

# **5th International Conference on Information Warfare and Security 2010**

**(ICIW 2012)**

**Dayton, Ohio, USA  
8-9 April 2010**

**Editors:**

**Edwin Leigh Armistead**

**ISBN: 978-1-62276-674-1**

**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, (2010). 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. (2013)

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](mailto: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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

## Contents

<b>Paper Title</b>	<b>Author(s)</b>	<b>Page No.</b>
Preface		vi
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		viii
Biographies of contributing authors		ix
Mission Impact: Role of Protection of Information Systems	<i>Evan Anderson<sup>1</sup>, Joobin Choobineh<sup>1</sup>, Michael Fazen<sup>1</sup>, and Michael Grimaila<sup>2</sup></i> <i><sup>1</sup>Texas A&amp;M University, College Station, USA</i> <i><sup>2</sup>Air Force Institute of Technology, Wright Patterson AFB, USA</i>	1
Operational art and Strategy in Cyberspace	<i>Sam Arwood, Robert Mills and Richard Raines</i> <i>Air Force Institute of Technology, Wright-Patterson AFB, USA</i>	16
BotNet Communication in an Asymmetric Information Warfare Campaign	<i>Curt Barnard and Barry Mullins</i> <i>Air Force Institute of Technology, Wright-Patterson AFB, USA</i>	23
Distributed Hierarchical Identity Management: a vision	<i>Uri Blumenthal, Joshua Haines and Gerald O'Leary</i> <i>MIT Lincoln Laboratory, Lexington, USA</i>	28
Expanding Cyberspace Education and Training	<i>Jeff Boleng and Michael Henson</i> <i>US Air Force Academy, Colorado, USA</i>	37
Investigation of Network Security Risks Inherent to IPv6	<i>Julie Boxwell Ard</i> <i>University of California, Davis, USA</i>	44
Civilians in Information Warfare: Conscription of Telecom Networks and State Responsibility for International Cyber Defense	<i>Susan Brenner<sup>1</sup> and Maeve Dion<sup>2</sup></i> <i><sup>1</sup>University of Dayton School of Law, USA</i> <i><sup>2</sup>George Mason University School of Law, USA</i>	49
Covert Channels in the HTTP Network Protocol: Channel Characterization and Detecting Man-in-the-Middle Attacks	<i>Erik Brown, Bo Yuan, Daryl Johnson and Peter Lutz</i> <i>Rochester Institute of Technology, Rochester, USA</i>	56
Framework for Developing Realistic MANET Simulations	<i>Ivan Burke<sup>1</sup>, Shahen Naidoo<sup>1</sup> and Martin Olivier<sup>2</sup></i> <i><sup>1</sup>Council for Scientific and Industrial Research, Pretoria South Africa</i> <i><sup>2</sup>University of Pretoria, South Africa</i>	65
Real-Time Detection of Distributed Zero- Day Attacks in ad hoc Networks	<i>James Cannady</i> <i>Nova Southeastern University, Fort Lauderdale, USA</i>	72
Intelligence Activities in Greece and Rome: Extracting Lessons	<i>Evan Dembskey</i> <i>Tshwane University of Technology, South Africa</i>	82
Simple Trust Protocol for Wired and Wireless SCADA Networks	<i>Jose Fadul, Kenneth Hopkinson, Todd Andel, Stuart Kurkowski, James Moore</i> <i>Air Force Institute of Technology, USA</i>	89

