cybercrime, cybersecurity, digital evidence tampering, digital forensics, anti-forensics, visualization

Weaknesses of IoT Devices in the Access Networks Used by People in Their Homes

Aarne Hummelholm

Faculty of Information Technology, University of Jyväskylä, Finland

aarne.hummelholm@elisanet.fi
DOI: 10.34190/EWS.21.036

Abstract: Today, the rapid development of information technology, components, systems, and applications poses major challenges for designers of networks, new services, and new types of smart devices to make devices and systems secure and usable in this digital world. Different types of smart devices are used everywhere, and people are being provided with more effective services to meet their everyday needs. Those smart devices are increasingly connected to many different types of sensors and IoT devices, whose security solutions are weak or non-existent due to the urgency of manufacturers to bring devices to market as quickly as possible. As a result, they have no time to create good security solutions for those devices. Those sensors, actuators and IoT devices are used in industrial environments, different types of municipal systems, different types of homes devices and systems, buildings' systems, free-time environments, healthcare systems, cars, ships, and so on. Access network devices are connected to smart devices or access nodes and through those access networks devices information is sent to data centers, where they use different types of services and store information they are collecting. People use their smart devices for different services and in different environments, and they often buy apps from app stores that may not be secure enough. Normal store-bought smart devices do not include hardened functionality and are therefore easy to hack or malware can easily be installed on them. Those vulnerabilities give hackers and cyber attackers possibilities to attack systems via those sensors, actuators and IoT devices and install malware in those systems and on devices. Due to the rapid development of sensors, actuators, and IoT devices, hackers and network attackers are aware of this and are developing new types of malware that are optimized for use in such environments. One example of the latest Malware is Mirai, which has been used in attacks against smart devices and processor controllers, IoT devices, actuators, and sensors. It is also used against routers, gateways and switches. There are also new variants that may be even more harmful when they are used against systems. Even if we make the communication connection from smart devices to data center secure enough, it is still not enough because the sensors, actuators and IoT devices are full of vulnerabilities.

Keywords: sensors, actuators, IoT devices, vulnerabilities, security, attacks

Cyber Security Analysis for Ships in Remote Pilotage Environment

Aarne Hummelholm, Jouni Pöyhönen, Tiina Kovanen and Martti Lehto

University of Jyväskylä, Finland

aarne.hummelholm@elisanet.fi; jouni.a.poyhonen@jyu.fi;
tiina.r.j.kovanen@jyu.fi; martti.j.lehto@jyu.fi
DOI: 10.34190/EWS.21.025

Abstract: International and national maritime transportation systems are essential parts of critical infrastructures in every society. Digitalization makes possible to increase levels of autonomy in maritime transportation systems. In the research point of view, it will be done step by step. In Finland, to develop the remote pilotage on fairway environment is an example of this process. The function of all legacy and modern ships are essential parts of its cyber security. The integration of operational systems and information systems on ships take place on the ship's intranet in order to improve the cooperation of the various functions of the ships. Integration brings together new services and functions coming from digitalisation, the development of new maritime and autonomous traffic managements, the integration of monitoring and control functions, and the development of functions streamlining services. As ships increasingly use information systems to exchange information between different integrated systems on ships and ground systems, and between on-board operating systems and on-board communication systems, the examination of the digital structure and its´ dependencies is a very important part of cyber security analysis work. It enables to identify different functions in the system level, carry out risk assessments and identify their residual risks with sufficient accuracy. In the same way, the dependencies of different information systems need to be considered and, based on these dependencies, security and cyber security risks need to be identified. This paper presents a probability approach to cyberattacks versus a probability to defend attacks and at the end to evaluate cyber security risks related to the operations of ships. Cyber security of information systems used on board ships must be approved before the systems are put into service. In order to define this large entity in a controlled way into different parts, one good way is to use the enterprise architecture framework and its methods to visualize entire systems, subassemblies, and dependencies. The paper examines these ship's systems cyber security elements and the necessary security mechanisms to better manage the information and cyber security situation awareness now and in the future integrated operating environments on the way to autonomous ships.

Keywords: critical infrastructure, remote pilotage, ship, cyber security risks, probability, situation awareness

A Review of National Cyber Security Strategies (NCSS) Using the ENISA Evaluation Framework

Angela Jackson-Summers

U.S. Coast Guard Academy, New London, USA

angela.g.jackson-summers@uscga.edu
DOI: 10.34190/EWS.21.040

Abstract: During the COVID-19 pandemic, cyber threats have continued to increase prompting increased awareness and preparedness from malicious security attacks. In April 2020, a joint alert, *COVID-19 Exploited by Malicious Cyber Actors*, was issued from the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Given the advancement of cyber threats, especially during our current COVID-19 pandemic, national cyber security strategy (NCSS) effectiveness remains important. The purpose of this study is intended to determine existing challenges in NCSS effectiveness. Using textual analysis, the national cyber security strategies (NCSS') for 18 countries were evaluated against the European Union Agency for Cybersecurity's (ENISA) Evaluation Framework dated November 2014. The results of this study reflected a need for maturation and timelier updates to NCSS'. Gaps and recommendations are discussed and provide future research considerations. This study's contribution provides additional insights to researchers, practitioners, and other stakeholders focused on national cyber security policy, related strategies, and risk management practices.

Keywords: cyber security, national strategy, national security, security policy, risk management

Some Cybersecurity Governance Imperatives in Securing the Fourth Industrial Revolution

Victor Jaquire[1], Petrus Duvenage[1] and Sebastian von Solms[2]

[1]Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa

[2]Centre for Cyber Security, University of Johannesburg, South Africa

victorJ@uj.ac.za
pcduvenage@uj.ac.za
basievs@uj.ac.za
DOI: 10.34190/EWS.21.056

Abstract: The fourth industrial revolution (4IR) will "transform the workplace from the existing pattern to the "human centred" characteristics" and just as there is a "tendency to merge man and machine to shorten the distance between natural sciences, humanities and social sciences, the same is expected to happen with science and technology" (Scepanović 2019). Scepanović (2019) further indicates that these processes will require a "shift to interdisciplinary teaching, research and innovation, education and in particular higher education", and that "the 4IR has a special role, being a complex, dialectical and exciting activity which promises to transform society for the better". In contrast, Onik, Kim and Yang (2019) state that the 4IR will "expose the maximum personal information the world has ever seen" and observe that "although people are considered as an asset, several recent information leaking incidents have shaken the whole world in perspective of data privacy". Also within the 4IR context, Sander (2019) refers to the realities of cyber-attacks, indicating that "Peacetime cyber-attacks are destructive cyber operations, encompassing acts undertaken by a State – or actors whose conduct is attributable to a State under international law – that uses cyber capabilities to alter, disrupt, degrade or destroy the computer systems or networks of a foreign State, or the information or programs resident in those systems or networks" It therefore becomes clear that there should be cyber security considerations with regard to the envisaged outcomes and realities culminating from the 4IR. This paper contributes to a series of previous papers on cyber security and cyber counterintelligence (CCI). Its primary aim is to add to the bourgeoning academic discourse on emerging cyber concerns through a discussion of some cyber security governance imperatives in relation to the 4IR. To this end, the paper highlights some positive and negative realities (outcomes) of the 4IR, including some background to the 4IR's impact. We then proceed with examining some potentially dire consequences flowing from the 4IR. Finally, the paper advances a proposition on addressing these consequences. Our proposition is specifically focussed on

three imperatives to an effective cybersecurity governance approach in securing the 4IR, namely: 'strategy', 'intelligence and counterintelligence' as well as 'capacity building and skills development'.

Keywords: cyber security, cyber counterintelligence, governance, cyber threat intelligence, defensive and offensive cybersecurity, fourth industrial revolution

Critical Infrastructure Protection: Employer Expectations for Cyber Security Education in Finland

Janne Jaurimaa, Karo Saharinen and Sampo Kotikoski

JAMK University of Applied Sciences, Jyväskylä, Finland

m1270@student.jamk.fi
karo.saharinen@jamk.fi
sampo.kotikoski@jamk.fi
DOI: 10.34190/EWS.21.015

Abstract: In the human factor of cyber security, high level technical experts are considered as multidisciplinary technical gurus who are familiar with every aspect of IT environments including operating systems, code languages and protocols. University curricula and guiding frameworks, such e.g. NICE Cyber Security Workforce Framework, are designed to produce professionals to match the endless needs of working life. The cornerstones of achieving good working results can be considered as the level of expertise competence of the employee performing the task, as well as combining personal skills and abilities with the competence profile of the given task. Does the cyber domain need slightly lower educated, vocational level employees? As part of the National Security Policy in Finland, the vocational qualification in information and communications technology has recently started to produce suitable workforce for cyber labor on the European Qualifications Framework level 4 (EQF-4). In this research paper we answer the question how well the vocational education meets the demands of the employers as suitable workforce in cyber security in Finland. The study also investigated what kind of cyber security employees the Finnish employers currently need; what is the required level of education, level of experience and direction of competence. The research data was collected through a structured questionnaire survey, which was directed to critical national infrastructure protection companies such as Finnish telecom operators, ICT service providers, defense sector, and other governmental actors. The questionnaire results were examined with quantitative methods. Based on our results, regarding the content of education at EQF4-level, employers believe that the emphasis should be placed on basic technical skills and adherence to

guidelines, while choosing more detailed specific areas of expertise is less important at this level of education. Based on the responses, in general cyber security related work has higher education level requirements than EQF4-level could provide. The results of the study can be used as guidelines for the development of the future curricula and in the strategic leadership of companies employing cyber security professionals.

Keywords: human factor, security policy, critical infrastructure protection, strategic leadership

Digital Forensic Readiness Implementation in SDN: Issues and Challenges

Nickson Karie[1, 2] and Craig Valli[1, 2]

[1]Cyber Security Cooperative Research Centre, Australia
[2]Security Research Institute, Edith Cowan University, Australia

nickson.karie@cybersecuritycrc.org.au
c.valli@ecu.edu.au
DOI: 10.34190/EWS.21.091

Abstract: The continued evolution in computer network technologies has seen the introduction of new paradigms like Software Defined Networking (SDN) which has altered many traditional networking principles in today's business environments. SDN has brought about unprecedented change to the way organisations plan, develop, and enact their networking technology and infrastructure strategies. However, SDN does not only offer new opportunities and abilities for organisations to redesign their entire network infrastructure but also presents a different set of issues and challenges that need to be resolved. One such challenge is the implementation of Digital Forensic Readiness (DFR) in SDN environments. This paper, therefore, examines existing literature and highlights the different issues and challenges impacting the implementation of DFR in SDN. However, the paper also goes further to offer insights on the different countermeasures that organisations can embrace to enhance their ability to respond to cybersecurity incidents as well as help them in implementing DFR in SDN environments.

Keywords: digital forensic readiness, software defined networking, issues and challenges, cyber security incidents, countermeasures

Cyber Wargaming on the Strategic/Political Level: Exploring Cyber Warfare in a Matrix Wargame

Thorsten Kodalle

The Bundeswehr Command and Staff College, Hamburg, Germany

thorstenkodalle@bundeswehr.org
thorstenkodalle@hotmail.com
DOI: 10.34190/EWS.21.500

Abstract: NATO understands cyber within a cognitive, virtual and physical domain and on technical, tactical, operational, strategic and political levels. The NATO SAS 129 Research Task Group (RTG) "Gamification of Cyber Defence/Resilience" explores the advantages of gamification, especially Serious Games in the form of wargames, card-driven games and matrix wargames to support training and education in all domains and on all these levels. Within their task is the development of specific prototypes for these specific domains and levels. The Bundeswehr Command and Staff Course of the German Armed Forces implemented within their competence-based training and education system the Matrix Wargame "Kaliningrad 2018" (MWG Kaliningrad 2018) in 2018 for security policy education on the strategic and political level. MWG Kaliningrad 2018 was used several times in the Basic Staff Officer Course and the General Staff Officer Course National but also with students from the Hamburg University of Technology (TUH). This paper describes the history of the implementation of the game, evaluations from the course participants and insights from the most recent research and development approaches to develop a "Global Matrix Wargame" with a particular emphasis on information operations, information warfare and cyber warfare on the semantical level. It will examine how a matrix wargame can be a practical approach to reach specific cyber-related cognitive learning goals and appreciate a whole of government and whole of society approach to cyber resilience. It describes a good practice approach to a research and development and education (R&D&E) approach to discuss resilience in an open society. This is the second of three articles for the Conference Proceedings of ECCWS 2020. There are redundancies in the introduction, and the first article examines terminological uncertainties more.

Keywords: game-based learning (GBL), matrix wargames, cyber warfare on the semantic level, information operations

Cyber-Threat Analysis in the Remote Pilotage System

Tiina Kovanen, Jouni Pöyhönen and Martti Lehto

University of Jyväskylä, Finland

tiina.r.j.kovanen@jyu.fi
jouni.a.poyhonen@jyu.fi
martti.j.lehto@jyu.fi
DOI: 10.347190/EWS.21.067

Abstract: Fairway pilotage is advancing toward a more digitalized future where an automated remote pilotage system such as ePilotage (a remote piloting system of systems) is possible. ePilotage is an example of a system in which an increased number of digital solutions are entering new environments where traditional engineering solutions are still in use. This development introduces increased risk of a malicious cyber adversary taking deliberate actions against the system. Cyber threats are a multidimensional phenomenon with many aspects to consider for technical and non-technical audiences. Often, the threat is perceived from a limited number of viewpoints, and important discoveries may be missed. Many organizations adapt public models to their needs and in the process lose some interoperability between different organizations. This is a compromise that has to be weighed. ePilotage is a very special viewpoint as it incorporates a large network of separate systems and stakeholders. By examining the impacts of cyber-threat actions in this connected environment, we found that the impacts affecting one subsystem are propagated to affect other systems. This effect combined with time-criticality implies that cooperation among subsystem stakeholders is essential. This requires common situational awareness to support fast and precise reactions. For this, there must be a common language to describe the situation. This is achieved by creating and using a common methodology for cyber-threat analysis. At the strategic level, there must be a description of the situation with non-technical terminology. This includes, for example, discussion of the attacker's motivations by studying different types of adversaries, such as cyber vandalism and cybercrime. Oat the tactical level, there must be more technical information on the threat actor's tactics, techniques, and procedures. By examining the cyber-threat actors' features and by combining them to known cyber-attack tactics, techniques and procedures, scenarios for ePilotage can be created. These scenarios provide information on the possible threats concerning this specific environment and its protection.

Keywords: maritime autonomy solution, ePilotage, cyber security, cyber threat analysis, scenarios

Impact of AI Regulations on Cybersecurity Practitioners

Louise Leenen[1,2], Trishana Ramluckan[3,4] and Brett van Niekerk[3]

[1]University of the Western Cape, South Africa
[2]Centre for AI Research, South Africa
[3]University of Kwazulu-Natal, South Africa
[4]Educor Holdings, South Africa

lleenen@uwc.ac.za
trishana.ramluckan@educor.co.za
vanniekerkb@ukzn.ac.za
DOI: 10.34190/EWS.21.014

Abstract: Cybersecurity and Artificial Intelligence (AI) are closely aligned; both domains are growing rapidly, they are inter-dependent and they face major challenges. Cybersecurity threats are of great concern globally and becoming increasingly difficult to address. AI is widely recognised to be crucial to the development of efficient cybersecurity measures. AI is a core tool in combatting cybercrime and other cybersecurity threats but many AI applications are, in turn, vulnerable to cybersecurity attacks. Most countries have some cybersecurity and privacy legislation in place or are in the process of putting regulations in place. However, AI regulation is still relatively new. Due to the close relationship between cybersecurity and AI, cybersecurity practitioners have to be aware of national, regional and international AI regulations. In this paper, an overview of the progress in terms of AI governance and regulations is provided, including national AI policies and international agreements on AI issues. The paper concludes with recommendations for the cybersecurity community.

Keywords: artificial intelligence regulations, cybersecurity governance, AI principles, ethics in AI

Is Hacking Back Ever Worth it?

