

The 4th International Conference on Information Warfare and Security

Graduate School of Business,
University of Cape Town,
Breakwater Campus,
Cape Town,
South Africa

26-27 March 2009

Edited by
Leigh Armistead
Edith Cowan University
Perth Australia

Copyright The Authors, 2009. 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.

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

ISBN: 978-1-906638-28-3 CD

Published by Academic Publishing Limited
Reading
UK
44-118-972-4148
www.academic-publishing.org

ICIW 2009

Paper Title	Author(s)	Guide Page	Page No.
Preface		iii	iii
Biographies of Programme Chair, and Keynote Speakers		v	v
Biographies of contributing authors		vii	vii
On the use of Internet Voting on Compromised Computers	<i>Philippe Beaucamps¹, Daniel Reynaud-Plantey¹, Jean-Yves Marion¹ and Eric Filio²</i> <i>¹Equipe CARTE – LORIA, Vandoeuvre-lès-Nancy Cedex France</i> <i>²Army Signals Academy, Rennes, France</i>	1	1-9
2D Verses 3D Tactical Supremacy in Urban Operations	<i>Chris Flaherty</i> <i>Visiting Fellow, the University of New South Wales, Australia</i>	2	10-17
The Changing Nature of Leadership in Finnish Military Organisational Culture: The Melting of Mechanistic Command and Control in Media-Networked Circumstances	<i>Aki-Mauri Huhtinen</i> <i>National Defence University, Helsinki, Finland</i>	3	18-26
Warning to Information Operations Planners: Ignore the Information-Seeking Patterns and the Legal Protection of Information Warfare Victims in the Middle East at Your Peril	<i>Berg Hyacinthe</i> <i>Université de Paris-Assas School of Law, CERSA-CNRS, France</i> <i>Infosense Technologies and Research, Inc., USA</i>	5	27-34
The Role of Funding and Training for the Management of the Computer Forensics Investigation	<i>Hamid Jahankhani¹, Amie Taa² and Kenneth Revett³</i> <i>¹School of Engineering and Information Sciences, Middlesex University, UK</i> <i>²Ex-law enforcement officer, Metropolitan Police, UK</i> <i>³University of Westminster, London, UK</i>	6	35-42
A Model for Peace Support Operations: An Overview of the ICT and Interoperability Requirements	<i>Louise Leenen, Mapule Modise and Herman le Roux</i> <i>DPSS, Council for Industrial and Scientific Research, Pretoria, South Africa</i>	7	43-52
Is Buying and Transacting Online Easier and Safer Than Down Town? : An Emerging Economy Perspective	<i>Edna Martim¹, Moses Dlamini¹, Darelle van Greunen², Jan Eloff³ and Marlien Herselman⁴</i> <i>¹SAP Research CEC Pretoria, South Africa</i> <i>²Nelson Mandela Metropolitan University, South Africa</i> <i>³University of Pretoria³, South Africa</i> <i>⁴Tshwane University of Technology, Pretoria, South Africa</i>	8	53-59

Paper Title	Author(s)	Guide Page	Page No.
Analyzing Functional Entropy of Software Intent Protection Schemes	<i>Todd McDonald, Eric Trias, and Alan Lin Air Force Institute of Technology, Wright Patterson, USA</i>	9	60-67
Laws and Regulations of USAF Military Operations in Cyberspace	<i>Thomas Moore, Michael Grimaila, and Dennis Strouble Air Force Institute of Technology, Wright Patterson, USA</i>	10	68-76
Let Your Fingers Do the Fighting: Pre-Acquisition Exploits - The Technology Crucible	<i>John Nugent University of Dallas Graduate School of Management, Texas, USA</i>	11	77-84
Computer Network Attack (CNA) Exploit and Vulnerability Trends for Department of Defence Red and Blue Assessment Teams	<i>David Rohret CSC, Inc., San Antonio, Texas, USA</i>	12	85-89
VoIP Over MANETs: A Performance Analysis of OLSR	<i>Noreen Santos, Barry Mullins, Rusty Baldwin and Ryan Thomas Air Force Institute of Technology, Dayton, Ohio, USA</i>	13	90-100
Developing an Academic Curriculum in Information Operations: The First Steps	<i>Corey Schou¹, Julie Ryan² and Leigh Armistead³ ¹Idaho State University, Pocatello, Idaho, USA ²George Washington University, Washington DC, USA ³Edith Cowan University, Perth, Australia</i>	14	101-110
A Statistical Analysis of Large Passwords Lists, Used to Optimize Brute Force Attacks	<i>Renier Pelsler van Heerden and Johannes Vorster CSIR, Pretoria, South Africa</i>	15	111-128
Towards a Conceptual Framework for Cyberterrorism	<i>Namosha Veerasamy Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa</i>	16	129-137
Considerations for Management from the Onset of Information Terrorism	<i>Ken Webb Edith Cowan University, Perth, Western Australia</i>	17	138-145

Preface

These Proceedings are the work of researchers contributing to the 4th International Conference on Information Warfare and Security (ICIW 2009), hosted this year by the South African Council for Scientific and Industrial Research (CSIR) in Cape Town, South Africa. The Conference Chair is Johannes Vorster from the CSIR and once again I am pleased to be Programme Chair.

This year for the first time the conference has ventured away from the USA and we are pleased, in these proceedings, to see research from other parts of the world into different aspects of Information Warfare and Information Security.

The opening keynote address this year is given by General Brazzoli from the South African Air Force and on day two of the conference, the opening keynote speaker is R Adm R.W.Higgs, of the South African Navy.

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 36 abstracts, after the double blind, peer review process there are 16 papers published in these Conference Proceedings, including contributions from Australia, Finland, France, South Africa the United Kingdom and the United States.

I wish you a most enjoyable conference.

