

**Proceedings  
of the  
9th European Conference  
on Information Warfare and  
Security**

**Hosted by [strategyinternational.org](http://strategyinternational.org)  
and the Department of Applied  
Informatics**

**University of Macedonia  
Thessaloniki  
Greece  
1-2 July 2010**

Edited by  
Josef Demergis  
University of Macedonia  
Thessaloniki  
Greece

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 can be purchased from <http://academic-conferences.org/2-proceedings.htm>

ISBN: 978-1-906638-67-2 (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	v
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		xi	vii
Biographies of contributing authors		xiv	ix
How the Pride Attacks	<i>Sabah Al-Fedaghi Kuwait University, Kuwait</i>	1	1
Towards Symmetrization of Asymmetric air Dominance: The Potential key Role Playing by Home-Made low Cost Unmanned Aerial Systems	<i>Laurent Beaudoin and Antoine Gademer ESIEA, Paris, France</i>	2	11
Electronic Digital Passport as a Means of Partial Response to the Lack of Intelligence in the Field of Border Control	<i>Alexander Bligh Ariel University Center, Ariel, Israel</i>	3	19
Zero-Sum Games of Deception	<i>Sviatoslav Braynov University of Illinois at Springfield, USA</i>	4	28
Developing Strategic Perspectives for Enterprise Risk Management Towards Information Assurance	<i>Aristeidis Chatzipoulidis<sup>1</sup>, Ioannis Mavridis<sup>1</sup> and Theodoros Kargidis<sup>2</sup> <sup>1</sup>University of Macedonia, Thessaloniki, Greece <sup>2</sup>Alexander Technological Educational Institute, Thessaloniki, Greece</i>	4	35

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Sniffing With the Portuguese Identify Card for fun and Profit	<i>Paul Crocker<sup>1,2</sup>, Vasco Nicolau<sup>1</sup> and Simão Melo de Sousa<sup>1</sup></i> <i><sup>1</sup>University of Beira Interior Covilhã, Portugal</i> <i><sup>2</sup>Institute of Telecommunications, Covilhã, Portugal</i>	5	43
Information Warfare in Greece and Rome: Cryptography and Steganography	<i>Evan Dembskey</i> <i>Tshwane University of Technology, South Africa</i>	6	56
Anti-Forensic Techniques Based on Malicious Cryptography	<i>Eric Filiol</i> <i>ESIEA - Operational virology and cryptology laboratory, Laval, France</i>	7	63
Exploiting the Hutu/Tutsi Divide: The Relationship Between Extremist Propaganda and Genocide in Rwanda	<i>Sarah Gendron</i> <i>Marquette University, Milwaukee, USA</i>	7	73
Smart Card, the Invisible Bullet	<i>Vincent Guyot</i> <i>ESIEA, Paris, France</i>	8	80
Cyber Antagonism Between Hacker Groups Develops new Challenges	<i>Roland Heickerö</i> <i>Swedish Defence Research Agency (FOI), Stockholm, Sweden</i>	9	8/8
The Malicious Insider Problem: An Integrated View on Individual, Organizational and Contextual Influencing Factors	<i>Ulrike Hugl</i> <i>University of Innsbruck, Austria</i>	10	93
The Way of Warfare in Three Possible Worlds – From art of war to Information Warfare	<i>Aki-Mauri Huhtinen</i> <i>National Defence University, Helsinki, Finland</i>	10	102

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Changing Security Speech and Environment: From Nation States to Corporation Security	<i>Aki-Mauri Huhtinen<sup>1</sup> and Kari Laitinen<sup>2</sup></i> <i><sup>1</sup>National Defence University, Helsinki, Finland</i> <i><sup>2</sup>Police College of Finland, Tampere, Finland</i>	11	109
Influence Operations and Behavioural Change	<i>William Hutchinson<sup>1, 2</sup> and Matthew Warren<sup>2</sup></i> <i><sup>1</sup>SECAU, Edith Cowan University, Western Australia</i> <i><sup>2</sup>Deakin University, Victoria, Australia</i>	12	116
Identities, Anonymity and Information Warfare	<i>Stuart Jacobs, Lou Chitkushev and Tanya Zlateva</i> <i>Boston University, MA, USA</i>	13	120
How to Grasp Emerging Futures of Information Wars?	<i>Auli Keskinen</i> <i>National Defence University, Helsinki, Finland</i>	14	128
Future Requirements for Deception in Naval Defence	<i>Theodoros Kostis<sup>1</sup>, Athanasios Goudosis<sup>1</sup>, Konstantinos Galanis<sup>2</sup> and Ioannis Koukos<sup>3</sup></i> <i><sup>1</sup>University of the Aegean, Karlovassi, Greece</i> <i><sup>2</sup>Ethnodata S.A., Greece</i> <i><sup>3</sup>Hellenic Naval Academy, Greece</i>	15	137
Detecting XML Data Irregularities by Means of Lexical Analysis and Parsing	<i>Dirk Kotze and Martin Olivier</i> <i>University of Pretoria, South Africa</i>	16	151