Antoine Lemay[1] and Sylvain Leblanc[2]

[1]Cyber Defence Corporation, Montréal, Canada
[2]Department of Electrical and Computer Engineering, Royal Military College of Canada, Kingston, Canada

antoine.lemay@live.ca
sylvain.leblanc@rmc.ca
DOI: 10.34190/EWS.21.020

Abstract: As nefarious activity in the cyber domain continues to increase, more and more actors are contemplating "hacking back" as a strategy for defence. At first glance, such deterrence may seem desirable because it intuitively offers a disincentive to the attacker to attack one's assets; a purely defensive stance that does not cause the attacker harm may appear to do nothing to prevent or stop aggression. We must ask however, if that logic can work in practice. By looking at historical examples of cyber exchanges, we will show that many attempts to "hack back" tend to widen the scope of a conflict rather than limit it; we found that the only time when the approach works is when a credible threat of serious harm to the attacker is imposed. In fact, whether we looked at the exchanges from patriotic hackers, tit-for-tat retaliation appears to only invite additional aggression from one's original adversary, which ultimately widens the conflict rather than appease it. On the other hand, by examining the psychological effect of the Shamoon virus, one can surmise that the United States perceived that further attacks against Iran would incur significant cost to the United States. This was likely because Iran's capabilities to reverse engineer the attacks which would leave the United States vulnerable in the context of an asymmetric Iranian response, a counter-value proposition caused by common and increasing automation in the management of United States critical infrastructure. Similarly, even though United States retaliation for the Sony Picture hack was proportional in its effect, it demonstrated the ability to significantly damage North Korea's core connectivity, a fact that can be interpreted as signalling a crippling counter-force capability. In both instances, it seems that it was the threat of escalation, rather than retaliation itself, which proved effective. These observations lead to further questions which will be explored in the paper. Notably, whether cyber threat projection settles in escalation ladders frameworks as was the case with nuclear weapons, or whether the need for secrecy, required to maintain capability, interferes with the need for establishing credibility in threats of escalation.

Keywords: cyber retaliation, cyber deterence, cyber conflict, cyber escalation

EU Digital Sovereignty: A Regulatory Power Searching for its Strategic Autonomy in the Digital Domain

Andrew Liaropoulos

University of Piraeus, Greece
Laboratory of Intelligence and Cyber-Security

aliarop@unipi.gr
andrewliaropoulos@gmail.com
DOI: 10.34190/EWS.21.037

Abstract: Digital technologies have gradually affected the way societies interact, how companies deliver services and how people are governed. Policymakers around the world have realized the importance of digital technologies on their countries' security and autonomy and have issued sovereignty claims regarding cyberspace. The European Union - an actor that aims to ensure that governments, the private sector, civil society organisations and end users around the world promote an open, free, and secure cyberspace - has recently added the concept of digital sovereignty in its political vocabulary. Taking for granted that there is no widely accepted and comprehensive approach regarding digital sovereignty, this paper will analyse the European discourse on digital sovereignty. It will first review the ambiguous concept of sovereignty and then explore the way it can be applied in the European digital domain. The aim is to highlight the dilemmas and constrains that the EU is facing in relation to regulating the digital domain, avoiding technological protectionism, promoting cyber-resilience, and understanding the game of digital geopolitics.

Keywords: EU, sovereignty, digital sovereignty, digital autonomy

Mandatory Cybersecurity Training for all Space Force Guardians

Banks Lin, Mark Reith and Wayne Henry

Air Force Institute of Technology, Wright-Patterson Air Force Base, USA

banks.lin@afit.edu
mark.reith.ctr@afit.edu
wayne.henry@afit.edu
DOI: 10.34190/EWS.21.107

Abstract: The most vulnerable and exploitable aspect of a computer network is often the user. Each user that operates an endpoint machine or system on the network increases the enterprise footprint for adversaries to target. Users introduce human error caused by the lack of knowledge or poor training on a particular tool or application. To date, the United States Air Force has not provided fundamental cybersecurity training for all its personnel. Currently, Airmen can go through basic or officer training and enter active duty without compelling training on cybersecurity. It is not until after airmen are sworn in that they are mandated to complete a computer-based cyber awareness training. This exposure to cybersecurity is essential but insufficient. This article proposes an enhanced level of mandatory cybersecurity education and training during basic and officer training to normalize conversations on cybersecurity to create an informed and well-educated United States Space Force. This ensures all Guardians understand the cyber vulnerabilities and threats to the point of it being common knowledge. Further, we use evidence-based cybersecurity training techniques to develop a course plan and learning objectives for Guardians to better retain and apply cybersecurity knowledge. This plan integrates realistic practice, cyber expertise, and personal reflections.

Keywords: mandatory cybersecurity training, evidence-based, annual refresher, space force

The Challenges to Cybersecurity Education in Developing Countries: A Case Study of Kosovo

Arianit Maraj[1], Cynthia Sutherland[2] and William Butler[2]

[1]AAB College, Faculty of Computer Sciences, Kosovo
[2]Capitol Technology University, Laurel, Maryland, USA

arianit.maraj@universitetiaab.com
cevalentine@captechu.edu
whbutler@captechu.edu
DOI: 10.34190/EWS.21.003

Abstract: Preventing cyberattacks depends on educating and training staff to acquire sufficient knowledge and skills to protect against such attacks. So far, in developing countries, there is little research focused on identifying factors that hinder the development of cybersecurity education in those countries. Therefore, studying these factors is very important. Cybersecurity is a relatively new profession and as such, suffers from a lack of standard mechanisms to bring the results of research into the curriculum and include students in academic research. The challenges to cybersecurity in developing Countries faced by Higher Educations Institutions (HEI) are huge. In general, it is not yet understood that HEIs are the core of the solution to the problems and challenges faced by Kosovo. Combining the core values of security, privacy, and HEI experimentation poses significant benefits to online security. The first step in meeting these challenges is to develop and execute an applicable education strategy. In Kosovo, there exists a cybersecurity strategy developed by the Government, which is deficient and not fully implemented or practiced. This strategy emphasizes the need to focus on providing a roadmap to develop a cybersecurity curriculum and advanced learning modules. However, so far, there is only one accredited cybersecurity academic program in Kosovo. This situation illustrates that cybersecurity education and training standards have not been given proper attention. Therefore, developing a standardized curriculum for cybersecurity is an urgent need. It is also recommended that a robust cybersecurity strategy, which focuses on cybersecurity education and training standards be developed. In this paper, the key factors in cybersecurity education and the main strategies and recommendations for advancing cybersecurity education in Kosovo will be explored and proposed.

Keywords: cybersecurity, education, training, awareness-raising, cyber strategy

Studying the Challenges and Factors Encouraging Girls in Cybersecurity: A Case Study

Arianit Maraj[1], Cynthia Sutherland[2] and William Butler[2]

[1]AAB College, Faculty of Computer Sciences, Kosovo
[2]Capitol Technology University, Laurel, Maryland, USA

arianit.maraj@universitetiaab.com
cevalentine@captechu.edu
whbutler@captechu.edu
DOI: 10.34190/EWS.21.004

Abstract: Today, there is a clear gender gap in cyberspace. Many barriers hinder the advancement of women in cybersecurity. In addition, a lot of studies point out that IT (Information Technology) is a more male-oriented world, which is one of the reasons why so few women pursue a career in cybersecurity. In this paper, we will try to explore the challenges and possible reasons for and suggest solutions to address this gap. Encouraging girls in cybersecurity will not only contribute for developing a strong cybersecurity workforce, but also one that should be prepared for offering more cybersecurity solutions. Through this paper, different stakeholders will also better understand their roles, duties, responsibilities and benefits for reducing a gender gap. The only way to cope with technological challenges is through educating and raising awareness of young women. Our idea is to provide a roadmap to cybersecurity awareness and training of young girls in developing Countries, with a focus in Western Balkans Countries, and help them to understand that the cybersecurity field offers a rewarding career for women. Our thesis is that increased awareness opportunities offered would help to increase the participation of girls and women in STEM (Science, Technology, Engineering and Mathematics) for the long term. In general, this paper will identify the challenges in encouraging young girls to seek cybersecurity related careers.

Keywords: cybersecurity, STEM, girls, education, mentoring, training

IoT Security and Forensics: A Case Study

Erik David Martin[1] Iain Sutherland[2] and Joakim Kargaard[3]

[1]Sopra Steria, Stavanger, Norway
[2]Noroff University College, Elvegata 2A, Norway
[3]Noroff Education Elvegata 2A, Norway

Erik.martin@soprasteria.com
Iain.sutherland@noroff.no
Kim.kargaard@noroff.no
DOI: 10.34190/EWS.21.032

Abstract: The expansion of the Internet of Things (IoT) has resulted in a corresponding increase in the amount of data contained in IoT devices. This data relates either to device-use or the local environment and provides digital forensic investigators with sources as diverse as smart cameras, sensors and watches with an opportunity to potentially capture or corroborate evidence. A challenge is that the data collected as part of the ecosystem operation may be distributed between several locations: cloud storage, mobile phone applications and the physical IoT device. Conducting digital forensic investigations on these devices is demanding. The hardware, mobile phone applications and overall design are, in most cases, unique to the manufacturer and model. In some scenarios, physically accessing devices can provide an opportunity to extract forensically valuable data. According to previous studies by OWASP's top 10 IoT project, many IoT devices are vulnerable. This includes the digital and physical security aspects of the device. There have been numerous studies on individual devices, many using a vulnerability to access the device. Although vulnerabilities are often quickly patched, it is noticeable that several jurisdictions are inducing legal requirements for IoT devices to be secured. This is due to growing security concerns and the number of insecure IoT devices on the market. A popular IoT device was selected and examined, highlighting the importance of applying an appropriate forensic process when physically accessing these devices. The focus was on extracting forensic data using various appropriate methods, in this case, probing the Universal Asynchronous Receiver-Transmitter (UART) ports. The test device was accessed using UART, and it was then possible to discover the device's root password. The password was hardcoded and was not uniquely generated for every device, highlighting the security concerns targeted in recent legislation. Findings throughout the research allow a digital forensic investigator to access and extract data. This could potentially increase the chance of obtaining relevant evidence during an investigation.

Keywords: IoT, cybersecurity, data extraction, firmware, computer forensics, OWASP

Cybersecurity and local Government: Imperative, Challenges and Priorities

Mmalerato Masombuka[1], Marthie Grobler[2] and Petrus Duvenage[3]

[1]University of Stellenbosch, South Africa
[2]CSIRO's Data61, Melbourne, Australia
[3]University of Johannesburg, South Africa

mmalerato.mc@gmail.com
marthie.grobler@data61.csiro.au
duvenage@live.co.za
DOI: 10.34190/EWS.21.501

Abstract: The South African government's pursuit of widespread internet access, its increasing use of and reliance on digital services as well as the emergence of new technologies have given rise to new threats and risks of cyberattacks. An effective cybersecurity approach in countering these threats requires a coherent effort involving all spheres of government. However, given the government's three-tiered structure (national, provincial, and local government), there seems to be disproportionality in the cybersecurity approach. Without distracting from the importance of cybersecurity at a national level, it is imperative for cybersecurity at provincial and local government to be prioritised, resourced and fit for purpose. While there are commonalities between these spheres, the contexts within which provincial and local government functions differ from the national. Thus, the one size fits all cybersecurity approach being employed by the national government is neither sufficiently inclusive nor fully downward scalable. The continuous evolution of cyberspace and the associated threats call for a concurrent and continuous adaptation in the approaches employed to build resilient cybersecurity on all levels of government. If not, local government, in particular, will continue to be an attractive target and a weak chink in the government's cybersecurity armour. Therefore, this paper aims to contribute to the discourse on cybersecurity at the local government level. In our focus on the insecurity that local governments face in the cyber domain, we use South Africa as an illustrative example. The paper discusses the imperative of raising the cybersecurity bar at local government level and examines the challenges in this regard. We then proceed with proposing key priorities that local government could implement to enhance cyber security - as part of which we explore the application of the Australian Signals Directorate's

Cyber Security Centre's Essential Eight Maturity Model and the NIST Cyber Security Framework (CSF) to local government.

Keywords: cybersecurity, cyberthreats, cyber resilience, local government, National Cybersecurity Policy Framework (NCPF)

KSA for Digital Forensic First Responder: A job Analysis Approach

Ruhama Mohammed Zain, Zahri Yunos, Nur Farhana Hazwani, Lee Hwee Hsiung and Mustaffa Ahmad

CyberSecurity Malaysia, Cyberjaya, Malaysia

ruhama@cybersecurity.my, zahri@cybersecurity.my, farhana.hazwani@cybersecurity.my, hh.lee@cybersecurity.my, mus@cybersecurity.my
DOI: 10.34190/EWS.21.002

Abstract: The role of cybersecurity professionals is important in protecting the computer network in many organizations. Indeed, it is a big challenge to find highly skilled talents when it comes to specialized areas such as Digital Forensics First Responders (DFFR). We need more cybersecurity knowledgeable workers and experts, people with the right know-how to tackle rapidly evolving cyberattacks, risks and threats. The job analysis workshop in this study is an exploratory research method used to collect data through group interaction. This method provides an opportunity to observe the interaction among participants on the topic under study. This paper contributes to the findings of DFFR job analysis conducted by CyberSecurity Malaysia. Eight (8) participants took part in the job analysis workshop, comprising representatives from academia, government and industry. The findings summarize a set of Knowledge and Skills elements required to support a list of DFFR job tasks. The framework provides principal guidelines for training developers and end-users in developing training programs, with focus on competency-based assessment. This is useful for developing training courses and assessment questions towards DFFR certification. Some lessons learned from the job analysis process provide opportunities for improvement in future job analysis workshops.

Keywords: competency framework, cybersecurity professional, cybersecurity education, KSA

The Unrehearsed Boom in Education Automation, Amid COVID-19 Flouts, a Potential Academic Integrity Cyber Risks (AICR)!

Fredrick Ochieng' Omogah

Medical Informatics, I.T & Computer Sciences at the Uzima University, Kisumu, Kenya

fo2001ke@yahoo.com
fomogah@gmail.com
DOI: 10.34190/EWS.21.090

Abstract: Covid-19, a Severe Acute Respiratory Syndrome SARS-CoV-2, is an aggressive and infectious disease responsible for massive health havoc and resulting in high mortality rates globally. As a result, on 11th March 2020, the WHO declared Covid-19 a world pandemic due to its grievous impact on human health and livelihood. Learning and teaching in institutions have been disrupted following lockdowns and subsequent closures of all learning institutions across the globe. This pandemic has been quite surging. Many renowned professors and doctors in Kenyan and African academia have perished. Kenya and Africa are left with no choice in education but to use online platforms. The unrehearsed boom in education automation by universities may be a potential academic integrity cyber risk because this rush is more than anticipated. Even though the pandemic could be a wake-up call, industry players and stakeholders should re-design the education sector to be compatible with the emerging digital economies and globalized villages we currently live in. As a challenge during the 21st Century, Covid-19 has forced many organizations to shift their day-to-day activities to rely more on technology, and our universities have not been left behind. One may ask, "Under what circumstances is the shift to and reliance on technology taking place?" Covid-19 could be a silver lining for education which is a great idea; however, education automation should NOT only be focused on the pandemic and how well technology can be used as a new "normal" but also how bad things can get in the event of technology failures and potential criminal conducts. Technology alone can never be a solution to automation. Better approaches MUST include People, Process then technology (PPT) so that a formal way for aligning technology with education strategies can be achieved to nurture best practices and controls for successful education automation implementation.

Keywords: impact on human health, online learning platforms, education automation, academic integrity cyber risks, learning management system, unrehearsed education

How Penetration Testers View Themselves: A Qualitative Study

Olav Opedal

Opedal Consulting LLC, Ellensburg, USA

olav@opedalconsulting.com
DOI: 10.34190/EWS.21.058

Abstract: Many organizations understand they need penetration testers to identify network security weaknesses. In response, penetration testing has become required for most major organizations. As a result, penetration testing became a cyber security occupation. Penetration testers perform activities similar to criminal hackers with one major difference: penetration testers work on behalf of the organization and they do not attempt to criminally exploit the organization. Earlier research identified that penetration tester personality traits are different from other computer professionals personality traits. Little is known about how professional penetration testers view themselves. Little research exists studying the use of hacking methods from the perspective of the penetration testers themselves. This qualitative study sought to increase understanding about penetration tester traits by exploring the views of penetration testers. The study included interviews with thirteen red team members at a global software firm in the Pacific Northwest.