Leigh Armistead
Edith Cowan University
Programme Chair

Conference Executive:

[Edwin Leigh Armistead](#), Edith Cowan University, Australia
[Andy Jones](#), Security Research Centre, BT, UK and Edith Cowan University, Australia
[William Mahoney](#), University of Nebraska Omaha, Omaha, USA
[Dan Kuehl](#), National Defense University, Washington DC, UK,
[Corey Schou](#), Idaho State University, 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); Jim Alves-Voss (University of Idaho, USA); Leigh Armistead (Edith Cowan University, Australia); Johnnes Arreympi (University of East London, UK); [Richard Baskerville](#) (Georgia State University, USA); Alan Berg (Critical Infrastructure and Cyber Protection Center, Capitol College, USA); Elisa Bertino (CERIAS, Purdue University, USA); Alexander Bligh (College of Judea and Samaria, Israel); [Sviatoslav Braynov](#) (University of Illinois, USA); Blaine Burnham (University of Nebraska, Omaha, USA); Roy Campbell (University of Illinois at Urbana and Champaign, USA); Catharina Candolin (Finnish Defence Forces, Helsinki, Finland); Rodney Clare (EDS and the Open University, UK); Nathan Clarke (University of Plymouth, UK); Geoffrey Darnton, (University of Bournemouth, UK); [Dipankar Dasgupta](#) (University of Memphis, USA); Dorothy Denning (Navel Postgraduate School, USA); Glenn Dietrich (University of Texas, USA); David Fahrenkrug (US Air Force, USA); Larry Florentine (Larry Florentine Associates, USA); [Xinwen Fu](#) (Dakota State University, 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); 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 (Airforce Institute of Technology, USA); Takakazu Kurokawa (National Defense Academy, Japan); Tuija Kuusisto (National Defence College, Finland); Irving Lachow (National Defense University, USA); Arun Lakhota (University of Louisiana Lafayette, USA); Michael Lavine (John Hopkins University, USA); Tara Leweling (Naval Postgraduate School, USA); Cherie Long (Clayton State University, Decatur, USA); Brian Lopez (Lawrence Livermore National Laboratory); Bin Lu (West Chester University, USA); Bill Mahoney (University of Nebraska, USA); John McCarthy (Buckinghamshire and Chiltern University College, UK); J Todd McDonald (Airforce Institute of Technology, USA); Anne McGee (Industrial College of the Armed Forces, USA); Robert Mills (Air Force Institute of Technology, Ohio, USA); Don Milne (Buckinghamshire and Chiltern University College, UK); Evangelos Moustakas (Middlesex University, UK); Srinivas Mukkamala (New Mexico Tech, Socorro, USA); Barry Mullins (Air Force Institute of Technology, Wright-Patterson, USA); Andrea Perego (Università degli Studi dell'Insubria, Italy); 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); Simon Shadbolt (EDS, UK); Dan Shoemaker (Univesity of Detroit Mercy, USA); William Sousan (University of Nebraska, Omaha, USA); Ingrid Splettstoesser (York University, North York, Canada); [Kevin Streff](#) (Dakota State University, USA); Steve Tate (University of North Carolina at Greensboro, USA); [Doug Twitchell](#) (Illinois State University, USA); Renier van Heerden (CSIR, Pretoria, South Africa); Stylianos Vidalis (Newport Business School, UK); Fahad Waseem (Unviersity of Northumbria, UK); Kenneth Webb, Edith Cowan University, Australia); Douglas Webster (USSTRATCOM Global Innovation & Strategy Center, USA); [Tom Wilsdon](#) (University of South Australia, Australia); Takahiro Yonekawa (HUB Networks, Inc., Tokyo, Japan); Zehai Zhou (Dakota State University, USA).

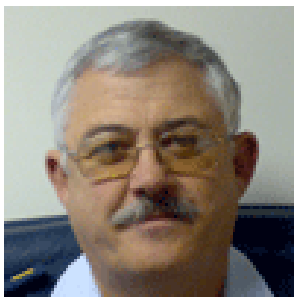
Biographies of Programme Chair and Keynote Speakers

Programme Chair

Leigh Armistead Currently the Senior Program Manager for Information Operations and Information Assurance for Honeywell Technology Solutions Inc, Leigh is also the editor of Information Operations: Warfare and The Hard Reality of Soft Power and Information Warfare: Separating Hype from Reality. A retired U.S. Naval Officer and former Master Faculty of IO at the Joint Forces Staff College, he is currently enrolled in a PhD program at Edith Cowan University in Perth, Australia. Leigh has published a number of articles on IO in addition to chairing numerous professional IO conferences around the world, including the International Conference on Information Warfare in 2006 and 2007, as well as the IQPC IO Conference in the United Kingdom from 2002 to 2005. Selected five years in a row as a research fellow for the International National Security Studies program to conduct IO-related research, he also helped to develop an online IO course for the National Security Agency

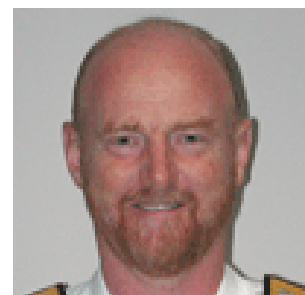


Keynote Speakers



Mario Brazzoli is a serving officer in the SADF and holds the title of Government Information Technology Officer in the Defense Secretariat. He has enjoyed a long and distinguished career in the South African Air Force having held a variety of different postings both domestically and as a Military Attaché abroad. In January 2003 he established the new Directorate Information Warfare within the Command and Management Information Systems Division of the South African defense force. Maj Gen Brazzoli holds a B MIL (B.Sc.) from the South African Military Academy as well as a M.Sc. degree in Engineering Management from the University of Pretoria.

