

**The Proceedings  
of the  
5th International  
Conference on Information  
Warfare and Security**

**The Air Force Institute of  
Technology,  
Wright-Patterson AFB, Ohio, USA**

**8-9 April 2010**

Edited by  
Dr. Edwin Leigh Armistead  
Edith Cowan University, Australia

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.

These Conference Proceedings have been submitted to the Thomson ISI for indexing.

Further copies of this book and previous year's proceedings can be purchased from <http://academic-conferences.org/2-proceedings.htm>

ISBN:97-1-906638-61-0 CD

Published by Academic Publishing Limited  
Reading  
UK  
44-118-972-4148  
[www.academic-publishing.org](http://www.academic-publishing.org)

## Contents

| <b>Paper Title</b>  | <b>Author(s)</b>  | <b>Guide Page</b> | <b>Page No.</b> |
|---|---|-------------------|-----------------|
| Preface   |   | x                 | vi              |
| Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs                                    |   | xiii              | viii            |
| Biographies of contributing authors   |   | xiv               | 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><br><i><sup>1</sup>Texas A&amp;M University, College Station, USA</i><br><i><sup>2</sup>Air Force Institute of Technology, Wright Patterson AFB, USA</i> | 1                 | 1               |
| Operational art and Strategy in Cyberspace  | <i>Sam Arwood, Robert Mills and Richard Raines</i><br><i>Air Force Institute of Technology, Wright-Patterson AFB, USA</i>   | 2                 | 16              |
| BotNet Communication in an Asymmetric Information Warfare Campaign  | <i>Curt Barnard and Barry Mullins</i><br><i>Air Force Institute of Technology, Wright-Patterson AFB, USA</i>  | 3                 | 23              |
| Distributed Hierarchical Identity Management: a vision  | <i>Uri Blumenthal, Joshua Haines and Gerald O'Leary</i><br><i>MIT Lincoln Laboratory, Lexington, USA</i>  | 4                 | 28              |
| Expanding Cyberspace Education and Training   | <i>Jeff Boleng and Michael Henson</i><br><i>US Air Force Academy, Colorado, USA</i>   | 5                 | 37              |
| Investigation of Network Security Risks Inherent to IPv6  | <i>Julie Boxwell Ard</i><br><i>University of California, Davis, USA</i>   | 6                 | 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><br><i><sup>1</sup>University of Dayton School of Law, USA</i><br><i><sup>2</sup>George Mason University School of Law, USA</i>  | 7                 | 49              |

| <b>Paper Title</b>   | <b>Author(s)</b>   | <b>Guide Page</b> | <b>Page No.</b> |
|--|--|-------------------|-----------------|
| 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<br/>Rochester Institute of Technology, Rochester, USA</i>   | 8                 | 56              |
| Framework for Developing Realistic MANET Simulations   | <i>Ivan Burke<sup>1</sup>, Shahen Naidoo<sup>1</sup> and Martin Olivier<sup>2</sup><br/><sup>1</sup>Council for Scientific and Industrial Research, Pretoria South Africa<br/><sup>2</sup>University of Pretoria, South Africa</i> | 9                 | 65              |
| Real-Time Detection of Distributed Zero-Day Attacks in ad hoc Networks   | <i>James Cannady<br/>Nova Southeastern University, Fort Lauderdale, USA</i>  | 10                | 72              |
| Intelligence Activities in Greece and Rome: Extracting Lessons   | <i>Evan Dembskey<br/>Tshwane University of Technology, South Africa</i>  | 11                | 82              |
| Simple Trust Protocol for Wired and Wireless SCADA Networks  | <i>Jose Fadul, Kenneth Hopkinson, Todd Andel, Stuart Kurkowski, James Moore<br/>Air Force Institute of Technology, USA</i>   | 12                | 89              |
| Security in the Emerging African Broadband Environment   | <i>Bryon Fryer, Kris Merritt and Eric Trias<br/>Air Force Institute of Technology (AFIT), Dayton, Ohio, USA</i>  | 13                | 98              |
| Critical Infrastructure Control Systems Vulnerabilities  | <i>Marchello Graddy and Dennis Strouble<br/>Air Force Institute of Technology, Wright-Patterson AFB, USA</i>   | 14                | 106             |
| Legal Frameworks to Confront Cybercrime: a Global Academic Perspective   | <i>Virginia Greiman and Lou Chitkushev<br/>Boston University, MA, USA</i>  | 15                | 112             |

| <b>Paper Title</b>  | <b>Author(s)</b>   | <b>Guide Page</b> | <b>Page No.</b> |
|---|--|-------------------|-----------------|
| 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></i><br><i><sup>1</sup>Air Force Institute of Technology, Wright Patterson AFB, USA</i><br><i><sup>2</sup>Air Force Research Laboratory, Wright Patterson AFB, USA</i> | 16                | 120             |
| Explosion of Connections  | <i>Harry Haury</i><br><i>NuParadigm Government Systems, Inc., Saint Louis, MO, USA</i>   | 17                | 128             |
| Information Asset Value Quantification Expanded                             | <i>Denzil Helleesen<sup>1</sup> and Michael Grimaila<sup>2</sup></i><br><i><sup>1</sup>Air Force Network Integration Center (AFNIC), Scott AFB, USA</i><br><i><sup>2</sup>Air Force Institute of Technology, Wright-Patterson AFB, USA</i>   | 18                | 138             |
| Pearl Harbor 2.0: When Cyber-Acts Lead to the Battlefield                   | <i>Wayne Henry, Jacob Stange and Eric Trias</i><br><i>Air Force Institute of Technology, WPAFB, USA</i>  | 19                | 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></i><br><i><sup>1</sup>Finnish National Defence University, Helsinki, Finland</i><br><i><sup>2</sup>Goldbelt Hawk LLC, Hampton, USA</i><br><i><sup>3</sup>Idaho State University, Pocatello, USA</i>                  | 20                | 155             |
| Improving the Latent Dirichlet Allocation Document Model With WordNet       | <i>Laura Isaly, Eric Trias and Gilbert Peterson</i><br><i>Air Force Institute of Technology, Wright-Patterson AFB, USA</i>   | 21                | 163             |

| <b>Paper Title</b>  | <b>Author(s)</b>   | <b>Guide Page</b> | <b>Page No.</b> |
|---|--|-------------------|-----------------|
| 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></i><br><i><sup>1</sup>Defence Peace Safety and Security: CSIR, Pretoria, South Africa</i><br><i><sup>2</sup>Government Information Technology Officer in the Defence Secretariat, Pretoria, South Africa</i>                                | 22                | 171             |
| A Collaborative Process Based Risk Analysis for Information Security Management Systems                   | <i>Bilge Karabacak<sup>1</sup> and Sevgi Ozkan<sup>2</sup></i><br><i><sup>1</sup>TUBITAK, Ankara, Turkey</i><br><i><sup>2</sup>METU, Ankara, Turkey</i>  | 23                | 182             |
| Ensuring Communication Security in Delay-Tolerant Networks  | <i>Anssi Kärkkäinen</i><br><i>Defence Command Finland, Helsinki, Finland</i>   | 24                | 193             |
| 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><br><i><sup>1</sup>Hewlett-Packard Laboratories, USA</i><br><i><sup>2</sup>NuParadigm, USA</i><br><i><sup>3</sup>SPAWAR, US Navy, USA</i>   | 25                | 202             |
| Malware Detection via a Graphics Processing Unit  | <i>Nicholas Kovach and Barry Mullins</i><br><i>Air Force Institute of Technology, Wright-Patterson AFB, USA</i>  | 26                | 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><br><i><sup>1</sup>GVP College of Engineering, Visakhapatnam, India</i><br><i><sup>2</sup>AU College of Engineering, Visakhapatnam, India</i><br><i><sup>3</sup>High Court of Andhra Pradesh, Hyderabad, India</i> | 27                | 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><br><i>Bucks New University, High Wycombe, UK</i><br><i>Derby University, UK</i>   | 28                | 223             |

| <b>Paper Title</b>  | <b>Author(s)</b>  | <b>Guide Page</b> | <b>Page No.</b> |
|---|---|-------------------|-----------------|
| 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><br><i><sup>1</sup>Faculty of Engineering at Helwan University, Cairo, Egypt</i><br><i><sup>2</sup>American University in Cairo, Egypt</i> | 29                | 232             |
| An Application of Deception in Cyberspace: Operating System Obfuscation   | <i>Sherry Murphy, Todd McDonald, and Robert Mills</i><br><i>Air Force Institute of Technology, Wright Patterson, USA</i>  | 30                | 241             |
| Insider Threat Detection Using Distributed Event Correlation of Web Server Logs                                     | <i>Justin Myers, Michael Grimaila, and Robert Mills</i><br><i>Air Force Institute of Technology, USA</i>  | 31                | 251             |
| Verify Then Trust: A New Perspective on Preventing Social Engineering   | <i>Kristopher Nagy, Brian Hale and Dennis Strouble</i><br><i>Air Force Institute of Technology, Wright-Patterson AFB, Ohio, USA</i>   | 32                | 259             |
| Cyberspace: Definition and Implications   | <i>Rain Ottis and Peeter Lorents</i><br><i>Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia</i>   | 33                | 267             |
| Transparent Emergency Data Destruction  | <i>Warren Roberts, Christopher Johnson and John Hale</i><br><i>University of Tulsa, USA</i>   | 34                | 271             |
| Cyber-Based Behavioral Fingerprinting   | <i>David Robinson and George Cybenko</i><br><i>Dartmouth College, Hanover, USA</i>  | 35                | 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><br><i>Joint Information Operations Warfare Center (JIOWC)/Joint Electronic Warfare Center (JEWIC) San Antonio, USA</i>   | 36                | 285             |
| A Hybrid Approach to Teaching Information Warfare   | <i>Dino Schweitzer and Steve Fulton</i><br><i>United States Air Force Academy, USA</i>  | 37                | 299             |

| <b>Paper Title</b>  | <b>Author(s)</b>  | <b>Guide Page</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<br/>University of Memphis, USA</i> | 38                | 308             |
| Malware Antimalware Games   | <i>Anshuman Singh, Arun Lakhotia and Andrew Walenstein<br/>University of Louisiana at Lafayette, USA</i>          | 39                | 319             |
| Evaluating the Security of Enterprise VoIP Networks   | <i>Peter Thermos<br/>Palindrome Technologies, USA</i>   | 40                | 328             |
| An FPGA-Based Malicious DNS Packet Detection Tool   | <i>Brennon Thomas and Barry Mullins<br/>Air Force Institute of Technology, Wright-Patterson AFB, USA</i>          | 41                | 337             |
| Digital Forensics Detection and Disruption of JPEG Steganaography   | <i>George Trawick and Drew Hamilton<br/>Auburn University, Auburn Alabama, USA</i>                                | 42                | 343             |
| A High-Level Mapping of Cyberterrorism to the OODA Loop   | <i>Namosha Veerasamy<br/>Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa</i>        | 43                | 352             |
| An Adaptation Based Survivability Framework for Mission Critical Systems  | <i>Yanjun Zuo<br/>University of North Dakota, Grand Forks, USA</i>  | 44                | 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<br/>A U College of Engineering (A), Andhra Pradesh, India</i>               | 47                | 373             |
| Automatic Discovery of Attack Messages and Pre- and Post-Conditions for Attack Graph Generation                       | <i>Marco Carvalho and Choh Man Teng<br/>Institute for Human and Machine Cognition, Pensacola, USA</i>             | 48                | 378             |

| <b>Paper Title</b>   | <b>Author(s)</b>  | <b>Guide Page</b> | <b>Page No.</b> |
|--|---|-------------------|-----------------|
| 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></i><br><i><sup>1</sup>Applied Visions, Inc., Secure Decisions Division, Northport, USA</i><br><i><sup>2</sup>Warrior, LLC, Arlington, USA</i>                              | 49                | 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></i><br><i><sup>1</sup>Air Force Institute of Technology, WPAFB, Ohio, USA</i><br><i><sup>2</sup>Air Force Research Laboratory, WPAFB, Ohio, USA</i> | 50                | 398             |
| Language-Driven Assurance for Regulatory Compliance of Control Systems   | <i>Robin Gandhi, William Mahoney, Ken Dick and Zachary Wilson</i><br><i>University of Nebraska at Omaha, USA</i>  | 51                | 407             |
| AIMFIRST: Planning for Mission Assurance   | <i>Tom Haigh, Steven Harp and Charles Payne</i><br><i>Adventium Enterprises, Minneapolis, USA</i>   | 52                | 416             |
| Moderating Roles of Organizational Capabilities Affecting Information Security Strategy Effectiveness: A Structural Equation Modeling Analysis                                   | <i>Jacqueline Hall, Shahram Sarkani, and Thomas Mazzuchi</i><br><i>The George Washington University, Washington, USA</i>  | 53                | 427             |
| 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><br><i><sup>1</sup>Assas School of Law—cersa-cnrs Sorbonne, France</i><br><i><sup>2</sup>Fleurantin &amp; Associates, Florida, USA</i>  | 54                | 437             |
| Evaluating the Impact of Cyber Attacks on Missions   | <i>Scott Musman, Aaron Temin, Mike Tanner, Dick Fox and Brian Pridemore</i><br><i>MITRE Corp, McLean, VA, USA</i>   | 55                | 446             |

| <b>Paper Title</b>   | <b>Author(s)</b>   | <b>Guide Page</b> | <b>Page No.</b> |
|--|--|-------------------|-----------------|
| NEO Thinks EBO - a way to Shape Perceptions  | <i>Nuno Perry<sup>1</sup> and Paulo Nunes<sup>1, 2</sup></i><br><i><sup>1</sup>Competitive Intelligence and Information Warfare Association Club, Funchal, Portugal</i><br><i><sup>2</sup>Centro de Investigação da Academia Militar, Lisbon, Portugal</i> | 56                | 457             |
| Decision-Making by Effective Information Security Managers   | <i>James Pettigrew, Julie Ryan, Kyle Salous and Thomas Mazzuchi</i><br><i>George Washington University, Washington DC, USA</i>   | 57                | 465             |
| Security Monitoring and Attack Detection in Non-IP Based Systems   | <i>Steven Templeton</i><br><i>University of California, Davis, USA</i>   | 58                | 473             |
| Federating Enterprises Architectures Using Reference Models  | <i>Jeffery Wilson, Thomas Mazzuchi, and Shahram Sarkani</i><br><i>The George Washington University, Washington DC, USA</i>   | 59                | 481             |
| <b>Practitioner Papers</b>   |  |                   |                 |
| The Weaponry and Strategies of Digital Conflict  | <i>Kevin Coleman</i><br><i>Security and Intelligence Center at the Technolytics Institute, USA</i>   | 63                | 491             |
| Security Assessment Techniques for Software Assurance – a “Virtual Team” Approach  | <i>Derek Isaacs</i><br><i>Boecore Inc. Colorado Springs USA</i>  | 64                | 500             |
| Asymmetrical Warfare: Challenges and Strategies for Countering Botnets   | <i>Gunter Ollmann</i><br><i>Damballa Inc, Atlanta, USA</i>   | 65                | 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><br><i><sup>1</sup>Defence Peace Safety and Security: CSIR, Pretoria, South Africa</i><br><i><sup>2</sup>Monzé Consultants, Pretoria, South Africa</i>     | 66                | 513             |

| <b>Paper Title</b>   | <b>Author(s)</b>   | <b>Guide Page</b> | <b>Page No.</b> |
|--|--|-------------------|-----------------|
| The Extremist Edition of Social Networking: The Inevitable Marriage of Cyber Jihad and Web 2.0 | <i>Dondi West and Christina Latham Booz Allen Hamilton, Hanover, Maryland, USA</i> | 67                | 525             |
| <b>Poster</b>  |  |                   |                 |
| Decision making in the Cyber Domian: The Influence of Trust and Mood                           | <i>Charlene Stokes Airforce Research Lab</i>                                       | 71                |                 |

## Preface

These Proceedings are the work of researchers contributing to the 5th International Conference on Information Warfare and Security (ICIW 2010), hosted this year by the Air Force Institute of Technology in Dayton, Ohio, USA. The Conference Chair is Michael Grimaila from AFIT and once again I am pleased to be Programme Chair.

The opening keynote address this year is given by Dr. Michael VanPutte, Defense Advanced Research Projects Agency (DARPA), USA on the topic of *Mission Assurance - Cornerstone of Computer Network Operations*. The second day will be opened by Dr. Steve Rogers, Air Force Research Laboratory, AFIT, Ohio, USA who will talk about *Integrated human computer solutions for the 'wicked' problems we face*.

An important benefit of attending this conference is the ability to share ideas and meet the people who hold them. The range of papers will ensure an interesting and enlightened discussion over the full two day schedule. The topics covered by the papers this year illustrate the depth of the information operations' research area, with the subject matter ranging from the highly technical to the more strategic visions of the use and influence of information.

With an initial submission of 108 abstracts, after the double blind, peer review process there are 62 papers published in these Conference Proceedings, including contributions from Egypt, Estonia, Finland, France, India, Portugal, South Africa, Turkey, the United Kingdom and the United States.

I wish you a most enjoyable conference.