Keywords: qualitative content analysis, latent Dirichlet allocation, topic modeling, penetration testers

Cyber Range: Preparing for Crisis or Something Just for Technical People?

Jani Päijänen[1], Karo Saharinen[1], Jarno Salonen[2], Tuomo Sipola[1], Jan Vykopal[3] and Tero Kokkonen[1]

[1]JAMK University of Applied Sciences, Jyväskylä, Finland
[2]VTT Technical Research Centre of Finland, Tampere, Finland
[3]Masaryk University, Brno, Czech Republic

jani.paijanen@jamk.fi, karo.saharinen@jamk.fi, jarno.salonen@vtt.fi, tuomo.sipola@jamk.fi, vykopal@ics.muni.cz, tero.kokkonen@jamk.fi
DOI: 10.34190/EWS.21.012

Abstract: Digitalization has increased the significance of cybersecurity within the current highly interconnected society. The number and complexity of different cyber-attacks as well as other malicious activities has increased during the last decade and affected the efforts needed to maintain a sufficient level of cyber resilience in organisations. Due to Industry 4.0 and the advanced use of IT and OT technologies and the adaptation of IoT devices, sensors, AI technology, etc., cybersecurity can no longer considered to be taken lightly when trying to gain a competitive advantage in business. When transferring from traditional reactive cybersecurity measures to proactive cyber resilience, cyber ranges are considered a particularly useful tool for keeping the organisation in the game. With their background in defence research (e.g., DARPA NCP in 2008), cyber ranges are defined as interactive simulated platforms representing networks, systems, tools, and/or applications in a safe, legal environment that can be used for developing cyber skills or testing products and services. Cyber ranges can be considered vital in facilitating and fostering cybersecurity training, certification, and general education. Despite the definition, cyber ranges seem to be only used by military or so-called "technical people" when quite a few more organisations could benefit from them. This article attempts to reveal the secrets behind cyber ranges and their use focusing on suitable target environments, common functions, and use cases. Our main objective is to identify a classification of cyber ranges and skills related to these diverse types of ranges. We emphasise the cyber resilience of any type of organisation that demands the use of cyber range type of training. Different training scenarios improve different sets of organisational skills. The article is based on an extensive survey on cyber ranges, their use, and technical capabilities that was conducted in CyberSec4Europe project.

Keywords: cyber range, cyber resilience, cyber training, organisational skills, cybersecurity

Multiple-Extortion Ransomware: The Case for Active Cyber Threat Intelligence

Bryson Payne and Edward Mienie

University of North Georgia, Dahlonega, USA

bryson.payne@ung.edu
edward.mienie@ung.edu
DOI: 10.34190/EWS.021.075

Abstract: In just over three decades since its introduction, ransomware has become a primary security risk to businesses and users, and it is now the fastest-growing category of cybercrime. In addition, ransomware attacks on healthcare, energy and water distribution, and defense contractor organizations have begun to impact both human security and national security. Traditional ransomware encrypts files on an infected computer to block users' access until a sum of money or ransom is paid, often via cryptocurrencies like Bitcoin or Ethereum. Businesses and individuals who fall victim to ransomware are faced with the expense of paying the ransom, restoring files from backup if available, or losing files altogether and starting from scratch. Beginning in late 2019, cybercriminals stepped up their game by deploying new attacks known as "double-extortion" ransomware, wherein files are stolen before being encrypted. Even if an organization might be able to recover its data from backups, by stealing the files first, the attacker can still profit either by selling any confidential data on the dark web or by further extorting the business and threatening to leak sensitive information unless an even larger ransom is paid. As of 2021, double-extortion ransomware is still in its infancy, but the authors anticipate and describe possible long-term trends toward even more persistent multiple-extortion tactics, in which stolen data could continue to be used by cybercriminals, terrorists, and rogue nation-states potentially decades in the future. Traditional, passive measures in cybersecurity and business continuity, like firewalls, antivirus software, and frequent backups, are not sufficient to protect organizations from this new type of data theft and extortion enterprise. Government agencies and private corporations alike are beginning to employ active cyber threat hunters and intelligence analysts to detect and neutralize this newest class of persistent threat. This research examines multiple approaches to more advanced defense against such threats, including the emerging roles of cyber threat hunting and cyber threat intelligence, and the impact of this new type of tradecraft on both current and future multiple-extortion ransomware tactics.

Keywords: ransomware, malware, cyberattacks, cybersecurity, cyber threat hunting, cyber threat intelligence

Resilience Management Concept for Railways and Metro Cyber-Physical Systems

Jyri Rajamäki

Laurea University of Applied Sciences, Espoo, Finland

jyri.rajamaki@laurea.fi
DOI: 10.34190/EWS.21.074

Abstract: Railways and metros are good examples of cyber-physical systems (CPS). They are safe, efficient, reliable and environmentally friendly. However, being such critical infrastructures turns metro, railway and related intermodal transport operators into attractive targets for cyber and/or physical attacks. SAFETY4RAILS H2020 project of the European Commission delivers methods and systems to increase the safety and resilience of track-based inter-city railway and intra-city metro transportation. Safety engineers have established strategies over decades to remove risks and increase safety that become manifest in railway systems. On the other hand, resilience is a multi-faced and not yet standardized concept so that a number of definitions and assessment methods exist, and until now, resilience management has largely focused on descriptive or diagnostic analytics following an expert judgment-based approach. This paper aims at introducing a conceptualization for resilience management of CPS and to bring the lessons to be learned from earlier projects for SAFETY4RAILS. The approach, earlier studied in the healthcare sector, is based on an integration of the concept of cyber-trust with cybersecurity science and resilience science. The paper proposes five principles that arise from the theory for resilience management processes of CPS: (1) design and implement a security management plan, (2) employ all appropriate security technologies, (3) ensure the adequacy and quality of security information, (4) make sure that situational awareness is always up to date, and (5) design and implement a resilience management plan that covers all four event management cycles (plan/prepare, absorb, recovery, adapt) and interdependencies with other systems. In addition, the paper discusses the meaning of these principles in the rail transportation sector. The paper represents the author's views having taken part in SAFTEY4RAILS stakeholder workshops as part of the stakeholder needs and requirements analysis in the early stages of the project.

Keywords: cybersecurity, resilience management, cyber-physical systems, SAFETY4RAILS project, rail transportation systems

Digital Evidence in Disciplinary Hearings: Perspectives From South Africa

Trishana Ramluckan[1, 2], Brett van Niekerk[1] and Harold Patrick[1]

[1]University of KwaZulu-Natal, South Africa
[2]Educor Holdings, South Africa

ramluckant@ukzn.ac.za
vanniekerkb@ukzn.ac.za
patrick@ukzn.ac.za
DOI: 10.34190/EWS.21.024

Abstract: The prevalence of digital communications results in the need for presenting digital evidence in legal and disciplinary hearings. Whilst South African legislation does provide some guidelines for the use of digital evidence, labour laws do not explicitly consider digital evidence and its role in disciplinary hearings is not explicitly guided. This may result in improper use of digital evidence during disciplinary hearings, which may result in unfair labour practices. This paper considers South African legislation and best practice documents to identify challenges of digital evidence and provide recommendations for improving organisational use of digital evidence in internal proceedings.

Keywords: digital evidence, forensic investigation, labour law, digital media preservation, standards

Security and Safety of Unmanned Air Vehicles: An Overview

Sérgio Ramos, Tiago Cruz and Paulo Simões

University of Coimbra, CISUC, DEI, Portugal

sdramos@dei.uc.pt
tjcruz@dei.uc.pt
psimoes@dei.uc.pt
DOI: 10.34190/EWS.21.027

Abstract: Cyber-physical systems permeate the fabric of our society, being a crucial part of what makes it possible. As such, ensuring their security is a primal concern that cannot be neglected, whether it relates to essential services, transportation or factories. But new scenarios and use cases are emerging, which require equal

concern and care, as it is the case for Unmanned Air Vehicle (UAVs) technologies. Over the past years, several technological developments made it possible to create effective and inexpensive embedded computing and communications capabilities which, in their turn, were crucial for the development of modern UAVs. Such vehicles are quite diversified in terms of form and function, encompassing a wide range of implementations, from conventional drones to quad or octocopters. UAVs can be quite versatile, having found different applications, from leisure to warfare. Even though UAVs can help achieving better performance for transportation, surveillance, agriculture and healthcare, this technology shares most of the risks and dangers of IoT devices, since UAVs, or Drones, are devices with multiple sensors that can be integrated on Wireless Sensor Networks (WSNs), in a similar way as an IoT device. Drones are a doorway from the digital world to interact directly in the physical world. It is predicted that as more and more UAVs are being produced, passing from thousands to millions of drones on air every day, it increases the chance of someone hacking a drone and, for example, making it collide with a rotor of an airplane. Even though drones may not have sheer firepower, their speed and mass mean they still constitute a potential danger in many scenarios, with potentially catastrophic results. Therefore, it is vital to understand the security risks and vulnerabilities associated with UAVs in order to develop mechanisms to ensure proper safety requirements, also fostering general trust and paving the way for new services and opportunities. This paper presents an overview on the most recent developments on drone security and safety. It also presents a comparison between UAVs and IoT devices, highlighting the similarities between IoT and drone cybersecurity issues. Finally, it proposes possible solutions and countermeasures for other UAV vulnerabilities and their feasibility on the constrained field of drone ecosystems.

Keywords: unmanned air vehicles, internet of things (IoT), cybersecurity, cyber warfare

The Rising Power of Cyber Proxies

Janine Schmoldt

University of Erfurt, Faculty of Economics, Law and Social Sciences, Germany

janine.schmoldt@uni-erfurt.de
DOI: 10.34190/EWS.21.068

Abstract: More and more states support cyber proxies. States work with proxies rather than sanctioning them. This is because cyber proxies are incredibly useful –

they not only enhance the cyber warfare capabilities of the supporting states, they also provide them with a degree of plausible deniability. This ascent a future superpower status. China for instance uses cyber proxies in order to "deter the United States (…)" which "may ensure eventual strategic parity with the United States in technological and military prowess" (Hjortdal 2011). Simultaneously, cyber proxies are seen as an inherent threat to the stability of nation states as they are capable of subverting the national and political stability. Is then the support of cyber proxies not inconsistent with the aim to limit potential threats to the stability of nation states? Through the support of nation states, cyber proxies can enhance their technical skills with the result, that they elevate their political role. Cyber proxies have become extremely powerful, supporting them means that they are directed "away from operating against the state" (Hang 2014). Thus, even more governments have decided that it is better to work with rather than against cyber proxies. But this also leads to the question of whether states can be held responsible under international law for the actions of the cyber proxies and hackers.

Keywords: cyber proxies, cyberwarfare, patriotic hackers, international law

Connected, Continual Conflict: Towards a Cybernetic Model of Warfare

Keith Scott

De Montfort University, Leicester, UK

jklscott@dmu.ac.uk
DOI: 10.34190/EWS.21.046

Abstract: "Our enemies are innovative and resourceful, and so are we. They never stop thinking about new ways to harm our country and our people, and neither do we." (George W. Bush) The purpose of this paper is to argue that to see 'cyber warfare' as a discrete form of combat, or as merely a combination of Electronic and Information Warfare, is a fundamental error. We must see 'cyber' as shorthand for 'cyberNETIC', and cyber warfare as a form of conflict which operates across all domains, and where action in one domain inevitably influences other zones of conflict. The UK military is seeking to reshape itself according to the concept of Integrated Operating, and this paper contends that such a model is essential. Marshall McLuhan defined World War 3 as 'a guerrilla information war with no division between military and civilian participation'; a cybernetic conflict is infinitely more complex, erasing the boundaries between kinetic and non-kinetic warfare, between civilian and military, and indeed between peace and war

themselves. The paper will consider a scenario demonstrating what such a multi-domain conflict might be like, considering the use of non-human combatants operating in cooperation and against human forces, and the impossibility of maintaining a clear division between 'war' and 'operations other than war'. Ultimately, it will contend that the current structures of military forces are too rigid and rooted in earlier eras of warfare to allow us to respond effectively to the conflicts that await us in the all-too-near future. Norbert Wiener sought to avoid applying his knowledge of cybernetics to the military domain; this paper argues that it must be done. It is, in short, the most useful theoretical framework for waging hybrid, non-linear warfare.

Keywords: cyber warfare, strategy, hybrid warfare

Emergency Response Model as a Part of the Smart Society

Jussi Simola[1,2], Martti Lehto[1] and Jyri Rajamäki[2]

[1]University of Jyväskylä, Finland
[2]Laurea Universtiy of Applied Sciences, Finland

jussi.hm.simola@jyu.fi
martti.j.lehto@jyu.fi
jyri.rajamaki@laurea.fi
DOI: 10.34190/EWS.21.079

Abstract: Centralized hybrid emergency model with predictive emergency response functions are necessary when the purpose is to protect the critical infrastructure (CI). A shared common operational picture among Public Protection and Disaster Relief (PPDR) authorities means that a real-time communication link from the local level to the state-level exists. If a cyberattack would interrupt electricity transmission, telecommunication networks will discontinue operating. Cyberattack becomes physical in the urban and maritime area if an intrusion has not been detected. Hybrid threats require hybrid responses. The purpose of this qualitative research was to find out technological-related fundamental risks and challenges which are outside the official risk classification. The primary outcomes can be summarized so that there are crucial human-based factors that affect the whole cyber-ecosystem. Cybersecurity maturity, operational preparedness, and decision-making reliability are not separate parts of continuity management. If fundamental risk factors are not recognized, technical early warning solutions become useless. Therefore, decision-makers need reliable information for decision-making that does not expose them to hazards. One of the primary aims of

hybrid influence is to change political decision-making. Practically, this means a need to rationalize organizational, administrative, and operative functions in public safety organizations. Trusted information sharing among decision-makers, intelligence authorities, and data protection authorities must be ensured by using Artificial Intelligence (AI) systems. In advanced design, protection of critical infrastructure would be ensured automatically as part of the cyber platform's functionalities where human-made decisions are also analyzed. Confidential information sharing to third parties becomes complicated when the weaknesses of crucial decision-making procedures have recognized. Citizens' confidence in the intelligent system activities may strengthen because of the decision-making process's reliability. Existing emergency response services are dependent on human ability.

Keywords: critical infrastructure protection, cyber ecosystem, emergency response, public protection, and disaster relief, artificial intelligence

Joint All-Domain Command and Control and Information Warfare: A Conceptual Model of Warfighting

Joshua Sipper

Air Force Cyber College, Air University, Montgomery, USA

jasipper@gmail.com
DOI: 10.34190/EWS.21.018

Abstract: A riot of change strategically and operationally has erupted within the joint force, drawing in two powerful concepts: joint all-domain operations (JADO) and information warfare (IW). With renewed emphasis on IW with the cyber-enabled construct including the consequential information related capabilities (IRC) of information operations (IO), intelligence, surveillance, and reconnaissance (ISR), and electromagnetic warfare (EW), and a cross-cutting requirement for joint all-domain command and control (JADC2), the joint force is on the cusp of a significant strategic shift. The following paper and its discussion will explore linkages between IW and JADC2, explain how IW benefits and enables JADC2, and present a conceptual model detailing how IW and JADC2 can work together to produce operational effects and advance US strategic interests now and into the future.

Keywords: cyber, information, warfare, intelligence, joint

Defensive Cyber Deception: A Game Theoretic Approach

Abderrahmane Sokri

DRDC CORA, Ottawa, Canada

Sokriab@gmail.com
DOI: 10.34190/EWS.21.077

Abstract: While traditional protective and reactive measures in cyberspace are crucial for cyber security, they cannot be a panacea against all sophisticated and well organized adversaries. Cyber deception reasoning has been recognized as a well-suited solution to enhance traditional security controls. Deception is a technique used to mislead attackers, increase their uncertainty, and push them to behave against their interests. This paper offers a new game formulation and a formal discussion on the strategic use of honeypots in network security. The adversarial interaction is formulated as a leader-follower game where the defender disguises honeypots as normal systems. Results indicate that the attacker would target the most valued system no matter what its state is (fake or normal). The most valuable target is identified using the financial concept of Exceedance Curve. This curve is derived by randomizing each reward and cost in the expected utilities of the defender and the attacker. A case study is presented and discussed to illustrate the suggested game and characterize its equilibria.