R Adm R.W. Higgs. is a serving officer in the SADF and holds the title of Flag Officer Fleet in the South African Navy. His distinguished naval career has included extensive sea time in both surface vessels and the submarine service. R Adm Higgs was appointed to Washington in 1998 as the Naval Attaché. In 2000, he led the Defence Office of Ambassador Sheila Sisulu. He was elected Chairman of the Naval Attaché Association in Washington for 2000. He has published several award winning papers on both international and regional security strategy. He holds a B Mil (B Sc) from the Military Academy in Saldanha Bay and a Master's Degree in International Relations from Salve Regina University, Rhode Island, USA.



Biographies of contributing authors (in alphabetical order)

Leigh Armistead is Currently the Senior Program Manager for Information Operations and Information Assurance for Honeywell Technology Solutions Inc, Leigh is also the editor of Information Operations: Warfare and The Hard Reality of Soft Power and Information Warfare: Separating Hype from Reality. A retired U.S. Naval Officer and former Master Faculty of IO at the Joint Forces Staff College, he is currently enrolled in a PhD program at Edith Cowan University in Perth, Australia. Leigh has published a number of articles on IO in addition to chairing numerous professional IO conferences around the world, including the International Conference on Information Warfare in 2006 and 2007, as well as the IQPC IO Conference in the United Kingdom from 2002 to 2005. Selected five years in a row as a research fellow for the International National Security Studies program to conduct IO-related research, he also helped to develop an online IO course for the National Security Agency.

Philippe Beaucamps is currently a PhD student at the Loria / CNRS in Nancy, France. His research is centered around computer viruses and more globally computer-related threats. Part of this research is devoted to the formalization and protection against viral mutation techniques.

Moses Dlamini received his BSc Computer Science and Mathematics in 2002. In 2006, he received his Honours BSc Computer Science. He has worked as an assistant lecturer at the University of Pretoria. He is now working at SAP Research CEC Pretoria and working towards finishing his MSc in Computer Science at the University of Pretoria.

Christopher Flaherty is a Visiting Fellow at the School of Risk and Safety Sciences, living in London. Dr. Flaherty specialises in terrorism assessment and terrorism tactics. Modern terrorism in urban environments poses particular problems for response. At UNSW, Dr. Flaherty and Dr. Tony Green are developing methods for improving the response of agencies involved in security.

Aki Huhtinen, PhD. Huhtinen is Docent of practical philosophy in the University of Helsinki and Docent of social consequences of media and information technology in the University of Lapland. Huhtinen works at the Department of Management and Leadership Studies at the Finnish National Defence College. He is a leader of a research group and professor at the National Defence University, Department of Management and Leadership Studies since September 1, 2004. The job description includes compiling the yearly research plan for the department, directing research of students of different levels, lecturing on research, co-operation with other universities and international faculties of the field. In addition, since September 1, 2004, the job description includes starting up programs for doctorate studies and docenture. The last book, "Messy War", has a postmodern scientific research about warfare.

Berg Hyacinthe completed his PhD from Florida State University where he focused on Information Warfare, Social Informatics, and Emergent Technologies. Currently, he holds the position of Assistant Professor and Scientific Advisor to Taibah University's Strategic Science & Advanced Technology Research Unit in the Kingdom of Saudi Arabia. He is a U.S patent holder—with new pending patents—whose works have been featured in conferences held at the U.S. Naval Postgraduate School, Monterey; Defence Academy of the United Kingdom, Shrivenham; National Defense College, Helsinki; DARPA-sponsored Technologies for Homeland Security Conference, Florida. Dr. Hyacinthe is featured in Harvard's Smithsonian/NASA Astrophysics Data System and also at Assas School of Law

(La Sorbonne). As a legal scholar with proven expertise in foresight and forecast of digital information technologies, Dr. Hyacinthe is pioneering, against the current “anarchical state” of information warfare, a domestic law approach to the definition and regulation of 21st century information warfare conducts, damages, and responsibilities. As such, his latest research activities have been continuously intensified towards the completion of his second doctoral dissertation: The Juridical Notion of Information Warfare (Doctor of Laws/LLD from Assas School of Law).

Louise Leenen is a Senior Researcher at the South African Council for Scientific and Industrial Research in the Information Systems Research Group (IS). IS focuses on the use of ICT in Peace Support Operations. Leenen holds a MSc in Computer Science and has recently submitted a PhD thesis on the solution of partial Constraint Satisfaction Problems for examination.

Herman Le Roux has been with the South African Council for Scientific and Industrial Research since April 1998 and is at present a Principal Engineer in the Mathematical and Computational Modelling Research Group. He is involved in Modelling and Simulation-based Acquisition Decision Support, specifically for the South African National Defence Force. Le Roux holds a Masters Degree in Computer Engineering and is currently pursuing a PhD in Command and Control Modelling.

Todd McDonald Lt Col J. 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.

John Nugent, Dr, CPA, CFE, CFF, CISM, FCPA is the founding director of Center of Information Assurance (IA) and MBA and MM programs in IA, and serves as an associate professor at the Graduate School of Management, University of Dallas where he teaches courses on business strategy, IA, wireless, telecommunications and capstone courses. Previously, John served as a Fortune 10 subsidiary CEO serving as president and a board of director member of a number of AT&T subsidiaries. There he oversaw the development of over 100 state of the art secure products ranging from chips, to communication products, to secure switches and satellite systems. John was awarded the Defense Electronics “10 Rising Stars” award in July 1989 as well as the Diplome de Citoyen D’Honneur, Republic of France in June 1988 for his work there. John is a member of the U.S. Secret Service’s North Texas Electronic Crimes Task Force and is a sub-committee chair of several American Bar Association (ABA) committees that research and publish on cyber security, cyber law, privacy, and Information Assurance matters.