<b>Paper Title</b>	<b>Author(s)</b>	<b>Page No.</b>
Security in the Emerging African Broadband Environment	<i>Bryon Fryer, Kris Merritt and Eric Trias Air Force Institute of Technology (AFIT), Dayton, Ohio, USA</i>	98
Critical Infrastructure Control Systems Vulnerabilities	<i>Marchello Graddy and Dennis Strouble Air Force Institute of Technology, Wright-Patterson AFB, USA</i>	106
Legal Frameworks to Confront Cybercrime: a Global Academic Perspective	<i>Virginia Greiman and Lou Chitkushev Boston University, MA, USA</i>	112
Communicating Potential Mission Impact Using Shared Mission Representations	<i>Brian Hale<sup>1</sup>, Michael Grimaila<sup>1</sup>, Robert Mills<sup>1</sup>, Michael Haas<sup>1</sup>, and Phillip Maynard<sup>2</sup> <sup>1</sup>Air Force Institute of Technology, Wright Patterson AFB, USA <sup>2</sup>Air Force Research Laboratory, Wright Patterson AFB, USA</i>	120
Explosion of Connections	<i>Harry Haury NuParadigm Government Systems, Inc., Saint Louis, MO, USA</i>	128
Information Asset Value Quantification Expanded	<i>Denzil Helleesen<sup>1</sup> and Michael Grimaila<sup>2</sup> <sup>1</sup>Air Force Network Integration Center (AFNIC), Scott AFB, USA <sup>2</sup>Air Force Institute of Technology, Wright-Patterson AFB, USA</i>	138
Pearl Harbor 2.0: When Cyber-Acts Lead to the Battlefield	<i>Wayne Henry, Jacob Stange and Eric Trias Air Force Institute of Technology, WPAFB, USA</i>	148
Educating and Training Soldiers for Information Operations	<i>Aki-Mauri Huhtinen<sup>1</sup>, Leigh Armistead<sup>2, 3</sup> and Corey Schou<sup>3</sup> <sup>1</sup>Finnish National Defence University, Helsinki, Finland <sup>2</sup>Goldbelt Hawk LLC, Hampton, USA <sup>3</sup>Idaho State University, Pocatello, USA</i>	155
Improving the Latent Dirichlet Allocation Document Model With WordNet	<i>Laura Isaly, Eric Trias and Gilbert Peterson Air Force Institute of Technology, Wright-Patterson AFB, USA</i>	163
The Impact of the Increase in Broadband Access on South African National Security and the Average Citizen	<i>Joey Jansen van Vuuren<sup>1</sup>, Jackie Phahlamohlaka<sup>1</sup> and Mario Brazzoli<sup>2</sup> <sup>1</sup>Defence Peace Safety and Security: CSIR, Pretoria, South Africa <sup>2</sup>Government Information Technology Officer in the Defence Secretariat, Pretoria, South Africa</i>	171
A Collaborative Process Based Risk Analysis for Information Security Management Systems	<i>Bilge Karabacak<sup>1</sup> and Sevgi Ozkan<sup>2</sup> <sup>1</sup>TUBITAK, Ankara, Turkey <sup>2</sup>METU, Ankara, Turkey</i>	182
Ensuring Communication Security in Delay-Tolerant Networks	<i>Anssi Kärkkäinen Defence Command Finland, Helsinki, Finland</i>	193