Keywords: game theory, leader-follower game, problem of common knowledge, cyber-defence, cyber-attack, cyber-security, exceedance curve, deception, honeypot

Using Semantic-Web Technologies for Situation Assessments of Ethical Hacking High-Value Targets

Sanjana Suresh, Rachel Fisher, Radha Patole, Andrew Zeyher and Thomas Heverin

Drexel University, USA

ss5264@drexel.edu, rcf49@drexel.edu, rdp74@drexel.edu, az458@drexel.edu, th424@drexel.edu

DOI: 10.34190/EWS.21.070

Abstract: Ethical hacking consists of scanning for targets, evaluating the targets, gaining access, maintaining access, and clearing tracks. The evaluation of targets represents a complex task due to the number of IP addresses, domain names, open ports, vulnerabilities, and exploits that must be examined. Ethical hackers synthesize data from various hacking tools to determine targets that are of high value and that are highly susceptible to cyber-attacks. These tasks represent situation assessment tasks. Previous research considers situation assessment tasks to be tasks that involve viewing an initial set of information about a problem and subsequently piecing together more information to solve the problem. Our research used semantic-web technologies, including ontologies, natural language processing (NLP), and semantic queries, to automate the situation assessment tasks conducted by ethical hackers when evaluating targets. More specifically, our research focused on automatically identifying education organizations that use industrial control system protocols which in turn have highly exploitable vulnerabilities and known exploits. We used semantic-web technologies to reduce an initial dataset of 126,636 potential targets to 155 distinct targets with these characteristics. Our research adds to previous research on situation assessment by showing how semantic-web technologies can be used to reduce the complexity of situation assessment tasks.

Keywords: ontology modeling, situation assessment, target evaluation

Educating the Examiner: Digital Forensics in an IoT and Embedded Environment

Iain Sutherland[1], Huw Read[1, 2] and Konstantinos Xynos[1, 3]

[1]Noroff University College, Agder, Norway
[2]Norwich University, Northfield, USA
[3]MycenX Consultancy Services, Stuttgart, Germany

iain.sutherland@noroff.no
hread@norwich.edu
kxynos@mycenx.com
DOI: 10.34190/EWS.21.041

Abstract: The Internet of Things (IoT) is an interconnected world of semi-autonomous systems capable of automation, communication and monitoring. It encompasses all manner of systems and embedded devices, communicating using various protocols and standards. Sometimes these devices are purpose built for commercial or industrial environments and at other times generic builds provide domestic solutions. These systems have the potential to hold a significant amount of information on user preferences and activities as well as on the surrounding environment. Some data will usually reside on the device itself, or as seen in many cases, within a manufacturer supported cloud solution. Mobile and web applications will then provide a way to interface with the data or the device. The question arises as to the readiness of the Digital Forensic Examiner. There is a requirement to correctly identify the value of IoT and embedded systems at the crime scene. Once identified, the examiner needs the skill and knowledge to access, interpret and present the information that may be contained in this ever-expanding wide variety of devices found in home and work environments. The skills required by the Digital Forensic Examiner has progressed further from the analysis of hard drives and file systems. It must address the growing demand and requirement to be able to understand how embedded firmware operates. In some cases, this includes interpreting embedded code, memory structures and proprietary file formats. This paper discusses the increasing complexity of the changing environment. It reviews the types of skills and training needs and the subject areas for consideration when training forensics examiners over the next five to ten years.

Keywords: digital forensics, IoT, investigative strategy, training, skill sets

Interdependence of Internal and External Security

Ilkka Tikanmäki[1], and Harri Ruoslahti[1]

[1]Security and Risk Management, Laurea University of Applied Sciences, Espoo, Finland
[2]Department of Warfare, National Defence University, Helsinki, Finland

Ilkka.tikanmaki@laurea.fi
harri.ruoslahti@laurea.fi
DOI: 10.34190/EWS.21.112

Abstract: Changes in the security environment, affecting both internal and external security, have been rapid in recent times. Security challenges related to hybrid phenomena, cybersecurity and organized cross-border crime significantly influence the development of the security environment. Global interdependence contributes to the nature of security, e.g., within the EU the free movement of goods and people have increased interdependence. The importance of situational awareness created and shared jointly by security actors is based on up-to-date information and assessments. Seamless cross-administrative collaboration promotes situational awareness (SA) and real-time situation picture. Thus, situational awareness is important for decision-making at different levels in various operating environments. Preparing for threats in accordance with the principle of total security is to safeguard the vital functions of society through cooperation between authorities, business, organizations, and citizens. Preparedness is a matter of comprehensive security and the vital functions in society involve cooperation between authorities, organizations, and citizens. As the operational environment is constantly changing, it has become increasingly difficult to distinguish between internal and external security and responding to changing threats may require revisions in policies and practices, and improved cooperation between actors. Significant changes in security situations may require addressing jurisdiction for security authorities and other actors, as jurisdiction is always based on the law. Effective cooperation between authorities requires responsible management, confidentiality, and appropriate allocation of resources. On an individual level, commitment, cooperative spirit, and personal contacts become critical to the success of collaborative work. The Common Operational Picture (COP) is a tool for achieving a good level of situational awareness, which in turn requires improved decision-making abilities and precise responses to situations that may arise. Positive developments are taking place in the field of information systems and information exchange between authorities. As threats change, so should the policies of states' internal and external security authorities be considered, also

requiring reviewing the competences of these authorities, and how national legislation enables the security authorities to act in the face of possible threats.

Keywords: comprehensive security, internal security, external security, cooperation, situation picture, situation awareness, hybrid, common information systems

The Host Nation Support for the International Cyber Operations

Maija Turunen

Finnish National Defence University, Helsinki, Finland

maijaturunen@yahoo.com
DOI: 10.34190/EWS.21.017

Abstract: International cooperation is one way to strengthen a state's cyber sovereignty, defense and create deterrence against potential adversaries. The provision or receipt of the international assistance may be considered in situations where the state is threatened or has already been the subject of an attack or military pressure contrary to the international law. A state may also allow foreign military forces to use its territory to defend a third state from an unlawful attack. The provision or receipt of the international assistance may also be considered in the situations where the humanitarian intervention is targeted at a third state. The host nation support has traditionally focused on logistical and/or material support to foreign forces on the soil of the host nation. This support may also have a cyber dimension, which makes the legal assessment of the support more complex. The nature and objectives of the operation, as well as the international law commitments of the host nation, affect the assessment of the international law and the operational challenges. In addition to legal challenges, the host nation support may also involve military, economic, political and technical challenges, such as interfaces with private actors. This paper focuses on the challenges considering the operational preparation of the environment in cyberspace. The aim is to identify, at a general level, problems that need to be resolved by the host nation before the international assistance can be provided or received. Theoretically the paper is based on the theory of the character of war, the preconditions for when the war can be waged and how the war should be waged, as well as what military actions are legitimate in war. Due to the research question, support for the cyber operations, this theory specifically applies to activities in the gray area, just before the actual escalation of the hostilities. This paper concludes that the host nation's

military cyber sovereignty affects how flexibly the international assistance for cyber operations can be provided or received.

Keywords: host nation support, cyber operations, international assistance, international law, cyber sovereignty

A GDPR Compliant SIEM Solution

Ana Vazão[1], Leonel Santos[1,2], Adaíl Oliveira[1,2] and Carlos Rabadão[1,2]

[1]School of Technology and Management, Polytechnic of Leiria, Portugal
[2]Computer Science and Communication Research Centre, Polytechnic of Leiria, Portugal

2170101@my.ipleiria.pt; leonel.santos@ipleiria.pt; adail.oliveira@ipleiria.pt; carlos.rabadao@ipleiria.pt
DOI: 10.34190/EWS.21.081

Abstract: Nowadays, cybersecurity is one of the greatest challenges that organizations are facing. One of the ways to deal with this challenge is the analysis and monitoring of computer security events to detect the numerous threats that can compromise your assets. Through the Security Information and Event Management (SIEM) systems, it is possible to carry out, in real time, the monitoring and analysis of the logs of the various systems of an IT infrastructure, and to detect and alert to possible security incidents. With the implementation of the General Data Protection Regulation (GDPR), organizations became stricter in ensuring the privacy of their employees' information, namely the data contained in the logs gathered in the various computer systems, and which contains personal data, such as IP addresses, usernames and systems accessed. Therefore, this regulation represents new challenges for the SIEM implementation. In this article, firstly the basic concepts of SIEM systems and their main functionalities were introduced. Later, the challenges posed by GDPR in the implementation of SIEM systems were also presented, namely the mandatory anonymization and pseudonymization of the sensitive data, the retention time of the logs and their encryption, and a set of technical measures that must be adopted during the implementation of a SIEM system. Afterwards, several open-source SIEM systems were compared, based on a literature review. Through this comparative study, an open-source SIEM system was elected to be used in a future implementation of a prototype, aimed to demonstrate the suitability of the technical measures previously identified as

necessary for the implementation of a GDPR compliant SIEM system. In short, with this work the authors intend to identify and validate the technical measures that must be implemented in a SIEM system, in order to comply with the objectives of this type of systems and in accordance with the requirements of the GDPR.

Keywords: SIEM, GDPR, security incidents, log files, monitoring, legislation and regulation

The Threat of Juice Jacking

Namosha Veerasamy

Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa

DOI: 10.34190/EWS.21.023

Abstract: Cyber attacks can affect the confidentiality, integrity and availability of data/ systems. Some attacks aim to steal data whereas others try cause destruction. One such vulnerability stems from the malicious use of USB chargers. When travelling and our smartphone battery level is very low, users may find a nearby charging station. However, users need to think twice before simply plugging in their device. What seems like an innocent charge could turn into a golden opportunity for attackers. Malware could actually be introduced into smartphones and other devices through the USB charger. Juice jacking is emerging as a potential risk as cyber criminals aim to infect users and potentially steal their passwords and infiltrate bank accounts. Users could even get locked out of their devices. This paper takes a closer look at this developing threat. These public charging stations are now being fraudulently used by attackers to gain access to sensitive information. Scammers are now using USB chargers as a method to steal data or install malware. However, users may be unaware of the potential risk. In this research, the malicious use of USB charging stations found in spots popular with travellers are revealed. In addition, protective measures are described in order to help users from falling victim to this latest cyber threat. Attackers try to take advantage of the situation in that most users trust their mobile devices more than their desktop devices. In addition to data theft, malicious attackers could also cause destruction of our mobile devices. When fast charging, malware could be installed onto a mobile device overwriting its firmware and arming it as a weapon. The firmware could be overwritten and the phone overloaded. The charger is thus compromised and used to overload a device. These various attack vectors are discussed in the paper to show the danger of juice jacking.

Keywords: juice jacking, USB, charge station

Status Detector for Fuzzing-Based Vulnerability Mining of IEC 61850 Protocol

Gábor Visky[1], Arturs Lavrenovs[1] and Olaf Maennel[2]

[1]NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

[2]Department of Computer Science, Tallinn University of Technology, Tallinn, Estonia

gabor.visky@ccdcoe.org
arturs.lavrenovs@ccdcoe.org
olaf.maennel@ttu.ee
DOI: 10.34190/EWS.21.007

Abstract: As smart grid technology and smart substations are becoming more common in power distribution, the use of the IEC 61850 protocol is increasing, as is the importance of the cybersecurity of the system's components. A vulnerable device can have a significant effect on the power supply in the event of a cyber-attack. The vulnerabilities of controlling devices should be identified and patched in the testing phase before deployment. Communication protocol fuzzing is a widely used, dynamic black-box testing method. It consists of sending billions of combinations of dynamically-generated incorrect input data to the device being examined and observing its behaviour. If an attempt is successful, a vulnerability can be discovered using the incorrect data as a starting point. Many IEC 61850-related vulnerability-mining research publications are available where the misbehaviour detection is based on the analysis of network traffic and the response of intelligent electronic devices (IEDs). It applies to the manufacturing message specification (MMS) protocol since it is used in the substation and determined by the client/server mode. By contrast, the generic object-oriented substation event (GOOSE) and sampled measure values (SMV) protocols are both based on a publish/subscription mechanism where no answer is expected from the clients. Therefore, other feedback solutions are needed. This paper describes a new solution. Instead of using the ping response and network traffic analysis to determine whether the device is functioning as intended, the application analyses the real-time video stream made on the human-machine interface of the tested device and the moment of the successful attempt is determined by machine learning model. Automatic video analysis can identify the input that caused an error. The paper introduces the challenges of vulnerability mining with fuzzing in

GOOSE and SMV protocols focusing on the indication of the status of the tested device and characterises the developed status detector. Finally, it describes the optimal size of learning datasets and the usability and reliability of the proposed solution.

Keywords: fuzzing, vulnerability mining, machine learning, generic object-oriented substation event, sampled measure value

Mobile Phone Surveillance: An Overview of Privacy and Security Legal Risks

Murdoch Watney

University of Johannesburg, South Africa

mwatney@uj.ac.za

DOI: 10.34190/EWS.21.021

Abstract: The discussion focuses on the collection, use and disclosure of personal information pertaining to a mobile phone and the circumstances in which state and corporate (non-state) surveillance may not be lawful. It highlights the tension between government, law enforcement agencies, companies, businesses and the users of mobile phones relating to mobile phone surveillance. It revolves around data control. It also touches on the ownership of information on a mobile phone and the apps downloaded on a smart phone. It emphasises that personal information has substantial value. There are many stakeholders who want access to this information. Law enforcement may wish access to it for investigating a crime whereas companies may want access to it to profit from it by means of advertisement revenue, for example. The issue of phone surveillance came under serious global scrutiny in 2013 when a United States (U.S.) National Security Agency (NSA) contractor, Snowden, disclosed that the NSA had secretly been building a vast database of US telephone records. The disclosure of the government's violation of privacy impacted negatively on government accountability and public trust. Seven years later in 2020, the U.S. Supreme Court of Appeals for the Ninth Circuit found that such warrantless bulk surveillance had been unconstitutional. Mobile phones were unfortunately not designed with the emphasis on privacy and security. Although state and non-state surveillance must take place within legislative parameters and should be subjected to checks and balances, the circumstances in which access to mobile phone information for various purposes may be gained and how it may be obtained, should be scrutinised regularly. Post Snowden the focus was mainly on state surveillance, but currently the enormity of the threat of surveillance capitalism is being appreciated. Corporate-enhanced

abilities to acquire, manipulate and sell personal information may seriously undermine privacy protection. This discussion provides an overview from a legal perspective of the various aspects pertaining to state and capitalistic (non-state/corporate) surveillance which may pose security and privacy risks to mobile phones users.

Keywords: mobile phone surveillance, collection, use and disclosure of mobile phone data, privacy and security risks of mobile phone usage, state surveillance, surveillance capitalism

PhD Research Papers

The Impact of GDPR Infringement Fines on the Market Value of Firms

Adrian Ford[1], Ameer Al-Nemrat[1], Seyed Ali Ghorashi[1] and Julia Davidson[2]

[1]School of Architecture, Computing and Engineering, University of East London, UK

[2]Royal Docks School of Business and Law, University of East London, UK

a.ford1701@uel.ac.uk

DOI: 10.34190/EWS.21.088

Abstract: Previous studies have shown (varying degrees of) evidence of a negative impact of data breach announcements on the share price of publicly listed companies. Following on from this research, further studies have been carried out in assessing the economic impact of the introduction of legislation in this area to encourage firms to invest in cyber security and protect the privacy of data subjects. Existing research has been predominantly US centric. This paper looks at the impact of the General Data Protection Regulation (GDPR) infringement fine announcements on the market value of mostly European publicly listed companies with a view to reinforcing the importance of data privacy compliance, thereby informing cyber security investment strategies for organisations. Using event study techniques, a dataset of 25 GDPR fine announcement events was analysed, and statistically significant cumulative abnormal returns (CAR) of around -1% on average up to three days after the event were identified. In almost all cases, this negative economic impact on market value far outweighed the monetary value of the fine itself, and relatively minor fines could result in major market valuation losses for companies, even those having large market capitalisations. A further dataset of four announcements where sizeable GDPR fines were subsequently appealed was also analysed and although positive returns for successful appeals were observed (and the reverse), they could not be shown to be statistically significant - perhaps due, at least in part, to COVID-19 related market volatility at that time. This research would be of benefit to business management, practitioners of cyber security, investors and shareholders as well as researchers in cyber security or related fields (pointers to future research are given). Data protection authorities may also find this work of interest.