David Rohret served in the US Air Force for nine years as a computer scientist developing graphic imaging systems, automated modeling, and artificial intelligence systems. For the last fifteen years Mr. Rohret has pursued network security interests to include team lead on an exploit development project, developing and vetting exploits for use on established red teams, and as the task lead for the Joint Electronic Warfare Center’s Advanced Concept Technology Demonstrations (ACTDs) CNS Red Team. In his current position at the JEWIC in San Antonio, TX, Mr Rohret leads a CNS Red Team against newly developed systems, as well as, testing and researching emerging technologies that may be integrated into ACTD programs. B.A. Computer Science, University of Iowa, 1981 M.S. Computer Science, La Salle University, 1994

Lady Noreen Santos received a Bachelors of Engineering degree in Electrical Engineering from Stevens Institute of Technology, Hoboken, N.J. in 2004 and has completed her Masters of Science degree in Computer Engineering at the Air Force Institute of Technology, Wright-Patterson AFB, OH in March 2009.

Dennis Strouble Dr. is an assistant professor of Systems Engineering Management at the Air Force Institute of Technology. He holds a Ph.D. in Management and a J.D., both from Texas Tech University. Currently, he teaches graduate courses in Systems Engineering Management, Information Resource Management, and Law, and leads sponsored research in support of the Systems Engineering and Information Research Management programs. Dr. Strouble has taught at several universities, has remained active in the area of law, and has founded and managed several businesses.

Renier van Heerden works as a senior researcher at Council for Scientific and Industrial Research (CSIR) in South Africa in the field of Information Warfare. Before working at the CSIR he worked as a software engineer at Denel Optronics and as a Lecturer at the University of Pretoria. He has obtained a degree in Electronic Engineering and a Masters in Computer Engineering at the University of Pretoria.

Namosha Veerasamy has obtained a BSc: IT Computer Science degree and a BSc. Computer Science (Hons) degree with distinction from the University of Pretoria. Namosha is qualified as a Certified Information Systems Security Professional (CISSP) and is currently completing her Masters in Computer Science at the University of Pretoria. She is employed as a researcher in the field of computer and network security at the Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa.

Ken Webb Dr. After graduating from the Royal Military College, Ken served as a qualified commissioned officer with the SAS and other special operations units where he spent much time on information warfare. Upon leaving the military, he worked globally in related fields and then completed a doctoral level research project for the Australian Research Council into enhancing national security from terrorist groups. He also became the counter-terrorism research leader for a Federal Government initiative.

On the use of Internet Voting on Compromised Computers

Philippe Beaucamps¹, Daniel Reynaud-Plantey¹, Jean-Yves Marion¹ and Eric Filiol²

¹Equipe CARTE – LORIA, Vandoeuvre-lès-Nancy Cedex France

²Army Signals Academy, Rennes, France

Abstract: Internet voting is the process of letting voters cast their vote over the Internet, at home or on public computers. It is a way to reduce the cost associated with elections and to obtain higher participation, but it also raises important security problems. In this paper, we study shortcomings related to this technology, and more particularly shortcomings due to the presence of dedicated malware on the voters' computers. Common literature usually focuses only on designing a secure voting protocol, either discarding the malware issue or proposing prohibitive solutions, such as the use of dedicated hardware. However the purpose of Internet voting is precisely to allow anyone to vote from home, making the use of dedicated hardware a non conceivable solution. Therefore, we analyse the reliability of possibly malware-infected mainstream computers. Specifically, we do not consider the security of the voting protocol but define the data available to the malware and the attacks that can be carried out thereby. We show that current Internet voting implementations are vulnerable to these attacks, due to weak or irrelevant security measures. Thus we describe reasonable solutions that aim at coping with the lack of security of current implementations on general-purpose computers, even though some attacks cannot be prevented but can only be mitigated. For example, it is impossible to prevent the malware from stealing the user credentials with no hardware support, but it is easy to design a system in which user credentials are useless to an attacker: therefore we can prevent more serious attacks such as automatic vote changing and voter impersonation. Among other solutions, we describe and study reliability of hybrid voting mechanisms, using a medium which can not be accessed by the malware, as well as of Human Interaction Proof implementations to prevent automatic vote changing and the election invalidation that could result from this class of attacks.

Keywords: Evoting, Internet voting, evoting malware, compromised browser, secure evoting, semantic captcha, trusted computing

2D Verses 3D Tactical Supremacy in Urban Operations

Chris Flaherty

Visiting Fellow, the University of New South Wales, Australia

Abstract: Applying Boyd's OODA Loop (for Observe, Orient, Decide and Act) to tactical analysis in civil urban environments presents a challenge to conventional counter terrorism thinking. The solution proposed here, is to take a revised approach to Boyd's OODA loop incorporating 3D tactics. 3D tactics is defined as tactics in the third dimension which is the space above and below ground level in land and urban operations. The observational and orientation parts of Boyd's loop are key problem areas, because these are poorly addressed by people thinking linearly in two-dimensional tactical analysis (2D Tactics). In general, mass gathered people located in highly complex urban structures incorporating features such as multi-level buildings, open spaces between buildings, crowd congregation points, and transport hubs within the central business district (CBD), is from a conventional 2D tactical viewpoint impossible to analyse. As well, the problem as to how to develop a counter terrorism analysis applicable to mass gathering space is not adequately addressed in contemporary tactical theory. This is because terror tactics are based on a radical approach, which to date has not been properly analysed.

Keywords: 3D tactics, information warfare, ooda loop, counter-terrorism

The Changing Nature of Leadership in Finnish Military Organisational Culture: The Melting of Mechanistic Command and Control in Media-Networked Circumstances

Aki-Mauri Huhtinen

National Defence University, Helsinki, Finland

Abstract: The phenomenon of 'technologisation' is among the main foci in critical strategy studies and also the key question of military leadership and management in the information age (see Dos and Kosonen 2007 and Mantere and Vaara 2007). Today, core infrastructure and the whole of society are dependent on information technology (IT). However, IT has caused unexpected and increased troubles in information systems. The economic losses caused by faulty software and failing information systems are enormous (Tervo and Ahonen 2008). Strategy is increasingly linked to specific systems and technology, especially in military organisations. A key concern of organisational strategy is to use scorecards to measure organisation and improve the competence and work performance of the personnel. However, the strategy process is typically conceptualised as a system driven by a specific logic. Here personnel in the organisation enjoy quite limited decision-making power. They are more 'resources' for the system than subjects involved in making decisions.

