

13th European Conference on Cyber Warfare and Security

(ECCWS 2014)

**Edited by
Andrew Liaropoulos
George Tsihrintzis**

Editors:

**Andrew Liaropoulos
George Tsihrintzis**

ISBN: 978-1-63266-831-8

Printed from e-media with permission by:

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



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

Copyright© The Authors, (2014). All Rights Reserved.

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

Papers have been double-blind peer reviewed before final submission to the conference. Initially, paper abstracts were read and selected by the conference panel for submission as possible papers for the conference.

Many thanks to the reviewers who helped ensure the quality of the full papers.

Printed by Curran Associates, Inc. (2014)

Published by Academic Conferences Ltd.
Curtis Farm Kidmore End
Reading RG4 9AY 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: 845-758-2634
Email: curran@proceedings.com
Web: www.proceedings.com

Contents

Paper Title	Author(s)	Page No.
Preface		iii
Committee		iv
Biographies		vi
Possible Scenarios and Maneuvers for Cyber Operational Area	Ugur Akyazi	1
Digital Forensics as a Science in Higher Education	Olga Angelopoulou and Stilianos Vidalis	8
Knowledge Accessibility and Cyber Macht	Leigh Armistead and Scott Starsman	17
A Strategic Approach to Managing Security in SCADA Systems	Mehdi Asgarkhani and Elena Sitnikova	23
Fuzzy Application With Expert System for Conducting Information Security Risk Analysis	Jiří Bartoš, Bogdan Walek, Cyril Klimeš and Radim Farana	33
Identity Multipliers and the Mistaken Twittering of ‘Birds of a Feather’	David Cook	42
Secret Sharing Framework Based on Digital Certificates	Paul Crocker and Adolfo Peixinho	49
Improving Cyber-Security Awareness on Industrial Control Systems: The CockpitCI Approach	Tiago Cruz, Jorge Proença, Paulo Simões, Matthieu Aubigny, Moussa Ouedraogo, Antonio Graziano and Lasith Yasakhetu	59
Putting Counterintelligence in Cyber Counterintelligence: Back to the Future	Petrus Duvenage and Sebastian von Solms	70
Information Security Economics: Induced Risks and Latent Costs	Evangelos Frangopoulos, Mariki Eloff and Lucas Venter	80
The Opportunities of National Cyber Strategy and Social Media	Arto Hirvelä, Aki-Mauri Huhtinen and Tommi Kangasmaa	88
Online Social Networks: A Vehicle for Malware Propagation	Ehinome Ikhaliya and Johnnes Arreyambi	95
Countering Threats - a Comprehensive Model for Utilization of Social Media for Security and law Enforcement Authorities	Margarita Jaitner and Harry Kantola	102
Potential Cyber Warfare Capabilities of Major Technology Vendors	Audun Jøsang	110
Manpower Planning and Management in Cyber Defense	Ilker Kilaz, Akif Onder and Murat Yanik	116
The Effectiveness of Online Gaming as Part of a Security Awareness Program	William Aubrey Labuschagne and Mariki Eloff	125
Cyberconflict and Theoretical Paradigms: Current Trends and Future Challenges in the Literature	Andrew Liaropoulos	133
Planning Method of Information Security for Military Organizations	José Martins, Henrique dos Santos, Mendes Dias and José Borges	140
Comparison of two Specifications to Fulfill Security Control Objectives	Riku Nykänen and Tommi Kärkkäinen	150
Challenges in Information Security Protection	Teresa Pereira and Henrique Santos	160
Enrolment Time as a Requirement for Face Recognition Biometric Systems	Vítor Sá, Sérgio Magalhães and Henrique Santos	167

Paper Title	Author(s)	Page No.
Retaining Control Over Private Virtual Machines Hosted by a Cloud Provider Using Mandatory Access Control, Trusted Boot and Attestation	Armin Simma and Philipp Rusch	172
Cyber Security and Civil Engagement: Case of Lithuanian Virtual Community Projects	Aelita Skaržauskienė, Agnė Tvaronavičienė and Gintarė Paražinskaitė	181
Determination of Meme Proliferation Factors	Namosha Veerasamy and William Aubrey Labuschagne	188
Integration of a Network Aware Traffic Generation Device Into a Computer Network Emulation Platform	Suné von Solms and Schalk Peach	198
Legal Solutions to State-Level Cyber Intrusion Under International law: A Maze of Legal Uncertainty or not?	Murdoch Watney	206
An Annotated Bibliographical Survey on Cyber Intelligence for Cyber Intelligence Officers	Cagatay Yucel and Ahmet Koltuksuz	213
PHD Research papers		221
Intrusion Detection System Using Bayesian Network Modeling	Chaminda Alocious, Nasser Abouzakhar, Hannan Xiao and Bruce Christianson	223
A Near-Miss Management System to Facilitate Forensic Investigation of Software Failures	Madeleine Bihina Bella, Jan Eloff and Martin Olivier	233
Requirements for Preparing the Cloud to Become Ready for Digital Forensic Investigation	Moses Dlamini, Hein Venter, Jan Eloff and Mariki Eloff	242
A Generic Framework for Enhancing the Quality Digital Evidence Reports	Nickson Karie and Hein Venter	251
A Framework to Address Challenges Encountered When Designing a Cyber-Range	Brendan Lawless, Jason Flood and Anthony Keane	258
A Cyber Attack Evaluation Methodology	Kosmas Pipyros, Lilian Mitrou, Dimitris Gritzalis and Theodore Apostolopoulos	264
The Changing Character of war in the Global Information Age	Anthimos Alexandros Tsirigotis	271
Masters Research papers		279
Spymasters Tools: A Comparative Approach to Side Channel Attacks	Tuğçe Kalkavan	281
Models for the Forensic Monitoring of Cloud Virtual Machines	Dirk Ras and Hein Venter	290
Non Academic paper		301
Distinguishing Cyber Espionage Activity to Prioritize Threats	John Hultquist	303
Work In Progress paper		309
NATO Article Statue 5 in Terms of a Cyber-War	Selcuk Dal and Kadir Ozyurt	311

O h o

= 7 u ‡ O o