Keywords: cyber security, data privacy breaches, market value, economic impact, GDPR, event study

Side Channel Attacks and Mitigations 2015-2020: A Taxonomy of Published Work

Andrew Johnson

Faculty of Computing, Engineering and Mathematics, University of South Wales, UK

andrew.johnson@southwales.ac.uk
DOI: 10.34190/EWS.21.035

Abstract: Side Channel Attacks (SCAs) have become a prominent area of both research and organisational cyber defence strategies in recent years. With the advent of microprocessor performance optimizations such as speculative execution and branch prediction enhancements to Intel processors in 1996, it is possible for an adversary to target the vulnerabilities that are inherent in the optimization design. This paper presents a taxonomy of published works on the theme of hardware based SCAs and some of their mitigations from the inclusive years 2015-2020. It includes research of peer reviewed published work including open access publications. The results of research undertaken represents a large proportion of papers during the time period from select searches across three online database sources: IEEE(Institute of Electrical and Electronic Engineers); ACM (Association for Computing Machinery) Digital Library; Scopus (Elsevier/Science Direct). The taxonomy includes 684 papers from both conference and journal article publications which include SCAs, mitigations and surveys. The choice of online databases used was based on the functionality of the search engines to enable a download of search results to a 'BibTex' format for data analysis. The aim of this work is to identify and present SCAs and mitigations with two objectives: To present the published work data analysis results from the searches that show the most common and varied scope of SCA hardware targets, methods, techniques, and mitigations. To identify trends in the SCA research field over the selected time period and also present some of the more recent SCA papers that expand future research prospects.

Keywords: side-channel attacks, side-channel mitigations, taxonomy, hardware

Sanctions and Cyberspace: The Case of the EU's Cyber Sanctions Regime

Eleni Kapsokoli

University of Piraeus, Greece
Laboratory of Intelligence and Cyber-Security

ekapsokoli@unipi.gr
elenikapsokoli1989@gmail.com
DOI: 10.34190/EWS.21.029

Abstract: Over the past years, the European Union has faced a number of cybersecurity challenges that range from cyberattacks to the critical infrastructure to cases of ransomware. In order to face these security challenges, the EU has developed all the necessary strategies and policies, including the launch of the Cyber Diplomacy Toolbox in 2017. This toolbox includes among others, the policy instrument of cyber sanctions (Council Decision 2019/796 and Council Regulation 2019/797). The purpose of this paper is to review the EU's cyber sanctions regime. In order to do that, we will apply key questions that have arisen in the sanctions literature and apply them in the case of the EU. In particular, we will examine the technical, political and judicial parameters, which involve the implementations of cyber sanctions. Issues like the reliable attribution of cyberattacks, the clarifications of relevant norms of responsible state behavior in cyberspace, the level of cooperation with the private sector and the scale and type of cyber sanctions are only some of the factors that will determine the success of the cyber sanctions regime. Having established a clear theoretical framework on the implementation of cyber sanctions, we will briefly review the empirical evidence, which involves the sanctions package that the EU announced on 17 May 2019 and the amending version published on 30 July 2020, against various entities and individuals. The end goal is to reach a conclusion on whether cyber sanctions are of symbolic nature, or can be considered as an effective policy instrument for the EU. This paper highlights the uses and limits of the EU cyber sanctions regime, which is a rather recent development and therefore under developed in the relevant literature.

Keywords: sanctions, cybersecurity, cyber sanctions, attribution, European Union

How the Civilian Sector in Sweden Perceive Threats From Offensive Cyberspace Operations

Joakim Kävrestad[1] and Gazmend Huskaj[1, 2, 3]

[1]School of Informatics, University of Skövde, Sweden
[2]Department of Military Studies, Swedish Defence University, Stockholm, Sweden
[3]Center for Asymmetric Threat and Terrorism Studies, Swedish Defence University, Stockholm, Sweden

Joakim.kavrestad@his.se
Gazmend.huskaj@fhs.se
DOI: 10.34190/EWS.21.106

Abstract: The presence of state-sponsored actors executing offensive cyberspace operations (OCO) has been made evident in recent years. The term offensive cyberspace operations encompass a range of different actions, including cyberespionage, disinformation campaigns, spread of malware and more. Based on an analysis of past events, it is evident that state-sponsored actors are causing harm to the civilian sector using OCO. However, the degree to which civilian organizations understand the threat from state-sponsored actors is currently unknown. This research seeks to provide new a better understanding of OCO and their impact on civilian organizations. To highlight this domain, the case of the threat actor Advanced Persistent Threat 1 (APT1) is presented, and its impact on three civilian organizations discussed. Semi-structured interviews were used to research how the threats from OCO and state-sponsored actors are perceived by civilian organizations. First, a computational literature review was used to get an overview of related work and establish question themes. Next, the question themes were used to develop questions for the interview guide, followed by separate interviews with five security professionals working in civilian organizations. The interviews were analysed using thematic coding and the identified themes summarized as the result of this research. The results show that all respondents are aware of the threat from OCO, but they perceive it in different ways. While all respondents acknowledge state-sponsored actors at a threat agent executing OCO, some respondent's argue that state-sponsored actors are actively seeking footholds in systems for future use while others state that the main goal of state-sponsored actors is to steal information. This suggests that the understanding of the threat imposed by OCO is limited, or at least inconsistent, among civilian security experts. As an interview study, the generalisability of this research is limited. However, it does demonstrate that the civilian society does not share a

common view of the threat from state-sponsored actors and OCO. As such, it demonstrates a need for future research in this domain and can serve as a starting point for such projects.

Keywords: cybersecurity, state-sponsored, advanced persistent threat, civilian, offensive cyberspace operations

Aviation Sector Computer Security Incident Response Teams: Guidelines and Best Practice

Faith Lekota and Marijke Coetzee

University of Johannesburg, South Africa

nombu30@gmail.com
marijkec@uj.ac.za
DOI: 10.34190/EWS.21.028

Abstract: The digitisation of the aviation sector provides benefits for passengers and consumers while at the same time introducing complexity, as the integration of legacy systems with new technologies is not straightforward. In this process, aviation systems vulnerabilities are making the industry more susceptible to attacks from cybercriminals. Cybercriminals exploit system vulnerabilities to compromise aviation systems, leading to significant disruptions and compromise of air transport safety. The emergence of cyber-attacks within the aviation industry has led to establishing the aviation sector Computer Security Incident Response Teams (CSIRTs). There is a general recognition that it is essential to build cyber resilience into aviation systems by ensuring better management of cyber-attacks and a willingness to share information on challenges and solutions. Unfortunately, the aviation sector CSIRTs are not commonly found across the world. In this regard, both the European Union (E.U.) and the United States of America (USA) are taking the lead by providing effective cybersecurity incident response services to their constituencies. The Aviation Information Sharing and Analysis Center (A-ISAC) was established in the United States of America (USA), while Europe is pursuing its initiative via the European Centre for Cyber Security in Aviation (ECCSA). This paper aims to analyse established aviation CSIRTs both in the European Union and the United States of America. The critical aspects such as team composition, services provided to constituencies, dissemination of information using secure and effective methods, collaboration with other CSIRTs, including best practice normative standards and legal compliance. The paper further outlines challenges in the management of aviation CSIRTs. Guidelines and lessons learned from globally

established aviation sector CSIRTs are gleaned due to the review to provide guidance when implementing an aviation sector CSIRT.

Keywords: aviation, CSIRTs, incident response, information sharing, collaboration, secure information dissemination

Biocyberwarfare and Crime: A Juncture of Rethought

Xavier-Lewis Palmer[1], Ernestine Powell[2] and Lucas Potter[1]

[1]Biomedical Engineering Institute, Department of Engineering and Technology, Old Dominion University, Norfolk, USA
[2]Department of Neuroscience, Christopher Newport University, Newport News, USA

xpalm001@odu.edu
ernestine.powell.12@cnu.edu
lpott005@odu.edu
DOI: 10.34190/EWS.21.073

Abstract: The existence of BCS (Biocybersecurity), alternatively known as Cyberbiosecurity (CBS), as a hybrid field has been established over the past few years that explores vulnerabilities created at cyber-bio and cyber-physical intersections. Institutional leads, like Murch and DiEuliis (2019), have set about mapping the enterprise, uncovering a wide variety of vulnerabilities affecting the numerous cyber-physical and bio-digital vulnerabilities in the fields that comprise it (Berger, 2020; DiEuliis, 2020). Scholars like George (2019) and Wang (2020), have discussed the national security implications of the field, in addition to groups such as the Blue Ribbon, an American Bipartisan Commission on Biodefense, who have started assessing the risks where biology and cyber technologies converge as of last year in terms of national biodefense (Evans and Selgelid, 2015; George, 2019; Jefferson et al, 2014; Riley, 2019; Wang, 2020). This is not exhaustive and it is accurate to say that there is much to define and address within the wide map that has been drawn. One of which is the proper delineation between biocyberwar and biocybercrime. As it is, this small but growing field exists at the nexus of cybersecurity and biological sciences, where cyber, cyber-physical, and biosecurity meet (Murch et al, 2018). These, by large, are owed to the manifold improvements or creations of improvements in biotechnology, biomedical engineering, and adjacent technologies that BCS can affect. This paper aims to explore a possible delineation between biocyberwarfare and biocybercrime in order to and start the conversation before the technologies sufficiently catch up.

Keywords: biocybersecurity, cyberbiosecurity, cybersecurity, crime, biosecurity

Matters of Biocybersecurity With Consideration to Propaganda Outlets and Biological Agents

Xavier-Lewis Palmer[1, 3], Ernestine Powell[2] and Lucas Potter[3]

[1]School of Cybersecurity, Old Dominion University Norfolk, USA
[2]Department of Neuroscience, Christopher Newport University, Newport News, VA, USA
[3]Biomedical Engineering Institute, Department of Engineering and Technology, Old Dominion University, Norfolk, USA

xpalm001@odu.edu
ernestine.powell.12@cnu.edu
lpott005@odu.edu
DOI: 10.34190/EWS.21.085

Abstract: The modern era holds vast modalities in human data utilization. Within Biocybersecurity (BCS), categories of biological information, especially medical information transmitted online, can be viewed as pathways to destabilize organizations. Therefore, analysis of how the public, along with medical providers, process such data, and the methods by which false information, particularly propaganda, can be used to upset the flow of verified information to populations of medical professionals, is important for maintenance of public health. Herein, we discuss some interplay of BCS within the scope of propaganda and considerations for navigating the field.

Keywords: biocybersecurity, cyberbiosecurity, cybersecurity, public health, biosecurity

Bio-Cyber Operations Inspired by the Human Immune System

Seyedali Pourmoafi and Stilianos Vidalis

University of Hertfordshire, Hatfield, Hertfordshire

S.pourmoafi@herts.ac.uk
S.vidalis@herts.ac.uk
DOI: 10.34190/EWS.21.089

Abstract: Bio-Cyber operation is a new field of research that is inspired by the Human Immune System. The human body has found solutions for problems that cybersecurity professionals have been trying to resolve for the past few decades. Cybersecurity should draw lessons from the human immune system on how to detect and deter attacks. Systems and devices are likely to leak sensitive information or data. A 'cyber immune' technology can be used to detect unknown cyber-attacks and provide a powerful mechanism for defence. In this paper we focus on work that describes the recent advances on Bio-Cyber operations, and we present our conceptual cyber operations model. By looking into the field of human biology we aspire to provide significant insight into the bio-cybersecurity domain.

Keywords: Bio-Cyber operation, human immune system, biological-inspired computing

Space Cyber Threats and Need for Enhanced Resilience of Space Assets

Jakub Pražák

Faculty of Social Sciences, Charles University, Prague, Czechia

prazak.jakub94@gmail.com
DOI: 10.34190/EWS.21.006

Abstract: Space systems represent a vital part of great powers' critical infrastructure and are the concern of national security. Space provides essential civilian and military services which disruption would result in severe consequences leading from economic losses to catastrophic events. However, the emergence of "New Space" with an increased number of commercial enterprises and space systems, accompanied by the worsening relations between major space powers, raises severe concerns about space security and protection of space assets. In addition to that, most space systems are inherently dual-use; being a potential

subject of both civilian and military utilization and interest. Accordingly, space powers are actively engaged in developing advanced counterspace capabilities that could be used to their advantage. Nevertheless, despite the security risks, little focus is paid to protecting space assets against cyber-attacks and security breaches. Cyberattacks may diverge from theft or denial of information to control or destruction of satellite systems, their subcomponents, or supporting infrastructure. Cyber-attacks provide advantageous disruptive capability due to its limited attribution, range of effect, flexibility, accessibility and affordable cost. Moreover, space systems often lack substantial cyber resilience, and cyber-attacks can be combined with other counterspace capabilities such as electronic or kinetic anti-satellite weapons for decisive outcomes. Thus, the article aims to illuminate the opportunities and consequences of malicious space cyber operations and address cyber protection of space assets. The article elaborates on cyber threats that could be used for offensive and hybrid operations in outer space and discusses their implications for space relations and space warfare strategies. The emphasis is given on the space weaponization and perception of space as a new theatre of war in the reflection of the deficient space regime and the need for enhanced cyber resilience of space assets.

Keywords: space security, cyber security, satellite, cyber resilience, space weapon, space warfare

e-Health as a Target in Cyberwar: Expecting the Worst

Samuel Wairimu

Department of Mathematics and Computer Science, Karlstad University, Universitetsgatan 2, Sweden

samuel.wairimu@kau.se
DOI: 10.34190/EWS.21.054

Abstract: Healthcare organisations have become a key target for attackers as evidenced by the global increase in cyber-attacks. These cyber-attacks are attributed to various attackers who differ in motivations and skills, with the common motivation being financial gain due to the rich personal data contained in patients' health records. But what would happen if the motivation changed? What would happen if the motivation is driven by targeting key people, mass exploitation or taking lives? What would happen if a strategic cyber-attack knocks out a society's critical infrastructure? This article investigates the possibility of targeting e-Health in the context of cyberwar. It assesses the privacy in healthcare and compares the consequences and impact of conventional cyber-attacks within the healthcare

sector, against the consequences and impact of cyberwar on the same. The outcome indicates that e-Health in the context cyberwar could result to active reconnaissance of patient records, which could lead to the targeting of key and influential people through Personally Identifiable Information (PII), mass exploitation, and personal attacks derived from Personal Health Information (PHI), which could result to irreversible damage or death.

Keywords: e-Health, privacy, cyberwar, cyber-attack, critical-infrastructure, healthcare

Talos: A Prototype Intrusion Detection and Prevention System for Profiling Ransomware Behaviour

Ashley Charles Wood, Thaddeus Eze and Lee Speakman

University of Chester, UK

ashley.wood@chester.ac.uk
t.eze@chester.ac.uk
l.speakman@chester.ac.uk
DOI: 10.34190/EWS.21.026

Abstract: In this paper, we profile the behaviour and functionality of multiple recent variants of WannaCry and CrySiS/Dharma, through static and dynamic malware analysis. We then analyse and detail the commonly occurring behavioural features of ransomware. These features are utilised to develop a prototype Intrusion Detection and Prevention System (IDPS) named Talos, which comprises of several detection mechanisms/components. Benchmarking is later performed to test and validate the performance of the proposed Talos IDPS system and the results discussed in detail. It is established that the Talos system can successfully detect all ransomware variants tested, in an average of 1.7 seconds and instigate remedial action in a timely manner following first detection. The paper concludes with a summarisation of our main findings and discussion of potential future works which may be carried out to allow the effective detection and prevention of ransomware on systems and networks.