April 2010  
Leigh Armistead  
Edith Cowan University  
Programme Chair

## Conference Executive:

[Michael Grimaila](#), Center for Cyberspace Research, WPAFB, Ohio, USA  
[Edwin Leigh Armistead](#), Edith Cowan University, Australia  
[Robert Mills](#), Air Force Institute of Technology, WPAFB, Ohio, USA  
[Rusty Baldwin](#), Air Force Institute of Technology, WPAFB, Ohio, USA  
[Barry Mullins](#), Air Force Institute of Technology, WPAFB, Ohio, USA  
[Gilbert Peterson](#), Air Force Institute of Technology, WPAFB, Ohio, USA  
[Dorothy Denning](#), Naval Postgraduate School, Monterey, CA, USA  
[Doug Webster](#), MITRE Corporation - United States Strategic Command's Global Innovation & Strategy Center  
[Kevin Streff](#), Dakota State University, USA  
[Andy Jones](#), Security Research Centre, BT, UK  
[William Mahoney](#), University of Nebraska Omaha, Omaha, USA  
[Dan Kuehl](#), National Defense University, Washington DC, USA  
[Corey Schou](#), Idaho State University, USA  
[Bhavani Thuraisingham](#), University of Texas at Dallas, USA

### **Program Committee**

Lt Col [Jeffrey Humphries](#), Air Force Institute of Technology, WPAFB, Ohio, USA  
Lt Col [Todd McDonald](#), Air Force Institute of Technology, WPAFB, Ohio, USA  
Lt Col [Stuart Kurkowski](#), Air Force Institute of Technology, WPAFB, Ohio, USA  
Maj [Todd Andel](#), Air Force Institute of Technology, WPAFB, Ohio, USA  
Maj [Eric Trias](#), Air Force Institute of Technology, WPAFB, Ohio, USA  
[Dennis Strouble](#), Air Force Institute of Technology, WPAFB, Ohio, USA  
[Juan Lopez](#), Air Force Institute of Technology, WPAFB, Ohio, USA

### **Committee Members:**

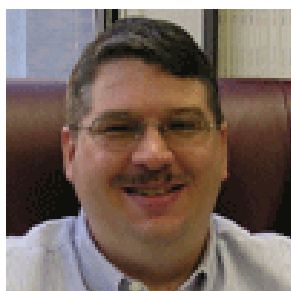
The conference programme committee consists of key people in the information systems, information warfare and information security communities around the world. The following people have confirmed their participation:

Gail-Joon Ahn (University of North Carolina at Charlotte, USA); Jim Alves-Voss (University of Idaho, USA); Todd Andel (Air Force Institute of Technology, USA); Leigh Armistead (Edith Cowan University, Australia); [Johnnes Arreymbi](#) (University of East London, UK); Rusty Baldwin (Air Force Institute of Technology, USA); [Richard Baskerville](#) (Georgia State University, USA); Allan Berg (Critical Infrastructure and Cyber Protection Center, Capitol College, USA); [Sviatoslav Braynov](#) (University of Illinois, USA); Acma Bulent (Anadolu University, Eskisehir, Turkey); Blaine Burnham (University of Nebraska, Omaha, USA); Catharina Candolin (Finnish Defence Forces, Helsinki, Finland); Rodney Clare (EDS and the Open University, UK); Nathan Clarke (University of Plymouth, UK); Ronen Cohen (Ariel University Centre, Israel); Geoffrey Darnton, (University of Bournemouth, UK); [Dipankar Dasgupta](#) (Intelligent Security Systems, USA); Dorothy Denning (Naval Postgraduate School, USA); Glenn Dietrich (University of Texas, USA); David Fahrenkrug (US Air Force, USA); Kevin Gleason (KMG Consulting, MA, USA); [Sanjay Goel](#) (University at Albany, USA); [Michael Grimaila](#) (Air Force Institute of Technology, Ohio, USA); Daniel Grosu (Wayne State University, USA); [Drew Hamilton](#) (Auburn University, USA); Dwight Haworth (University of Nebraska at Omaha, USA); Philip Hippensteel (Penn State University, USA); Jeffrey Humphries (Air Force Institute of Technology, USA); Bill Hutchinson (Edith Cowan University, Australia); Berg P Hyacinthe (Assas School of Law, Universite Paris, France); Cynthia Irvine (Naval Postgraduate School, USA); Andy Jones (British Telecom, UK); James Joshi (University of Pittsburgh, USA); Leonard Kabeya Mukeba (Kigali Institute of Science and Technology, Rwanda); Prashant Krishnamurthy (University of Pittsburgh, USA); Dan Kuehl (National Defense Forces, USA); Stuart Kurkowski (Air Force Institute of Technology, USA); Takakazu Kurokawa (National Defense Academy, Japan); Rauno Kuusisto (National Defence College, Finland); Tuija Kuusisto (Internal Security ICT Agency, Finland); Arun Lakhota (University of Louisiana Lafayette, USA); Louise Leenan (CSIR, South Africa); [Sam Liles](#) (Purdue University Calumet, USA); Cherie Long (Clayton State University, Decatur, USA); Brian Lopez (Lawrence Livermore National Laboratory); Juan Lopez (Air Force Institute of Technology, USA); [Bin Lu](#) (West Chester University, USA); Bill

Mahoney (University of Nebraska, USA); Billy Maloney (UAHuntsville and Dynetics Inc., Huntsville, USA); John McCarthy (Buckinghamshire and Chiltern University College, UK); J Todd McDonald (Airforce Institute of Technology, USA); Robert Mills (Air Force Institute of Technology, Ohio, USA); [Don Milne](#) (Buckinghamshire and Chiltern University College, UK); [Srinivas Mukkamala](#) (New Mexico Tech, Socorro, USA); Barry Mullins (Air Force Institute of Technology, USA); [Andrea Perego](#) (Università degli Studi dell'Insubria, Italy); Gilbert Patterson (Air Force Institute of Technology, USA); Jackie Phahlamohlaka (Council for Scientific and Industrial Research, Petoria, South Africa); Richard Raines (Airforce Institute of Technology, USA); Ken Revett (University of Westminster, UK); [Neil Rowe](#) (US Naval Postgraduate School, USA); Julie Ryan (George Washington University, USA); Corey Schou (Idaho State University, USA); [Dan Shoemaker](#) (University of Detroit Mercy, USA); William Sousan (University of Nebraska, Omaha, USA); [Kevin Streff](#) (Dakota State University, USA); Dennis Strouble (Air Force Institute of Technology, USA); Eric Trias (Air Force Institute of Technology, USA); Bhavani Thuraisingham (University of Dallas at Texas, USA); [Doug Twitchell](#) (Illinois State University, USA); Renier van Heerden (CSIR, Pretoria, South Africa); Stylianos Vidalis (Newport Business School, UK); Fahad Waseem (University of Northumbria, UK); Kenneth Webb, Edith Cowan University, Australia; Douglas Webster (USSTRATCOM Global Innovation & Strategy Center, USA); Zehai Zhou (Dakota State University, USA).

# Biographies of Conference Chairs, Programme Chairs and Keynote Speakers

## Conference Chairs



**Dr. Michael Grimaila.** Michael is an associate professor and a member of the Center for Cyberspace Research at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. He is a Certified Information Security Manager (CISM), Certified Information System Security Professional (CISSP), and holds NSA IAM/IEM certifications. He teaches and conducts research in the areas of information assurance, information warfare, and information operations. Dr. Grimaila serves as an Editorial Board member of the

Information System Security Association (ISSA) Journal and has served on the DoD/NII IA Best Practices and Metrics Working Groups. He is a member of the ACM, IRMA, ISACA, ISC2, ISSA, ISSEA, and is a senior member of the IEEE. Michael holds a BS, Electrical Engineering; MS, Electrical Engineering; and PhD, Computer Engineering, all from Texas A&M University, USA

## Programme Chairs

**Dr Edwin “Leigh” Armistead.** Leigh is the Director of Business Development for Goldbelt Hawk LLC, the Programme Chair for the International Conference of Information Warfare and an Adjunct Lecturer for Edith Cowen University in Perth, Australia. He has written nine books, 18 journal articles, presented 17 academic papers and served as a Chairman for 16 professional and academic conferences. Formerly a Master Faculty at the Joint Forces Staff College, Leigh received his PhD from Edith Cowan University with an emphasis on *Information Operations*. He also serves as a Co-Editor for the *Journal of International Warfare*, and the Editorial Review Board for European Conference on Information Warfare.

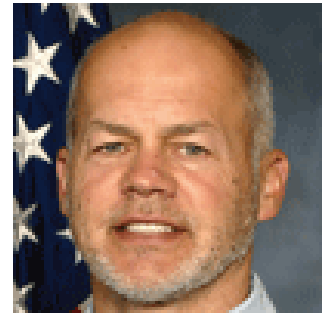


## Keynote Speakers



**Dr. Michael VanPutte.** Michael joined the Defense Advanced Research Projects Agency (DARPA) in 2006 as a Program Manager in the Strategic Technology Office. His interests lie in information assurance and computer network operations, artificial intelligence, and multi-agent systems. He is currently the DARPA program manager for multiple defensive cyber programs including the National Cyber Range, Dynamic Quarantine of Worms, and the Cyber Genome Program as well as a number of SBIRs, studies and research initiatives focused on revolutionizing cyber security and cyber scientific experimentation. Dr. VanPutte retired from the Army in September 2008 having served as an infantryman, airborne ranger, combat engineer officer and computer systems engineer. From 2002 to 2006 Dr. VanPutte held a number of positions in the Joint Task Force - Global Network Operations, U.S. Strategic Command including Technical Analysis Branch Chief, Strategic Defense Operations Branch Chief and Deputy Director of Operations. Dr. VanPutte was the Chief of the Knowledge Engineering Group, U.S. Army War College from 1997 to 1999. Mike received a BS from The Ohio State University, an MS in Computer Science from the University of Missouri, Columbia, and a Ph.D. in Computer Science from the Naval Postgraduate School.

**Dr. Steven Rogers.** Steven is the Senior Scientist for Automatic Target Recognition and Sensor Fusion, Air Force Research Laboratory, Air Force Materiel Command, Wright-Patterson AFB, OH. He serves as the principal scientific authority and independent researcher in the field of multi-sensor automatic target recognition (ATR) and sensor fusion. Steve has had an extensive career in both government service and civilian industry. He is a Fellow of both the IEEE and SPIE and was chosen to be the organizing chair the first IEEE World Conference on Computational Intelligence as well as being the Plenary Speaker for two WCCIs.



## **Biographies of contributing authors (in alphabetical order)**

**Fathy Amer** is the professor of Electronics in the department of Communications and Electronics, Helwan University, Cairo, Egypt. Previously, He was an associate professor at faculty of training at El ahsaa, Saudia Arabia from 1995 to 2004. His research interests include Microelectronics and Testing and Information Hiding.

**Julie Boxwell Ard** is pursuing a PhD in Computer Engineering at the University of California, Davis, CA. She holds a Bachelors in Applied Mathematics from Texas A&M University and returns to academia from industry where she supported advanced Government research. Ms. Ard's PhD focus is Computer Security.

**Edwin "Leigh" Armistead** is the Director of Business Development for Goldbelt Hawk LLC, the Programme Chair for the International Conference of Information Warfare and an Adjunct Lecturer for Edith Cowen University in Perth, Australia. He has written nine books, 18 journal articles, presented 17 academic papers and served as a Chairman for 16 professional and academic conferences. Formerly a Master Faculty at the Joint Forces Staff College, Leigh received his PhD from Edith Cowan University with an emphasis on Information Operations.

**Peri Avadhani** is a professor in the department of Computer Science and Engineering of Andhra University. He has guided one Ph.D student and right now he is guiding 10 Ph.D Scholars from various institutes. He has guided more than 93 M.Tech. Projects. He received many honors and he has been the member for many expert committees, member of Board of Studies for various universities, Resource person etc for various organizations. He has co-authored 4 books.

**Curtis Barnard** is a Master's student majoring in Cyber Operations at the Air Force Institute of Technology and a recipient of the CyberCorp fellowship provided by the National Science foundation. He completed his undergraduate studies at Rose-Hulman Institute of Technology with a BS in Computer Science.

**Lalitha Bhaskari** is an Associate professor in the department of Computer Science and Engineering of Andhra University. Her areas of interest include Theory of computation, Data Security, Image Processing, Data communications, Pattern Recognition. Apart from her regular academic activities she holds prestigious responsibilities like Associate Member in the Institute of Engineers, Member in IEEE, Associate Member in the Pentagon Research Foundation, Hyderabad, India.

**Susan Brenner** is NCR Distinguished Professor of Law and Technology at the University of Dayton School of Law. She has spoken at numerous conferences, and is the author of law review articles dealing with cybercrime and cyberconflict. In 2009 Oxford published her most recent book: *Cyber Threats: Emerging Fault Lines of the Nation-States*.

**Thomas Brennon** is currently pursuing a Master's degree in Cyber Operations at the Air Force Institute of Technology at Wright-Patterson AFB. He previously spent three years on active duty as a communications officer at the former Air Force Communications Agency. He received a BS degree in Electrical Engineering from Rensselaer Polytechnic Institute.

**Erik Brown** received a Bachelors of Science Degree in Information Security and Forensics from Rochester

**Ivan Burke** is a Msc student in the department of Computer Science at the University of Pretoria, South Africa. He also works full time at the Council of Scientific and Industrial Research South Africa in the department of Defense Peace Safety and Security, where he works within the Command, Control and Information Warfare research group

**James Cannady** is an Associate Professor in the Graduate School of Computer and Information Sciences at Nova Southeastern University (NSU). Dr. Cannady's research efforts concern the intersection between artificial intelligence and information security. In particular he is working to develop new adaptive intelligent systems that can be applied to protect computer systems and networks.

**Marco Carvalho** is a Research Scientist at the Florida Institute for Human and Machine Cognition (IHMC). His background is in Mechanical Engineering (Dynamical Systems) and Computer Science. He received his Ph.D. from Tulane University, and has participated and led several research projects sponsored by the DoD and Industry in the areas of biologically inspired security and cognitive network management.

**Lou Chitkushev** is Chairman of Computer Science Department at Boston University's Metropolitan College and Director of Information Security and Biometrics Laboratory. He is co-founder and Associate Director of The Boston University Center for Reliable Information Systems and Cyber Security, and he played a crucial role in the initiatives that led to Boston University's designation as a Center of Academic Excellence in Information Assurance by the National Security Agency and Department of Homeland Security.

**Jobin Choobineh** research areas include Management Information Systems, Business Database Systems, and Systems Analysis and Design. He has authored or been a coauthor of more than fifty (50) articles. He has served as the chair of 8 and committee member of 11 Ph.D. students. Dr. Choobineh is currently an Associate Editor of *INFORMS Journal on Computing* and serves on the editorial board of the *International Journal of Business Information Systems*.

**Anita D'amico** is the Director of the Secure Decisions division of Applied Visions, Inc. Her research and publications are in the areas of information visualization, computer network defense, cognitive analysis, and technology transition into the operational environment. She received a B.A. from University of Pennsylvania, and an M.S. and Ph.D. in psychology from Adelphi University.

**Mike Davis** is the warranted Chief Systems Engineer for Navy large deck ships and aircraft C4I integration at SPAWAR Headquarters (USN). He also held PEO C4I IA/Security leadership roles in PMW 160/1. He currently serves as the San Diego ISSA Vice President and Technical Advisor for “The Security Networks” –Mike has over 20 years experience in IT/IA technical and operational leadership positions in many diverse government and commercial programs/projects/venues. He earned graduate degrees in Management and Electrical Engineering.

**Evan Dembskey** comes from Johannesburg, South Africa, and has studied both ICT and Ancient History to a masters level. He is currently pursuing a doctorate in computer science. In the future, he hopes to combine his love of science and history.

**Thomas Dube** currently serves in the United States Air Force as a Ph.D. student at the Air Force Institute of Technology. Most recently, he worked in the tactics and assessment squadrons at the Air Force Information Operations Center at Lackland AFB, TX. His previous research examined the use of malware defenses for non-malicious software. He also developed near real-time simulation systems at the Air Force Research Laboratory.

**Jose Fadul** is a doctoral student in the Air Force Institute of Technology's Department of Electrical and Computer Engineering. He received an M.S. in software engineering from the Air Force Institute of Technology (AFIT) at Wright-Patterson AFB, Ohio and a B.S. in electrical engineering from the University of Central Florida, Orlando, Florida.

**Steve Fulton** is a visiting scholar at the US Air Force Academy. A 20+ year employee of the US Department of Defense, Dr. Fulton holds a BS Computer Science (Armstrong Atlantic State University), MS Education (University of Maryland, Baltimore County), MA Information Management (Syracuse University) and D. Mgt (University of Maryland University College).

**Joshua Gluckman** is an assistant professor in the department of computer science at the American University of Cairo. Previously, he was an assistant professor at Polytechnic University. He received a B.A. from the University of Virginia, a M.S. from the College of William and Mary, and a Ph.D. in computer science from Columbia University.

**Virginia Greiman**, Professor of International Law and Mega Project Finance at Boston University is a recognized expert on global infrastructure development, privatization and legal reform. Her experience includes high level appointments for the U.S. Department of Justice and legal adviser to the U.S. Department of State and the U.S. Agency for International Development in Eastern and Central Europe, Asia, and Africa on privatization and development projects.

**Tom Haigh** has over twenty-five years of experience in Cyber Security. Before coming to Adventium he was VP for Research and CTO at the Secure Computing Corp. At Adventium Dr. Haigh has led a number of projects that apply automated reasoning to Cyber Security. His Ph.D. from the University of Wisconsin is in mathematics.