<b>Paper Title</b>	<b>Author(s)</b>	<b>Page No.</b>
From ABAC to ZBAC: The Evolution of Access Control Models	<i>Alan Karp<sup>1</sup>, Harry Haury<sup>2</sup> and Michael Davis<sup>3</sup></i> <i><sup>1</sup>Hewlett-Packard Laboratories, USA</i> <i><sup>2</sup>NuParadigm, USA</i> <i><sup>3</sup>SPAWAR, US Navy, USA</i>	202
Malware Detection via a Graphics Processing Unit	<i>Nicholas Kovach and Barry Mullins</i> <i>Air Force Institute of Technology,</i> <i>Wright-Patterson AFB, USA</i>	212
Digital Evidence Collection in Cyber Forensics Using Snort	<i>Thrinadh Praveen Kumar<sup>1</sup>, Lalitha Bhaskari<sup>2</sup>, P. Avadhani<sup>2</sup> and P. Vijaya Kumar<sup>3</sup></i> <i><sup>1</sup>GVP College of Engineering,</i> <i>Visakhapatnam, India</i> <i><sup>2</sup>AU College of Engineering,</i> <i>Visakhapatnam, India</i> <i><sup>3</sup>High Court of Andhra Pradesh,</i> <i>Hyderabad, India</i>	216
Growth Through Uncertainty – the Secure e-Business Evolution of the Small Firm	<i>John McCarthy, Alan Benjamin, Don Milne, Bryan Mills and Peter Wyer</i> <i>Bucks New University, High Wycombe,</i> <i>UK</i> <i>Derby University, UK</i>	223
Hiding Appropriate Messages in the LSB of JPEG Images	<i>Hamdy Morsy<sup>1</sup>, Ahmed Hussein<sup>1</sup>, Joshua Gluckman<sup>2</sup> and Fathy Amer<sup>1</sup></i> <i><sup>1</sup>Faculty of Engineering at Helwan</i> <i>University, Cairo, Egypt</i> <i><sup>2</sup>American University in Cairo, Egypt</i>	232
An Application of Deception in Cyberspace: Operating System Obfuscation	<i>Sherry Murphy, Todd McDonald, and Robert Mills</i> <i>Air Force Institute of Technology, Wright</i> <i>Patterson, USA</i>	241
Insider Threat Detection Using Distributed Event Correlation of Web Server Logs	<i>Justin Myers, Michael Grimaila, and Robert Mills</i> <i>Air Force Institute of Technology, USA</i>	251
Verify Then Trust: A New Perspective on Preventing Social Engineering	<i>Kristopher Nagy, Brian Hale and Dennis Strouble</i> <i>Air Force Institute of Technology,</i> <i>Wright-Patterson AFB, Ohio, USA</i>	259
Cyberspace: Definition and Implications	<i>Rain Ottis and Peeter Lorents</i> <i>Cooperative Cyber Defence Centre of</i> <i>Excellence, Tallinn, Estonia</i>	267
Transparent Emergency Data Destruction	<i>Warren Roberts, Christopher Johnson and John Hale</i> <i>University of Tulsa, USA</i>	271
Cyber-Based Behavioral Fingerprinting	<i>David Robinson and George Cybenko</i> <i>Dartmouth College, Hanover, USA</i>	279
Exploitation of Blue Team SATCOM and MILSAT Assets for red Team Covert Exploitation and Back-Channel Communications	<i>David Rohret and Jonathan Holston</i> <i>Joint Information Operations Warfare</i> <i>Center (JIOWC)/Joint Electronic Warfare</i> <i>Center (JEWIC) San Antonio, USA</i>	281
A Hybrid Approach to Teaching Information Warfare	<i>Dino Schweitzer and Steve Fulton</i> <i>United States Air Force Academy, USA</i>	299

<b>Paper Title</b>	<b>Author(s)</b>	<b>Page No.</b>
A Stochastic Game Model with Imperfect Information in Cyber Security	<i>Sajjan Shiva, Sankardas Roy, Harkeerat Bedi, Dipankar Dasgupta and Qishi Wu University of Memphis, USA</i>	308
Malware Antimalware Games	<i>Anshuman Singh, Arun Lakhotia and Andrew Walenstein University of Louisiana at Lafayette, USA</i>	319
Evaluating the Security of Enterprise VoIP Networks	<i>Peter Thermos Palindrome Technologies, USA</i>	328
An FPGA-Based Malicious DNS Packet Detection Tool	<i>Brennon Thomas and Barry Mullins Air Force Institute of Technology, Wright-Patterson AFB, USA</i>	337
Digital Forensics Detection and Disruption of JPEG Steganaography	<i>George Trawick and Drew Hamilton Auburn University, Auburn Alabama, USA</i>	343
A High-Level Mapping of Cyberterrorism to the OODA Loop	<i>Namosha Veerasamy Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa</i>	352
An Adaptation Based Survivability Framework for Mission Critical Systems	<i>Yanjun Zuo University of North Dakota, Grand Forks, USA</i>	361
<b>Research in Progress Papers</b>		
A Blind Scheme Watermarking Algorithm for Data Hiding in RGB Images Using Gödelization Technique Under Spatial Domain	<i>Peri Avadhani and Lalitha Bhaskari A U College of Engineering (A), Andhra Pradesh, India</i>	373
Automatic Discovery of Attack Messages and Pre- and Post-Conditions for Attack Graph Generation	<i>Marco Carvalho and Choh Man Teng Institute for Human and Machine Cognition, Pensacola, USA</i>	378
Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships Between Cyber Assets, Missions and Users	<i>Anita D'Amico<sup>1</sup>, Laurin Buchanan<sup>1</sup>, John Goodall<sup>1</sup> and Paul Walczak<sup>2</sup> <sup>1</sup>Applied Visions, Inc., Secure Decisions Division, Northport, USA <sup>2</sup>Warrior, LLC, Arlington, USA</i>	388
An Investigation of Malware Type Classification	<i>Thomas Dube<sup>1</sup>, Richard Raines<sup>1</sup>, Bert Peterson<sup>1</sup>, Kenneth Bauer<sup>1</sup>, Steven Rogers<sup>2</sup> <sup>1</sup>Air Force Institute of Technology, WPAFB, Ohio, USA <sup>2</sup>Air Force Research Laboratory, WPAFB, Ohio, USA</i>	398
Language-Driven Assurance for Regulatory Compliance of Control Systems	<i>Robin Gandhi, William Mahoney, Ken Dick and Zachary Wilson University of Nebraska at Omaha, USA</i>	407
AIMFIRST: Planning for Mission Assurance	<i>Tom Haigh, Steven Harp and Charles Payne Adventium Enterprises, Minneapolis, USA</i>	416
Moderating Roles of Organizational Capabilities Affecting Information Security Strategy Effectiveness: A Structural Equation Modeling Analysis	<i>Jacqueline Hall, Shahram Sarkani, and Thomas Mazzuchi The George Washington University, Washington, USA</i>	427