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Operations Management of Information Security at Enterprise Levels	<i>Pertti Kuokkanen Defence Command Finland, Finland</i>	17	160
The Finnish air Surveillance Radar System Evolution – From war Time Experience to Network Enabled Warfare System	<i>Martti Lehto<sup>1</sup> and Juha-Antti Lamberg<sup>2</sup> <sup>1</sup>National Defense University, Helsinki, Finland <sup>2</sup>Aalto University School of Science and Technology, Finland</i>	18	168
War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory	<i>Andrew Liaropoulos University of Piraeus, Greece</i>	18	177
“She Wolves and Russian Brides” – Women Enemies in war Propaganda”	<i>Tiina Lintunen University of Turku, Finland</i>	19	183
Towards a Framework for the Generation of Enhanced Attack and Background Network Traffic for Evaluation of Network-Based Intrusion Detection Systems	<i>Owen Lo, Jamie Graves and William Buchanan Edinburgh Napier University, UK</i>	20	190
Towards a Risk Management Based Approach for Protecting Internet Conversations	<i>Dimitrios Michalopoulos<sup>1</sup>, Ioannis Mavridis<sup>1</sup> and Vasileios Vitsas<sup>2</sup> <sup>1</sup>University of Macedonia, Thessaloniki, Greece <sup>2</sup>Alexander Technological Educational Institute of Thessaloniki, Greece</i>	21	201

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Analysis of Malicious Affiliate Network Activity as a Test Case for an Investigatory Framework	<i>Mathew Miehling<sup>1</sup>, William Buchanan<sup>1</sup>, John Old<sup>1</sup>, Alan Batey<sup>2</sup> and Arshad Rahman<sup>3</sup></i> <i><sup>1</sup>Napier University, Edinburgh, UK</i> <i><sup>2</sup>Detective Sergeant, Computer Crime Unit, Northumbria Police, UK</i> <i><sup>3</sup>Financial Services Authority, London, UK</i>	22	209
Block Based Steganography	<i>Hamdy Morsy<sup>1</sup>, Joshua Gluckman<sup>2</sup>, Ahmed Hussein<sup>1</sup> and Fathy Amer<sup>1</sup></i> <i><sup>1</sup>Helwan University, Cairo, Egypt</i> <i><sup>2</sup>American University in Cairo, Egypt</i>	22	218
Hacking for fun and Education: eLearning on Network Security	<i>Alexander Ott and Richard Sethmann</i> <i>University of Applied Sciences, Bremen, Germany</i>	23	229
Proactive Defense Tactics Against On-Line Cyber Militia	<i>Rain Ottis</i> <i>Cooperative Cyber Defence Centre of Excellence</i>	24	233
The Necessity of Implementing a Long-term Security Strategy in Public Administration Organizations from Romania	<i>Marius Petrescu, Ionut Barbu, Gabriela Popa, Valentina-Ofelia Robescu</i> <i>Valahia University from Targoviste, Romania</i>	25	238
An Applied Framework for Modelling a Critical Infrastructure System Incident	<i>Graeme Pye and Matthew Warren</i> <i>Deakin University, Geelong, Australia</i>	26	245

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Towards Reversible Cyberattacks	<i>Neil Rowe U.S. Naval Postgraduate School, Monterey, California, USA</i>	26	261
Reconfigurable Radio Systems: Towards Secure Collaboration for Peace Support and Public Safety	<i>Johan Sigholm Swedish National Defence College, Stockholm, Sweden</i>	27	268
An Alerting System for Interdependent Critical Infrastructures	<i>Paulo Simões<sup>1</sup>, Paolo Capodiecì<sup>2</sup>, Michele Minicino<sup>3</sup>, E. Ciancamerla<sup>3</sup>, S. Panzieri<sup>4</sup>, M. Castrucci<sup>5</sup> and Leonid Lev<sup>6</sup> <sup>1</sup>CISUC - DEI, University of Coimbra, Portugal <sup>2</sup>Selex Communications S.p.A., Italy <sup>3</sup>ENEA, Italy <sup>4</sup>Università di Roma Tre, Italy <sup>5</sup>University of Rome – La Sapienza, Italy <sup>6</sup>Israel Electric Corp., Israel</i>	28	275
Hard Disk Storage: Data Leakage	<i>Iain Sutherland and Gareth Davies University of Glamorgan, UK</i>	29	284
Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons	<i>Eneken Tikk and Kadri Kaska Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia</i>	29	288