Keywords: IDS, IPS, IDPS, ransomware, WannaCry, CrySiS/Dharma

Masters Research Papers

The use of Neural Networks to Classify Malware Families

Theodore Drewes and Joel Coffman

United States Air Force Academy, USA

teddrew34@gmail.com
joel.coffman@usafa.edu
DOI: 10.34190/EWS.21.060

Abstract: Many antivirus vendors detect and classify malicious software, but there is little consensus among vendors regarding the label assigned to each malware sample. With an increase in malware capability, new malware uses "automation to generate new variants of themselves" (Thanh and Zelinka 2019), creating relationships implying underlying families of malware to which individual samples of malware belong. In this work, we explore using a neural network to classify the family of a given malware sample, which is a first step to unify vendors' labels into a single ground truth classification. A consistent taxonomy (i.e., classification scheme for malware) facilitates consistent communication regarding malware and improved malware detection. Experiments with a data set of 13,000 malware samples reveals the merits of our approach.

Keywords: malware classification, malware taxonomy, neural networks, machine learning

Employing Machine Learning Paradigms for Detecting DNS Tunnelling

Jitesh Miglani and Christina Thorpe

Technological University Dublin, Blanchardstown, Ireland

jmig1995@gmail.com
Christina.thorpe@tudublin.ie
DOI: 10.34190/EWS.21.052

Abstract: Domain Name System (DNS) is an integral protocol which makes the resources available on the world wide web accessible. In recent times, there has been significant attention given to the development of different attack vectors against this protocol, out of which, DNS tunnelling is one of the most lethal attacks. Hackers use DNS tunnelling as a covert channel to cover their traces, exfiltrate data, and bypass the security policies enforced by the firewalls. Intrusion detection

systems do not generally scan the DNS queries because it produces a lot of data which is not feasible to be analysed with a tool. This research proposes an active approach of detecting DNS tunnelling by capturing all packets in a local network and employing Machine Learning (ML) models to detect tunnelled data. The main aim of this research is to employ ML techniques to classify and separate DNS tunnelling packets from legitimate packets, compare the results generated based on their precision, detection time and computational effort, and determine an ideal solution for the problem. The research uses Ensemble Learning techniques which is a subset of Supervised ML to prepare a classifier that can detect DNS tunnelling. We also focus on the inherited implications of using ML which can be unknowingly faced while employing ML techniques, such as model overfitting, data bias, and complex and unrealistic model creation. The datasets used for this research are created using an emulated real-time network scenario. Our results show that ML classifiers can solve the problem of DNS tunnelling detection. Ensemble learning techniques outperforms decision tree by a large margin. Moreover, boosting models always produced better overall accuracy than bagging models, at the expense of a longer training time.

Keywords: DNS tunnelling, machine learning, attack detection

Analysis of API Driven Application to Detect Smishing Attacks

Pranav Phadke and Christina Thorpe

Technological University Dublin, Blanchardstown, Ireland

phadke.pranav09@gmail.com
christina.thorpe@tudublin.ie
DOI: 10.34190/EWS.21.051

Abstract: In the past decade, the use of mobile smart phones has increased exponentially. The pervasiveness of these devices has motivated criminals to design ways to exploit the mobile technology to obtain confidential information or to execute malicious software. The term used to describe these social engineering attacks using mobile phone technology is Smishing, which is a play on the previously well-known Phishing attack perpetrated over email. Smishing uses Short Message Service or SMS as its attack vector to send malicious Uniform Resource Locators (URLs) along with the text message. Users are more aware of phishing emails and there are a lot of detection mechanisms developed to avoid such attacks. However, SMS is often neglected, and considering the small size of the mobile screen compared to a computer, it is difficult to detect and manually verify

a phishing URL which is sent in a text message. When clicked, a smishing URL can either redirect the user to some phishing page or try to install a malicious payload on the mobile phone. Both scenarios are risky and can cause potential loss. The aim of this research is to develop a new application to detect Smishing attacks on Android devices by integrating existing phishing Application Program Interfaces (APIs) in a prototype application. The application is designed to run in the background and verify whether the URL in the text message is phishing or not. Five freely available APIs were tested on a dataset of 1500 URL to compare them in terms of accuracy and latency. Our results show that the VirusTotal API gives the most accurate detection rate of 99.27%, but the slowest response time of 12-15 seconds per query; the Safe-Browsing API, gives an 87% accuracy with 0.15ms response time. For time sensitive applications, Safe-Browsing would provide the best solution, however, for security sensitive applications, Virus Total would be a better option.

Keywords: phishing, smishing, application programming interface, cybersecurity, attack detection

Evolving Satellite Control Challenges: The Arrival of Mega-Constellations and Potential Complications for Operational Cybersecurity

Carl Poole, Mark Reith and Robert Bettinger

Air Force Institute of Technology, Wright-Patterson AFB, USA

Carl.Poole@afit.edu
Mark.Reith@afit.edu
Robert.Bettinger@afit.edu
DOI: 10.34190/EWS.21.082

Abstract: The introduction of automated satellite control systems into a space mission environment historically dominated by human-in-the-loop operations will require the extraneous establishment of cybersecurity measures to ensure space system safety and security. With the addition and expansive growth of the "mega-constellation," the old methods of satellite command and control are no longer cost effective. The proliferation of low Earth orbit (LEO) with thousands of satellites will require increasing levels of automation in order to handle internal operations, or the operations driven for the control of each constellation. The implementation of commercial off the shelf parts, coupled with on-board satellite computer systems that resemble the standard personal computer will allow for greater levels of

automation and, therefore, fewer human interactions required to control newer satellites. On the ground segment side of satellite control, the influx of privately owned communication antennas for rent and a move to cloud-based operations or mission centers will present new requirements in cyber protection for both DoD and commercial satellite operations. This paper will highlight the changes these technical advancements will bring to the current satellite control architecture. It will also discuss likely ways that industry will evolve with the implementation of new requirements like the Cybersecurity Maturity Model Certification, finishing with a proposed change to how space and cyber space professionals can realign their interactions in order to address any emerging threats. It is no longer a matter of if automation will play a significant role in satellite operations, but how fast can the satellite operators adapt to the onset of control automation to promote cybersecurity in an increasingly competitive, contested, and congested space domain. One way for promoting such cybersecurity in space control is to introduce cybersecurity/monitoring training at all levels of satellite operations to align with the desire of creating a highly digitally-capable Space Force.

Keywords: satellite automation, mega-constellations, cybersecurity, ground station service, software defined equipment, future space operations

Work in Progress Papers

Inter-Process CFI for Peer/Reciprocal Monitoring in RISC-V-Based Binaries

Toyosi Oyinloye, Lee Speakman and Thaddeus Eze

University of Chester, UK

t.oyinloye@chester.ac.uk
l.speakman@chester.ac.uk
t.eze@chester.ac.uk
DOI: 10.34190/EWS.21.115

Abstract: Attacks stemming from software vulnerabilities that cause memory corruption often result in control flow hijacks and hold a place of notoriety in software exploitation. Attackers take advantage of vulnerabilities due to programming flaws to execute malicious code for redirecting the intended execution flow of applications. Existing defences offer limited protection due to their specificity to system architecture, operating systems or hardware requirements and are often circumvented by increasingly sophisticated attack techniques. This paper focuses on securing applications that are built on and run on the Reduced Instruction Set Computer Five (RISC-V *pronounced risk-five*) architecture, which is fast becoming popular on embedded devices such as smartphones, tablets, or other Internet of Things. Studies have revealed different threats that could emerge in an environment that is based on RISC-V architecture, drawing attention to growing demands for more resilient protections for RISC-V binaries. A concept based on Control Flow Integrity (CFI) appears to give promising solutions to control flow hijacks via various forms of implementation. The innovation in this research proposes an implementation of CFI with scrambled labels and logging of rogue attempts on vulnerable RISC-V-based applications. This would subsequently be extended for peer/reciprocal monitoring between similar binaries on RISC-V platforms.

Keywords: control flow integrity, RISC-V, buffer overflow, memory corruption, cybersecurity

Use of Blockchain Technologies Within the Creative Industry to Combat Fraud in the Production and (Re)Sale of Collectibles

Alexander Pfeiffer[1, 2, 3], Stephen Bezzina[2, 3] and Thomas Wernbacher[1]

[1]Center for Applied Game Studies, Donau-Universität Krems (DUK), Austria
[2]University of Malta (UoM), Msida, Malta
[3]B&P Emerging Technologies Consultancy Lab Ltd., St. Julian's, Malta

Alexander.pfeiffer@donau-uni.ac.at
mail@stephenbezzina.com
Thomas.wernbacher@donau-uni.ac.at
DOI: 10.34190/EWS.21.055

Abstract: The music industry has evolved significantly over the last few decades, from cassette to compact disk to MP3 and now to subscription-based streaming. Simultaneously, there has been a return to analogue, especially to vinyl records. In 2021, a major record label will introduce a new kind of vinyl. From the original master tapes, one-of-a-kind copies will be made. These will be manufactured in very limited quantities and sold exclusively as collectors' items. In a world where purchasing these collectibles is as simple as tapping the screen and where there are also numerous trading markets between private individuals, new creative ways to protect consumers and digitally protected analogue collectibles must be found. This relates to both the product's authenticity and the legitimate possession of the valuable vinyl. This work in progress paper aims to determine whether digital identities of suppliers, distributors, and consumers on the one hand, and decentralized encrypted data storage on the other, can be potentially the future technology to safeguard collectibles that the creative industry should be more than just looking at.

Keywords: collectibles, blockchain, digital ID, vinyl

Peer2Peer Communication via Testnet Systems of Blockchain Networks: A new Playground for Cyberterrorists?

Alexander Pfeiffer[1, 2, 3], Thomas Wernbacher[1] and Stephen Bezzina[2, 3]

[1]Center for Applied Game Studies, Donau-Universität Krems (DUK), Austria
[2]University of Malta (UoM), Msida, Malta
[3]B&P Emerging Technologies Consultancy Lab Ltd., St. Julian's, Malta

Alexander.pfeiffer@donau-uni.ac.at
Thomas.wernbacher@donau-uni.ac.at
mail@stephenbezzina.com
DOI: 10.34190/EWS.21.049

Abstract: Peer2Peer communication can take place in the traditional way via e-mail, forums or social media. One also finds dedicated apps for communication or organized in groups, such as WhatsApp, Telegram or Discord, the latter being particularly popular with digital gamers. Online games are another medium which can foster communication between people over a data connection, as direct messages can be sent through the provisions of the digital game worlds. Depending on the game provider and its headquarters, the terms and conditions differ in how the data is transmitted and processed. Access to private communications is important for governments and especially for the police work, for both to prevent and follow up on cybercrime and terrorist acts. On the other hand, the private and civil rights movements push for such interventions to occur only in the case of absolutely justified suspicion, with otherwise restricted access to transmitted conversations and data of private individuals and companies. Therefore, it is important that such access to messages is confirmed in advance by a law court. But even with approval, it is still difficult for the authorities to gain access from a technical perspective. While IP addresses and open communication can be intercepted quite easily, it is more difficult when secure messenger apps are used and only possible if there is direct access to the user's device or the app operator provides the authorities access via a master key. In digital games, access is even more complicated. In this work-in-progress paper the authors want to address a currently overlooked aspect of Peer2Peer communication; which is the provision of text messages via (testnet) blockchain systems, with special regard to the possibility of attaching encrypted messages to the transaction of blockchain tokens. It is to be noted that on the testnet versions of the blockchain systems no "KYC"

takes place. While on the mainnet versions of the blockchain systems the purchase of tokens to send them later can only be done anonymously "over the counter", the testnet of most blockchain systems is completely free available. Everyone can create a blockchain Wallet, request testnet tokens and start sending encrypted messages anonymously. This work-in-progress paper aims to highlight and explain the authors' planned research in this field.

Keywords: blockchain, DLT, social media, utility tokens, cryptocurrencies, rewards

Ethics of Cybersecurity in Digital Healthcare and Well-Being of Elderly at Home

Jyri Rajamäki

Laurea University of Applied Sciences, Espoo, Finland

jyri.rajamaki@laurea.fi
DOI: 10.34190/EWS.21.009

Abstract: The SHAPES Horizon 2020 project supports the well-being of the elderly at home. The growing complexity of the digital ecosystem in combination with increasing global risks involves various ethical issues associated with cybersecurity. An important dilemma is that overemphasising cybersecurity may violate fundamental values such as equality and fairness, but on the other hand, neglecting cybersecurity could undermine citizens' trust and confidence in the digital infrastructure, policymakers and state authorities. One example of ethical issues concerning health and well-being is that if a medical implant producer protects the data transfer between implant and receiver server utilising suitable cryptology, this significantly increases the energy consumption of the implant and frequently requires more surgeries for battery exchange. The object of this work in progress paper is to help to provide necessary tools and guidelines to health and well-being service developers in the SHAPES project for their ethical consideration of cybersecurity actions. This paper examines different views and approaches to the ethics of cybersecurity in healthcare and finds the most relevant and puzzling issues for the SHAPES project. The paper investigates the ethical issues, for example, applying the approach of principlism based on four principles of biomedical ethics (respect for autonomy, nonmaleficence, beneficence and justice), and ethics of care. The important aims of the employment of information and communication technology in healthcare are efficiency and quality of services, the privacy of information and confidentiality of communication, the usability of services, and safety. Four important value clusters in cybersecurity are security, privacy, fairness, and accountability. From these four different ethical aspects (biomedical ethics,

ethics of care, core value clusters in cybersecurity, and technical aims), this paper proposes a new conceptual model for a system approach to analyse the ethical matters, which are related to cybersecurity in digital healthcare and well-being.

Keywords: ethics, cybersecurity, digital healthcare, SHAPES project, healthy ageing, well-being

ECHO Federated Cyber Range as a Tool for Validating SHAPES Services

Jyri Rajamäki and Harri Ruoslahti

Laurea University of Applied Sciences, Espoo, Finland

jyri.rajamaki@laurea.fi
harri.ruoslahti@laurea.fi
DOI: 10.34190/EWS.21.076

Abstract: ECHO is a cybersecurity pilot project under the H2020 Program. The ECHO Federated Cyber Range (E-FCR) provides enabling technology supporting ECHO Network operations, ensuring a safe and reliable multi-sector simulation environment in which to ensure viable delivery of identified technology roadmaps, as well as, hands-on cyber-skills development involving realistic sector specific or multi-sector simulations. A cyber range leverages cloud technologies to provide a virtualized environment in which realistic cyber scenarios can be instantiated. The eHealth platform by project SHAPES will rely on services and products provided by vendors. Operability and usability of the platform requires reliable, uninterrupted and well-managed actions from the systems utilized to run services of the eHealth platform. The SHAPES platform operates in the cyber domain and the taxonomy of cyber-risks vary from actions of people due lack of cybersecurity awareness to technology failures. Moreover, threats from malicious external sources might exploit vulnerabilities of SHAPES assets and therefore cause damage. Predefined security validation procedures facilitate to create a baseline for services and their desired level of security. This work-in-progress paper explores how to apply E-FCR during eHealth-services validation processes. The paper profits two Horizon-2020 projects: The ECHO cybersecurity project demonstrating how to utilize E-FCR in the healthcare domain; and the SHAPES healthcare project that needs a cybersecurity validation processes for services incorporated into the SHAPES platform.