<b>Paper Title</b>	<b>Author(s)</b>	<b>Page No.</b>
Information Operations in Space, Absence of Space Sovereignty, Growing Number of Nations Looking Spaceward: Threats and Fears Concerning Established Space-based Military Powers	<i>Berg Hyacinthe<sup>1</sup> and Larry Fleurantin<sup>2</sup></i> <i><sup>1</sup>Assas School of Law— cersa-cnrs Sorbonne, France</i> <i><sup>2</sup>Fleurantin &amp; Associates, Florida, USA</i>	437
Evaluating the Impact of Cyber Attacks on Missions	<i>Scott Musman, Aaron Temin, Mike Tanner, Dick Fox and Brian Pridemore</i> <i>MITRE Corp, McLean, VA, USA</i>	446
NEO Thinks EBO - a way to Shape Perceptions	<i>Nuno Perry<sup>1</sup> and Paulo Nunes<sup>1, 2</sup></i> <i><sup>1</sup>Competitive Intelligence and Information Warfare Association Club, Funchal, Portugal</i> <i><sup>2</sup>Centro de Investigação da Academia Militar, Lisbon, Portugal</i>	457
Decision-Making by Effective Information Security Managers	<i>James Pettigrew, Julie Ryan, Kyle Salous and Thomas Mazzuchi</i> <i>George Washington University, Washington DC, USA</i>	465
Security Monitoring and Attack Detection in Non-IP Based Systems	<i>Steven Templeton</i> <i>University of California, Davis, USA</i>	473
Federating Enterprises Architectures Using Reference Models	<i>Jeffery Wilson, Thomas Mazzuchi, and Shahram Sarkani</i> <i>The George Washington University, Washington DC, USA</i>	481
<b>Practitioner Papers</b>		
The Weaponry and Strategies of Digital Conflict	<i>Kevin Coleman</i> <i>Security and Intelligence Center at the Technolytics Institute, USA</i>	491
Security Assessment Techniques for Software Assurance – a “Virtual Team” Approach	<i>Derek Isaacs</i> <i>Boecore Inc. Colorado Springs USA</i>	500
Asymmetrical Warfare: Challenges and Strategies for Countering Botnets	<i>Gunter Ollmann</i> <i>Damballa Inc, Atlanta, USA</i>	507
Boundary Management and Integration Framework for a Joint Cyber Defence Capability for Military Forces: Analysis and Synthesis from a Through-Life Capability Management Perspective	<i>Joey Roodt<sup>1</sup>, René Oosthuizen<sup>2</sup> and Jan Jansen van Vuuren<sup>1</sup></i> <i><sup>1</sup>Defence Peace Safety and Security: CSIR, Pretoria, South Africa</i> <i><sup>2</sup>Monzé Consultants, Pretoria, South Africa</i>	513
The Extremist Edition of Social Networking: The Inevitable Marriage of Cyber Jihad and Web 2.0	<i>Dondi West and Christina Latham</i> <i>Booz Allen Hamilton, Hanover, Maryland, USA</i>	523