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Information Security Education in the Greek Universities and Technological Education Institutes	<i>Theodosios Tsiakis Technological Educational Institute of Kozani, Greece</i>	30	295
RIDICULING THE DEMON: The Comical Image of Lazy, Stupid, Ineffective, Helpless, Uncultured Russians During the Winter War 1939–1940 in Finland	<i>Vesa Vares University of Turku, Finland</i>	31	302
Motivation and Requirements for Determining a Network Warfare Capability	<i>Namosha Veerasamy and Jan Eloff University of Pretoria, South Africa</i>	32	310
<i>Mein Kampf</i> Revisited: Enemy Images as Inversions of the Self	<i>Marja Vuorinen University of Helsinki, Finland</i>	33	320
Development of a Supply Chain Management Security Risk Management Method: A Conceptual Model	<i>Matthew Warren and Shona Leitch Deakin University, Melbourne, Victoria, Australia</i>	34	327
Behavioural Profiling for Impostor Detection in Mobile Networks	<i>Ibrahim Zincir, Steven Furnell and Andy Phippen University of Plymouth, UK</i>	34	334
<b>Research in Progress papers</b>			
Legal Issues and Challenges Involved in Cyber World Business	<i>Shubhangi Sunil Bhatambrekar Modern College, Ganeshkhind, Pune, India</i>	39	<b>345</b>

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Knowledge Management and Knowledge Security – a Conceptual Comparison	<i>Ilona Ilvonen Tampere University of Technology, Finland</i>	39	352
A Conceptual Model Approach to Manage and Audit Information Systems Security	<i>Teresa Pereira<sup>1</sup> and Henrique Santos<sup>2</sup> <sup>1</sup>Polytechnic Institute of Viana do Castelo, Valença, Portugal <sup>2</sup>University of Minho, Guimarães, Portugal</i>	40	360
IST: Improved Steganography for Html	<i>Khan Farhan Rafat and Muhammad Sher International Islamic University, Islamabad, Pakistan</i>	41	<b>366</b>
Proactive Cyber Initiative: An Expert System Framework	<i>David Rohret Computer Sciences Corporation, Inc., San Antonio, USA</i>	41	378
Cyber Warfare: Virtual war Among Virtual Societies	<i>Anthimos Alexander Tsirigotis Hellenic Air Force, Athens, Greece</i>	43	389
<i>Novel Information Sharing Syntax for Data Sharing Between Police and Community Partners, Using Role-Based Security</i>	<i>Omair Uthmani<sup>1</sup>, William Buchanan<sup>1</sup>, Alistair Lawson<sup>1</sup>, Christoph Thuemmler<sup>1</sup>, Lu Fan<sup>1</sup>, Russell Scott<sup>2</sup>, Anne Lavery<sup>2</sup> and Chris Mooney<sup>3</sup> <sup>1</sup>Edinburgh Napier University, UK <sup>2</sup>Scottish Police College, Kincardine, UK <sup>3</sup>Glasgow Community &amp; Safety Services, Glasgow, UK</i>	44	394

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
<b>Practitioner Papers</b>			
BinThavro: Towards a Useful and Fast Tool for Goodware and Malware Analysis	<i>Benjamin Caillat, Anthony Desnos and Robert Erra ESIEA, Paris, France</i>	47	405
Forensic and Software (UN) Obfuscation	<i>Anthony Desnos and Eloi Vanderbéken ESIEA, France</i>	49	416

## Preface

This year sees the Ninth European Conference on Information Warfare and Security (ECIW 2010), which is jointly hosted by the Department of Applied Informatics, University of Macedonia, Thessaloniki, Greece and Strategyinternational.org. The Conference Co-Chairs are Ioannis Mavridis from the University of Macedonia and Vasilios Katos from the Democritus University of Thrace. The Co-Programme Chairs are Josef Demergis from the University of Macedonia, Thessaloniki and Marios Efthymiopoulos from Strategy International, Thessaloniki, Greece

The main aim of this Conference continues to be an opportunity for individuals working in the area of Information Warfare and Information Security to come together to share knowledge with peers interested in the same area of study.

