

17th European Conference on Cyber Warfare and Security (ECCWS 2018)

Oslo, Norway
28 – 29 June 2018

Editor:

Audun Josang

ISBN: 978-1-5108-6604-1

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright The Authors, (2018). All Rights Reserved. No reproduction, copy or transmission may be made without written permission from the individual authors.

Printed by Curran Associates, Inc. (2018)

Review Process

Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy

ACPIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:

<http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academicconferences-and-publishing-international-limited/>

Conference Proceedings

The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

Published by Academic Conferences and Publishing International Ltd.
33 Wood Lane
Sonning Common RG4 9SJ UK

Phone: 441 189 724 148
Fax: 441 189 724 691
info@academic-conferences.org

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2633
Email: curran@proceedings.com
Web: www.proceedings.com

Contents

Paper Title	Author(s)	Page No
Preface		v
Committee		vi
Biographies		vi i
Keynote Outlines		
Research papers		
Continuous Identity Verification in Cloud Storage Services Using Behavioural Profiling	Burhan Al-Bayati, Nathan Clarke, Paul Dowland and Fudong Li	1
Advanced Facial Recognition for Digital Forensics	Hiba Al-kawaz, Nathan Clarke, Steven Furnell, Fudong Li and Abdulrahman Alruban	11
A Multi-Algorithmic Approach for Gait Recognition	Hind Al-Obaidi, Fudong Li, Nathan Clarke, Bogdan Ghita and Salam Ketab	20
SecuSeal: Preventing Cybercrime Susceptibility Using Browser-Specific Warning Badges	Frans Blauw	29
Security Threats and Measures on Multifunctional Devices	Johnny Botha and Sune Von Solms	38
Super Bowl 50: Can Football Teach Students to Become Better Cybersecurity Professionals?	Matthew Bovee and Huw Read	49
Time-Line Alignment of Cyber Incidents in Heterogeneous Environments	Agnė Brilingaitė, Linas Bukauskas and Eduardas Kutka	57
Information Warfare: Modeling a Decision Makers Processes	Viacheslav Burlov Georgievich	66
Offensive and Defensive Cyberspace Operations Training: Are we There yet?	Jami Carroll	77
Committing the Perfect Crime: A Teaching Perspective	Lorena Carthy, Elisabeth Øvnsen, Rachael Little, Iain Sutherland, Huw Read	87
Building Automatic and Intelligent Cyber Attack-Defense Platform	Chung-Kuan Chen and Shiuhyng Winston Shieh	96
Does Conventional Deterrence Work in the Cyber Domain?	Jim Chen	106
Re-Establishing Trust Within and Among Partner Organizations Following a Cyber Incident	Mitch Cochran	112
Social Media Advocacy in the #MustFall Campaigns in South Africa	Zama Dlamini, Linda Malinga, Thulani Masiane and Maduvha Tshiololi	120
Digital Rights Management to Protect Private Data on the Internet	Jaco du Toit	128
A Selective Literature Review on Cyber Counterintelligence	Petrus Duvenage, Victor Jaquire and Sebastian von Solms	137
Cybersecurity in NATO and CSTO: Comparative Analysis of Legal and Political Frameworks	Ruben Elamiryan and Radomir Bolgov	146

Paper Title	Author(s)	Page No
Anti-Reconnaissance: Long Short-Term Memory Based Detection, Classification and Mitigation of Hostile Network Exploration	Daniel Fraunholz, Daniel Reti, Simon Duque Antón and Hans Dieter Schotten	156
Applications of Privacy and Security Research in the Upcoming Battlefield of Things	Lothar Fritsch and Simone Fischer-Hübner	164
China's Notion of Cybersecurity: The Importance of Strategic Cultures for Cyber Deterrence	Lars Gjesvik	174
Classification of Android App Permissions: Tell me What app you are and I Tell you What you are Allowed to do	Nils Gruschka, Luigi Lo Iacono and Jan Tolsdorf	181
Information Influence: Assessing the Advantage	Miah Hammond-Errey	190
A Proposed Hierarchical Taxonomy for Assessing the Primary Effects of Cyber Events: A Sector Analysis 2014-2016	Charles Harry	199
On the use of Ontology Data for Protecting Critical Infrastructures	João Henriques, Filipe Caldeira, Tiago Cruz, and Paulo Simões	208
Forensic Analysis of the Telegram Instant Messenger Application on Android Devices	Diana Hintea, Aleksandrs Sangins and Robert Bird	217
Building the Ideal Cyber Counterintelligence Dream Team	Victor Jaquire, Petrus Duvenage and Sebastian von Solms	224
Possibility of Using Cyber-PYSOP Through Nuclear Weapons: Symbolic Meaning and Risk Measurement of Nuclear Weapons in Social Network	Minhee Joo, Junwoo Seo, Mookyu Park, Haeng Rok Oh and Kyungho Lee	233
The Application of Computer Vision to Detect Malware	Andre Karamanian	240
Model for Efficient Development of Security Audit Criteria	Tomi Kelo, Juhani Eronen and Kimmo Rousku	244
Projected Territoriality: A Case Study of the Infrastructure of Russian 'Digital Borders'	Juha Kukkola and Mari Ristolainen	253
The Uses and Limits of Cyber Coercion	Andrew Liaropoulos	262
Smartphone Usage and Security Maturity: A South African Student Evaluation	Candice Louw and Basie Von Solms	268
A Computational Ontology for Cyber Operations	Clara Maathuis, Wolter Pieters and Jan van den Berg	278
Enhancing Digital Forensic Investigations Into Emails Through Sentiment Analysis	James Christopher McGuire and Wai Sze Leung	288
Undetectable Data Breach in IoT: Healthcare Data at Risk	Sophia Moganedi	296
Automating the Harmonisation of Heterogeneous Data in Digital Forensics	Hussam Mohammed, Nathan Clarke and Fudong Li	299
Cyber Intrusion Detection in Operations of Bulk Handling Ports	Kim Monks, Elena Sitnikova and Nour Moustafa	307
Secure IP Camera Video Streaming Through Kurento Media Server	Kgothatso Ngako	317
Modelling Closed National Networks: Effects in Cyber Operation Capabilities	Juha-Pekka Nikkarila, Bernt Åkesson, Vesa Kuikka and Juhani Hämäläinen	323