**Brian Hale** is a student at the Air Force Institute of Technology (AFIT) pursuing a Master's Degree in Information Resource Management. Prior to attending AFIT, Chief Hale was the Knowledge Operations Management and Postal Air Force Career Field Manager, Washington DC. He oversaw training, manpower, utilization, and related actions involving 11,000 personnel.

**Jacqueline Hall** is a doctoral candidate in Engineering Management and Systems Engineering at The George Washington University. She has a BS in Electrical Engineering with a minor in Mathematics and an MBA with a minor in Information Systems from Old Dominion University, as well an MS in Systems Engineering from the George Washington University.

**Berg Hyacinthe** (PhD, Florida State University; LLD Candidate, Assas School of Law, CERSA-CNRS, La Sorbonne) is internationally recognized as an eminent multidisciplinary scientific investigator. He held several positions at County and State levels of the U.S. Government in the Information Technology arena. A U.S. patent holder featured in Harvard's Smithsonian/NASA Astrophysics Data System,

**Ahmed Hussein** is an assistant professor in the School of Engineering, Helwan University, Egypt. He holds a Ph.D. and M.Sc. in Computer Science and Engineering from University of Connecticut, USA. His research interests include multimedia networking, peer-to-peer systems, network security, and wireless sensor networks

**Derek Isaacs** is a Sr. IA Engineer for Boecore Inc. working at Schriever AFB. He is involved in certification and accreditation support as well as security assessments (including Software Assurance, Vulnerability Assessments, wireless, and penetration testing) across a variety of systems, networks, and programs. Derek holds BS & MS degrees from the University of California, Riverside; and an MS degree in Computer Systems Security from Colorado Technical University.

**Laura Isaly** is a recent graduate of the Air Force Institute of Technology with a Master of Science in Computer Science. In 2005 she graduated from the University of South Carolina with a Bachelor of Science in Computer Engineering. Captain Isaly's next assignment is to the Air Force Technical Application Center (AFTAC) at Patrick AFB, FL.

**Bilge Karabacak** received B.S. degree from Bilkent University, in 1999 in Electronics Engineering. He received M.S. degree from Gebze Institute of Technology, in 2003 in Computer Engineering. He is currently pursuing Ph.D. in Middle East Technical University. He has been working as chief researcher at Scientific and Technological Research Council of Turkey since Febraury 2000.

**Anssi Kärkkäinen** graduated from the National Defence University in 2000. He also graduated a Master of Science (Engineering) degree from Helsinki University of Technology in 2005. Currently he is carrying out doctoral studies at the same university. His current assignment is a Staff Officer for Defence Command Finland.

**Nicholas Kovach** received a Bachelors of Science degree in Computer Science from Wittenberg University, Springfield, OH in 2008. He is currently pursuing a Masters of Science degree in Computer Science at the Air Force Institute of Technology, Wright-Patterson AFB, OH.

**Kuppili Thrinadh Praveen Kumar** is a currently working as Assistant professor in Gayatri Vidya Parishad College of Engineering, Visakhapatnam. He pursued his Master's degree in Computer Science and Technology with specialization in Computer Networks from A U College of Engineering, Andhra University, Visakhapatnam, INDIA. He pursued his Bachelor's degree in Electronics and communication engineering from Jawaharlal Nehru Technological University, Hyderabad, INDIA.

**Arun Lakhota** is the Lockheed Martin professor of computer science at Center for Advanced Computer Studies, University of Louisiana at Lafayette. His research interests are analysis of malicious programs and machine intelligence. He has won various distinctions including 2004 Louisiana Governor's University Technology Leader of the Year Award and Outstanding Teacher Award.

**John McCarthy** PhD, B.Sc. (hons) MBCS. John is the founder of LeadSure. John is highly entrepreneurial in nature and runs several IT companies. His background is in Internet Technology. He has spoken at major IT conferences around the world on the opportunities e-business can present to SME's..

**Todd McDonald** is an assistant professor of Computer Science in the Department of Electrical and Computer Engineering at AFIT. Lt Col McDonald received a BS degree in Computer Science from the United States Air Force Academy, an MS in Computer Engineering from AFIT, and a PhD in Computer Science from the Florida State University. His research interests include software protection, obfuscation and anti-tamper applications, and secure software engineering.

**Robert Mills** is an Associate Professor of Electrical Engineering at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB OH. He teaches graduate courses and leads sponsored research in support of AFIT's cyber operations and warfare program. His research interests include network management and security, communications systems, cyber warfare, and systems engineering.

**Hamdy Morsy** is a PhD student at Faculty of Engineering at Helwan University, Cairo, Egypt. He received his M.Sc. (2002) from Stevens Institute of Technology, Hoboken, NJ, USA. He is currently working as a senior teaching assistant at faculty of engineering at Helwan University.

**Justin Myers** received his B.S. in Computer Science from Cedarville University in 2008. He is currently a Master's Student and Research Assistant at Air Force Institute of Technology (AFIT), working with the Center for Cyberspace Research (CCR) on event correlation and insider threat detection.

**Gunter Ollmann** is the vice president for research at Damballa -Prior to joining Damballa, Ollmann held several strategic positions at IBM Internet Security Systems (IBM ISS) with the most recent being the Chief Security Strategist. In this role he was responsible for predicting the evolution of future threats and helping guide IBM's overall security research and protection strategy, as well as being the key IBM spokesperson on evolving threats and mitigation techniques.

**Nuno Perry**, Chief Information and Security Officer (IDRAM, Madeira). Degree in Information Systems and Management (ISCTE. Lisbon). Post-graduated in Computer Engineering and Telecommunications (ISCTE, Lisbon). Post-graduated in Competitive Intelligence / Information Warfare (Academia Militar, Lisbon). Member of Specialized Working Group of Competitive Intelligence and Information Warfare Association Clube (CIWAC, Lisbon)

**Rain Ottis** is a scientist at the Cooperative Cyber Defence Centre of Excellence. He is pursuing a PhD degree at Tallinn University of Technology (TUT), where he researches cyber conflicts and patriotic hacking from the national security perspective. He is a graduate of TUT (MSc, Informatics) and the United States Military Academy (BS, Computer Science).

**James Pettigrew** received a B.S (1978) in Biology from King College, Bristol, TN and a M.S (1987) in Management Information Systems from the University of Arizona, Tucson, AZ. He is a retired U.S. Air Force Officer and currently is a Senior Systems Engineer for the National Geospatial-Intelligence Agency.

**Warren Roberts** is a graduate research assistant with the Institute for Information Security (iSec) at the University of Tulsa. He started out with ISec's research into Risk-Adaptive Access Control, but has moved on to spear-head research into Transparent Emergency Data Destruction.

**Jan Roodt** has more than 25 years experience in modeling of complex systems from the growth of semiconductor crystals and rocket engine infrared signatures to systems at the IDEF0 level for capability development. His current work is focussed on approaches to marry qualitative and quantitative models of socio-technical systems.

**Roy Sankardas** He received his PhD degree in Information Technology from George Mason University, USA in 2008. Currently, he is a postdoctoral researcher in University of Memphis, USA. His research interests include sensor network security, ad hoc network security, and network security in general.

**Anshuman Singh** is a doctoral fellow and a PhD candidate in the Center for Advanced Computer Studies, University of Louisiana at Lafayette. He is currently working on his dissertation that aims to develop game. theoretical models of program obfuscator and deobfuscator interaction and in general the malware antimalware interaction. His research interests include abstract interpretation, program analysis, theoretical cryptography, computation models like interaction machines and evolving algebras.

**Dennis Strouble** is an assistant professor at the Air Force Institute of Technology at Wright-Patterson AFB where he teaches Systems Engineering Management, Law, and Information Technology. He has a BS degree from Pennsylvania State University, a Masters from the University of Southern California, and a PhD. and JD from Texas Tech University.

**Steven Templeton** has worked in security research and development for over 12 years on projects spanning the financial sector, military security systems, and electric energy regulatory compliance. He has a BA from University of California, San Diego, and a MS in computer science from University of California, Davis, where he is currently completing his PhD.

**George Trawick** is an active duty Army officer serving as a PhD candidate at Auburn University. LTC Trawick's experience ranges from battlefield network deployment and security with the 3<sup>rd</sup> ID to Joint level Information Assurance policy and implementation at Joint Forces command.

**Joey van Vuuren** is the Research Group Leader for Information Warfare at the Council for Scientific Research at the CSIR South Africa. This research group is mainly involved in research for the SANDF and Government sectors on Cyber Defence. She is already in academia and research for 25 years and currently focus on the analysis of Cyber threads.

**Namosha Veerasamy** has obtained her BSc: IT Computer Science and BSc. Computer Science (Hons) degree with distinction from the University of Pretoria. Miss Veerasamy is qualified as a Certified Information Systems Security Professional (CISSP) and is currently completing her Masters in Computer Science at the University of Pretoria.

**Dondi West** is an Associate at Booz Allen Hamilton and a former Information Warfare Officer in the U.S. Navy. He holds a B.S. in Mathematics, a M.S. in Applied Information Technology, and is a 2010 Juris Doctor Candidate at The University of Maryland School of Law, where is an Editor of the *Maryland Law Review*. Dondi's scholarly interests include information operations and warfare policy, information privacy law, and cyberspace law.

**Jeff Wilson** is a doctoral candidate in Systems Engineering at The George Washington University within the School of Engineering and Applied Science. He received a MS in Electrical Engineering from the Air Force Institute of Technology and a BS in Electrical Engineering from the US Air Force Academy.

**Yanjun Zuo** received his Ph.D. in computer science from the University of Arkansas, Fayetteville, USA in 2005. He also holds a master degree in computer science from the University of Arkansas and a master degree in business administration from the University of North Dakota, Grand Forks, USA. Currently he is an assistant professor at the University of North Dakota.

# Mission Impact: Role of Protection of Information Systems

Evan Anderson<sup>1</sup>, Joobin Choobineh<sup>1</sup>, Michael Fazen<sup>1</sup>, and Michael Grimaila<sup>2</sup>

<sup>1</sup>Texas A&M University, College Station, USA

<sup>2</sup>Air Force Institute of Technology, Wright Patterson AFB, USA

**Abstract:** Use of information technology (IT) hardware and software has become an integral component in the execution of modern combat operations. However, the use of this technology in support of military operations is constantly subject to adversarial threats. Confidentiality, Integrity, Availability, and Other (CIAO) breaches of information can adversely affect the outcome of military operations. In order to enable the quantification of the effect of these breaches, we model military operations using Business Process Modeling Notation (BPMN). Operations are represented as process models as a set of interconnected activities. Each of the activities of a mission is analyzed to identify dependencies on the underlying information technology (IT) resources. IT resources are in turn protected by protector resources. The dependencies are represented using two dependency matrices. One matrix represents the dependency of military activities on information resources. The other matrix represents the dependency of information resources on their protecting resources. Based on one of the author's actual combat experience, we present a hypothetical, but realistic, military operation. For this operation we develop the following: 1) a BPMN representation of the operation from the Receipt of Operations Order (military term for the start of the mission) to the Change of Mission (military term for the end of the operation), 2) the list of information resources that are needed to support the activities of the operation, 3) the list of the protectors for these information resources, 4) the dependency matrix between the components of the activities of the BPMN and the information resources, and 5) the dependency matrix between the information resources and their protectors. We will discuss the impact of CIAO breaches by tracing the chain of affects on the information resources, the activities, and eventually the outcome of the operation itself.

**Keywords:** Information security management, mission modeling, security models, BPMN

# **Operational art and Strategy in Cyberspace**

**Sam Arwood, Robert Mills and Richard Raines**

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

**Abstract:** While there has been much written about cyberspace and the potential of cyber warfare in general, there is little discussion about specific cyber warfare theory—that is how cyberspace capabilities can be integrated with other traditional military capabilities to influence an adversary, achieve effects, and win wars. The purpose of this paper is to stimulate conversation about operational art in cyberspace. Specifically, we present a planning approach that ties together national strategy, instruments of national power, and a well-known targeting strategy for complex systems. The result is a method of selecting targets that can be traced to higher-level strategies and outcomes.

**Keywords:** Cyber warfare theory, operational planning

# **BotNet Communication in an Asymmetric Information Warfare Campaign**

**Curt Barnard and Barry Mullins**

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

**Abstract:** As computer viruses have evolved, they have developed means of communicating that turned them into one of the greatest threats in modern computer security. Initially, viruses would connect to an Internet chat server to receive instructions, whether they be to launch a denial of service attack or to harvest credit card numbers from the computers they infected. Over time, these Botnets developed more advanced methods of communicating and now use peer-to-peer and other distributed protocols for issuing commands. This paper describes how infected machines in a Botnet communicate, and how the goal of a Botnet might cause the creator to tailor their communication to achieve that goal. This paper culminates with a brief summary of our research into Botnet communication channels.

**Keywords:** Botnets, data exfiltration, steganography, covert command and control

# **Distributed Hierarchical Identity Management: A Vision**

**Uri Blumenthal, Joshua Haines and Gerald O'Leary**  
**MIT Lincoln Laboratory, Lexington, USA**

**Abstract:** This paper addresses the issues of Global Public Key Infrastructure (PKI). It points out some reasons why PKI has not been as pervasive as it could be, what are its limitations, and what obstacles the current approach places on the road to global usability and interoperability. The paper widens the definition of attributes and proposes putting emphasis on Attribute Certificates. Multiple hierarchical authorities would manage these attributes. The paper brings forth reasons why and how such an approach could be scaled to global community. The paper describes technical and political challenges along this path, and ways to address them. The novelty of this approach is applying architectural design and experience from other Internet subsystems to Identity Management field.

**Keywords:** Globally interoperable PKI, Identity management

# Expanding Cyberspace Education and Training

**Jeff Boleng and Michael Henson**  
**US Air Force Academy, Colorado, USA**

**Abstract:** The global, pervasive interconnected grid of electrical, electronic, and information technologies has created a new domain in the same sense as the physical domains of land, air, and sea that we all depend on. The domain of cyberspace impacts everyone and is a key element of the global community and commerce. Warfare in the cyber domain is inevitable and ongoing. Participation in and dependence on the cyber domain is not limited to computer scientists or computer engineers. On the contrary, actions in the cyber domain impact everyone, but ironically, most cyber education and training is narrowly focused to technical specialties. This paper outlines our efforts at the US Air Force Academy to provide in depth cyber warfare experiences, including network defense, exploitation, and attack, to a wide range of students. Our goal is to provide a deep set of experiences to all our graduates so they are equipped with the knowledge and skills to effectively defend the United States in, through, and with cyberspace.

**Keywords:** Education, training, cyberspace, information warfare

# Investigation of Network Security Risks Inherent to IPv6

**Julie Boxwell Ard**

**University of California, Davis, USA**

**Abstract:** In 2005, the federal Government mandated that government agencies start using Internet Protocol version 6 (IPv6) by June 2008 (Evans 2005). However, the majority of IPv6 security tools are simply the v6-compatible version of the v4 tool. Even now, contemporary literature in the IT industry reflects the approach of providing IPv6-enabled security, not IPv6-specific security. Government networks depend on industry to provide security tools and since the federal Government, rather than the IT industry, is driving the transition from IPv4 to IPv6, they may implement IPv6 with security tools not designed for IPv6. This may provide less sophisticated hackers a window of opportunity to compromise previously inaccessible systems. This is an asymmetric threat to all users of IPv6 worldwide. As with the introduction of any new type of technology, particularly one as deeply integrated and far-reaching as IPv6, there is a danger of unknown vulnerabilities. It stands to reason that new types of attacks will exploit the new features of IPv6, which will cause vulnerabilities in networks running IPv6 traffic to types of attacks not seen before in IPv4 traffic. Additionally since IPv4 security is the basis for most IPv6 security tools, developers designed the new tools around v4 threats; this represents a serious vulnerability in Government and commercial networks, which will run IPv6 traffic. We review two types of Denial of Service attacks and discuss interoperability issues between IPSec and Network Address Translation (NAT). IPSec has several potential security benefits but administrators cannot widely deploy IPSEC until they resolve some nontechnical issues. Denial of Service attacks based on TCP Flood will likely have the same effectiveness on IPv6 networks that they have now on IPv4 networks, but Broadcast Amplification Attacks should be less common on IPv6 networks than they are currently on IPv4 networks. We also present ideas for future work that will contribute to a smoother and more secure transition from IPv4 to IPv6.

**Keywords:** IPv6, internet network security

# **Civilians in Information Warfare: Conscription of Telecom Networks and State Responsibility for International Cyber Defense**

**Susan Brenner<sup>1</sup> and Maeve Dion<sup>2</sup>**

**<sup>1</sup>University of Dayton School of Law, USA**

**<sup>2</sup>George Mason University School of Law, USA**

**Abstract:** Information warfare will likely operate across civilian-owned networks, but the role of civilians in information warfare is far from clear. This first section surveys nationalization and conscription as ways to ensure civilian-owned networks are available to support information warfare. Recent conflicts have demonstrated the difficulties of attributing state sponsorship to civilian cyber aggression and compelling cross-border cooperation in attack response. The second section assesses legal structures to help address these difficulties. Civilian involvement in information warfare raises new legal issues. Resolving these issues will require new strategies and new legal doctrines. This paper helps establish frameworks for permissible and prohibited conduct in both the domestic and international arenas, and encourages further scholarship on these legal topics.