The opening keynote is given by Kevin Henry from the Assurance Integrator firm Securis Inc., based in Canada and the second day will be opened by Vasilios Katos from Democritus University of Thrace, Greece. Vasilios will address the topic of *Satellite Transmission Security*.

A key aim of the conference is about sharing ideas and meeting the people who hold them. The range of papers will ensure an interesting two days. 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 86 abstracts, after the double blind, peer review process there are 51 papers published in these Conference Proceedings. These papers come from all parts of the globe including Australia, Austria, Egypt, Estonia, Finland, France, Germany, Greece, India, Kuwait, Pakistan, Portugal, Romania, South Africa, Sweden, United Kingdom and the United States of America.

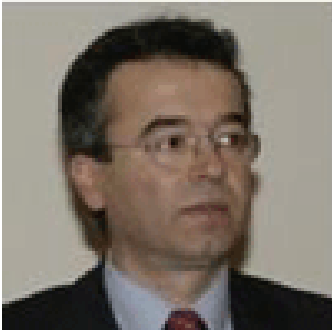
Group work and sharing of ideas are not confined to seminar sessions alone. On the second day participants will have the opportunity of participating in one of two interactive sessions aimed at stimulating leadership capabilities through a role play exercise and experimenting with technology used by some groups at the Pentagon to improve the decision making process.

I wish you a most interesting conference.

Josef Demergis  
July 2010

# Biographies of Conference Chairs, Programme Chairs and Keynote Speakers

## Conference Chairs



**Ioannis Mavridis** is an Assistant Professor of Information Systems Security at University of Macedonia, Department of Applied Informatics, Greece. He holds a Diploma in Computer Engineering and Informatics from the University of Patras and a Doctoral degree in Mobile Computing Security from the Aristotle University of Thessaloniki, Greece. He has been teaching Computer Science and Information Systems Security in the University of Macedonia and the Hellenic

Open University for the last nine years. He is a member of the Greek Computer Society, the Technical Chamber of Greece and the Working Group 11.3 on Database Security of International Federation for Information Processing (IFIP). He has participated in several research projects working in the area of IT security. His research interests include the areas of computer and network security, information assurance and security, cyber security, access control in collaborative, mobile, pervasive and grid systems, semantic web and security ontologies. He has published over 70 scientific articles in refereed international journals and conference proceedings, and co-written a book on information system and network security.

## Conference co-Chair and Keynote speaker

**Vasilios Katos** is Assistant Professor of Information and Communications Systems Security at the Department of Electrical and Computer Engineering of Democritus University of Thrace in Greece. He holds a Diploma in Electrical Engineering from the Democritus University of Thrace, an MBA from Keele University and a PhD from Aston University in the UK. Prior to his current post he was Principal Lecturer at the School of Computing at the



University of Portsmouth where he participated in the development of the interdisciplinary Masters course MSc in Forensic IT. He has worked in the industry as a security consultant, as an expert witness in information systems security and has delivered invited presentations at professional conferences. His research interests are in information security, privacy, digital forensics and incident response

## Programme Chairs



**Josef Demergis** holds a BA(Hons) in International Relations & Strategic Studies from the University of Lancaster. He has obtained a Master degree on War Studies from King's College London as well as an MSc on E-Commerce from the University of Westminster. He also holds an MRes on Environment Society and Politics from King's College London. He is currently a PhD Candidate of the University of Macedonia, with a research topic on the conduct of Electronic Foreign policy of the Hellenic State. Mr Demergis has written a variety of articles on subjects mainly dealing with strategy, defence, foreign policy and the use of information technologies. He is a guest lecturer at various military and police schools. He was also employed as a WTI expert of the Stability Pact for South-Eastern Europe Thessaloniki Office.

**Marios Efthymiopoulos** holds a PhD from the University of Crete while a Scholar of the Alexander S. Onassis Foundation. He is a graduate from the NATO Defence College (NADEFCOL), during his tenure as appointee by the Ministry of Foreign Affairs of Greece. He holds a Masters Degree from the University of Vienna -The Diplomatic Academy of Vienna- in International Relations. He attended the MSc in Russian and Post-Soviet Studies at the London School of Economics and Political Science (LSE), and he also holds a BA (Hons) in International Relations and Politics by the University of Lincolnshire and Humberside. He has published numerous articles in Greece in relations to NATO policies and foreign policies of Greece. He has also several publications in various countries, namely the UK, Australia, Italy. His research is concentrated on issues of strategic studies and international relations. His latest book -in Greek- is titled: *NATO's policies in the 21st century: The need for a renewed Security Concept and the ever lasting NATO-Russia Relations* (Sakkoulas A.E Athens Thessaloniki, December 2008). Presently Marios is a visiting lecturer at the Dept. of Social and Political Sciences, University of Cyprus.