Keywords: ECHO project, SHAPES project, federated cyber range, security validation

Abstracts Only

Establishing Real-Time Security for Levels 1 and 0 in SCADA Networks

Mark Baggett

Mission Secure, Houston, USA

mark@missionsecure.com

Abstract: A new type of SCADA and industrial control system (ICS) cybersecurity is emerging, one that assumes a determined adversary will gain access to the operational technology (OT) network. Under this paradigm, the priority is cyber resiliency. And for critical national infrastructure protection, cyber resiliency is the end goal. When today's adversaries breach the business network and subsequent segments, what is protecting the control systems managing physical processes from manipulation or disruption? With potentially catastrophic impacts on the business, employees, environment, and beyond, what is protecting the critical national infrastructure processes? Traditional ICS cybersecurity says protect control systems by layering barriers to keep adversaries at bay. But what happens when they fail? Level 0 in the OT network is the last line of defense. Protecting Level 0—field devices controlling physical processes like temperature, pressure, flow, and speed—should be at the core of any industrial cybersecurity approach. Three questions must be addressed to protect physical processes and ensure operational resiliency: 1. How do you maintain operability during a cyber attack? 2. How do you safely bring down processes when compromised by or under attack? 3. How do you recover and restore cyber-physical systems after the attack? A decade ago, we'd point to the control and safety systems to answer those questions. Today, we've seen both attacked and fail to operate as intended. Using comparative analysis and change detection between digital command and control signals (operator activity; ethernet, TCP/IP, or serial) and raw physical analog signals (physical component activity; 24 VDC, 4-20 mA) with system awareness at the network traffic level, operators gain unprecedented insight and protection for their critical processes. Addressing cyber threats where they are most catastrophic is where cybersecurity needs to begin. Therefore, SCADA and industrial control systems should not just be protected from intruders but, more importantly, resilient to cyber attacks.

Keywords: critical national infrastructure protection, SCADA, industrial control systems, cyber-physical systems, cybersecurity

Situational Awareness Dark Web

Micki Boland

Check Point Software Technologies LTD, Irving, USA

mboland@checkpoint.com

Abstract: Down the Rabbit Hole – A Tour into the Dark Web "Life is like an onion…" this is a quote by the famous American poet and three times Pulitzer winner, Carl Sandburg. By the time Sandburg wrote these lyrics in the 19th century, he could have never imagined how close to reality those words would become in the 21st century and specifically in the context of the Dark Web. Frequently, Alice in Wonderland is used as the main analogy to the Dark Web, but just like in the book, no one tells us how this magical world was made and what the motive for its creation was. If one wants to become wise on a matter and have a solid opinion on a subject, one needs to learn its historical events and evolution. In our journey through this session, we take you through the evolution, goals and motivation of the Dark Web. I will share with you what and whom you can find on the platforms as well as the major conflicts individuals face while exploring this web. The session also exposes you to the syndicates and structures running on the platforms. Surprisingly we see how those groups were among the first to embrace and implement Blockchain technology and created a major global demand for crypto currencies. This is the time to listen, learn and be exposed to the deepest secrets of the Dark Web.

Keywords: blockchain, crypto currencies, secrets, platforms, motivations

---

Are Endpoint Users Willing to Secure Themselves? A Cyber-Physical Comparison

Jan Kleiner

Masaryk University, Brno, Czech Republic

jkleiner@mail.muni.cz

Abstract: Endpoint users are usually viewed as the highest-risk element in the field of cybersecurity. States have traditionally focused more on securing the critical infrastructure while omitting their citizens. However, their poorly secured devices can be easily transformed into threats like botnets and used to attack critical

infrastructure and other essential systems. Some states have recently started to address this issue. For example, California has banned default and hard-coded passwords for electronic devices with a law, Estonian authorities perform educational cybersecurity efforts towards their citizens, and Israel has created a hotline for cyber incidents reporting. Academic research currently fails to address this issue adequately and thus to provide states with a knowledge base upon which more effective measures can be implemented. Little effort is also made to understand recipients of such measures. Our study partly fills this gap and investigates how endpoint users are willing to secure themselves against cyber threats. To do that, we used a survey to measure the willingness operationalised as a tendency to invest money or time. The data were collected in the Czech Republic in 2019. To make results more practically meaningful, we also employed a unique comparison with comparable physical threats through their impacts. This allowed us to assess respondents' willingness to secure themselves against cyberthreats that are usually hard-to-grasp for the general public in the context of familiar physical threats. The data were analysed with statistical analysis, concretely descriptive statistics, and the Wilcoxon signed-rank test. The results showed statistically significant differences between comparable cyber-physical pairs and their equal impacts. We conclude that a large portion of the sample was not able to assess the threat environment appropriately and that state's intervention with fitting countermeasures is needed. The resultant matrix containing frequencies of answers denotes what portion of respondents are willing to invest a certain amount of time and money into countering given threats providing a possible identification of weak points where state investments are needed the most.

Keywords: cybersecurity, state-endpoint user relationship, survey data collection design, cyber-physical comparison, political science study

ICT Uses in Peace and War

Brett van Niekerk

University of KwaZulu-Natal, Westville, South Africa

vanniekerkb@ukzn.ac.za

Abstract: The World Economic Forum's Global Risks Report 2020 (WEF, 2020) lists cyber-attacks as one of the top 10 risks regarding both likelihood and impact. In 2014 the IISS indicated that "coercive cyber capabilities are becoming a new instrument of state power, as countries seek to strengthen national security and exercise political influence. Military capabilities are being upgraded to monitor the

constantly changing cyber domain and to launch, and to defend against, cyber attacks" (IISS, 2014). Since the DDoS attacks against Estonia in 2007 and the Stuxnet infection of the Natanz nuclear facility became public, there has been a steady increase in cyber activity related to conflict and major political events. The increasing use of information, ICTs, and artificial intelligence in national security, military, and peacekeeping operations raises a number of ethical, legal, and technical concerns. There have been a number of initiatives attempting to provide frameworks and/or norms to address these concerns, such as the UN Group of Governmental Experts and the Open Ended Working Group, the Global Commission for the Stability for Cyberspace, and the Paris Call, amongst others. However, challenges remain as the norms are voluntary, and existing agreements are difficult to enforce. As an illustration of this, there have been cyber attacks reported on power grids, water treatment facilities, and other economically important infrastructure. This session will focus on the strategic, governance and international humanitarian law aspects with respect to the use of ICTs in scenarios of conflict and the maintaining of peace. Consideration will be given to the use of ICTs and cyber operations at the operational and tactical levels. The purpose of this discussion is for attendees to network and discuss current trends in this space and explore future avenues of research.

Keywords: cyber operations, influence operations, international humanitarian law, international security, peacekeeping

Defund the Police, Domestic Terrorism and Information Warfare: An Anticipatory Ethical Analysis

Richard Wilson

Towson University, USA

wilson@towson.edu

Abstract: This analysis is concerned with the issues that are related to the defund the police movement and the potential influence of the ideas within this movement on the future of law enforcement. From the perspective of those working in law enforcement there are a variety of problems that arise and that need to be addressed in order for law enforcement to perform its mission within our society. These problems are related to the Mission of Law Enforcement: According to the Police Officer Code of Ethics, the mission of law enforcement is "to serve the community; to safeguard lives and property; to protect the innocent against deception, the weak against oppression or intimidation and the peaceful against

violence or disorder; and to respect the constitutional rights of all to liberty, equality, and justice".1 In order to carry out their mission the police have to deal with jurisdictional problems at the local, state, and Federal levels. These jurisdictional hurdles are important when discussing how best to provide police service during the defund the police movement. At the local level, cities need to enter into interagency agreements to lift or expand jurisdictional boundaries in order to provide or obtain police services from neighboring areas. At the state level, agencies need state legislatures to enhance their subject matter jurisdiction by passing laws enabling them to perform the mission of those agencies affected by budget cuts. At the federal level, Congress will need to pass laws expanded the statutory authority of one agency to meet the mission of another if the agency is dissolved (ex. Immigration and Customs Enforcement has continually been the target of a defund movement, even before the BLM protests of 2020. The focus on these technical issues related to Defund the Police and how this will effect a dealing with Domestic terrorism. This discussion will allow a clear identification of the associated issues related to information warfare and ethical issues, which will provide a basis for identifying future problems that will be the foundation for an anticipatory ethical analysis. The anticipatory ethical analysis provide the foundation for developing policy for law enforcement presented by the defund the police movement.

Keywords: Defund, Police, Domestic, Terrorism, Information, Warfare, Anticipatory, Ethics

Media Ecology, Twitter and Information Warfare: Ethical and Anticipated ethical issues

Richard Wilson

Towson University, USA

wilson@towson.edu

Abstract: Every communication technology (medium) has fundamental physical, psychological, and social characteristics that are basically separate and fixed. These characteristics condition how users of a medium communicate, process information, give meaning to and make sense of the world. Every communication technology conditions users to think and to speak in specific ways. In order to understand how Twitter accomplishes this, the features that define Twitter need to be identified. Twitter is a microblogging platform, where tweets typically consists of short phrases, quick comments, images or links to video's limited to 280

characters. As a platform used for communication Twitter has having three key features: simplicity, impulsiveness and incivility. Information warfare is aimed atgaining a competitive advantage over an opponent. In the medium of Twitter, Information warfare can involve the manipulation of information trusted by the target of tweets without the target's awareness, so that the target of the tweets will make decisions against their interest but in the interest of the one conducting information warfare on Twitter. As a consequence, it is not clear when information warfare on Twitter begins, ends, and how strong, effective or destructive it is. In this analysis the rhetoric of Donald Trump and his use of Twitter to attack the press will be examined. There are four ways in which Trump has waged information warfare on the press on Twitter.

1. Trump is skilled at manipulating the news cycle.

2. Trump has created a closed feedback loop with Fox news.

3. Trump has attacked a free and independent press.

4. Trump’s rhetorical attacks on the press have been effective with his base.

Information warfare may involve the distortion of information, assurance(s) that one's own information is valid, spreading of propaganda or disinformation to demoralize or manipulate an opponent and the public, undermining the quality of the opposing force's information and denial of information-collection opportunities to opposing forces. The way in which trump has waged Information warfare is closely linked to psychological warfare. This analysis is concerned with examining the ethical and anticipated ethical issues with how Trump has employed communication technology to wage information warfare on Twitter.

Keywords: Media, Twitter, Information, Warfare,Anticipatory, Ethics

QAnon, Social Media Warfare, and Conspiracy Theories: An Ethical and Anticipatory Ethical Analysis

Richard Wilson

Towson University, USA

wilson@towson.edu

Abstract: Today the effort to undermine democracy comes in a wide range of forms. One example is the use of social media where leaders can wage information warfare upon their own citizens. This paper will examine how this has occurred with the group QAnon. QAnon's fabrications allege that a cabal of Satan-worshiping pedophiles is running a global child sex-trafficking ring and plotting against US President Donald Trump, who is battling against the cabal. The theory also commonly asserts that Trump is planning a day of reckoning known as ""The Storm"", when thousands of members of the cabal will be arrested. No part of the theory is based on fact. The theory proper began with an October 2017 post by ""Q"", who was presumably a single American individual. It is likely 'Q' has become a group of people. Q claimed to be a high-level government official with Q clearance having access to classified information involving the Trump administration and its opponents in the United States. NBC News reported that three people took the original Q post and spread it across multiple social media platforms to build an internet following. Hybrid Warfare, often practiced within social media, does not have a universally recognized definition; it is describes any sort of clandestine non-military destabilization efforts. Whether it is economic subversion or propaganda dissemination, these techniques have already been around, and there is nothing novel, except perhaps in terms of how these techniques have adapted to incorporate modern-day technologies including especially the social media. It is assumed in this analysis that every conspiracy theory presents a moral issue. To offer a conspiracy theory as an explanation for an action or as the cause of an event is to make an accusation. The accusation that lies at the heart of the conspiracy is the truthfulness of what is claimed to be true by the perpetuator of the conspiracy theory. This analysis has its goal to identify the ethical issues with conspiracy theories used by Leaders and groups such as QAnon in social media and to attempt to anticipate ethical and political issues with the continued use of these conspiracy theories for the purposes of social media warfare.

Keywords: QAnon, Social Media Warfare, Conspiracy Theories, Anticipatory Ethics

‘Soft’ Warfare, State Sponsored Information Deception, and Social Media: Ethical and Anticipated Ethical Issues

Richard Wilson

Towson University, USA

wilson@towson.edu

Abstract: This analysis aims at extending Nye’s notion of “soft power” into the domain of “soft warfare” and social media warfare. According to Nye, “diplomacy, trade agreements, and other policy instruments may also be used, alongside or in lieu of threats of military force or other ‘hard power’ (kinetic use of forceful measures) in order to persuade adversary nations to cooperate more readily with any given states strategic goals”. Hybrid warfare has already been employed to combine persuading nations with cyber tactics, with kinetic use of force, to achieve political and strategic goals. The use of hybrid warfare has been clearly exhibited in Estonia, Georgia, Ukraine and the annexation of Crimea. The concept of “Soft” warfare adds further distinctions into the discussion of the hybrid strategies that have already been successful in cyber warfare. Lucas offers the following insight into the nature of soft warfare: “Soft warfare (or ’unarmed conflict’), is a comparatively new term designating actual warfare tactics that rely on measures other than kinetic force or conventional armed conflict, to achieve the potential goals and national interests or aspirations for which war”. The conditions for the possibility of these alterations within the definition of warfare are presented by the evolution of cyberspace and how alterations in cyberspace can influence cyber conflicts. Political influence can be achieved by nation states using social media that can involve employing a wide variety of actors including state actors, non state actor groups as well as individuals. These are some of the factors that have to be taken into consideration when we to gain an understanding of contemporary political disputes. Social media allow for the combination of these different approaches to warfare which can be involved in political strategies for one nation state to attempt to influence other nation states. Examples drawn from recent events will be used to illustrate how Information deception using social media now plays an increasingly important role in “soft warfare.” This analysis gives an account of how Soviet Cold War Strategy has been transformed through soft warfare and information deception to attempt to undermine western democracies. The presentation will also discuss Ethical and Anticipate Ethical Issues.

Keywords: Soft Warfare, State, Sponsored, Information, Deception, Social, Media, Anticipatory, Ethics

White Rage, Information Warfare and Bodily Performance: Ethical and Anticipated Ethical Issues

Richard Wilson

Towson University, USA

wilson@towson.edu

Abstract: The social decentering of hegemonic masculinity and the decentering of white privilege creates the conditions for the possibility for manipulating disgruntled audiences. Manipulation of fear and anxiety in a targeted audience can lead to white rage. White rage follows a rhetorical style and forms the basis for a style of communication that can be effectively employed in information warfare. An important and under studied part of the information warfare is a type of warfare carried out through the use of nonverbal paraverbal (intonation, vocal tone) performances. These elements are combined in a performance that stokes racial and ethnic animus. In addition to traditional rhetorical linguistic rhetorical devices precognitive and autonomic energy engages bodies. Racist and ethnic animus can be understood as partially affective in nature and can become part of the bodies precognitive and autonomic energy sensate structure. Bodily performance including the grain of the voice and gestures, can be understood as at least part bodily performances that invite others to engage in the bodily affects. Rhythms, vocal patterns, turns of phrase affect the bodies of audiences. These aesthetic effects trigger racist and ethnic rage at a nonrational emotive and affective level in audiences. Information warfare that employs bodily performance and precognitive and autonomic energy can manipulate audiences by favoring white male privilege through aggression, anger, and through being derisive of anyone different from those who are different from oneself and not favored. Polarizing rhetoric and propaganda are employed to motivate members of an ingroup to hate and scapegoat outgroups. This analysis will use examples drawn from Donald Trump and examine both his rhetorical discourse and bodily performance of white rage, to conduct information warfare as mechanisms for subverting democracy . After examining the ethical issues related to the bodily performance of white rage this discussion will conduct an anticipatory ethical analysis of information warfare employing white rage and bodily performance.