**Keywords:** Information warfare, civilian networks, nationalization, conscription, state responsibility, international law

# Covert Channels in the HTTP Network Protocol: Channel Characterization and Detecting Man-in-the-Middle Attacks

**Erik Brown, Bo Yuan, Daryl Johnson and Peter Lutz**  
**Rochester Institute of Technology, Rochester, USA**

**Abstract:** Network covert channels provide two entities the ability to communicate stealthily. Hypertext Transfer Protocol (HTTP), which accounts for approximately half of all traffic on the Internet (Burke, 2007), has become the fertile ground for various network covert channels. Proliferation of network covert channels throughout the World Wide Web and other areas of cyberspace has raised new security concerns and brought both challenges and enhancements to the area of Information Warfare. Covert channels impact our ability to observe and orient in this domain and need to be better understood. They are however, extremely difficult to study as a whole. Network covert channels tend to be protocol, implementation, and/or application specific. Similar to biology or botany, where we classify plants and animals, the first step of research is to define a classification scheme. In the paper, it is intended to define a set of common characteristics, classify and analyze several known covert channels in HTTP with respect to these characteristics. New HTTP based covert channels are discussed and their characteristics presented as well. Although many applications of covert channels are malicious in nature, this paper argues that there are beneficial applications of network covert channels, such as detecting Man-in-the-Middle attacks.

**Keywords:** Network covert channels, data hiding, HTTP, network security, man-in-the-middle

# Framework for Developing Realistic MANET Simulations

Ivan Burke<sup>1</sup>, Shahen Naidoo<sup>1</sup> and Martin Olivier<sup>2</sup>

<sup>1</sup>Council for Scientific and Industrial Research, Pretoria South Africa

<sup>2</sup>University of Pretoria, South Africa

**Abstract:** Mobile Ad hoc Networks have become an attractive option for military and disaster-response operations. Its ad hoc nature allows for fast deployment and requires no pre-existing network infrastructure. Most of the MANET protocol development is achieved by means of simulation due to the cost of running real world applications. However, it has become apparent in recent research papers that the simulations of these networks do not adequately reflect reality. In this paper, we aim to investigate some of the assumptions that are made during MANET protocol development and how these assumptions affect the results of these studies. A framework is suggested to help assist future studies to be more attentive to these assumptions. This framework aims at improving the credibility of MANET research for future deployment of MANET systems.

**Keywords:** Realistic, mobile ad hoc network, framework, credibility

# Real-Time Detection of Distributed Zero-Day Attacks in ad hoc Networks

**James Cannady**

**Nova Southeastern University, Fort Lauderdale, USA**

**Abstract:** Current intrusion detection approaches rely upon previous exposure to an attack sequence before it can be accurately identified in subsequent exposures. Because of this, zero-day attacks, especially those that are distributed in ad hoc environments, are extremely difficult to detect accurately in real-time. Due to the potential for damage and exploitation that can be caused by zero-day attacks accurate and rapid detection is critical. This paper describes a lightweight self-organizing intrusion detection approach that is designed to detect distributed zero-day attacks in mobile ad hoc networks (MANET). Traditional methods of intrusion detection have limited effectiveness in a MANET and detection approaches designed for wireless networks are limited to the identification of previously identified and analyzed attacks or non-specific anomalous activity in the network data stream. The new approach uses a multi-stage modified fuzzy neural network architecture to detect both known and zero-day attacks against the MANET. The distributed detection process occurs in real-time and requires the exchange of far less data than in current distributed detection approaches. More importantly, it is the first approach that function within wireless ad hoc networks that is able to recognize new attacks before significant damage can occur to the protected network. This approach was validated experimentally in a controlled environment against several attack scenarios that were modified to preclude detection by existing rule-based and anomaly detection methods.

**Keywords:** MANET, intrusion detection, neural network

# **Intelligence Activities in Greece and Rome: Extracting Lessons**

**Evan Dembskey**

**Tshwane University of Technology, South Africa**

**Abstract:** The acquisition and use of information is an essential part of warfare and economic activity in all societies throughout time. The timely delivery of information has often turned the tide of battle to advantage, and the lack of it to disadvantage. It is clear from the literature that the Greeks and Romans had to some extent at least codified the practice of intelligence and warfare into formal practice. Starting with the premise that it is possible avoid repeating mistakes, we ask the question: Is it possible to draw parallels between modern warfare, particularly in Iraq and Afghanistan, and warfare in Ancient Greece and Rome? This paper, which is research in progress, is the first in a series that asks the question of whether or not it is possible to apply lessons from the ancient to the modern world. The focus is on the details of Roman and Greek intelligence gathering and transmission, and the consequences of intelligence failure.

**Keywords:** Ancient Greece, Rome, cryptography, Steganography, information warfare, Iraq, Afghanistan

# **Simple Trust Protocol for Wired and Wireless SCADA Networks**

**Jose Fadul, Kenneth Hopkinson, Todd Andel, Stuart Kurkowski, James Moore**

**Air Force Institute of Technology, USA**

**Abstract:** Existing Supervisory Control and Data Acquisition (SCADA) networks are not designed with security in mind. Traditional SCADA controllers react in an automated way that is oblivious to unanticipated malicious attacks, component malfunctions and other byzantine failures. A fast method is needed that takes trust into account in SCADA control systems. In this article, we develop the Simple Trust protocol to allow for low computational and bandwidth cost in evaluating trust between SCADA components and demonstrate (through simulation) its capability to meet SCADA critical timing constraints. This type of system is a first step towards more sophisticated SCADA controllers, which can proactively operate under malicious attacks and failure conditions.

**Keywords:** Trust, protocol, security, SCADA, wired networks, wireless networks

# **Security in the Emerging African Broadband Environment**

**Bryon Fryer, Kris Merritt and Eric Trias**

**Air Force Institute of Technology (AFIT), Dayton, Ohio, USA**

**Abstract:** With broadband service proposed to be widely available in Africa by 2011, computer insecurity implications that could affect more than Africa's borders abound. The insecurity issues are intensified by the increase in digital aid being offered Africans in the form of free computers as well as the widespread use of pirated operating systems, which lack current security patches and updates. The imminent threat this places on Africans and Internet users around the globe is one that needs further clarification, observation, and critical review. We examine the causal relationships between widespread software piracy, unpatched systems, ease of connection, and impacts on the potential exploitation of such a vulnerable environment. Ultimately, theoretical examination through qualitative analysis lead us to a set of finite issues that need to be addressed. Africa's computer systems are among the most vulnerable to exploitation. As broadband services become more accessible, nefarious actors exploiting the vulnerability presented by Africa's general computer insecurity could wreak havoc across the globe. Some entities have the ability to act now, but the window of opportunity is narrowing. This is a preliminary analysis of how this vulnerable environment is forming as well as who has the ability to mitigate the negative impact of this broadband explosion, such as operating system developers, antivirus vendors, local and national leaders, and information technology communities.

**Keywords:** Africa, Software Piracy, Botnet, Broadband, Social Responsibility

# **Critical Infrastructure Control Systems Vulnerabilities**

**Marchello Graddy and Dennis Strouble**

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

**Abstract:** As computer technology has permeated much of today's society, the interconnectedness of the world can be viewed as both an economic advantage and a security weakness. The networked world has nourished an environment in which cyber warfare can flourish. Cyber warfare has become a desired mode of fighting when attacking a highly industrialized and wired nation. Nations throughout the world are developing and executing cyber warfare strategies to disrupt their enemy's communications, logistics, transportation and military infrastructures. One of the most powerful attacks that can be rendered on a nation's ability to make war is a cyber attack on the computerized systems that control its critical infrastructure. Critical infrastructure includes a nation's communications, public works, financial and utility institutions. In the United States, the utility infrastructure control systems were designed as non-networked, stand alone entities to prevent unauthorized infiltration. With the privatization of utility services, these systems are now being integrated with corporate communication infrastructures in an effort to achieve cost savings and are now vulnerable to attack. The systems, with their dedicated software and hardware, are unable to be patched to address security concerns. Additionally, when utility services upgrade their control systems, budgetary constraints force them to select a commercially available software packages that are available throughout the world. These programs can also be purchased by the enemies of the state and then manipulated to gain knowledge of the system that can result in unfettered access to the nation's critical infrastructure control systems. Although public and private organizations throughout the nation have taken the initiative and made small strides in security, more must be done. The government of the United States must develop and enforce standards on infrastructure control systems to safeguard the nation's lifeblood, its critical infrastructure. This paper provides a non-technical overview of the United States' critical utility infrastructure control systems. The overview includes the proliferation of their use, their history, security threats and incidents. Also highlighted are some of the initiatives that both public and private organizations have taken to address this issue. Finally recommendations to increase security are made.

**Keywords:** Cyber warfare, infrastructure control systems

# Legal Frameworks to Confront Cybercrime: A Global Academic Perspective

**Virginia Greiman and Lou Chitkushev**  
**Boston University, USA**

**Abstract:** The goal of this research is to educate computer and engineering professionals on the developing field of cyberlaw and its relationship to cybersecurity. From a pedagogical perspective, understanding the Internet has become as essential as learning a language or learning to write. In our technology driven economy we must understand both its power and its limitations. Presently, cyberlaw scholarship is in its early stages particularly as it relates to surveillance issues and international legal frameworks for the prevention of cyber crime. Young students have much to contribute to this growing discipline and cyberlaw scholarship can contribute to the challenges faced by our Executive and Legislative Branches as they address important issues of national security and the growing incidence of cybercrime around the globe. Though many law schools offer courses on cyberlaw or ecommerce, there is an absence of these courses offered through the schools of management, computer science and engineering schools beyond a very basic level. Even scholars in the field have noted the importance of the subject matter, but there is a general lack of discussion among faculty as to how the course should be designed and delivered. Largely, these courses have focused on intellectual property rights and rights to privacy and have failed to cover the important topics of legal frameworks for surveillance, crime prevention, and the harmonization of laws among different cultures, jurisdictions and countries. The purpose of this paper is to develop a cyberlaw curriculum that will address the present void in this critical area of the law. The recommended curriculum will incorporate the current legal framework for regulating cyber crimes and contrast it with national cyberlaw systems around the globe. The curriculum will introduce basic theory, analytical dialogue, creative concepts, and relevant case studies that will persuade students to appreciate and apply cybersecurity concepts in their professional career. Using an empirical approach, our research will investigate, assess and evaluate legal frameworks for cybersecurity. The curriculum will be of value to students, professionals and academicians interested in (1) advancing their knowledge of the necessity for international law on cybercrime and warfare, (2) understanding legal authorities, jurisdiction and boundaries in engaging adversarial cyber activities, and (3) developing legal frameworks to provide cybersecurity for critical infrastructure.

**Keywords:** Cyberlaw, cybersecurity, surveillance, internet

# Communicating Potential Mission Impact Using Shared Mission Representations

**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**

**Abstract:** Commercial, governmental, and military organizations alike have deeply embedded information technologies into their core mission processes due to enormous benefits provided by data, information, and knowledge management. Despite the development, promulgation, and implementation of information assurance best practices, inevitably an organization will experience an information incident (e.g., the loss of confidentiality, integrity, availability, non-repudiation, and/or authenticity of an information asset). When this occurs, it is imperative to inform those that are critically dependent on the affected information resources in a timely and relevant manner so that appropriate contingency measures can be taken to assure mission operations. While various methods have been proposed to improve the timeliness of incident notification, little work has been done to investigate how to improve the relevance of notification to affected decision makers. In this paper, we explore recent developments in improving the relevance of notification that use shared mission representations as a means to efficiently communicate potential mission impacts following an information incident. Specifically, we consider the use of shared representations of the organizational functions, tasks, and processes, annotated with information dependencies and constraints, as a means to communicate relevant mission impacts to decision makers in a timely manner. We conjecture that the use of annotated models provides the ability to provide meaningful, actionable understanding of the potential impact following an information incident.

**Keywords:** Mission impact assessment, situational awareness, mission assurance

# Explosion of Connections

Harry Haury

NuParadigm Government Systems, Inc., Saint Louis, MO, USA

**Abstract:** A radical new approach to IA is required to address the fundamental change in computing arising from the loss of physical and logical boundaries. The author of this paper proposes a unique architectural solution to the problem that addresses the loss of these boundaries and should also prove to be scalable while supporting high performance computing requirements at the same time. The solution lies in the construct of a new mechanism of enforcing “virtual” boundaries and controlling the flow of information across those boundaries based on a discrete and limited set of new components. The required components include a trusted set of object guards that can enforce in-bound and out-bound policy at intersection boundaries as they apply to attributed data, the use of digital signatures and authorization policy for all access by persons and non-person entities and movement of data through the system, the establishment of a means of creating ownership domains at the information level, creating protected object tunnels between participating systems in order to establish broadly deployed but cryptographically isolated communities, the development of a low cost trusted computing platform supporting community and application isolation or the isolation of computing platforms by community, and the creation of a ubiquitous standard for moving key material, policy, program code, and certificates around the Internet to pre-position the material necessary for processing, policy adjudication, and authorization in order to minimize real time interaction between systems and to allow independent processing nodes to maintain the highest level of independence in real time as is possible. This paper builds a framework for resolving what may be the most important threat to national security and our economy to develop over the last 50 years. Further, it shows why this will solve the problem using practical to implement components compatible with today’s evolving development and integration patterns.

**Keywords:** Information technology, sharing, IT sectors

# Information Asset Value Quantification Expanded

Denzil Hellesen<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

**Abstract:** History exhaustively demonstrates information as critical to the military and has only further increased as information is used to conduct all aspects of modern military decision making and operations. The value of information has increased to the level of being identified as a commodity or asset through organizational activities of information collecting, processing, analyzing, distributing, and aggregating for purposes of tactical, operational and strategic planning, and command decision making. Vital to an organization is the confidentiality, integrity, availability, quality and timeliness of the information as a violation of information can detrimentally affect the success of an organization's military or business activities. It is crucial when an information violation or breach occurs for timely and accurate determination of loss, damage, and impact resulting from the breach to include notification to affected organizational units that are depending upon the information. In this paper, we continue research expanding development of an Information Asset Valuation (IAV) process for a qualitative valuation methodology used for assigning value to information asset (InfoA) within a military context. Valuation of information as an asset relies upon both tangible and intangible valuation measures to create a linkage between the organizational mission and the supporting InfoA. We review existing non-military information valuation methodologies used in the accounting and information technology disciplines to determine their applicability in a military context for understanding the effectiveness of each discipline as adaptable models for IAV. The intention of this work is the development of foundational methodologies supporting the creation of an automated Cyber Incident Mission Impact Assessment (CIMIA) Decision Support Software (DSS) tool to provide near real time cyber environmental awareness. CIMIA addresses the competing functions of mission capability (operations) and the sustaining computer infrastructure (communications) for effective decision making prior to, during, and post cyber incident situations. The objective of this work is to identify potential methodologies for InfoA factor measurements of accessibility, availability, confidentiality, context, essentiality, integrity, non-repudiation, substitutability, temporality which impact information valuation. A standardized taxonomy of information valuation measures would help improve consistency, reduce uncertainty, and promote documentation of information value during the risk assessment process, and enable the aggregation of information asset value in support of higher level decision making processes.

**Keywords:** Information valuation, asset, subjective assessment, information asset, InfoA

# **Pearl Harbor 2.0: When Cyber-Acts Lead to the Battlefield**

**Wayne Henry, Jacob Stange and Eric Trias  
Air Force Institute of Technology, WPAFB, USA**

**Abstract:** Today, America is under constant siege in cyberspace, with an uncountable number of daily attacks ranging from benign to insidious. Which of these attacks would draw America into a major conflict like Pearl Harbor in 1941 or the terrorist's acts on September 11, 2001? Despite the exponential increase in cyberspace attacks, no international policy has adequately established a characterization for what acts constitute an "act of war." The issues left unaddressed by this vacuum in policy include the determination of cyber attack fallout, the appropriate attribution of these attacks to particular actors and the severity of response gauged by seriousness of the act and culpability of the actor. Our paper assumes that we can accurately ascribe cyber actions to a specific actor through forensic and other means. Additionally, the focus and scope of any cyber attack damage is always determinable. We view these factors as we might view a real attack in retrospect: as if all actors, targets of interest, and the full extent of the damages are known and attributed. Taking these considerations into account, we present a method for classifying the gravity of cyber attacks (based on the act and the actor); in particular, the de facto act of war and appropriate levels of response. Without international cooperation to establish an acceptable policy for responses to suspicious and/or malicious cyber-activity, the world will see more devastating cyber campaigns such as Estonia in 2007, Lithuania and Georgia in 2008, and Kazakhstan in 2009. In this paper, we present a taxonomy using an effects-based approach to examine cyber-activities, specifically, those that would constitute a threat or use of force, such that they would evoke actions from the defender to use force in self-defense. Simply put, what actions would lead to an act of war? We hope this research will encourage policymakers to establish clear guidance to deter, recognize and respond to cyber attacks.

**Keywords:** War, cyber, policy, Pearl Harbor, act of war, use of force

# Educating and Training Soldiers for Information Operations

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

**Abstract:** Military Training and Education is evolving because of the growing influence of Information Operations (IO) and Information Warfare (IW). This influence has grown from the tremendous changes in both technology and social issues. Traditional military training has dealt with key elements such as operational concepts of war, doctrine and law; leadership; combat skills; weapons skills; and operating effectively under stress. Yet the technology has changed from stones to cannons to silicon based weapons, while the basic curriculum for soldiers in some cases has not changed for centuries. One might say *plus ca change, plus c'est la meme chose* but it is more than that. Traditional training and combat skills often do not match the modern battle field. We must progress beyond the traditional combined arms doctrine. Modern soldiers must not only be traditional warriors; they must be competent in information operations and information warfare. This paper addresses how we are to initiate this integration.