## Keynote Speaker



**Kevin Henry** is recognized as one of the worldwide Leaders in the field of Information Assurance. A Senior Consultant with many years experience Information Security and Audit, Risk Management and Business Continuity, Kevin also has a passion for teaching, being a dynamic and enthusiastic speaker - drawing the audience into the presentation with a

wealth of real-life experience, and practical, relevant information. Kevin is employed by Securix Inc., a well-known Information Assurance Integrator with a strong reputation for on-time delivery for clients nationwide. Kevin is the co-chair of the CBK committee for the CISSP and several other certifications, as well as an author with published articles in over a dozen books and magazines, Kevin has been responsible for educational systems, products and instructors for major clients such as BCI, IEEE, SCIPP International, and (ISC)2. Kevin is based in Ottawa, Canada.

## **Mini Track Chairs**

**Eric Filiol.** He has been an officer in the French Army for 20 years. He is now head scientist officer and professor in a research lab working for different department in France (justice, police, defence, academic). He holds a PhD in mathematics and computer science, a habilitation thesis in computer science, an engineer diploma in cryptology and has graduated from NATO in InfoOps. His research works relates to computer security with the attacker's mind.



**Pertti Kuokkanen** received his D.Soc.Sc degree in communication and computer science from the University of Helsinki, Finland, in 2009. He conducted post-graduate research in computer science with primary interests in modelling of decision support applications. He is currently the program manager at the Defence Command Finland.

**Aki Huhtinen, Professor, Major G.S.,PhD.** 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. Aki works at the Department of Management and Leadership Studies at the Finnish National Defence College.



**Rain Ottis** works as a scientist at the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. He is also a PhD student in Tallinn University of Technology. His research interests include conflicts in cyberspace and volunteer cyber militias.

**Marja Vuorinen** is a social science historian at the University of Helsinki. She is a student of power and elites, specialising in media studies and the history of ideas. Currently she is putting the finishing touches to her doctoral dissertation, dealing with the Finnish nobility as the 'good enemy' of the progressive 19<sup>th</sup> century intelligentsia. She is keen to move on, to apply her semiotic tool kit to other historical enemy images.



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

**Sabah Al-Fedaghi** holds an MS and a PhD in computer science from Northwestern University, Evanston, Illinois, and a BS in computer science from Arizona State University, Tempe, USA. He has published papers in journals and contributed to conferences. He is an associate professor in the Computer Engineering Department, Kuwait University. He previously headed the Electrical and Computer Engineering Department (1991–1994) and the Computer Engineering Department (2000–2007).

**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.

**Shubhangi Sunil Bhatambrekar** is the Head of the Computer Science Department. He holds M.Sc, M. Phil.(Phy), MCA, DCL. With 17 years of experience, he was Chairperson of the Board of Studies in Computer Science and a Member Academic Council at University of Pune (2000-2005). He is a Member Board of Studies Computer Management at University of Pune and a Member of the Board of Studies in Computer Science at Bharati , University. He is a Senior Life Member of the Computer Society of India and a member for India of the IFIP (TC3-Education Group) 2003-06.

**Alexander Bligh PhD** – is Schusterman visiting professor of political science at the University of Notre Dame, Indiana, US, and professor of political science at Ariel University Center, Israel. His is also teaching at Bar Ilan University Department of Political Science. He was formerly deputy advisor (1987-1990) and advisor (1990-1992) to the Prime Minister of Israel on Arab affairs; expert on counter-terrorism. He has published numerous books and articles on these topics as well as the politics of the Middle East. Bligh has rich experience in leading war and simulation games.

**Sviatoslav (Svet) Braynov** is Associate Professor in the Computer Science Department at the University of Illinois at Springfield in the USA. He has

published more than 50 papers in refereed conferences and journals, chaired and co-chaired several conferences and workshops, and delivered multiple invited presentations and tutorials. His research interests include computer security, game theory, electronic commerce, and artificial intelligence.