War has never before been open to anonymous individuals sitting at a distant location armed with computers and other electronic devices. Classically, military commanders are highly productive and result-oriented, and they can be very effective when achieving goals is the primary focus. The stereotypical requirement for military leadership is also to be logical and rational, insisting on covering all alternatives in a decision-making situation. The inspirational style and radical new ideas, or the supportive leadership dimension, have often remained quite marginal. Typically, military organisations face serious deadline challenges, so command-and-control (C2) methods form a fairly natural leadership culture. Generally, organisations in the information age have shifted from a C2 culture toward a more human-centred, supportive, and empowering environment. In military culture, this change will become a strategic issue. The old, C2 culture may not be able to succeed in a networked environment.

Networked technology has penetrated field/tactical structures and the middle or operational level of organisations, but still thinking and acting at the top levels rely on a mechanistic and hierarchical worldview. The entertainment industry and individualisation of media set new demands for leadership. The bigger the gap in the skills and will between the technological application and organisation and, on the other hand, the people who use them, the greater the risk of the resources that have been invested in the technology being wasted.

Power is normally a function of size, and the bigger any organization is, the bigger the bureaucracy that runs it. The culture of independent thinking is lacking in the big military organizations. There are factors present today which are actually increasing the degree of centralizing authority. We have noted that at the tactical level technical means of command and control have stifled initiative taking. There is always some form of technology available to deal with combat: alternatives have thus been limited. The issue here is in large part that big organizations are not just bureaucratic, but because of their very size, they have to be very ordered. (Thornton 2007, 160-170)

Through the new theory of network-centric warfare, this article examines the Finnish Defence Forces organisational transformation from 'Weberian' hierarchical organisation to network-centric organisation. Focus is placed on change in organisational culture from a Finnish starting point. As more and more visible civilian and military crisis management operations of the Western armed forces take place in public, the interactions among military subcultures (different branches, for example) are also changing. Above all, management environments can differ greatly from those of the past. The change also is intimately tied to issues of good management and leadership.

Keywords: Strategic leadership, organisational culture, 'technologisation', revolution in military affairs, C2 model in information warfare

Warning to Information Operations Planners: Ignore the Information-Seeking Patterns and the Legal Protection of Information Warfare Victims in the Middle East at Your Peril

Berg Hyacinthe

Université de Paris-Assas School of Law, CERSA-CNRS, France

Infosense Technologies and Research, Inc., USA

Abstract: The success of pre-emptive strikes and decisive military operations depends profoundly on reliable human intelligence and the versatile skills of 21st century “cyber warriors” whose Information Operations (IO) activities are conducted through the pentagonal synchrony —land, sea, air, cyberspace, and outer-space— of modern warfare. As such, Command-and-Control over the aforementioned quintet is developing, in nanoseconds, towards its full “interstellar” potentials.

These operations are commonly effectuated, alas, under a defunct judicial reasoning that has been sustained by Information Warfare (IW)’s anarchical regime of “legal ambiguities”. Of course, following a plethora of exploratory attempts, the time to regulate has come; but still the question arises, how and under what legal framework should explicit IW guidelines be established? In response, a foundational *domestic law approach* is proposed, herein, with the primary objective of overcoming widely documented *shortcomings of international law* in the complex realm of IW. Essentially, with a transcendental domestic legal framework in the background, the time to hold an honest discussion on *IW conducts, weapons, damages and responsibility*, at the UN, is now.

Keywords: Lethal IW technologies, culture-blind IO, physical IW weapons, interstellar weapons, Middle East conflicts, law

The Role of Funding and Training for the Management of the Computer Forensics Investigation

Hamid Jahankhani¹, Amie Taal² and Kenneth Revett³

¹School of Engineering and Information Sciences, Middlesex University, UK

²Ex-law enforcement officer, Metropolitan Police, UK

³University of Westminster, London, UK

Abstract: Until recently E-crime had to be dealt with under legal provisions meant for old crimes such as conspiracy to commit fraud, theft, harassment and identity theft. Matters changed slightly in 1990 when the Computer Misuse Act was passed but even then it was far from sufficient and mainly covered crimes involving hacking. Fuelled by frequent sensational media headlines and news coverage of cyber-crime in the UK and the lack of enough police action, this paper attempts to provide an unbiased perspective from the law enforcement arena. This paper critically assesses the importance of funding, proper education and training to handle, manage and investigate computer evidence. We present an emerging methodology for managing the Computer Forensics process based on guidance to assist law enforcement in dealing with computer evidence. Lastly, this paper looks at the importance of having a form of accreditation to validate experience, skills and qualifications and how this may be achieved. We conclude with indications of further work and other emerging issues.

Keywords: Digital forensics, training, funding, ACPO, cyber crime, information security, CCTV

A Model for Peace Support Operations: An Overview of the ICT and Interoperability Requirements

Louise Leenen, Mapule Modise and Herman le Roux

DPSS, Council for Industrial and Scientific Research, Pretoria, South Africa

Abstract: This paper is part of a long term research project conducted by the Council for Scientific and Industrial Research (CSIR) In South Africa. The objective of the project is to construct a model for the planning and execution of Peace Support Operations (PSOs). In this paper we describe the development methodology for a PSO planning model and we investigate the required interoperability information and communication technologies (ICT) requirements for PSOs.