**Keywords:** Information Warfare, training, education, soldiers, cyber, information operations

# Improving the Latent Dirichlet Allocation Document Model with WordNet

Laura Isaly, Eric Trias and Gilbert Peterson

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

**Abstract:** In the e-intelligence/counter-intelligence domain, actionable information must be extracted, filtered, and correlated from massive amounts of disparate often free text data. The usefulness of the information depends on how we accomplish these steps and present the most relevant information to the analyst. One method for extracting information from free text is Latent Dirichlet Allocation (LDA), a document categorization technique to classify documents into cohesive topics. Although LDA accounts for some implicit relationships such as synonymy (same meaning) it often ignores other semantic relationships such as polysemy (different meanings), hyponym (subordinate), and meronym (part of). To compensate for this deficiency, we incorporate explicit word ontologies, such as WordNet, into the LDA algorithm to account for various semantic relationships. Experiments over well-known document collections, 20 Newsgroups, NIPS, and OHSUMED, demonstrate that incorporating such background knowledge improves perplexity measure over LDA alone.

**Keywords:** Latent Dirichlet Allocation (LDA), semantic ontology, synset, Information Retrieval (IR)

# The Impact of the Increase in Broadband Access on South African National Security and the Average Citizen

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

**Abstract:** South Africa is the entry point to the African continent and with the impending increase in broadband access from 120 Gbps to 12 Tbps over the next 2 years, it could in future be used as a hub for launching cyber warfare type attacks on the rest of the world. In addition, there are arguments that RSA's strong ties with China could place it at high risk of cyber war attacks. Presently because of very low broadband penetration in South Africa and in Africa, chances of it being used to launch attacks to other countries are limited. However, the fact that it will be hosting the 2010 FIFA World Cup increases the vulnerabilities as was experienced with previous soccer world cups in other countries. In either case there are national security implications associated with an increase in broadband access. In addition the compromised PC's of citizens could in future be used as a hub for launching cyber warfare type attacks on the rest of the world. This in turn will pose a national security threat not only to South Africa but also to the rest of the world. The central argument in this paper is that the exponential increase in internet broadband will result in an increase in security threats that will also take the battlefield to the home of the average citizen in rural South Africa. The paper adopts an argumentative analytical approach with the intention to sensitise all nations on issues of national security. We draw on the South African case to demonstrate the potential impact on South Africa that could follow the planned increase in broadband access in Africa as well as on the average RSA citizen. A national security generic framework is used to analyse these threats and the impact on the average citizen. In conclusion the paper proposes ways of addressing the threats flowing from the security threat analysis.

**Keywords:** Cyber warfare, national security South Africa, broadband access, rural areas, home battlefield, security threat analysis

# **A Collaborative Process Based Risk Analysis for Information Security Management Systems**

**Bilge Karabacak<sup>1</sup> and Sevgi Ozkan<sup>2</sup>**

**<sup>1</sup>TUBITAK, Ankara, Turkey**

**<sup>2</sup>METU, Ankara, Turkey**

**Abstract:** Today, many organizations quote intent for ISO/IEC 27001:2005 certification. Also, some organizations are en route to certification or already certified. Certification process requires performing a risk analysis in the specified scope. Risk analysis is a challenging process especially when the topic is information security. Today, a number of methods and tools are available for information security risk analysis. The hard task is to use the best fit for the certification. In this work we have proposed a process based risk analysis method which is suitable for ISO/IEC 27001:2005 certifications. Our risk analysis method allows the participation of staff to the determination of the scope and provides a good fit for the certification process. The proposed method has been conducted for an organization and the results of the applications are shared with the audience. The proposed collaborative risk analysis method allows for the participation of staff and managers while still being manageable in a timely manner to uncover crucial information security risks.

**Keywords:** ISO/IEC 27001:2005, information security, risk analysis, flow chart, process approach

# Ensuring Communication Security in Delay-Tolerant Networks

**Anssi Kärkkäinen**

**Defence Command Finland, Helsinki, Finland**

**Abstract:** Delay-tolerant networking (DTN) is an approach to communication network architecture that addresses the technical issues in heterogeneous networks that lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, such as tactical military networks. Disruption may occur because of the limits of wireless radio range, scarcity of mobile tactical nodes, energy resources, attack, and noise. Addressing security issues has been a major focus of the delay-tolerant networking protocols. Security concerns for delay-tolerant networks vary depending on the environment and application, though authentication, availability and privacy are often critical. These security guarantees are difficult to establish in a network without persistent connectivity. Solutions have typically been modified from mobile ad hoc network and distributed security research, such as the use of distributed certificate authorities and PKI schemes. In this paper, these challenging security issues are described and an architectural security framework of DTN is defined. The paper proposes some basic functionality and an architecture to describe the desired communication security features. Implementation issues of technologies are also discussed, but the final verification of these techniques is not presented.

**Keywords:** Security, delay-tolerant network, tactical military networks

# From ABAC to ZBAC: The Evolution of Access Control Models

Alan Karp<sup>1</sup>, Harry Haury<sup>2</sup> and Michael Davis<sup>3</sup>

<sup>1</sup>Hewlett-Packard Laboratories, USA

<sup>2</sup>NuParadigm, USA

<sup>3</sup>SPAWAR, US Navy, USA

**Abstract:** Several attempts at using the Services Oriented Architecture have failed to achieve their goals of scalability, security, and manageability. These systems, which base access decisions on the authentication of the requester, have been found to be inflexible, don't scale well, and are difficult to use and upgrade. In this paper we describe how access control models have evolved to solve manageability problems as the systems we used have scaled up in size and as they became more distributed. We then introduce an approach to access control that solves the problems we see today and show that this approach is a natural extension of previous methods. In the early days of the mainframe, people realized that the biggest need was to prevent one user from interfering with the work of others sharing the machine. They developed an appropriate access control model, one that depended on the identity of the user. Permission to use a system resource, such as a file, was indexed by the user's identity. We call this approach Identification Based Access Control (IBAC). As the number of users grew, the burden on the administrator became untenable, which led to the introduction of additional concepts, such as "owner" and "group." Distributed systems proved to be problematic for IBAC. Managing the access rights on the individual machines became too large a burden and too prone to error, which led to the introduction of Role Based Access Control (RBAC). Problems with RBAC became apparent when it was extended across domains. Attribute Based Access Control (ABAC) was proposed as a solution to those issues. The access decision would be based on attributes that the user could prove to have, such as clearance level or citizenship. IBAC, RBAC, and ABAC all rely on authentication of the requester at the site and time of the request, so we lump them together and label them as authentication Based Access Control (NBAC). All these methods require tight coupling among domains to federate identities or to define the meaning of roles or attributes. Further, these approaches make it hard to delegate subsets of a principal's rights. The result is that common use patterns, such as service chaining, can only be implemented by crippling functionality or violating the Principle of Least Privilege. Recognizing those issues led us to develop an access control model that uses an authorization presented with the request to make an access decision, an approach we call authorization Based Access Control (ZBAC). We have found that this approach does not have the security and manageability issues inherent in NBAC. Further, our ZBAC implementation works entirely within the existing Services Oriented Architecture standards. Access control is a fundamental requirement for a secure Global Information Grid (GIG), attempts to implement even simple use cases with conventional approaches have resulted in large violations of the Principle of Least Privilege. We have shown that ZBAC handles these cases with improved scalability and reduced management burden. We have been working to develop new architectural approaches and concepts to securing SOA/Net Centric environments and have developed a scalable, high performance approach to access control, ZBAC, with general SOA security and inter-domain trust based on authority delegation and the use of trust anchors between communities. ZBAC has much wider applicability to enabling cross domain protection of assertions, data content and meta-data than other access control approaches. The architectural pattern is compatible with existing web services and SOA standards and should be able to be inserted into many critical programs once it is accepted as a viable solution to the many existing IA gaps in this arena.

**Keywords:** Access control; services oriented architecture; SOA; web services; federated identity management; FIdM

# Malware Detection via a Graphics Processing Unit

Nicholas Kovach and Barry Mullins

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

**Abstract:** Malware analysis involves processing large amounts of storage to look for suspicious files. This is time consuming and requires a large amount of processing power, often affecting other applications running on a personal computer. By using hardware included in most personal computers, a performance increase can be seen. The processing of files can be done on a graphics processing unit (GPU), contained in common video cards. A GPU is perfect for this because of its strong similarities to a central processing unit (CPU). Since the GPU has multiple processing units (32–128) it has an advantage over a CPU (1-8 processing units). This allows a single data stream to be processed using different metrics in parallel, while consuming minimal clock cycles from the CPU. A GPU also has its own memory, separated from the CPU, but also has the ability to share part of the CPU's memory. By using the GPU on a personal computer, other applications and the file processing for malware do not experience performance decreases by fighting over CPU usage. Using a GPU for file processing can also be applied to network intrusion detection systems (NIDS) and firewall based applications in addition to anti-malware applications. This research in progress investigates the use of GPUs for monitoring/detecting malicious activity. Specifically, we are processing files for malicious activity using different file sizes as well as malicious and non-malicious files which allows the performance and feasibility of using GPUs to be determined. We anticipate faster anti-malware products, faster NIDS response times, faster firewall applications, and a decrease in the time required to analyze files to generate signatures and understand exactly what the file is doing.

**Keywords:** Malware detection, graphics processing unit

# Digital Evidence Collection in Cyber Forensics Using Snort

Thrinadh Praveen Kumar<sup>1</sup>, Lalitha Bhaskari<sup>2</sup>, P. Avadhani<sup>2</sup> and P. Vijaya Kumar<sup>3</sup>

<sup>1</sup>GVP College of Engineering, Visakhapatnam, India

<sup>2</sup>AU College of Engineering, Visakhapatnam, India

<sup>3</sup>High Court of Andhra Pradesh, Hyderabad, India

**Abstract:** With the tremendous growth and usage of Internet, there is a considerable increase in the number of network attacks. This raises the need for improving security measures such as intrusion detection systems (IDS) in recent years where IDS's have become very crucial for Internet Security frameworks. The results of hacking, Trojans, worms and above all cyber crime is becoming a reality, thus hampering network security leading to devastating consequences. In this digital era, there is a profound need to generate legally admissible evidences of cyber crime or other illegal on-line behaviors which might be helpful in decreasing such malicious attacks. With the increasing scale and impact of cyber attacks, various network security techniques have been developed to fight against invisible attackers. These techniques address different aspects of security needs to eliminate cyber attack threats. We can never block all paths for cyber crime, effective investigation techniques would help us collect, analyze and present evidences of cyber attacks to hold the attackers responsible for their malicious actions. The issue of privacy and data protection is emerging as a central debate in forensic computing research. This perspective considers the nature of the intrusion detection and network monitoring security provided thus evaluating the system in terms of its evidence acquisition capabilities, the legal admissibility of the digital evidence generated, privacy implications of intrusion detection systems and network monitoring. The exploitation of IDS's as sources of legal evidence, including preservation of evidence, continuity of evidence and transparency of forensic method are to be considered to be fulfilled in the court of cyber law. In this paper an attempt was made to collect evidences of malicious activities using Snort which is a lightweight Intrusion Detection system. In Cyber forensics the evidence is captured from networks and interpretation is substantially based on knowledge of cyber attacks. Basing upon these evidences an attempt was made to locate the attackers and reconstruct their attack actions through analysis of intrusion evidence. The implementation of Snort is done using Aho-Corasick algorithm for pattern searching.

**Keywords:** Digital evidence, cyber forensics, cyber crime, intrusion detection system, Aho-Corasick algorithm

# **Growth Through Uncertainty – the Secure e-Business Evolution of the Small Firm**

**John McCarthy, Alan Benjamin, Don Milne, Bryan Mills and Peter Wyer  
Bucks New University, High Wycombe, UK  
Derby University, UK**

**Abstract:** Small firms must cope with an unpredictable external ICT environment. Media coverage of ICT security risks and lack of in house knowledge in small firms is resulting in them viewing e-business as too complex or difficult to manage. This is causing concern to governments, policy makers and the ICT industry. There is a tendency for support providers to prescribe the uptake of formal, rational strategic planning processes as appropriate tools to underpin identification of unfolding external change situations including ICT security threats. It can be argued, however, that the predominantly open ended nature of external change situations, combined with the more informal and idiosyncratic nature of small firm management processes, constrain the potential for utilization of formal long term planning. In turn, this raises the issue of how small firms identify and act upon their external change environments, and the question of how ICT security threats are managed within small firms. This paper focuses upon the distinctiveness of small business and utilizes an innovative action research methodology to enhance understanding of the nature and form of e-business evolution within micro and small firms. The investigation facilitates, through the creative Participatory Action Research approach, the actual process of e-business implementation. It uses this approach as a form of “research laboratory” to identify and analyse ICT security threats and factors which enable utilization of e-business. Integral to and within the context of the Participatory Action Research based approach this work uses an E-Business Development Platform which is unique to this study. This circumvents initial cost, ICT security and skills deficiencies which are commonly found to constrain small business uptake of ICT. Thereby providing a live action based ICT implementation context to facilitate an in depth investigation of ICT security issues and factors associated with small firm e-business uptake. The findings are discussed with regard to practical insight findings capable of informing small business management and development practice, e-business evolution and ICT security and the relationship strategies that could be utilized by an ICT provider facilitating a small firm. The paper concludes with consideration of its contribution to and enhancement of current academic insight.

**Keywords:** ICT security, SME. small firms, e-business development

# Hiding Appropriate Messages in the LSB of JPEG Images

Hamdy Morsy<sup>1</sup>, Ahmed Hussein<sup>1</sup>, Joshua Gluckman<sup>2</sup> and Fathy Amer<sup>1</sup>

<sup>1</sup>Faculty of Engineering at Helwan University, Cairo, Egypt

<sup>2</sup>American University in Cairo, Egypt

**Abstract:** Steganographic systems attempt to hide communication by embedding messages in an innocuous looking cover medium. Current steganographic systems provide relatively secured hidden data with small capacity for steganographic messages. In this paper, a new technique is introduced to hide data in the least significant bits (LSB) of the discrete cosine transform (DCT) coefficients of JPEG images. This technique embeds data in a way that maximizes the ratio between even and odd DCT coefficients so as to preserve the first order statistics of JPEG images. Message bits are divided into segments and each segment is possibly modified by embedding the bitwise complement so as to ensure a high ratio between even and odd coefficients. The embedding process is referred to as the hiding appropriate messages (HAM) algorithm. The HAM algorithm searches for optimum segment length to offer high capacity, approximately 0.36 bits/pixel, with statistically minimal changes compared to existing steganographic algorithms. A comparison between HAM and existing steganographic systems is presented.

**Keywords:** Steganography, information hiding, steganalysis, LSB embedding, covert communication

# **An Application of Deception in Cyberspace: Operating System Obfuscation**

**Sherry Murphy, Todd McDonald, and Robert Mills  
Air Force Institute of Technology, Wright Patterson, USA**

**Abstract:** The art of deception has played an integral role in military operations throughout history. In this research we investigate the efficacy of using operating system (OS) obfuscation as a form of deception in the cyber domain. Specifically, we study the effectiveness of host-based OS obfuscation as a way of understanding whether the technique warrants further research and application development before becoming an integral part of Air Force network defense. We accomplish this objective by examining the theoretical foundation of cyber deception and then evaluating a specific OS obfuscation tool against selected OS fingerprinting tools. The results from our experiment show that current OS obfuscation tools are developed enough to consistently mask OS information on systems running a Windows OS.

**Keywords:** Operating System masking, polymorphic host-based defense, digital decoys, deception, network reconnaissance, network scanning

# Insider Threat Detection Using Distributed Event Correlation of Web Server Logs

**Justin Myers, Michael Grimaila, and Robert Mills**  
**Air Force Institute of Technology, USA**

**Abstract:** In this paper, we discuss the distributed correlation of events generated by Apache and Microsoft IIS web server applications and stored in log files to detect potentially malicious insider activities. Specifically, we investigate the use of a lightweight event correlation tool called the Simple Event Correlator (SEC) for the purposes of distributed event correlation. SEC is a popular, lightweight, highly configurable, cross platform event correlation tool written in the Perl programming language and licensed under the terms of GNU General Public License. Our research harnesses the ability of SEC to generate synthetic events to facilitate the distribution of event correlation activities among web servers on a network. These synthetic events can be generated in a user-defined format by SEC in response to a series of events in the input log file(s) which matches a pattern as defined in an SEC configuration file. Augmenting raw events with synthetic events provides the capability to reduce uncertainty, improve semantic understanding, and enable higher level reasoning when conducting event correlation in a complex environment. The utility of SEC for detecting potentially malicious activities by trusted insiders is demonstrated in an experimental network of systems running web servers and configured with SEC. Our results show that we can efficiently detect a number of potentially malicious web server scenarios including website spidering and data exfiltration. Further, the results demonstrate that distributed event correlation can provide benefit in enterprise-wide deployments of event correlation when compared to centralized heavy weight, client-server database applications that incur significant overhead in terms of network traffic, storage space and computational effort. The benefit of a distributed event correlation architecture is the result of the distribution of workload associated with event correlation, the reduction in network bandwidth required to transport events back to centralize repository, and the ability to squelch event streams which do not provide addition value in the event correlation process. However, efficient distributed event correlation requires an a priori identification, characterization, and deployment of sequences of events that are deemed as potentially malicious. While initially this activity is resource intensive, it can provide long term benefit as it causes security personnel to identify, document, maintain, and refine a collection of event sequences deemed to place the organizational resources at risk.