**Aristeidis Chatzipoulidis** received his main degree from Alexander Technological Educational Institute in Marketing and his master degree from Strathclyde Business School in International Marketing. Currently, he is a PhD student at the University of Macedonia and his main research focus on governance, risk, compliance and management disciplines.

**Lou Chitkushev** is the chairman of Computer Science Department at Boston University's Metropolitan College, director of Information Security and Biometrics Laboratories and the head of the Graduate program in Telecommunications. He is co-founder and Associate Director of Boston University Center for Reliable Information Systems and Cyber Security (RISCS) which was established to promote and coordinate research on reliable and secure computation and information assurance education by developing ideas and tools to protect critical computational infrastructure. He holds a Ph.D. in Biomedical Engineering from Boston University, M.S. in Biomedical Engineering from Medical College of Virginia, and an M.S. and B.S in Electronics and Telecommunications from the University of Belgrade. He has extensive international industrial and academic consulting experience in areas of telecommunications, data assurance, and biomedical informatics.

**Paul Crocker** has a degree in Mathematics and PhD in Applied Mathematics from the University of Leeds, UK. After working in software development and support in 1996 he joined the Mathematics and Computer Science Department at the University of Beira Interior, Portugal. His research and teaching interest include parallel and concurrent Computing, Security and Operating systems. He is a member of the Instituto de Telecomunicações research organization.

**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.

**Anthony Desnos** is currently a research engineer at ESIEA (SI&S team) in Paris, France. His research focuses on computer virology/security, and more particularly about new generations of virus and anti-virus. He is involved in a number of open source security projects, including Libthor, Sanson The Headman, Draugr and ERESI.

**Sarah Gendron** is an Assistant Professor of French Literature at Marquette University (USA). She has authored multiple articles and one book on literary theory, *Repetition, Difference, and Knowledge*. She has also published several translations, including Simone de Beauvoir's "Notes for a Novel." Gendron's current research and publications focus on visual and textual representations related to genocide.

**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.

**Vincent Guyot** works in Paris, France, as Associate Professor at SIS lab (ESIEA Group) and Research Associate Professor at LIP6 lab (UPMC-Paris Universit s). He also collaborates with engineering schools of ParisTech (Paris Institute of Technology). He holds a PhD in networking and smart cards security, and an engineer diploma in computer science. He lectures on smart card technology at different universities, organizes IEEE international research conferences, has edited special issues of journals and co-authored several books on this topic. His research interests include the areas of networking mobility and security, smart cards and RFID.

**Roland Heicker ** is a deputy research director at the Swedish Defence Research Agency, FOI where he manages projects in the area of information assurance and cyber warfare. He has worked as a program manager and senior product manager at Ericsson and Telia Mobile. He has a PhD in Industrial Economy and Organization/Work Science from Royal Institute of Technology.

**Ulrike Hugl** Studies economics and social sciences at the University of Innsbruck, Austria (further studies in pedagogic and law). She has worked for a number of years in the fields of personnel development, organization, and marketing. University affiliations include project coordinator of an entire university reform project at the University of Innsbruck; researcher and lecturer at the University of St. Gallen in the Institute for Information Management. She is currently in the Innsbruck School of Management where her Research/project experiences include privacy/information security; technology implementation processes; e-/m-learning.

**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

**Ilona Ilvonen** earned her M.Sc. degree in 2006 at Tampere University of Technology in Finland. In her master thesis she studied information security management in SME's. She has continued the research on information security and knowledge protection in small organizations, and has published several conference papers on the topic. Her doctoral dissertation will explore the concept of knowledge security and she will finish her doctoral studies in 2012.

**Kadri Kaska** holds a Master of Arts degree in law from the University of Tartu, Estonia. After eight years in the national communications agency, dealing with regulatory issues such as resource and infrastructure management, advising in the market regulation process, and being involved in the drafting of communications legislation, she joined the Cooperative Cyber Defence Centre of Excellence in 2008 and currently works there as a legal analyst. Her research interests include legal and economic aspects of cyber security, legal factors involved in cyber incident trend evolvement, and cyber crime.

**Auli Keskinen** is Adjunct Professor in Political Science at the University of Tampere and Adjunct Professor in Futures Research at Finnish National Defence University as well as at Finland Futures Research Centre at University of Turku. Recently she has acted as innovation manager at the EU FP7 ROADIDEA Project for Foreca Consulting Ltd.

**Theodoros Kostis** CEng MIEE is a researcher at the University of the Aegean, Greece. He specializes in the information warfare aspects of high range resolution radar systems. His current areas of interest include aerial, surface and underwater defence at sea, simulator systems and elements of deceptive stratagems.