Peace support operations, by their very nature, can be extremely complex endeavours. They are characterised by multiple stakeholders working together to solve ill-structured problems. In the case of the South African National Defence Force (SANDF), this means the deployment of different arms of service together with other potential stakeholders such as a coalition of multinational forces, government agencies, civilian agencies, local populations, warring factions, and media agencies. The diverse presence of multiple stakeholders requires a reciprocal interdependence among these various elements, and this necessitates complex coordination and a great demand for ongoing and accurate communication (Chisholm 1986). Higher technological complexity requires higher levels of communication (Gailbraith 1977).

The complexity is exacerbated by the fact that peace support missions are long in duration and success cannot be achieved by conducting a series of unrelated actions. The decision/action cycle is continuous and every action must contribute to the overall mission. Rapid decision making under conditions of volatility and uncertainty adds to the complexity. Forces, including commanders, are also rotated after serving a term, thus at hand-over loss of situation awareness may occur.

The Command and Control for these operations place additional burdens on the ICT that support it. In essence, required Information Warfare (IW) capabilities and technologies in Peace Support Operations (PSO) are the ICT that provides a Joint Command and Control capability.

In the first part of this paper, we describe a methodology to construct a planning model for PSO and we motivate the use of morphological analysis to develop a first phase of the model. In the second part, we identify the required ICT for PSOs, and investigate interoperability requirements for Joint Command and Control in PSOs. Our findings are based on interviews conducted with various individuals that are involved in PSOs, as well as a literature study. The Joint Command, Control and Consultation Information Exchange Data Model enjoys international acceptance as a basis for interoperability. Some countries have even accepted it as a national data model. This model will be used as a starting point of the interoperability standards investigation.

Keywords: Peace support operations, command and control, situational awareness, morphological analysis, JC3IEDM

Is Buying and Transacting Online Easier and Safer Than Down Town? : An Emerging Economy Perspective

Edna Martim¹, Moses Dlamini¹, Darelle van Greunen², Jan Eloff³ and Marlien Herselman⁴

¹SAP Research CEC Pretoria, South Africa

²Nelson Mandela Metropolitan University, South Africa

³University of Pretoria³, South Africa

⁴Tshwane University of Technology, Pretoria, South Africa

Abstract: Security and usability are crucial factors for the successful operation of any e-commerce system. However, they have traditionally been considered a design trade-off. In an effort to align them, this paper highlights the design principles and guidelines for usable and secure systems. These principles and guidelines are used to evaluate and demonstrate several real-life cases of effective and less effective security and usability implementations in an emerging economy (South African) context.

Keywords: Security, usability, e-commerce, retail, banking, emerging economy

Analyzing Functional Entropy of Software Intent Protection Schemes

Todd McDonald, Eric Trias, and Alan Lin

Air Force Institute of Technology, Wright Patterson, USA

Abstract: Defending a legitimate software program from a malicious host is a most challenging task. In particular, adversaries may subvert forensics tools, find and exploit known application weaknesses, and reverse-engineer code in order to understand and thwart their intended purposes. From a developer's perspective, one standard defense is to dramatically increase the computational resources an adversary expends on analyzing the client code. We explore in this paper ideas related to intent protection, an approach to software security that combines recoverable changes in black-box program behaviour with white-box structural changes. If we assume that the best intent protection transformations are those which are random and also produce a hiding property of interest, one characteristic of interest in this model is whether structural randomness correlates with functional randomness. We present experimental results that relate random input/output patterns with systematic code transformations and random creation. Accordingly, we offer observations on the relationship between functional entropy and correlation with generalized software intent protection schemes.

Keywords: Program protection, computer security, obfuscation, hacking, cryptography

Laws and Regulations of USAF Military Operations in Cyberspace

**Thomas Moore, Michael Grimaila, and Dennis Strouble
Air Force Institute of Technology, Wright Patterson, USA**

Abstract: In December 2005, the United States Air Force (USAF) changed its mission statement by adding “cyberspace” to its traditional domains of air and space. A key motivation for the change can be found in a statement by former USAF General T. Michael Moseley during a speech in which he stated, “Our enemies are already operating in cyberspace, exploiting the low entry costs, the minimal technological investment needed to inflict serious harm”. The significance of cyberspace as an operational domain prompted General Moseley to send a “Go Do” letter to USAF Lieutenant General Robert J. Elder, commander of Eighth Air Force. In his letter, General Moseley conveyed his intent, “to redefine air power by extending the Air Force’s global reach and global power into a new domain.” Since this time, many changes have occurred within the USAF to formalize operational capabilities in the cyber domain. One key question that has been continuously raised is “What are the legal implications of conducting military operations in cyberspace?” While some believe that existing laws adequately address the issues arising from military use of cyberspace, others believe that new laws are required to clarify the intent of existing laws and improve our ability to fight in cyberspace. The purpose of this paper is to examine the legal implications of conducting military operations through an analysis of pre-existing doctrine, laws and regulations. We will explain why the USAF is moving into the cyberspace domain; review the relevant Department of Defense, Joint, and USAF guidance; review applicable US laws; and explain how current laws and regulations can be applied and interpreted to military operations conducted in cyberspace.

Keywords: Cyber warfare law, cyber warfare doctrine, cyber warfare regulations

Let Your Fingers Do the Fighting: Pre-Acquisition Exploits - The Technology Crucible

John Nugent

University of Dallas Graduate School of Management, Texas, USA

Abstract: This paper addresses a new form of information warfare in the form of a serious hidden technology exploitation that poses a fundamental risk to all users of IT, telecommunications, and other “powered” systems, and proffers approaches for dealing with such threats. Such challenges if left unaddressed, represent the ultimate form of warfare.