**Keywords:** Logging infrastructure, event correlation, insider threat detection

# **Verify Then Trust: A New Perspective on Preventing Social Engineering**

**Kristopher Nagy, Brian Hale and Dennis Strouble**

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

**Abstract:** Social engineering is an age-old deception tactic. Yet today, social engineering techniques continue to prove effective in exploiting human weaknesses to circumvent advancements in security practices and technologies. Given these modern-day social engineering threats and a shift to a "need to share" information culture across the Department of Defense, there is an expressed need for greater social engineering prevention and awareness. To illustrate the adaptive nature and innovative thinking of social engineers, several methods of social engineering techniques, including military deception, dumpster diving, phishing, confidence tricks, and baiting are presented. Furthermore, this paper examines measures to prevent social engineering and asserts a new "verify then trust" information protection attitude is required to combat against social engineering techniques. The paper begins with a brief background on the history of social engineering to illustrate the fact that social cons and ploys have existed for thousands of years. Then, the five most common social engineering methods are discussed through examples. Next, the authors reveal the secret to eliminating nearly all social engineering attempts and suggest prevention programs for employees, managers, and information technology support staff. Finally, a model suggesting a relationship between information sharing and information protection is presented. We are undoubtedly in an age of increased information sharing and the implications of inadequate information protection can be devastating; the model emphasizes the fact that increased information sharing requires increased information protection and verification procedures.

**Keywords:** Deception, information warfare, security, social engineering

# Cyberspace: Definition and Implications

Rain Ottis and Peeter Lorents

Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

**Abstract:** In recent years the term “cyber” has been used to describe almost anything that has to do with networks and computers, especially in the security field. Another emerging field of study is looking at conflicts in cyberspace, including state-on-state cyber warfare, cyber terrorism, cyber militias etc. Unfortunately, however, there is no consensus on what “cyberspace” is, let alone what are the implications of conflicts in cyberspace. In order to clarify this situation, we offer the following definition: *cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems.* We describe the background of the definition and show why this approach may be preferable over others. Specifically, we revisit the terms coined by Norbert Wiener (the father of cybernetics) and William Gibson. We show that time-dependence is an overlooked aspect of cyber space and make a case for including it in our proposed definition. In addition, we look at the implications that can be drawn from the time-dependence of cyberspace, especially in regard to cyber conflicts, which we define as *a confrontation between two or more parties, where at least one party uses cyber attacks against the other(s).* Specifically we review the implications on the potential for rapid deployments of offensive and defensive actions in cyberspace, the feasibility of mapping cyberspace, and the need for constant patrolling and reconnaissance.

**Keywords:** Cyberspace, cyber conflicts, cyber attacks, time, definition

# Transparent Emergency Data Destruction

Warren Roberts, Christopher Johnson and John Hale  
University of Tulsa, USA

**Abstract:** A wide variety of tools offer users the ability to encrypt their sensitive information with private pass-phrases or key files. These technologies do little – if anything – to protect users from being compelled to produce the pass-phrase or key file. Under duress, a user may have few options other than producing his pass-phrase making his data accessible to an adversary. Additionally, human memorable passwords are almost always weaker than the randomly generated keys used to encrypt data. We propose to offer the user the opportunity to destroy his own data, making it inaccessible to himself as well as his adversary. All sensitive data will be stored on an encrypted volume. When the user tries to boot the system, he will be prompted for a password. Under normal circumstances, the user will enter his access password, the hard drive will be decrypted on the fly, and the system will operate normally. When a user is under duress or suspects that he will lose physical control of his system he can enter a predetermined duress pass-phrase instead of his standard access pass-phrase. The encrypted volume containing his sensitive information will be quickly destroyed, but in order to avoid arousing the suspicion of his adversary the operating system will proceed to boot to a discreet desktop environment. Even a user who knew the previous access password will be unable to recover the destroyed information. The adversary can search the user's remaining files, but even a forensic analysis will not produce any sensitive data.

**Keywords:** Cryptography, confidentiality protection, anti-forensics, duress mitigation, data destruction

# Cyber-Based Behavioral Fingerprinting

David Robinson and George Cybenko  
Dartmouth College, Hanover, USA

**Abstract:** As a result of consistent double-digit year-over-year growth rates in e-commerce sales, marketing firms continue to aggressively seek better means to aid in classifying user's cyber behaviors, thereby improving personalization, product recommendation and prediction. While motivated purely by financial incentives, this type of work has provided great insights into the type of information which may be gained from user's online activities, and has made significant strides in cyber-based behavioral modeling. An aspect of this type of research receiving much less attention focuses on whether these cyber behaviors are descriptive enough to uniquely identify an individual user. While the ability to uniquely identify individuals based on their online activities has e-commerce ramifications, its greatest potential may be in the security realm. The ability to create a "cyber fingerprint" of an individual to uniquely distinguish them provides a baseline from which variations in behavior may be identified. Such a mechanism could then be used to detect and prevent insider threat, fraud, and hacker activity by triggering alerts when a user behaves in a manner inconsistent with their previously established "norm". In this paper, we investigate whether a user's search activities provide an accurate model for the identification of a user and propose a formal approach to calculate the minimal amount of data required to create such a model. We make use of three months worth of real world query logs and apply a supervised learning algorithm to ascertain whether users can be discriminated through search queries alone. Experimental results are provided demonstrating the effectiveness of our fingerprinting technique and sample size estimation methods. Finally, the implications of this research in areas such as e-commerce, insider threat detection, and fraud detection are discussed.

**Keywords:** User modeling, cyber fingerprint, behavior, meta-activity

# **Exploitation of Blue Team SATCOM and MILSAT Assets for red Team Covert Exploitation and Back-Channel Communications**

**David Rohret and Jonathan Holston**

**Joint Information Operations Warfare Center (JIOWC)/Joint Electronic Warfare Center (JEWIC) San Antonio, USA**

**Abstract:** Military organizations and commercial companies greatly depend on satellite communications and non-terrestrial data transfers for day-to-day business and warfare requirements. To reduce launch and production costs, militaries have adopted the use of commercial (corporate-owned) satellites, sharing available bandwidth and capabilities. Many of these commercial and military SATCOM assets are not protected from network and radio frequency (RF) attacks by adversaries using open-source and publically-available resources; operating from within developed or developing countries. Recent events have demonstrated that sophisticated military communication (MILCOM) satellites can be effortlessly compromised using low-cost equipment and radios available from commercial sources. Both digital and analogue signals can be captured, manipulated, and/or transmitted with little or no risk to the offending red forces, and low-cost global positioning system (GPS) jamming devices can be used to frustrate blue forces. Open-source programs for SATCOM transponders are available for download via hobbyist, equipment vendors, and black hat web sites with documentation and other resources for research and manipulation by red forces. Furthermore, red forces can utilize blue force SATCOM and MILSAT assets as a dependable and secure means for covert back-channel data and voice communications, increasing their ability to relay information while decreasing their detectable digital footprint. This paper identifies and demonstrates current open-source and publically-available capabilities for red teams assessing blue force SATCOM assets, to include: Identifying potential SATCOM and MILSAT targets Unauthorized use of satellite capabilities (covert communications) Uplink/downlink jamming and denial of service attacks Man-in-the-middle (MITM) attacks and Commandeering of SATCOM signals Eavesdropping Malware development and delivery using resources available on black hat and Ham radio hobbyist web sites This paper concludes by identifying vulnerabilities associated with currently deployed commercial and military satellite systems based solely on open-source and publically-available resources. The authors will conclude by presenting possible solutions for future SATCOM and MILSAT security.

**Keywords:** Satellite, adversary, SATCOM, MILSAT, vulnerability, exploitation, mitigation

# A Hybrid Approach to Teaching Information Warfare

Dino Schweitzer and Steve Fulton  
United States Air Force Academy, USA

**Abstract:** Many claim that warfare in the future will be conducted primarily in the cyber domain. As such, information warfare is a critical topic for future military members to comprehend. Many schools teach topics in computer security, information assurance, and information warfare through a variety of formats. At the Air Force Academy, we have taught a Computer Security and Information Warfare course for several years to prepare future officers for the realities of modern conflict. In the past, our course has had two primary focuses: fundamental concepts in the theory of computer security delivered primarily through lecture, and a hands-on laboratory component to gain practice in current offensive and defensive tools and techniques. As we have evolved the course, we have added other components to the course such as virtual labs, web labs, competitions, and a research project. In addition to be motivational to the students, this *hybrid* approach has been successful in engaging students who do not have a strong background in computer science. Web labs have been especially helpful in providing a realistic hands-on experience without going into the tremendous amount of detail and background that surround modern computer and network systems. The competition we have introduced is unique from other university level cyber competitions in its design and format. The research project attempts to expose students to a complete research experience. The combination of these elements serves as an active learning approach to teaching students critical topics in IW. We have also had success employing them outside of the classroom to a broad range of students in a summer program. This paper will describe traditional approaches, our environment, the hybrid approach we use, our experience with it, and future plans.

**Keywords:** Computer security education

# **A Stochastic Game Model with Imperfect Information in Cyber Security**

**Sajjan Shiva, Sankardas Roy, Harkeerat Bedi, Dipankar Dasgupta and Qishi Wu**

**University of Memphis, USA**

**Abstract:** While there are significant advances in information technology and infrastructure which offer new opportunities, cyberspace is still far from completely secured. Recently, researchers have started exploring the applicability of game theory to address the cyber security problem. The interaction between the attacks and the defense mechanisms can be considered as a game played between the attacker and the defender (system administrator). One of the techniques that has been proposed in the literature used stochastic game models to emulate network security games and showed how to determine the best strategy for the defender considering the possible attack strategy used by the attacker. However, the prior research assumes that the players have perfect information about the current state of the game, which generally does not hold in reality. Our model relaxes this assumption and enriches the prior game models by enabling them to capture more realistic scenarios. In particular, this paper presents a theoretical analysis by which the defender can compute his/her best strategy to reach the Nash equilibrium of a stochastic game assuming imperfect sensory information. In addition, this paper shows that if the defender follows the strategy prescribed by the perfect information model, the Nash equilibrium is not achieved and the attacker's payoff can be higher. Our theoretical analysis is tested in simulation experiments and the results validate our approach.

**Keywords:** Network security, game theory, stochastic games, nash equilibrium, imperfect information, simulation

# Malware Antimalware Games

**Anshuman Singh, Arun Lakhotia and Andrew Walenstein**  
**University of Louisiana at Lafayette, USA**

**Abstract:** Game theory has been used to model several areas of information security like network security, intrusion detection, information warfare and security investment. We first survey the game theoretical approaches in these areas of information security. We then explore the role of game theory in modeling an area of information security - the strategic interaction between malware writers and antimalware experts. We explore the modeling space for realistic modeling of the game, the players involved and their strategies in malware antimalware games. We also formalize our observations about modeling of action sets.

**Keywords:** Malware, game theory, information security

# Evaluating the Security of Enterprise VoIP Networks

**Peter Thermos**

**Palindrome Technologies, USA**

**Abstract:** The deployment of enterprise Unified Communications has become increasingly common the past few years. As organizations invest resources to ensure QoS and also meet delivery schedule, security is often overlooked. This paper reflects results from evaluating the security of VoIP implementations in several enterprise organizations and outlines the most common weaknesses that were found during testing and their impact to the organization. Furthermore, it underlines the notion that if security is implemented as an afterthought, it costs more

**Keywords:** VoIP, unified communications, security, testing, assurance

# An FPGA-Based Malicious DNS Packet Detection Tool

Brennon Thomas and Barry Mullins

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

**Abstract:** Billions and billions of packets traverse government and military networks every day. Often, these packets have legitimate destinations such as buying a book at *amazon.com* or downloading open source code using a File Transfer Protocol program. Unfortunately, the past few years have seen a massive increase in malicious, illegal, and suspicious traffic. One example is abusing the Domain Name System (DNS) protocol to exfiltrate sensitive data, establish backdoor tunnels, or control botnets. To counter this abuse and provide better incident detection, a physical hardware system is under development to detect these suspicious DNS packets. The system is constructed on a Xilinx Virtex-II Pro Field Programmable Gate Array (FPGA) and is based on a system originally developed to detect BitTorrent and Voice over Internet Protocol packets of interest. The first iteration prototype is limited in both processing speed (300 MHz) and by a 100 Mbps Ethernet interface. Despite the hardware shortfalls, preliminary experiments are promising for the system. The system inspects each packet, determines if it is a DNS packet, compares the first four characters of the lowest level domain against a DNS whitelist, and if the domain is not allowed, logs it for further analysis. The first experiment resulted in 100% malicious packet detection under an 88 Mbps network utilization. In the experiment, 50 malicious DNS packets were sent at one second intervals while the network was flooded with NetBIOS traffic. The second experiment resulted in an average of 91% malicious packet detection under an 88.7 Mbps network utilization. In the experiment, 2000 malicious DNS packets were sent as fast as possible while the network was flooded with non-malicious DNS traffic. For both experiments, DNS whitelist sizes of 1K, 10K, and 100K were used. Future work will focus on transferring the system to the Virtex-5 FPGA which contains a 550 MHz processor and a 1 Gbps Ethernet interface. In addition, the DNS whitelist size will be increased until the system fails to detect 50% of packets of interest. The goal is to determine if the system can be scaled to gigabit network speeds while also handling larger DNS whitelist sizes. The system seeks to aid network defenders in identifying and tracking malicious DNS packets traversing government networks while also providing better incident response awareness.

**Keywords:** DNS, FPGA, Virtex, exfiltration, botnet, tunnel

# Digital Forensics Detection and Disruption of JPEG Steganaography

**George Trawick and Drew Hamilton**  
**Auburn University, Auburn Alabama, USA**

**Abstract:** As the use of digital media and internet communications have grown for business and personal use, so has the use of digital communications by criminal and terrorist elements. Of particular interest in both criminal investigations and national security is the use of covert communications channels by terrorist and criminals. The use of covert communications by criminal elements is not new, what are new are the nearly undetectable digital methods available that allow for large quantities of information to be exchanged secretly. Criminal elements are using applications that implement digital steganography to plan, coordinate and execute their unlawful activity. In addition to having a immense number of steganographic implementations to exploit, as an additional layer of security criminals often combine steganography with encryption which is proving to be a nearly insurmountable hurdle that law enforcement and government agencies are not currently able to overcome. I propose a method that allows for the detection, disruption, tracking and possibly extraction of steganographic messages hidden on a suspect's digital storage device. In the field of steganography, detection and extraction research clearly outpaces research in tracking and disruption. The available research in improving steganographic implementation is proving to be quite extensive. However, the current state of the research shows that few if any have researched the combined capabilities of stegananalysis, non-traditional hashing and digital artifacts to give law enforcement the tools and methods necessary to counteract the criminal's ability to hide information using steganography. The research will be focused on a particular genre of steganography that is implemented using JPEG images. In particular this research will focus on those steganographic implementations that exploit the transform domain of the JPEG compression algorithm. There are strong indications that within the JPEG compression algorithm are possible artifacts that remain constant between repeated compressions as well as, documented artifacts that are left behind by known steganographic software. I propose to combine these methodologies with emerging methods of non-traditional hashing to expose likely stenographic images within a finite set or database of images and identify a possible digital fingerprint allowing law enforcement new capabilities in suppression of the use of steganography as a tool for criminal activities.

**Keywords:** Steganography, JPEG, forensics, security

# **A High-Level Mapping of Cyberterrorism to the OODA Loop**

**Namosha Veerasamy**

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

**Abstract:** Cyberterrorism relates to the convergence of the two worlds of terrorism and cyberspace. Technically cyberterrorism can be carried out through various information security exploits like targeting Supervisory Control and Data Acquisition (SCADA) systems or Denial of Services attacks on critical governmental web sites. Various factors have an influence on cyberterrorism and include the social factors, capabilities, goals, modes of operation and practices. In order to analyse how these various factors influence the development of a cyberterrorist, a mapping to the Observe- Orient, Decide, Act (OODA) loop is proposed. The OODA loop, previously proposed by Col. John Boyd, provides an apt framework to structure and describe issues that contribute to the development and operation of a cyberterrorist. The aim of this paper is to describe how various observations made by sections of the world population direct people into making decisions and committing acts of cyberterror. The paper will thus look at issues like the environmental factors, social standing, culture, religion, tribal relations, loyalties, and the drive for power and self-fulfilment. In addition, the mapping will also consider how information is received, transformed and utilised by cyberterrorists, by considering the evolution of information in the Information Hierarchy. The proposed model will thus map various aspects pertinent to the field of cyberterrorism to capture a more dynamic representation of the interacting forces. The mapping will try to show the main relationships between the OODA loop, Information Hierarchy and various factors like characteristics, social factors, terrorist types, capabilities, goals, targets, attack levels, support functions, practices and modes of operation. Overall, the goal of this paper is to succinctly represent some of the psychological and technical issues relating to cyberterrorism. The OODA loop will be utilised to convey these ideas as well mapping to other relevant fields like the Information Hierarchy. Overall, various components that impact the field of cyberterrorism will be integrated to show a more holistic representation of various operating forces.