**Dirk Kotze** is a part-time student from Pretoria, South Africa. He is currently conducting research for an MSc in Computer Science, specialising in Digital Forensics. Currently he is employed as a software developer at Nanoteq, an engineering firm specialising in cryptographic hardware. Previously he worked as an IT Auditor at PricewaterhouseCoopers.

**Pertti Kuokkanen** received his D.Soc.Sc degree in communication and computer science from the University of Helsinki, Finland, in 2009. He conducted post-graduate research in computer science with primary interests in modelling of decision support applications. He is currently the program manager at the Defence Command Finland.

**Martti Lehto** has over 30 years of experience mainly as developer and leader of C4ISR Systems in Finnish Defence Force and Air Force. He is a PhD student in the National Defence University and researcher in University of

Jyväskylä, Faculty of Information Technology. He has about 20 publications and research reports on areas of C4ISR systems, information warfare, security and defence policy, leadership and management. Since 2001 he has been also the Editor-in-Chief of the Military Magazine which is the leading military publication in Finland.

**Andrew Liaropoulos** is a Lecturer in University of Piraeus, Department of International and European Studies. His research interests include international security, intelligence reform, strategy, military transformation, crisis management and foreign policy analysis. Dr. Liaropoulos is also a Senior Analyst in the Research Institute for European and American Studies (RIEAS).

**Tiina Lintunen** completed her MA in 1998. Since then she has worked as an independent researcher in different historical projects in the private and public sectors. At present, she works as a postgraduate researcher in the Department of Contemporary History at the University of Turku, Finland. She defended her licentiate thesis (i.e. a degree between MA and PhD) successfully in April 2006. After that she was appointed into a five-year position as a researcher at her home department. In addition to completing her PhD, her work consists of teaching duties on the BA and MA level. The topic of her doctoral thesis is Women in the Finnish Civil War.

**Owen Lo** recently graduated from Edinburgh Napier University with a BEng (Hons) degree. He studied Computer Networks and Distributed Systems. His main area of research has been in the subject of network security, especially in the evaluation of network-based intrusion detection systems. Furthermore, he has a general interest in all aspects of computer technology including both hardware and software computing.

**Mathew Miehling** originally from New Jersey in the USA, completed his undergraduate BSc in Computer Science at Ursinus College in Pennsylvania. From there, he pursued an MSc in Advanced Networking at Edinburgh Napier University. After the completion of his Master's, Mathew stayed at Edinburgh Napier and is currently working toward his PhD under the supervision of Professor Bill Buchanan.

**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.

**Alexander Ott** is a student of the University of Applied Sciences, Bremen Specializing in network security, virtualization and Linux. He is currently working on diploma thesis.

**Teresa Pereira** is currently an assistant lecturer at the Superior School of Business Studies of Polytechnic Institute of Viana do Castelo in Portugal. She is also a Ph.D student at the Department of Information Systems of University of Minho. She graduated in Mathematics and Computer Science (5 years programme) at University of Minho in 2002 and obtained the MSc degree in Information Technologies (pre-Bologna) in 2006. From 2002 to 2004 she worked as a researcher in the OmniPaper project (IST-2001-32174) funded under 5th FWP (Fifth Framework Programme). Teresa's research interests include Semantic Web, Information management, ontologies, security audit, management information systems and information systems security.

**Marius Petrescu**, Secretary of State - National Register Office for State Secret Information . Prof. Ph.D. – teaches Macro and Microeconomy at Valahia University from Targoviste, Ph.D. students tutor, member of CEDIMES (2006), correspondent member of Central European Academy of Science and Arts (2000), Doctor honoris causa of Balkanic Academy of Sciences and Culture – Sofia/Bulgaria (2003), author of more than 50 books, scientific materials and textbooks for the use of students. Author of more than scientific papers presented at international conferences in the field of Management, Marketing and Information Security.

**Khan Farhan Rafat** has completed his PhD course work under supervision of Professor Dr. M Sher, Head of Department, Computer Science, International Islamic University, Islamabad, Pakistan, and is carrying out research. He has twenty years experience in the field of Information Security ranging from computer programming to designing and implementation of security policies.

**Neil Rowe** is Professor of Computer Science at the U.S. Naval Postgraduate School where he has been since 1983. He has a Ph.D. in Computer Science from Stanford University (1983), and E.E., S.M., and S.B. degrees from the Massachusetts Institute of Technology. His main research interest is the modeling of deception, and he also does research on information security, surveillance systems, image processing, and data mining.