Paper Title	Author(s)	Page No
Cyber Force Establishment: Defence Strategy for Protecting Malaysia's Critical National Information Infrastructure Against Cyber Threats	Norazman Mohamad Nor, Azizi Miskon, Zahri Yunos, Mustaffa Ahmad and Ahmad Mujahid Ahmad Zaidi	330
Concepts of Automating Forensic Case Management	Glenn Nor, Iain Sutherland and Andrew Blyth	338
Cyber Resilience as an Information Operations Action to Assure the Mission	David Ormrod and Benjamin Turnbull	343
Disrupting Adversary Decision Logic: An Experience Report	Partha Pal, Nathaniel Lageman and Nathaniel Soule	351
Situational Awareness for Hybrid Warfare: Risk Measurement Between Cyber Warfare and Nuclear Warfare	Mookyu Park, Junwoo Seo, Jaehyeok Han, Haengrok Oh and Kyungho Lee	360
Secure Your SSH Keys! Motivation and Practical Implementation of a HSM-Based Approach Securing Private SSH-Keys	Sven Plaga, Norbert Wiedermann, Gerhard Hansch and Thomas Newe	370
Application of Cyber Resilience Review to an Electricity Company	Jouni Pöyhönen, Viivi Nuojua, Martti Lehto and Jyri Rajamäki	380
Forced Vacation: A Rogue Switch Detection Technique	Kyle Prins and Vijay Bhuse	390
A Secure and User Friendly Multi-Purpose Asymmetric Key Derivation System (MPKDS)	Alexandre Pujol, Christina Thorpe and Liam Murphy	400
Avatar Rights: How Protected are Avatars?	Elina Radionova-Girsa	410
Educational Competences With Regard to Critical Infrastructure Protection	Jyri Rajamäki and Harri Ruoslahti	415
The Ethics of Open Source Intelligence Applied by Maritime Law Enforcement Authorities	Jyri Rajamäki, Sari Sarlio-Siintola and Jussi Simola	424
A Cultural Exploration of the Social Media Manipulators	Char Sample, John McAlaney, Jonathan Bakdash and Helen Thackray	432
Cyber Interoperability and Cooperation: Why are States Reluctant?	Muzaffer Satiroglu	441
Patriotic Hackers are Civilians Sporadically Participating in Hostilities	Janine Schmoldt	447
Wannacry About the Tragedy of the Commons? Game-Theory and the Failure of Global Vulnerability Disclosure	Matthias Schulze and Thomas Reinhold	454
A Second Amendment for Cyber? Possession, Prohibition and Personal Liberty for the Information age	Keith Scott	464
Factors Contributing to the Proliferation of Software as a Weapon	Jantje Silomon	471
Improving Cyber Situational Awareness in Maritime Surveillance	Jussi Simola and Jyri Rajamäki	480
Australian Cyber Security Policy Through a European Lens	Matthew Warren and Shona Leitch	489
The Legal Position of Social Media Intermediaries in Addressing Fake News	Murdoch Watney	496

Paper Title	Author(s)	Page No
Phd Research Papers		505
Security as a Context, Generative Force and Policy Concern for the Co-Production of Cyberspace: Historical Overview Since WWII Until the end of the Cold War	Noran Shafik Fouad	507
Jihadi Operational art in the Digital Realm, its Ideological Origins and Implications	Ferdinand Haberl	515
Cyber Threat Analysis in Smart City Environments	Aarne Hummelholm	523
The Protection of Russia's Critical Information Infrastructure	Martti Kari	533
Education for Cognitive Agility: Improved Understanding and Governance of Cyberpower	Benjamin Knox, Ricardo Lugo, Kirsi Helkala, Stefan Sütterlin and Øyvind Jøsok	541
Current Problems of Protecting the Institution of State Secrets: Evidence From the United States and Great Britain	Nadezhda Kulibaba and Radomir Bolgov	551
Using Anomaly Detection Based Techniques to Detect HTTP-Based Botnet C&C Traffic	Laxmikanta Mohanty and Debasish Jena	557
Scalable Distributed Traffic Monitoring for Enterprise Networks With Spark Streaming	Andrés Ocampo, Tim Wauters, Bruno Volckaert and Filip De Turck	563
A Taxonomy of Computational Models for Trust Computing in Decision-Making Procedures	Mirko Tagliaferri and Alessandro Aldini	571
Masters Research Papers		579
Crime Prevention: How to Avoid Subscription Traps?	Vesa Hietanen and Jyri Rajamäki	581
Towards an Artificial Intelligence Framework to Actively Defend Cyberspace	Mmalerato Masombuka, Marthie Grobler and Bruce Watson	589
Non Academic Papers		597
The Cyber-Energy Nexus: The U.S and the International Operational Energy Perspective	Arnold Dupuy, Daniel Nussbaum and Stefan Pickl	599
Get Ahead of Coming Disruptions in Cyber Security by Working Collaboratively	Christine Ziske and Ulf Ziske	604
Cyber Weapons and the U.S. Constitution	Neal Kushwaha and Bruce Watson	612