Heretofore, IT and telecommunications professionals in particular have been concerned principally with “post acquisition” exploits from viruses, worms, Trojans, password hacking, rootkits, EMI/RFI attacks, etc. Such traditional threats have been deemed to be from outside the protected boundaries of the enterprise. However, today it is becoming apparent that a much more pernicious threat exists in the form of “pre-acquisition” hidden exploits, exploits embedded in the product prior to acquisition, against which most are ill prepared to defend themselves. Such exploits represent the ultimate “Trojan Horse” attack in that the users themselves bring the compromised equipment into the protected boundaries of the enterprise thereby compromising traditional protections provided by authentication, access, and firewall defenses. And with numerous state organs apparently working with the manufacturers in their respective countries, the exploitation of other nation states and the enterprises within those states is real and substantive. These “pre-acquisition” technology exploits are examined and approaches are proffered to help in mitigating such challenges and risks.

Keywords: Technology exploits, cybertrust, systrust, sas 70, aicpa, common criteria, trojans

Computer Network Attack (CNA) Exploit and Vulnerability Trends for Department of Defence Red and Blue Assessment Teams

David Rohret

CSC, Inc., San Antonio, Texas, USA

Abstract: The effectiveness of Department of Defence (DoD) computer network Red and Blue teaming depends upon accurate trend analysis data, which allows assessment teams to tailor their vulnerability analysis and penetration testing methods and techniques to the specific networks and architectures they will be assessing. Most trends and analysis data are derived primarily from commercial and open-source research that are non-specific, even generic in nature. Organizations and researchers attempt to track information from very large data sets derived from high-level observations of Internet and intranet traffic, generalizing attack and vulnerability analysis for a wide and varied audience/clientele. This approach to trends research provides high level statistical data that does not benefit Red team analyst in determining the most effective method of assessing specific systems and networks.

Poor delineation of the terms “event” and “incident” compound the problem in many open-source and commercial trend reports, as the two terms represent different aspects of an attack and are often incorrectly derived, skewing or invalidating the results. Additionally data may be emphasized or suppressed depending on the reporting organizations goals, products, and or specialization in network security.

Unlike malicious hackers or adversaries, Red and Blue teams providing assessments and vulnerability studies for government and commercial clientele are usually required to accomplish their assessments within a specific time frame and within a fixed budget. Commercial and custom vulnerability trends analysis may take months and requires extensive resources, which may not be available to the assessment teams in a timely manner. These obstacles are further compounded by interdepartmental segregation of duties within Government agencies that limit or prohibit uncharted actions based on funding guidelines and/or mission statements.

This paper endeavours to identify issues preventing the identification of timely and specific vulnerability and network attack trends data, providing an alternative to current trends research methodology for Computer Network Security (CNS) Red and Blue teams assessing specific non-generic networks and network-centric data systems.

Keywords: Red team vulnerability exploit trends analysis

VoIP Over MANETs: A Performance Analysis of OLSR

**Noreen Santos, Barry Mullins, Rusty Baldwin and Ryan Thomas
Air Force Institute of Technology, Dayton, Ohio, USA**

Abstract: Using Voice over Internet Protocol (VoIP) in Mobile Ad hoc Networks (MANETs) takes advantage of the mobility and versatility of a MANET environment and the flexibility and interoperability a digital voice format affords. Current issues with this combination of technologies include routing traffic in the MANET. Previous research has shown that VoIP-like traffic is capable of being routed through an ad hoc network using the Ad hoc On-demand Distance Vector (AODV) routing protocol (a reactive routing protocol). However, the Optimized Link State Routing (OLSR) protocol is a proactive routing protocol also used in MANETs that may also be suitable. This research determines the suitability of OLSR as a routing protocol for MANETs running VoIP applications.

Representative VoIP traffic is submitted to a MANET and the metrics of end-to-end delay and packet loss are observed. The factors of node density, number of data streams and mobility are varied creating a full-factorial experimental design of 18 distinct scenarios. OPNET modeler simulates the MANET, and VoIP traffic is introduced using one source node that sends traffic to random destinations throughout the network.

Results show that node density, number of data streams and mobility most affect delay and packet loss. As the number of data streams increase, both delay and packet loss also increases. Increase in the number of nodes in the simulation area (1,000 m by 1,000 m) decrease delay, showing that packet loss is affected by the number of nodes in the MANET.

Delay is between 0.069 ms to 0.717 ms which is significantly lower than the recommended 150 ms threshold for VoIP applications. Packet loss is between 0.32% and 9.97%, which is less than the 10% allowable packet loss for acceptable VoIP quality. These results show that OLSR is a suitable routing protocol for MANETs running VoIP applications.

Keywords: OLSR, MANET, ad hoc, VoIP, routing protocols, OPNET

Developing an Academic Curriculum in Information Operations: The First Steps

Corey Schou¹, Julie Ryan² and Leigh Armistead³

¹Idaho State University, Pocatello, Idaho, USA

²George Washington University, Washington DC, USA

³Edith Cowan University, Perth, Australia

Abstract: In their 2006 article *Information Operations Education: Lessons Learned from Information Assurance*, Schou, Kuehl, and Armistead outlined the need for an academic response to the development of a better methodology of an Information Operations (IO) Education program. These academics recommended fourteen areas of specific effort. In addition to the recommendation for a scholarship program, there was also a call to establish specific IO academic programs. While a large number of universities have developed more specialized Information Assurance (IA) or computer security programs, the broader aspects of IO are still not seen as worthy of study by the academic community. Among other things, these academics posed two fundamental questions:

1. Why does this dichotomy exist?
2. Why is there such a broad consensus on the need for this kind of education and training by the United States military, when the academic community does not offer equivalent education or classes

An effective response requires not only a curriculum but a shared body of knowledge and a shared language or taxonomy. The proposed technique suggested in that earlier paper used a subset of the eDACUM product that is part of an established set of bodies of knowledge for the computer security and Information Assurance (IA) disciplines. The eDACUM (Electronic Develop A Curriculum) technique and processes uses proprietary software developed at an American university that now houses one of the largest repositories of IA knowledge-base data. These data are now being re-mapped into IO knowledge domains. This is the beginning of establishing a taxonomic classification of the IO discipline is a critical first step in developing a structured curriculum. As expected, preliminary results show that there is a high commonality with the information assurance discipline; however, the categories used to classify the knowledge items have a different basis. Elements of the preliminary study are being mapped currently into candidate course material.

