

13th International Conference on Cyber Warfare and Security (ICCWS 2018)

Washington, DC, USA
8 – 9 March 2018

Editors:

John S. Hurley
Jim Q. Chen

ISBN: 978-1-5108-5963-0

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.

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. (2018)

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 Nos
Preface		vi
Committee		vii
Biographies		ix
Developing Simulated Cyber-Attack Scenarios Against Virtualized Adversary Networks	Luis Aybar, Gurminder Singh and Alan Shaffer	1
Impact Assessment of Cyber Actions on Missions or Business Processes: A Systematic Literature Review	Hayretdin Bahşi, Chibuzor Joseph Udokwu, Unal Tatar and Alexander Norta	11
Support for Secure Code Execution in Server Operating Systems	Vijay Bhuse and Kyle Hekhuis	21
The United Nations and Russian Initiatives on International Information Security	Radomir Bolgov, Olga Filatova and Vatanyar Yag'ya	31
IoT-Related DDoS Ethical Issues: A System of Systems Approach	Sarah Bouazzaoui, Omer Poyraz, Charles Daniels and Ange-Lionel Toba	39
Developing Low-Cost and Effective ICS Cyber Training Environments	Luke Bradford, Barry Mullins, Stephen Dunlap and Mark Reith	47
Framework for Assessing Cyber Risk/Effects in Context of Air Force Operations	Clint Bramlette and Mark Reith	52
The Methodological Basis for Solving the Problems of the Information Warfare and Security Protection	Viacheslav Georgievich Burlov	64
Recommendations to Develop and Hire More Highly Qualified Women and Minorities Cybersecurity Professionals	Darrell Norman Burrell and Calvin Nobles	75
The Critical Need for Formal Leadership Development Programs for Cybersecurity and Information Technology Professionals	Darrell Norman Burrell, Amalisha Sabie Aridi and Calvin Nobles	82
Integrating Cyberspace Power into Military Power in Joint Operations Context	Mustafa Canan and Andres Sousa-Poza	92
Cognitive Schemas and Disinformation Effects on Decision Making in lay Populations	Mustafa Canan and Rik Warren	101
The Severity of Cyber Attacks on Education and Research Institutions: A Function of Their Security Posture	John Chapman, Anitha Chinnaswamy and Alexeis Garcia-Perez	111
Effectively Exercising Deterrence in the Cyber Domain	Jim Chen	120
Cyber Resilience: An Essential new Paradigm for Ensuring National Survival	William Arthur Conklin and Anne Kohnke	126
Reorganizing for Information Competition	Alexander Crowther	131
On SCADA PLC and Fieldbus Cyber-Security	Cordell Davidson, Todd Andel, Mark Yampolskiy, Todd McDonald, Brad Glisson and Tom Thomas	140