**Keywords:** Cyberterrorism, information hierarchy, OODA loop

# **An Adaptation Based Survivability Framework for Mission Critical Systems**

**YanJun Zuo**

**University of North Dakota, Grand Forks, USA**

**Abstract:** Survivability refers to the ability of a system to continuously function despite malicious attacks and system failures. Different from a traditional system, a survivable system responds seamlessly to unexpected events and reliably supports the organization's mission. In this paper, we propose an adaptation based framework for critical systems to respond to malicious attacks by system adaptation and component reconfiguration. The framework enables a system to quickly determine the most appropriate security primitives to change and figure out how to adjust those parameters in order to ensure system survivability "on-the-fly" during an attack period. We specify the system architecture for system survivability management and control. System topology rules are discussed from the system engineering perspective. An example of critical system in financial service is presented to illustrate how a set of security primitives are configured to improve the system survivability.

**Keywords:** Critical system, survivability, adaptation, reconfiguration, architecture, incident response

# **Research in Progress Papers**



# **A Blind Scheme Watermarking Algorithm for Data Hiding in RGB Images Using Gödelization Technique Under Spatial Domain**

**Peri Avadhani and Lalitha Bhaskari**

**A U College of Engineering (A), Andhra Pradesh, India**

**Abstract:** The growth of internet technology in the present era is creating a pressing need to develop several new methods for copyright protection, ownership and security of the digital contents. These concerns have triggered significant research to find ways to hide data into digital media. Data hiding can be done in two domains, namely spatial domain and frequency domain. The work focuses on the robustness and data hiding capacity limitations in the spatial domain. In this paper, a layered algorithm for hiding a watermark (image/ text) in RGB (color) images based on Gödel numbering, Alphabetic Coding(AC) and Auxiliary carry watermarking method proposed by Lalitha Bhaskari, Damodaram, Avadhani(2006:666-668) proved to be more secure and robust. Unlike other methods, no prior information about the original watermark, hiding locations, strengths are needed in the proposed blind watermark scheme. The security levels are gradually enhanced from the proposed auxiliary carry watermark method combined with LSB method, to a proposed modified auxiliary carry method combined with Gödelization and alphabetic coding methods. The proposed methodology follows three layered approach for embedding the watermark into the original image ensuring no degradation of the original image and providing security to the watermark. In the first layer, watermark which is to be hidden in color image is encoded into Gödel numbers, termed as Gödelization as proposed by Lalitha Bhaskari, Avadhani, Damodaram(2009: 209-213). In the second layer, the encoded string obtained from the first layer is compressed using AC technique. In the last layer, the resultant data which is in a compressed encoded string format is hidden in the cover image using a proposed method known as modified auxiliary carry watermark method. During the watermark extraction process, depending upon the key generated, the watermark is extracted from the watermarked image and experimental results proved that the proposed algorithm employed more data payload capacity than the traditional methods and is robust to attacks in spatial domain. The computational complexity is low, yet providing more security.

**Keywords:** Alphabetic coding, auxiliary carry watermarking, Gödelization, Steganography

# Automatic Discovery of Attack Messages and Pre- and Post-Conditions for Attack Graph Generation

Marco Carvalho and Choh Man Teng

Institute for Human and Machine Cognition, Pensacola, USA

**Abstract:** Network attack graphs are directed graph-representations of possible attack paths and vulnerabilities in a computer network. Each attack path is a sequence of steps taken by an attacker to achieve one or more goals in the target system. While there are some variations in the representations of the graph proposed by different researchers, typically the edges represent possible actions (or exploits) available to an attacker, and vertices represent the possible states for the system and applications. Attack graphs are often manually created or, less often, automatically generated from a set of attack models and detailed information about the network topology and its applications. There have been several proposals for the automatic identification and representation of attack models, but they all rely on some prerequisite knowledge of the pre- and post-conditions for the different attack steps. A pre-condition may include requirements such as “attacker must have root privileges”, while a post-condition defines the state of the system after an action is taken. In this paper we propose algorithms for the automatic identification of likely pre- and post-conditions that can be used for the generation of attack graphs. Our approach extracts such candidate conditions from observational data. By monitoring low-level events on multiple network nodes, in correlation with detected anomalies or attacks, our approach can automatically and unobtrusively identify the attributes of interest for the attack model required for attack graph generation. The paper provides a brief review of the requirements for automatic attack graph generation, and describes our proposed approach in detail. We also present preliminary simulation results for the automatic discovery of attack messages and their pre- and post-conditions, in a simplified fully connected network environment.

**Keywords:** Attack graphs, network security, damage detection, graphical models

# **Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships Between Cyber Assets, Missions and Users**

**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**

**Abstract:** Awareness of the dependencies between cyber assets, missions and users is critical to assessing the mission impact of cyber attacks and maintaining continuity of business operations. However, there is no systematic method for defining the complex mapping between cyber assets (hardware, software, data), missions and users. This paper reports the results of an interdisciplinary workshop on how to map relationships between cyber assets and the users, missions, business processes and other entities that depend on those assets. The workshop yielded information about types of impact assessment beyond mission and financial analyses; scenarios illustrating the complex relationships between assets, mission and users; and models for expressing those relationships. The results will be used to develop a system that will automatically populate an ontology from commonly available network data and allow computer network defense, information technology and disaster recovery practitioners to query the system for information about the impact of the loss or degradation a cyber asset. Two workshops were held: the first focused primarily on mapping relationships between cyber assets, missions and users in commercial operations, and the second workshop focused on military operations. The participants included people whose operational responsibility is to assure the availability of cyber assets for critical missions, and technology providers and researchers in areas related to the mapping of cyber assets to missions. They represented the armed services, intelligence community, small and large businesses, county government, universities, research companies and large systems integrators. The workshop goals addressed in this paper are: 1) define the types of impacts one needs to assess when a cyber asset is attacked or fails; 2) analyze scenarios that illustrate impacts of a failed cyber asset on missions and users; and 3) model relationships between cyber assets, missions and users.

**Keywords:** Mission impact; mission assurance; business continuity; ontology; information security; cyber war

# **An Investigation of Malware Type Classification**

**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**

**Abstract:** The increasing cybercrime trend places increased pressures on struggling organizations to defend themselves from an influx of custom malware attacks. These customized ‘cyber weapons’ are undetectable to antivirus signature-based scanners and difficult to detect with heuristic-based scanners. Governments and many organizations simply cannot wait for commercial malware detection solutions, because researchers likely will never receive a targeted malware artifact—it may be the only instance in existence—unless the customer first finds it themselves and submits it for review. Unbeknownst to many antivirus customers, who mistakenly think they are watching the malware game from the safety and security of the sidelines, wily cyber criminals have quietly begun targeting them as the weakest players on the field. While several critical malware problems remain the focus of intense research, this research paper investigates methods of automatically identifying disparities between malware types using machine learning techniques. The results from these experiments can help all interested entities to better identify and classify specific artifacts that they discover possibly even enabling more expedient recovery procedures. Other applications of these methods include automatically classifying malware types for large malware repositories or assisting antivirus researcher agreement on a specific universal malware type standard. Fostering agreement in the antivirus research community on a universal type standard benefits both the research community and antivirus customers, because standards allow for effective and appropriate response and recovery procedures. These standards also allow academic research efforts to effectively leverage the expertise of the antivirus researcher community. Preliminary results on relatively small datasets demonstrate reasonable confidence in classification accuracy for three different malware types based on partial and full agreement between three major antivirus company products. This methodology serves as a quick look classification for identification and prioritization of work for appropriate information technology personnel. Increasing the number of samples, applying a variety of machine learning techniques, and incorporating other software types to this research will increase the significance of these results and help to define the essence of various software classes.

**Keywords:** Malware, classification, machine learning, network defense

# Language-Driven Assurance for Regulatory Compliance of Control Systems

**Robin Gandhi, William Mahoney, Ken Dick and Zachary Wilson**  
**University of Nebraska at Omaha, USA**

**Abstract:** We present a novel approach to precisely specify constraints mandated by regulatory requirements on a control system and monitor the corresponding compliance status in near-real-time. Our research focuses on the design of a language that bridges the gap between abstract regulatory policies and the realities of implementation. Essentially, each regulatory check, a “policy monitor”, is authored in a new language we are developing called ADACS (Autonomous component-based policy Description Language for Anomaly monitoring in Control Systems). The semantics of our language are closer to discrete real-time system interactions expressed as events encoded in XML messages, and the language is compiled into binaries of a general purpose language that is portable across many hardware and software platforms. Considering a large number of legacy SCADA systems in place today along with the sensitive nature of their operation, we rely on rapid modeling and simulation of control system components to develop policy monitors in ADACS. Simulation of the system operational behavior facilitates the authoring, tailoring and tuning the corresponding language elements that watch for violations of the regulated behavior. In addition the ability to simulate system interdependencies allow the language author to verify the policy monitors, which will later be used in a live SCADA environment. We anticipate that out-of-band XML-based event generation from distributed and heterogeneous legacy SCADA systems will suit well to integrate the policy monitors developed currently in the simulation environment. The syntax and semantics of ADACS language and events are described, and finally we discuss our future research directions.

**Keywords:** Regulatory compliance, domain specific languages, control systems, SCADA

# **AIMFIRST: Planning for Mission Assurance**

**Tom Haigh, Steven Harp and Charles Payne  
Adventium Enterprises, Minneapolis, USA**

**Abstract:** Today network and system managers are not equipped to support mission assurance objectives. Often they are unaware of the mission impact of their actions, e.g. changing firewall or router rules or bringing a server down for maintenance, until someone associated with a mission complains of a negative impact. Worse yet, when the network configuration changes for any reason—a cyber or kinetic attack, an act of nature, etc.—the managers have no way to assess the mission impact of the change or to plan ways to work around the disruption. Mission Assured Networking (MAN) requires automated support for analyzing the network needs of missions to determine the feasibility of executing a given set of missions with a given network configuration. When a set of missions is infeasible, managers need support to help determine a network configuration schedule that optimizes the value of the subset of missions the network can support. The schedule would contain a sequence of configurations that changes as missions or phases of missions begin or complete, and that can adapt to unanticipated changes in the network configuration. On the Automated Intelligent Management for Integrated Strategy and Tactics (AIMFIRST) project, we are investigating an approach for providing automated MAN support. In this work in progress paper we describe the AIMFIRST concept and our approach for implementing it. This involves modeling missions using input from mission planners and adapting network discovery and modeling tools. AIMFIRST applies automated reasoning and mathematical programming techniques to the analysis of mission tasks, detecting infeasible states and providing assistance in conflict resolution.

**Keywords:** Mission, model, network, assurance, reasoning, optimization

# **Moderating Roles of Organizational Capabilities Affecting Information Security Strategy Effectiveness: A Structural Equation Modeling Analysis**

**Jacqueline Hall, Shahram Sarkani, and Thomas Mazzuchi**  
**The George Washington University, Washington, USA**

**Abstract:** In today's modern business world, most organizations use information as a critical business asset to gain competitive advantage and create market value. Increasingly, an organization's ability to protect information assets plays a critical role in its ability to meet regulatory compliance requirements, increase customer trust, preserve brand strength or company reputation, maintain business resiliency, and thereby enhance organizational performance. As information technologies, global connectedness, and business requirements continue to evolve at a fast pace, organizations must recognize the importance of implementing an overall information security strategy to protect business information asset from increasingly sophisticated threats. Given the dynamic level of business environments, the identification and understanding of the required capabilities to deliver an information security strategy becomes the key success factor. At the strategic level, organizations must be able to answer the question, "What are the minimum essential organizational capabilities required to support effective planning and execution of an overall information security strategy that best achieves organizational objectives and gains competitive advantage?" The aim of this study is to contribute to the body of knowledge about the organizational aspect of information security. It seeks to examine the issue of information security from the perspective of organizational capabilities. Based on strategic management and information security literature, this perspective suggests that organizational capabilities moderate the relationship between information security strategy implementation success and organization performance. A theoretical model is proposed and validated to demonstrate this relationship changes as a function of organizational capabilities. The organizational capabilities considered here consist of the ability to develop high quality situational awareness and understanding of the internal and external environments, the ability to collaborate, make and communicate decisions, the ability to possess appropriate means and resources to respond, along with the ability to coordinate and deploy organizational assets. A structural equation modeling approach is used to quantitatively analyze data and to test the validity of the research hypotheses. Results from this study are expected to yield practical value for business leaders and to provide a basis for understanding the viable predisposition of an organization in the context of information security as it competes in today's challenging marketplace.

**Keywords:** Information security strategy, effective implementation, organizational capabilities, organization performance, competitive advantage, structural equation modeling

# Information Operations in Space, Absence of Space Sovereignty, Growing Number of Nations Looking Spaceward: Threats and Fears Concerning Established Space-based Military Powers

Berg Hyacinthe<sup>1</sup> and Larry Fleurantin<sup>2</sup>

<sup>1</sup>Assas School of Law— CERSA-CNRS Sorbonne, France

<sup>2</sup>Fleurantin & Associates, Florida, USA

**Abstract:** The success of military Information Operations (IO) depends intrinsically upon the degree of sovereignty held by the Commander-in-Chief over strategic military weapons and their means of delivery. The recrudescence of “Space Superiority” as a strategic paradigm, embraced by military superpowers as well as emergent regional powers, compels wary analysts to focus on communications satellites — vital, yet, vulnerable nodes of the Information Warfare (IW) machinery. These satellites have become high-value military targets in an increasingly crowded theater far beyond Earth’s capillary boundaries: Space and Outer Space. Symmetrically, while several key international instruments (e.g., United Nations Treaties and Principles on Space Law) impose strict limitations to an individual nation’s Space activities, the Outer Space Treaty of 1967 explicitly prohibits weapons of mass destruction (WMD) anywhere in Space, military bases, weapons testing, and maneuvers on the surface of any celestial body. On the particular issue of Space sovereignty, Article 2 of the Outer Space Treaty expressly establishes Space and Outer Space as “the province of all mankind, and, therefore, not subject to sovereign claims by any nation”. Therefore, it will be argued that Space-based military satellites and other military spacecrafts are, *de lege lata*, strategic weapon components operating subtly on *non-sovereign* territories. This Article aims at paralleling and contrasting the foregoing lines of argument in the context of a rising number of nations looking “spaceward” in recent years. Furthermore, it argues, according to several juridical analogies and military principles that, the establishment of full Command-and-Control should precede claims of sovereignty over any space: terrestrial space, cyberspace, Space, or Outer Space. Within a broader context, the authors sought to answer two primary research questions: Did the original architects of Space-based military power mistakenly adopt a “convenient” interpretation of the notion of sovereignty? Did they miscalculate the universal nature of human inventiveness?

**Keywords:** Space militarization, space sovereignty, Information Operations in space, space laws and treaties, communications satellites, and ASAT weapons

# Evaluating the Impact of Cyber Attacks on Missions

**Scott Musman, Aaron Temin, Mike Tanner, Dick Fox and Brian Pridemore  
MITRE Corp, McLean, USA**

**Abstract;** Using current methods, it is virtually impossible to determine the impact of a cyber attack on the attainment of mission objectives. Do we know which mission elements are affected? Can we continue to operate and fulfill the mission? Should we wait for recovery? Can we salvage part of the mission? Since it is currently so difficult for humans to comprehend the mission impact of a cyber incident, our ability to respond is much less effective than it could be. We believe that improved knowledge of the mission impact of a cyber attack will lead to improved, more targeted responses, creating more attack resistant systems that can operate through cyber attacks. Our work addresses the “mission” part of “mission assurance,” focusing on cyber mission impact assessment (CMIA). Our challenge is to create mission models that can link information technology (IT) capabilities to an organization’s business processes associated with Measures of Effectiveness and Performance (e.g., attrition of enemy forces , targets destroyed, blue force protection). Measuring mission impact requires knowing the mission activities that fulfill mission needs, the supporting cyber assets, and understanding how the effects of an attack change mission capability. This paper is about developing the techniques that make estimating the mission impact of cyber attacks possible.

**Keywords:** Mission assurance; information assurance; cybersecurity; cyber attack consequences

# NEO Thinks EBO - a way to Shape Perceptions

Nuno Perry<sup>1</sup> and Paulo Nunes<sup>1,2</sup>

<sup>1</sup>Competitive Intelligence and Information Warfare Association Club,  
Funchal, Portugal

<sup>2</sup>Centro de Investigação da Academia Militar, Lisbon, Portugal

**Abstract:** The concept is not new. In fact we've learned from Sun Tzu that "*Those skilled in war subdue the enemy's army without battle.*" However Effects Based Operations definition, development and operationalization has been subjected to disparate analyses, doctrines, interpretations and became a controversial issue. This paper addresses Effects-Based Operations (EBO) and Effects-Based Approach to Operations (EBAO) conceptualization and applicability to the full spectrum of human interactions, focused on the economic and information domains in a synchronized whole-of-government/coalition approach. It intends to answer to the question: How can EBO/EBAO be addressed in the information age? A comprehensive analysis of existing doctrine, scientific papers and thesis concur to the foundations of a theoretical background. Due to its relevancy, the memorandum for U.S. Joint Forces Command, signed by General J. N. Mattis on the 14<sup>th</sup> of August 2008 subjected to the assessment of EBO and the respective rationale (but not only this document) is assessed against that theoretical background. Along its argumentation this paper also aims to demonstrate that the conflictual interactions on the geopolitical and geoeconomic domains of cyberspace reinforce the evidences for the use of non-attrition operations to succeed in an environment of adaptive and complex systems of systems. The intensive use of internet, created networked dependencies and subsequent networked vulnerabilities that can and are exploited in an Information Warfare context, targeting not only military objectives but also national critical infrastructures, logistical networks, strategic industries and of course leaderships. Recent cyberattacks to Estonia and Georgia are symptomatic of coordinated actions on the information domain. Classic attrition instruments of combat are inefficient in this environment. Achieving information superiority is the ultimate goal for a strategic decision maker. Dealing with a humanitarian crisis, a disaster relief effort, a military conflict, combating terrorism or any other asymmetric actor, resolving a severe diplomatic incident, conducting a hostile company takeover, facing a global financial crises or any other human endeavour requests more the direct physical intervention. Information superiority empowers the decision maker with the knowledge to achieve better results deploying information operations that will support the strategy and this demands the intensive use of Intelligence supported by invasive information systems like the Echelon or the Carnivore in ways that goes beyond their original purpose namely for economic interests. To shape the perception of our adversaries, allies and neutrals, affecting their cognitive sphere thus their decision capacity, is the most efficient way to our desired outcomes. This shape of perception is doable through a comprehensive and network centric approach to operations. One can not propose a methodology or a process because it is neither of those but rather a way of thinking operations.