This developmental route was taken because IA and IO are two sides of the same coin. From that original academic proposal, an international project to select key knowledge items that are shared between IO and IA has begun. In this, further efforts to continue this project will be described.

Keywords: Information operations, information assurance, curriculum, knowledge items, internationalization, (isc)

A Statistical Analysis of Large Passwords Lists, Used to Optimize Brute Force Attacks

**Renier Pelsner van Heerden and Johannes Vorster
CSIR, Pretoria, South Africa**

Abstract: The use of passwords has become endemic in everyday life, and passwords have penetrated most aspects of modern life. The purpose of this paper was to investigate the types of information that can be deduced from password lists, where such lists can be obtained and whether the information obtained can be used to aid brute force password attacks. The World Wide Web and other Internet related search methods were used to obtain password lists. We found that Peer to Peer networks have the most information available. From previous studies and the World Wide Web, the ten most popular passwords from different systems were obtained. Not surprisingly, “password”, “123” and “abc” were found to be the most common passwords. We also obtained the default passwords used by hardware manufacturers from the World Wide Web.

The availability of password lists, their basic structure, the most popular passwords and the frequency of character use were investigated. We investigated the possibility of a more efficient method for cracking passwords by using password statistics. Password statistics and patterns were deduced from a password data set: consisting of 46000 MySpace passwords. The 46000 MySpace usernames and passwords were released late in 2007 after the discovery of a security flaw in MySpace.

The rate at which passwords can be decoded (or cracked) was calculated for different character sets. The most common characters and character sequences were used to optimise brute force password cracking. This method was compared to normal brute force techniques. We concluded that this relationship can be used to optimise a brute force password cracking system in very limited situations.

Passwords are used as the first line of defence in information systems. Thus more effective attack and defence strategies can be developed with a better understanding of the overall statistical properties of passwords. Passwords were demonstrated to be a flawed security mechanism.

Keywords: Passwords

Towards a Conceptual Framework for Cyberterrorism

Namosha Veerasamy

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

Abstract: Terrorism has entered a new wave in that the latest battleground to emerge is cyberspace. Cyberterrorism reflects a current concern in the way terrorists will seek to strike the innocent and wreak havoc. Since explosives are no longer the only means to bring a system down, many are uneasy about random cyber attacks that could leave us with difficult conditions due to the disruption of critical services. As a result of our increased dependency on networked communications, the outcomes of such interruptions could be quite disastrous. Cyberterrorism is an aspect of cybercrime that has thus become a growing interest in this the Digital Age. Various hacking and computer intrusion scenarios could possibly play a critical role in cyberterrorism. In the global battle of information and network warfare, cyberterrorism has become a more dominant force. However, much misconception exists over what exactly cyberterrorism entails. Media has sensationalised the possibility of cyberterrorism attacks causing great havoc. Images of eccentric activists taking down critical infrastructures like power stations or railway lines bombard us. Many live in fear of the possibility of vital resources being taken down.

The role of security violations and hacking techniques also need to be better investigated to better understand the reality of such threats. Various theories surround cyberterrorism. However, there is a need for a more structured approach to understanding the various components of cyberterrorism.

A conceptual framework outlining the core aspects of cyberterrorism is therefore proposed. This paper focuses on clarifying the field of cyberterrorism through a conceptual framework that addresses the techniques, objectives, target, types, effects, characteristics and capabilities required. The framework strives to provide a more descriptive synopsis of the field of cyberterrorism. It therefore aims to form a good baseline to contextually place the area of cyberterrorism against the backdrop of other computer and network related crime.

Keywords: Cyberterrorism, cybercrime, warfare, hacking, framework

Considerations for Management from the Onset of Information Terrorism

Ken Webb

Edith Cowan University, Perth, Western Australia

Abstract: This Paper is an extension to one presented by the author at a previous ICIW conference and forms the basis of a chapter in the soon to be published book titled "Cyber-Security and Global Information Assurance: Threat Analysis and Response Solutions".

It results from qualitatively researching a government information dilemma that a heightened risk for management has emerged from a national security environment that is now increasingly spawning asymmetric forms of Warfare. In particular, it is evident that there has been a major lift in security across the world over the past 5-10 years and increasing identification of terrorists now able to conduct Information Warfare. Also concerning is that there continues to be many interpretations of what constitutes this threat.

The research meant collecting data using relatively structured interviews of those people around the world who hold key national security decision-making positions in government plus others from across the spectrum of society with the necessary knowledge in the research area. Constant literature review and relevant major conference attendance and workshops with delegates applied throughout the study to provide triangulation and rigour for this.

The research participants feel that the results of the research have immediate application to national security management. Particularly, in terms of informing key parties about Information Warfare conducted by terrorist groups, which is a phenomenon that causes thinking of alternative scenarios and future options to manage national security from asymmetric threats. This paper outlines the macro considerations for philosophising about these so new ideas to manage information generally can evolve.

Thus, in addition to extensively reviewing literature mainly on Information Warfare and Terrorism to define the threat of Information Terrorism, the security considerations for management and information warfare practitioners in general that have resultantly evolved are broadly outlined. This happens because it is argued that managers need to think about theory emerging from this increasing threat, as it forms the basis for future thinking.

Keywords: Information terrorism, information warfare, management theory, national security, culture, group dynamics