Paper Title	Author(s)	Page Nos
Data Fidelity in the Post-Truth Era Part 1: Network Data	Michael De Lucia, Steve Hutchinson and Char Sample	149
Operating Systems of Choice for Professional Hackers	Sarah Delasko and Weifeng Chen	159
Technical and OSINT Analysis of the TOR Foundation	Maxence Delong, Eric Filiol, Clément Coddet, Olivier Fatou and Clément Suhard	164
Virtual Cyber Warfare Experiments Based on Empirically Observed Adversarial Intrusion Chain Behavior	Geoffrey Dobson, Aunshul Rege and Kathleen Carley	174
Overview of Software Security Issues in Direct-Recording Electronic Voting Machines	Michael Dunn and Laurence Merkle	182
The Role of Weaponized Malware in Cyber Conflict and Espionage	Chuck Easttom	191
Detecting Insteon Home Automation Network Attacks Using a Software Defined Radio (SDR) Radio Frequency Air Monitor	Roderick Ervin, Michael Temple, Addison Betances and Christopher Talbot	200
Strategic Communication in the Context of Modern Information Confrontation: EU and NATO vs Russia and ISIS	Olga Filatova and Radomir Bolgov	208
Blood and Packets: Attacking Network Administrators to Weaken Network Security	Michael Fowler	219
Biometrics and the European Migrant Crisis	Carlos Gaviria, Sam Baroni and Michael David	226
Speeding up Planning of Cyber Attacks Using AI Techniques: State of the Art	Tim Grant	235
Cyber Espionage: The Silent Crime of Cyberspace	Virginia Greiman	245
Building Mission-Centric Cyber Risk Assessments	Jeffrey Guion and Mark Reith	252
Introducing the Six-Ware Cyber Security Framework Concept to Enhancing Cyber Security Environment	Rudy Gultom, Wayan Midhio, T. Silitonga and S. Pudjiatmoko	262
Preventing SSH Remote Attacks Using Moving Target Defense	Vahid Heydari	272
Collateral Damage Outcomes are Prominent in Cyber Warfare, Despite Targeting	Corey Hirsch	281
Nostradamus Ratios: Why is Russia an Outlier?	Michael Bennett Hotchkiss	287
Beyond the Struggle: Artificial Intelligence in the Department of Defense (DoD)	John S Hurley	297
Cyber Deterrence: An Illustration of Implementation	Gazmend Huskaj and Esmiralda Moradian	304
Improving Signature-Based Packet Analysis Efficiency: A Case Study	Steve Hutchinson, Jennifer Cowley and Jason Ellis	312
A Model for Measuring Perceived Cyberpower	Joey Jansen van Vuuren and Louise Leenen	320
Strengthening Strategic Approach to Counter Cyberspace Threats in Nigeria	Anas Mu'azu Kademi	328

Paper Title	Author(s)	Page Nos
Mitigation of Cyber Warfare in Space Through Reed Solomon Codes	Min Kang, Kenneth Hopkinson, Addison Betances and Mark Reith	338
Economics-Based Risk Management of Distributed Denial of Service Attacks: A Distance Learning Case Study	Omer Keskin, Unal Tatar, Omer Poyraz, Ariel Pinto and Adrian Gheorghe	343
Cyber Threat Landscape in Energy Sector	Tiina Kovanen, Viivi Nuojua and Martti Lehto	353
Russian Cyber Power and Structural Asymmetry	Juha Kukkola	362
Enhancing Cyber Defense Situational Awareness Using 3D Visualizations	Kaur Kullman, Jennifer Cowley and Noam Ben-Asher	369
Educating Future Cyber Strategists Through Wargaming: Options, Challenges and Gaps	Hyong Lee	379
Facing the Culture Gap in Operationalising Cyber Within a Military Context	Louise Leenen, Michael Aschman, Marthie Grobler and Adelai van Heerden	387
Cognitive Biases in Cyber Decision-Making	Antoine Lemay and Sylvain Leblanc	395
Security From the Core: Design of a Next Generation Cyber Resilient Architecture	Alexander Löw and Markus Maybaum	402
Hybrid Information Environment: Grounded Theory Analysis	Erja Mustonen-Ollila, Martti Lehto and Aki-Mauri Huhtinen	412
Improving Information Security Through Risk Management and Enterprise Architecture Integration	Sarah Nather	420
Chateau Cyber: Applying Historical Events to Military Innovation in the Cyber Domain	Geronimo Nuño	427
Suggesting a Honeypot Design to Capture Hacker Psychology, Personality and Sophistication	Murat Odemis, Cagatay Yucel, Ahmet Koltuksuz and Gokhan Ozbilgin	432
Rethinking USAF Cyber Education and Training	Mark Reith, Eric Trias, Chad Dacus, Seth Martin and Landon Tomcho	439
Hardware Trojan Cyber-Physical Threats to Supply Chains	Kurt Sauer, Michael David and Kouichi Sakurai	448
IW™?: Building Global Community, Facebook and Cyber Security in the Post-Westphalian age	Keith Scott	456
Application of Journey Mapping and Crime Scripting to the Phenomenon of Trolling	Tiia Somer, Anna Tiido, Char Sample and Timothy Mitchener-Nissen	465
National Cyber Power and the Inward Culture of Control	Ana Stuparu	474
Redefining the Air-gap for our Weapon Systems	Evan Swihart and Mark Reith	482
Violations of Good Security Practices in Graphical Passwords Schemes: Enterprise Constraints on Scheme-Design	Johannes Vorster, Barry Irwin and Renier van Heerden	487
Beyond the Loop: Can Cyber-Secure, Autonomous Micro-UAVs Stop Active Shooters?	Harry Wingo	497