**Keywords:** EBO; EBAO; cyberspace; geo-economy

# Decision-Making by Effective Information Security Managers

James Pettigrew, Julie Ryan, Kyle Salous and Thomas Mazzuchi  
George Washington University, Washington DC, USA

**Abstract:** A pilot study was conducted in the last half of 2009 exploring how responsible managers make decisions with regards to information security in the enterprise. This pilot study is part of a larger research effort focused on exploring this topic. This is an interesting problem to study because security managers must make decisions based on instinct and experience rather than empirical security performance data. Yet some of the security managers are doing a decent job despite the lack of any empirical data. They face daily decisions on a variety of issues dealing with maintaining and improving the security integrity of their enterprises. While this is a constant problem confronting these managers, many are very successful. These effective managers, recognized by reputation, community and anecdotally, have ways of measuring effectiveness. However, these measures are more art and the data is only in the heads of the managers. Exploratory research was conducted to validate a method to explore how security managers make decisions about the allocation of security resources for their enterprise information security architectures. This paper presents the initial findings from the pilot study. The subjects of this pilot study were the Chief Technology and Chief Security Officers (CTO and CSO) of a large enterprise. The research method used was open-ended interviews followed by transcript analysis and categorization. The interview transcripts were analyzed to identify important themes and processes resulting in twenty-three categories of decision influences. While all categories are defined, five were common to the CTO and CSO and are highlighted. A key finding is that while the CTO and CSO share some concerns, they also have unique perspectives. This will be explored in future research from the perspective of effective team building for enterprise security management. The results of this pilot study will be used to compose a larger research effort to explore and document decision processes for successful security managers.

**Keywords:** Information security management, decision-making, open-interview

# Security Monitoring and Attack Detection in Non-IP Based Systems

**Steven Templeton**  
**University of California, Davis, USA**

**Abstract:** The control systems that support our nation are an important target class in asymmetric combat. These include critical infrastructure components such as the electric grid, gas and oil pipelines, water treatment systems and transportation networks. They also include those control systems that support manufacturing and chemical production, maritime vessels, as well as those systems related to avionics, navigation and weapons control. Because these systems generally are protected by strong physical access controls, a cyber attack may be their greatest concern. The last decade has seen a significant and growing interest in control system security. This has been driven by the increase use of contemporary networking protocols and operating systems such as Ethernet, TCP/IP, and Microsoft Windows. Although commodity equipment and a large, available pool of technicians familiar with the technology may offer a cost savings, it also brings with it all the vulnerabilities and widespread knowledge of tools and techniques to attack these systems. This has made securing modernized control systems the primary focus of control system security. However, many systems have not been “modernized” and many never will be. Many of these systems have planned operational lives exceeding 20 years. The existing technology works well and given the size of many operations, conversion will not be practical until a clear need arises. The communications protocols being used were designed for reliability and to be robust under harsh environmental and electromagnetic conditions. These are non-IP based communications. The focus on security related to modernization tends to overlook these systems, particularly in the area of security monitoring and attack detection. This paper looks at these non-IP networks, how they can be monitored, attacks on and through them, and how these attacks may be detected. We feel that advances in this area are important to securing those systems on which we most depend.

**Keywords:** Control system security, intrusion detection, security monitoring, critical infrastructure protection, sensor networks, SCADA

# Federating Enterprises Architectures Using Reference Models

Jeffery Wilson, Thomas Mazzuchi, and Shahram Sarkani  
The George Washington University, Washington DC, USA

**Abstract:** Using reference models to federate Enterprise Architectures (EA) across multiple agencies is investigated in this research-in-progress as a means to provide greater mission capabilities and increased efficiencies. Security is an important aspect of the reference model to enable federation and the model emphasizes security throughout all model layers from policy to information technology to physical security. Quantitative measures will be used to evaluate the reference model's effect on the agencies themselves and their shared missions/business goals beyond their agency enterprise. Federal departments and agencies are under increased pressure to provide effective government and citizen services with improved efficiency. Enterprise Architectures are used to align agencies strategic goals and business objectives to resources. Federal agencies in turn are mandated by the Office of Management and Budget (OMB) to map and align their EAs to the Federal Enterprise Architecture (FEA) reference models. As agencies collaborate with each other to achieve either better strategic performance or resource savings, the ability to share information about their EAs is critical to their success. A set of federal agencies is pursuing better strategic performance and resource savings by federating their EAs using a 10-Layer Architecture Reference Model traceable to the Federal Enterprise Architecture (FEA) and inspired by the International Organization for Standardization (ISO) Model of Architecture for Open Systems Interconnection (OSI) adapted for component based architectures. Expert judgment techniques will be used to elicit expert opinion on the effectiveness of the 10-Layer Architecture Reference Model in federating EAs. Specifically, the model's effectiveness for shared, interdependent missions and potential for identifying shared applications/infrastructure will be evaluated. If effective, this model could be useful in other EA federation efforts between departments/agencies within government and also potentially within the commercial sector between corporate divisions. Unique in this case study research is the use and evaluation of the 10-Layer Architecture Reference Model in federating EAs.

**Keywords:** Enterprise architecture, reference model, security architecture



# Practitioner Papers



# The Weaponry and Strategies of Digital Conflict

Kevin Coleman

Security and Intelligence Center at the Technolytics Institute, USA

**Abstract:** The global reliance on computers, networks and systems continues to grow. As our dependency grows so do the threats that target our military C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance), as well as the operational components and electronic controls for our critical infrastructure. During our collaborative research one individual proclaimed it C8ISR. (Command, Control, Communications, Computers, Combat systems, Collaboration, Coordination, Code, Intelligence, Surveillance and Reconnaissance) Given the U.S. military is the most modern, computerized force in the world, the challenge of cyber defense is far greater than for any other military in the world. Over the past decade we have experienced a substantial rise in the complexity and sophistication of cyber attacks, as well as a frightening increase in the impact of some of the attacks. Every computer is a potential cyber weapon waiting to be loaded and used by extremists, criminals, terrorists and rogue nation states. As the world becomes more and more dependent on computers and information technology, the greater the risk of cyber attacks. Government and military leaders now face this fact and our critical systems and infrastructure remain at great risk! This risk has made the ability to defend these critical systems and wage cyber attacks core capabilities required for the modern military. In the age of cyber conflict, leaders need to understand the weapons and strategies used to wage this rapidly evolving type of warfare. Public and private cooperation is not critical, it is essential if these threats are going to be addressed and proper safeguards put in place to protect the critical infrastructure from increasingly hostile cyber attacks. The realities associated with the threat of cyber conflict are beginning to set in after the attacks on Estonia, Georgia and Kyrgyzstan. The recent attacks over the July 4th holiday on the United States and South Korea have reinforced the need for immediate action and part of that action is education. Cyber warfare is now viewed as a component of a comprehensive national security strategy rather than a standalone option. It is paramount that the military, intelligence agencies, government leaders, and the homeland security community develop an appropriate doctrine to systematically and appropriately counter the threat of cyber terrorism and cyber warfare. This presentation is designed to introduce participants to the current threat environment and the current state of cyber vulnerabilities, cyber weapons and a framework for addressing cyber weapons.

**Keywords:** Cyber warfare, espionage, terrorism, weaponry, strategies

# Security Assessment Techniques for Software Assurance – a “Virtual Team” Approach

**Derek Isaacs**

**Boecore Inc. Colorado Springs Colorado, USA**

**Abstract:** Software Assurance / Software “Security” often imposes a requirement that applications be tested in a “live” (or as close to as is practicable) system – this often includes the surrounding implementation environment – as greater fidelity is needed for critical application testing and implementation confidence levels. Merely installing the software and performing a “short list” verification activity is insufficient – actual “hands on” execution of the software is needed – and when this can be done in a simulated live environment – a higher confidence level can be extended to the application target of evaluation (TOE) for implementation. This task is daunting not because of the nature of the testing – but of the need to setup and subsequently tear-down systems to participate in the performance of these tests. Fortunately – there are tools and techniques for testing application security – using a reduced set of hardware and yet maintaining operational fidelity. Virtual Machines (VM)’s and virtual network environments (team architectures) offer a method for providing this level of testing confidence while allowing for a greater variety of tests and test participant systems. This paper presents a series of architectures and scenarios proposed to implement such a testing environment that retains the viability (and fidelity) of a ‘real-world’ network environment while providing an isolated and restricted test and analysis area. This is shown through a series of scenarios and VM Team setups (scenario players) in a virtual machine based environment. This approach allows a number of benefits: Isolation of the testing environment Focus on the Target of Evaluation (TOE) for testing Capture and provide metrics on tool and technique usage and impact Provide limits and mitigation of risk and liability issues for the TOE The VM environment also offers a unique opportunity to simulate interactions between various known systems under test (TOE)’s in a ‘replicated’ environment. A set of proposed scenarios and an environmental architecture, including toolsets and targets of evaluation (TOE) systems is proposed. The applicability of the VM ‘team’ systems approach is discussed through a suite of scenarios designed to illustrate System evaluation, monitoring, and detection.

**Keywords:** Information assurance, software assurance, software testing, virtual systems

# **Asymmetrical Warfare: Challenges and Strategies for Countering Botnets**

**Gunter Ollmann**

**Damballa, Atlanta, USA**

**Abstract:** It's certainly no secret that the same technologies used for spam and identity theft on the Internet are being used to attack governmental and military targets. Likewise, it's no secret that any country with a well- developed Internet presence has active development efforts underway to mount and defend against cyberattacks. What isn't as well understood is how botnets create a perfect asymmetrical battlefield, one in which the smaller force can directly attack the larger entity on its home turf, with little or no fear of reprisal. This paper discusses how botnets can be applied to cyberwar, the challenges and risks of a typical online response, and alternate strategies for a smarter, more flexible approach to preventing botnet-driven online espionage.

**Keywords:** Botnet, cyberwarf, countermeasure, command-and-control, malware

# **Boundary Management and Integration Framework for a Joint Cyber Defence Capability for Military Forces: Analysis and Synthesis from a Through-Life Capability Management Perspective**

**Joey Roodt<sup>1</sup>, René Oosthuizen<sup>2</sup> and Jan Jansen van Vuuren<sup>1</sup>**

**<sup>1</sup>Defence Peace Safety and Security: CSIR, Pretoria, South Africa**

**<sup>2</sup>Monzé Consultants, Pretoria, South Africa**

**Abstract:** An Operational Capability for Joint Cyber Defence (JCD) must be extended in South Africa and an investigation was launched firstly to direct current Information Warfare definition and capability management activities toward establishing a Required Operational Capability (ROC) statement for a JCD capability, and secondly to provide a framework for the development of a directed and sustainable JCD capability. Currently the focus is on two areas; one is aimed at the lower levels of the systems hierarchy to develop the capabilities needed in information infrastructure defence and the second is aimed at establishing a capability at the strategic and operational levels, to aid in decision making at the level of force design. The paper reports on the development of a framework for the JCD system. The motivation for the framework is to support a cost effective and innovative approach to capability development in this area, and to develop an understanding of the operational and functional interdependencies of widely accepted domains of cyber defence. With this in mind, an assessment and decision support capability is proposed and discussed, relying on simulation and modelling tools amongst others, noting current thinking in organisational dynamics and complexity theory. An initial model is described that shows how mission requirements and the JCD Capability (and in fact, any other similar capability) may be synthesised into a coherent capability design. It is recommended that a mission-based, through-life capability management-driven acquisition approach be adopted toward establishing an effective and sustainable JCD capability, supported by a national decision making and analysis competence.

**Keywords:** Information warfare, joint cyber defence, capability life cycle, capability management, capability readiness levels, joint cyber defence framework

# **The Extremist Edition of Social Networking: The Inevitable Marriage of Cyber Jihad and Web 2.0**

**Dondi West and Christina Latham**

**Booz Allen Hamilton, Hanover, Maryland, USA**

**Abstract:** Within the Cyber Warfare community, there are several terms that have become very popular. For example: Cyber Jihad/Terrorism; Online Extremist; Twitter; Facebook; Social Networking; and Web 2.0. Collective dialog about the above terms, however, has not been forward thinking and often fail to predict how our adversaries may adopt these technologies. We are aware of extremists using the internet; we are aware that jihadist may be using Facebook and Twitter. However, we have been thinking like the mass consumers of these products that we are; not like the jihadist themselves. We must investigate whether an online extremist would openly use a mainstream social networking site and risk exposure due to the site's large number and geographic base of users. Although there is likely a minor presence of Jihadist on Facebook and similar social networking sites, for the most part, online extremist have not fully adopted these technologies that we refer to as Web 2.0. When online extremists adopt Web 2.0, it will not be on those sites that society has come to love. They will employ the very same technologies, it will look similar, but the presence of terrorism in Web 2.0 will not be like one would expect. Social networking technologies have become free and simple to deploy, allowing sites to be literally created in a matter of minutes. If an extremist social networking site is taken down, another one can be created in less than ten minutes. This paper highlights how online extremists are likely to adopt Web 2.0 and the resulting challenges. This paper begins by introducing the reader to Al-Qa'ida's use of the internet. Then, using Ning, the popular social networking platform as a case study, the paper then highlights the points that: (1) social networking technologies are very conducive to Cyber Jihad; (2) there will be no need for online extremist to use "mainstream" websites like Facebook or Twitter; and (3) the Cyber Warfare Community needs a plan to counter extremist use of their own social networking technologies.

**Keywords:** Social networking, Web 2.0, online extremist, cyber jihad, Facebook, Twitter



# Poster



# Decision Making in the Cyber Domain; The Influence of Trust and Mood

**Charlene Stokes, Joseph Lyons and Michael Haas**  
**AFRL, 711 HPW, RHXS, Wright-Patterson AFB, USA**

**Abstract:** Dwight D. Eisenhower once said “The problem in defense is how far you can go without destroying from within what you are trying to defend from without.” This axiom holds true today for network defense and reinforces the requirement of maintaining operations while utilizing systems compromised by cyber attack. Humans performing tasks and making decisions in this contested environment must build and maintain an awareness of the degraded capability of their support systems as well as the effects on themselves such that they can continue operations. Our knowledge of how cyber attacks affect human operators forms a critical component of future network defense strategy. Trust and mood are two factors that stand to contribute greatly to a user’s awareness and decision making in a cyber domain. Similar to findings associated with overreliance on automation (Parasuraman & Riley, 1997), situations of over-trust or compliance can result in a reduced detection threshold for system attacks. The influence of mood can exacerbate such effects by enhancing trust or the willingness to accept vulnerability or risk. Positive moods generally increase acceptance of risk, whereas negative moods promote risk aversion (Chou, Lee, & Ho, 2007; Yuen & Lee, 2003). The Affect Infusion Model (Forgas, 1995) suggests these effects occur due to biases in cognitive processing and information retrieval, prompting individuals to evaluate situations in a manner consistent with their current mood. In Phase 1 of our ongoing study, 40 subjects participated in a computer-based scenario, Convoy Leader (Lyons et al., 2008), where they make a route choice after being presented with two primary pieces of information: (1) a route recommendation from a local intelligence expert, and (2) a map display with route parameter information. Participants completed three trials, each of which presented three routes to choose from that involved varying levels of risk; the map and expert risk assessment information were not always congruent. Participants rated their perceived level of trust in both the expert and the map following each trial. Mood was assessed before and after each trial. A repeated-measures ANOVA (across trials) revealed significant effects for mood on perceived trust in the map display:  $F(1, 37) = 7.99, p < .01$  (positive affect);  $F(1, 37) = 5.13, p < .05$  (negative affect). Positive affect was related to reports of higher trust in the display, and negative affect was related to reports of lower trust in the display. Although the ANOVA was not significant, a similar pattern was evident in the correlations with trust in the expert. Furthermore, results revealed that subjects were 42 times more likely to trust the map display in their route choice and go against the expert’s recommendation in high vulnerability/conflicting conditions. In Phase 2 of our study, explicit corruption techniques will be injected into the map display associated with the route most often chosen in Phase 1. We will investigate if detection thresholds for a cyber attack, reported levels of suspicion, and trust vary by mood, self-efficacy, and stress appraisals of the situation.

**Keywords:** Trust, mood, emotion, cyber, influence