Keywords: White Rage, Information Warfare, Bodily Performance,: Ethics, Anticipated Ethical Issues

Additional Materials

Participant List

Surname	First Name	Institution	Email address
Alenius	Kari	University of Oulu, Katu, Finland	kari.alenius@oulu.fi
Allen	Dennis	Carnegie Mellon University, Software Engineering Institute, Pittsburgh, USA	dallen@cert.org
Baggett	Mark	Mission Secure, Houston, USA	mark@missionsecure.com
Banks	Lin	Air Force Institute of Technology, Dayton, USA	banks.lin@afit.edu
Barbour	Graham	Council for Scientific and Industrial Research, Pretoria, South Africa	gbarbour@csir.co.za
Bengtsson	Johnny	Swedish National Forensic Centre, Linköping, Sweden	johnny.bengtsson@polisen.se
Bobric	George-Daniel	Carol I National Defence University, Bucharest, Romania	dbobric08@gmail.com
Boland	Michele	Check Point Software Technologies LTD, Irving, USA	mboland@checkpoint.com
Chen	Long	Beihang University, Beijing, China	chen_long@buaa.edu.cn
Chen	Jim	U.S. National Defense University, Washington D.C., U.S.A.	jim.chen@ndu.edu
Chockalingam	Sabarathinam	Institute for Energy Technology, Halden, Norway	Sabarathinam.Chockalingam@ife.no
Coffman	Joel	United States Air Force Academy, , USA	joel.coffman@usafa.edu
Creek	Tristan	Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA	tristan.creek@afit.edu
Cruz	Tiago	University of Coimbra, CISUC, DEI, Portugal	tjcruz@dei.uc.pt
Drewes	Theodore	United States Air Force Academy, USAF Academy, USA	C21theodore.drewes@afacademy.af.edu

Surname	First Name	Institution	Email address
du Toit	Jaco	University of Johannesburg, South Africa	jacodt@uj.ac.za
Duvenage	Petrus	State Security Agency, Pretoria, South Africa	duvenage@live.co.za
Fesl	Jan	University of South Bohemia, Technical university in Prague, Ceske Budejovice, Czech republic	jfesl@prf.jcu.cz
Ford	Adrian	UEL, London, UK	a.ford1701@uel.ac.uk
Grant	Tim	R-BAR, Benschop, Netherlands	tim.grant.work@gmail.com
Habibnia	Babak	University College Dublin, Ireland	babak.habibnia@ucd.ie
Hummelholm	Aarne	University of Jyväskylä, Tampere, Suomi	aarne.hummelholm@elisanet.fi
Jackson-Summers	Angela	U.S. Coast Guard Academy, New London, CT, USA	Angela.G.Jackson-Summers@uscga.edu
Jaquire	Victor	University of Johannesburg, South Africa	jaquire@gmail.com
Johnson	Andrew	University of South Wales, Wales, UK	andrew.johnson@southwales.ac.uk
Kantola	Harry	Finnish National Defence University, Helsinki, Finland	harry.kantola@mil.fi
Kapsokoli	Eleni	University of Piraeus, Athens, Greece	ekapsokoli@unipi.gr
Karie	Nickson	Edith Cowan Univeristy, Joondalup, Australia	n.karie@ecu.edu.au not nickson.karie@cybersecuritycrc.org.au
Kävrestad	Joakim	University of Skövde, Sweden	joakim.kavrestad@his.se
Keinonen	Maria	Finnish Defence Forces, Helsinki, Finland	maria.keinonen@mil.fi
Kleiner	Jan	Masaryk University in Brno, Czech Republic	jkleiner@mail.muni.cz
Kodalle	Thorsten	The Bundeswehr Command and Staff College, Hamburg, Deutschland	thorstenkodalle@hotmail.com

Surname	First Name	Institution	Email address
Kovanen	Tiina	University of Jyväskylä, Finland	tiina.r.j.kovanen@jyu.fi
Leblanc	Sylvain	Royal Military College of Canada, Kingston, Canada	sylvain.leblanc@rmc.ca
Leenen	Louise	University of the Western Cape, Cape Town, South Africa	lleenen@uwc.ac.za
Lekota	Faith	University of Johannesburg, South Africa	nombu30@gmail.com
Liaropoulos	Andrew	University of Piraeus, Athens, Greece	andrewliaropoulos@gmail.com
Lipps	Christoph	German Research Center for Artificial Intelligence, Kaiserslautern, Germany	Christoph.Lipps@dfki.de
Maraj	Arianit	Faculty of Computer Sciences, AAB College, Kosovo	Arianit.Maraj@kosovotelecom.com
Martin	Erik David	Sopra Steria, Stavanger, Norway	erik.martin@soprasteria.com
McDonald	Andre	Council for Scientific and Industrial Research, Pretoria, South Africa	andre.mcdonald1@gmail.com
Mienie	Edward	University of North Georgia, Dahlonega, USA	edward.mienie@ung.edu
Miglani	Jitesh	Technological University Dublin, Blanchardstown, Ireland	christina.thorpe@tudublin.ie
Mmalerato	Masombuka	Stellenbosch University, Cape Town, South Africa	marley.mc@icloud.com
Mohammed Zain	Ruhama	CyberSecurity Malaysia, Cyberjaya, Malaysia	ruhama@cybersecurity.my
OMOGAH	FREDRICK	UZIMA UNIVERSITY, KISUMU, KENYA	fo2001ke@yahoo.com
Opedal	Olav	Opedal Consulting LLC, Ellensburg, US	olav@opedalconsulting.com
Oyinloye	Toyosi	University of Chester, UK	t.oyinloye@chester.ac.uk
Päijänen	Jani	JAMK University of Applied Sciences, Jyväskylä, Finland	jani.paijanen@jamk.fi
Payne	Bryson	University of North Georgia, Dahlonega, USA	bryson.payne@ung.edu
Pfeiffer	Alexander	Danube University Krems, Austria	alexander.pfeiffer@donau-uni.ac.at

Surname	First Name	Institution	Email address
Phadke	Pranav	Technological University Dublin, Blanchardstown, Ireland	christina.thorpe@tudublin.ie
Poole	Carl	Air Force Institute of Technology, Riverside, USA	carl.poole@afit.edu
Potter	Lucas	Old Dominion University, Newport News, USA	lpott005@odu.edu
Pourmoafi	Seyedali	University of Hertfordshire, Hatfield, UK	s.pourmoafi@herts.ac.uk
Pražák	Jakub	Charles University, Hranice IV, Czech Republic	prazak.jakub94@gmail.com
Rabadao	Carlos	Instituto Politécnico de Leiria, Portugal	carlos.rabadao@ipleiria.pt
Rajamäki	Jyri	Laurea University of Applied Sciences, Espoo, Finland	jyri.rajamaki@laurea.fi
Ramluckan	Trishana	University of KwaZulu-Natal, Durban, South Africa	ramluckant@ukzn.ac.za
Rautava	Jori-Pekka	Finnish Defence Research Agency, Riihimäki, Finland	jori-pekka.rautava@mil.fi
Ristolainen	Mari	Finnish Defence Research Agency, Riihimäki, Finland	mari.ristolainen@mil.fi
Ruoslahti	Harri	Laurea University of Applied Sciences, Espoo, Finland	Harri.Ruoslahti@laurea.fi
Saharinen	Karo	JAMK University of Applied Sciences, Jyväskylä, Finland	karo.saharinen@jamk.fi
Santos	Leonel	Instituto Politécnico de Leiria, Portugal	leonel.santos@ipleiria.pt
Schmoldt	Janine	University of Erfurt, Germany	janine.schmoldt@uni-erfurt.de janine-schm@web.de for attachments
Scott	Keith	De Montfort University, Leicester, UK	jklscott@dmu.ac.uk
Shifflett	Michael	USA	shifflettm1@gmail.com
Simola	Jussi	University of Jyväskylä, Finland	jussi.hm.simola@jyu.fi
Sipper	Joshua	Air Force Cyber College, Wetumpka, USA	JASIPPER@GMAIL.COM

Surname	First Name	Institution	Email address
Sokri	Abderrahmane	DRDC CORA, Ottawa, Canada	sokriab@gmail.com
Suresh	Sanjana	Drexel University, Philadelphia, USA	ss5264@drexel.edu
Sutherland	Iain	Noroff University College, Mosby, Norway	iain.sutherland@noroff.no
Thorpe	Christina	Technological University Dublin, Blanchardstown, Ireland	christina.thorpe@tudublin.ie
Tikanmäki	Ilkka	Laurea University of Applied Sciences, Espoo, Finland	ilkka.tikanmaki@laurea.fi
Turunen	Maija	Finnish National Defence University, Helsinki, Finland	maijaturunen@yahoo.com
van Niekerk	Brett	University of KwaZulu-Natal, Durban, South Africa	vanniekerkb@ukzn.ac.za
vanWyk	Maria Catharina	University of Johannesburg, South Africa	mwatney@uj.ac.za
Veerasamy	Namosha	Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa	nveerasamy@csir.co.za
Virtanen	Toni	Finnish Defence Research Agency, Riihimäki, Finland	toni.virtanen@mil.fi
Visky	Gabor	NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia	gabor.visky@ccdcoe.org
Wairimu	Samuel	Karlstad University, Karlstad, Sweden	samuel.wairimu@kau.se
Walker	Kat	Oldham, UK	katwalker2015@gmail.com
Whittaker	Simon	Belfast, UK	simon.whittaker@verticalstructure.com
Wilson	Richard	Towson University, USA	wilson@towson.edu
Wilson	Zuriada	State Security Agency, Pretoria, South Africa	zuriada1.wilson@gmail.com
Wood	Ashley	University of Chester, UK	ashley.wood@chester.ac.uk

The importance of paper citations and Google Scholar

As an academic researcher you will know the importance of having access to the work of other researchers in your field as well as making your own work available to others. In the area of academic publishing this is achieved through citation indexing. There are a number of bodies that undertake this task including Thompson ISI, Elsevier Scopus and Google Scholar – to name just a few.

At ACI we do all we can to ensure that the conference proceedings and the journals that we publish are made available to the major citation bodies and you can see a list relevant to this conference on the home page of the conference website.

However, it is also important for you, the author, to make sure that you have made your work available for citation – particularly with organizations such as Google Scholar. We are providing you here with the simple steps you need to take to do this and we would ask you to take the time to upload your paper as soon as you can.

Step one: Extract your paper from the full proceedings that you have downloaded from the Dropbox link provided to you.

Step two: Upload your paper to your own website, e.g.,

www.university.edu/~professor/jpdr2009.pdf ; and add a link to it on your publications page, such as www.university.edu/~professor/publications.html.

Make sure that the full text of your paper is in a PDF file that ends with ".pdf",

The Google Scholar search robots should normally find your paper and include it in Google Scholar within several weeks. If this doesn't work, you could check if your local institutional repository is already configured for indexing in Google Scholar, and upload your papers there.

More information is available from
http://scholar.google.com.au/intl/en/scholar/inclusion.html

We will separately upload the proceedings to Google Books which is also searched – but evidence has shown that individual upload results in quicker indexing by Google Scholar.

Your own institution may also subscribe to an institutional repository such as http://digitalcommons.bepress.com/ or http://dspace.org/

Providing the original reference of your paper is included you have our permission as publishers to have your paper uploaded to these repositories.

Sue Nugus ACIL

Academic Conferences International

Facilitating excellence in scholarship through double blind peer reviewed conferences on eight topics

Vision and Mission

Our vision is that there is an ever increasing need for high quality research in most if not all aspects of 21st century society. Universities are the primary provider of quality research education.

Quality research education requires the participation of both established faculty, newly appointed staff and research students. There is also the requirement for academe to reach out to the general society as comprehensively as possible.

As the university sector becomes increasingly focused on research excellence there is a need to provide more fora, primarily in the form of peer reviewed conferences, for academics to exchange ideas, questions, problems, and achievements concerning their personal research activities. These fora provide opportunities to exchange ideas, to experience critiques and to obtain some recognition for individuals' progress towards research excellence. The more international the forum the more effective it is.

Although publishing in highly rated indexed academic journals is still the most prized form of academic communication, the conference medium has become a significant outlet for research findings as well as an important facilitator to achieving this goal. All papers submitted to ACIL conferences are double blind peer reviewed and accepted papers are published in a book with an ISBN and ISSN. These conference proceedings are indexed by a number of authorities, including WOS, Scopus, Proquest, etc.

Our mission is to facilitate the creation of global academic research communities by providing all the administrative and management functions required to deliver a comprehensive academic conference experience.

This is supported by the provision of seminars, workshops and the publishing of suitable books, monographs and proceedings.

It is also supported by 5 academic journals three of which are indexed by Elsevier Scopus.

ACIL's conference activities

For over 20 years we have facilitated conferences globally. Originally our focus was only on ICT. Over the years we have broadened the scope, but there is still a strong leaning towards ICT. Currently there are 16 conferences run in various parts of the world which are attended by approximately 1,500 conference participants annually. Global reach is one of the dimensions that differentiates us. At any given conference there are regularly participants from 30 or more countries. Some of the conferences are accompanied by master classes in their associated field which are run on the day before the conference.

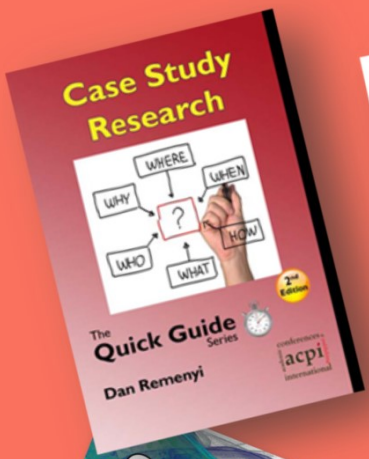
Seven conferences are associated with Excellence Awards for which we appoint judges, accept nominations, conduct evaluations and award prizes. The Games Based Learning Conference runs an established annual competition. Details of these events are contained in our website at www.academic-conferences.org

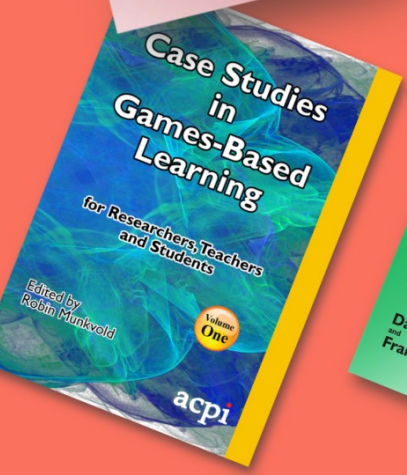
Contact information

If you would like to host a conference, facilitate a workshop or have a book published please contact louise@academic-conferences.org

WWW.ACADEMIC-BOOKSHOP.COM

Academic Bookshop!





Get 20% discount on our bookshop

USE CODE: BKSHP20

WHEN PROMPTED AT CHECKOUT TO CLAIM THE DISCOUNT

AVAILABLE AT:

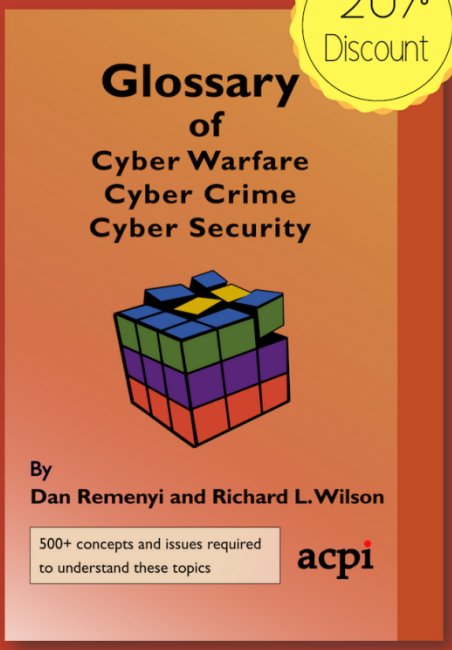
WWW.ACADEMIC-BOOKSHOP.COM

GLOSSARY OF CYBER WARFARE, CYBER CRIME AND CYBER SECURITY

Eliza Doolittle, in the fabulous Broadway show My Fair Lady famously says “Words, words, words, I’m so sick of words!” but then Elvis Presley and the Bee Gees more realistically pointed out “Words are all I have to.....! This book is only about words, words and more words. And words are the tools which academics have at their disposal to make their arguments. It is a central responsibility of academics to make sure that they really understand all the words they use and this is difficult especially in fast moving topics like Cyber Warfare, Cyber Crime and Cyber Security. The Humpty Dumpty maxim, "When I use a word, it means just what I choose it to mean - neither more nor less", does not wash in academe. This short book will help anyone working on the topics of Cyber Warfare, Cyber Crime and Cyber Security.

SPECIAL OFFER

20% Discount



Use code: bkshp20
When prompted at checkout to claim the discount

To buy a copy of this book follow the link:

HTTPS://TINYURL.COM/CYBER-SECURITY-CYBER-CRIME