Paper Title	Author(s)	Page Nos
A Programmable Threat Intelligence Framework for Containerized Clouds	Çağatay Yücel, Ahmet Koltuksuz, Murat Ödemiş, Anas Mu'azu Kademi and Gökhan Özbilgin	503
Phd Research Papers		511
Semantic Risk Assessment for Cybersecurity	Adiel Aviad, Krzysztof Wecel and Witold Abramowicz	513
Comparative Study of Cybersecurity Policy Among South Africa and Mozambique	Martina Jennifer Zucule de Barros and Horst Lazarek	521
Security Implications of National Development of Strategic, Ideational Cyberpower	Ginger Guzman	530
Honeypots and the Attackers Bias	Sharif Hassan and Ratan Guha	533
The Concept of the Critical Information Infrastructure of the Russian Federation	Martti Kari	543
Improving Cyber Defensive Stratagem Through APT Centric Offensive Security Assessment	Jacob Oakley	552
Analysis of Information Systems in the Context of Their Security	Hein Tun, Sergey Lupin, Aye Min Thike and Ko Ko Oo	561
Masters Research Papers		571
Analysis of Intrusion Detection Dataset NSL-KDD Using KNIME Analytics	Mohd Arafat, Archi Jain and Yan Wu	573
Modelling Misbehaviour in Automated Vehicle Intersections in a Synthetic Environment	Karl Bentjen, Scott Graham and Scott Nykl	584
Cyber Synthetic Modeling for Vehicle-to-Vehicle Applications	Jacob Connors, Scott Graham and Logan Mailloux	594
Look Again, Neo: A Software-Defined Networking Moving Target Defense	Samuel Mayer, Mark Reith and Barry Mullins	602
A Review of the Relationship Between Cyber-Physical Systems, Autonomous Vehicles and Their Trustworthiness	Craig Morrison, Elena Sitnikova and Shraga Shoval	611
A Strategic Framework for Cyber Attacks in the Military	Hector Roldan and Mark Reith	622
Securing Data in Transit Using Tunable two Channel Communication	Clark Wolfe, Scott Graham and Paul Simon	627
Non Academic Papers		635
Cyber Intelligence: A Framework for the Sharing of Data	Moniphia Hewling	637
Crypto Currency: Expanding the Underground Cyber Economy	David Rohret and Michael Vella	645
Best Practices for Designing and Conducting Cyber-Physical System Wargames	Daniel Sullivan, Edward Colbert, Alexander Kott, Luke Osterritter and Geoffrey Dobson	651
Work In Progress Papers		661
Teaming With Silicon Valley to Enable Multi-Domain Command and Control	Mason Bruza and Mark Reith	663

Paper Title	Author(s)	Page Nos
Deploying Social Network Security Awareness Through Mass Interpersonal Persuasion (MIP)	Ehinome Ikhaliya, Alan Serrano and Johnnes Arreymbi	668
Cold War Echoes: The Russian Effort to Interfere in the 2016 Election	Zack Schnur and Richard Wilson	675
Machine Learning and Data Mining for IPv6 Network Defence	Michael Weisman, P. Ritchey, G. Shearer, E. Colbert, E. Dauber, L. Knachel, D. Sullivan, T. Parker and R. Greenstadt	681