**Johan Sigholm** is a Ph.D. student in Military Technology at the Swedish National Defence College in Stockholm, Sweden, and the National Defence University in Helsinki, Finland. He holds the rank of Captain in the Swedish Air Force and received his M.Sc. degree in Computer Science and Engineering from Linköping University, Sweden. His main research interest is studying how emerging Information and Communication Technology can be used to support and facilitate military missions.

**Paulo Simões** is a Professor at the Department of Informatics Engineering of the University of Coimbra and a senior researcher at the Laboratory of Communications and Telematics. His main research interests are Security,

Network Management and Critical Infrastructures. He has around 40 journal and conference publications in these areas. He has been involved in several European research projects, both with technical and management activities. He also participated in several industry-funded research projects in these areas.

**Theodosios Tsiakis** received a B.S. degree in Economics from Dept of International and European Economic and Political Studies and Ph.D. in Information Security Economics from Dept of Applied Informatics in University of Macedonia (Greece) respectively. His areas of interest include Information Systems, Information Security Economics, Risk Management and Human Factors in Security.

**Anthimos-Alexadros Tsirigotis** graduated from the Air Force Academy as Air Defence Controller in 2000. In 2007 he attended an one-week seminar in Paris about "International Negotiations" (Ecole Nationale d'Administration). In 2008 he received his Master in International Relationships and European Studies from the University of Piraeus. In 2009 he was stationed at Elefsis Military Base at the Hellenic Airborne Early Warning and Control System.

**Omair Uthmani** is a researcher with the Centre for Distributed Computing, Networking and Security at the Edinburgh Napier University. His areas of interest include information security, governance and compliance and data sharing in policing and community partnerships at local and central government levels.

**Vesa Vares** is currently working as Senior Lecturer at the University of Turku, Department of Political History and Political Science. He has also worked as an acting Professor at the Universities of Turku and Tampere and as a visiting scholar at the Humboldt-Universität zu Berlin. He has specialized in studies of political ideas and rhetoric, especially on conservatism, liberalism and right-wing extremism and is now studying German influence in Finland before 1944.

**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. She is employed as a researcher in the field of Network Warfare at the Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa.

**Matt Warren** is the Head of School at the School of Information Systems, Deakin University, Australia. He has gained international recognition for his scholarly work in the areas of Information Security, Risk Analysis, Electronic

Commerce and Information Warfare. He has authored/co-authored over 180 books, book chapters, journal and conference papers.

**Ibrahim Zincir** is a lecturer in the Department of Computer Engineering at Yasar University in Izmir/Turkey while studying his PhD at University of Plymouth in the UK under the supervision of Professor Steven Furnell and Doctor Andy Phippen.



## How the Pride Attacks

Sabah Al-Fedaghi, Kuwait University, Kuwait

**Abstract:** The aim of this paper is to develop a general conceptual model for attack progression that can be applied to modeling of computer and communication threat risks. An attack is a group of activities including actions carried out by an adversary, the attacker, on a potential victim. The paper focuses on attacks that aim at overpowering the victim/prey to gain some benefit. This type of attack seems the most common in the field of computers. A brief review is given of various forms of modeling of information-security attacks with emphasis on use cases, and diagrams of misuse cases. Three kinds of attacks are examined from very diverse domains: (1) those in the animal world, where lion prides exhibit one of the most powerful tactics for overcoming prey, (2) those in the United States Air Force, where pilots use an *Attack Cycle* that includes *detect, locate, identify, decide, execute, target, and assess*, and (3) those in computer systems, where an attack has recently been described as comprising six phases: *Reconnaissance, Weaponization, Delivery, Compromise/Exploit, Command-and-control, and Exfiltration*. The paper examines existing models of the last two and introduces a new flow model to facilitate development of a general conceptual model of attacks. The flow model is defined in terms of a transition graph comprising five states. The flow model is a uniform method for representing things that “flow,” i.e., things that are received, processed, created, released, and/or transferred. Examples of “things that flow” (flowthings) include information, materials (e.g., in manufacturing), and money. A basic principle of the model is separation of various flowthings and identification of their flows. Accordingly, the conceptual picture of a pride’s attack includes streams of flows of signals (from the environment), information, plans, decisions, and actions. These flows can trigger each other. The conceptual description includes the spheres of the attacker and those of the defender. Matters located in the defender’s sphere are necessary for completely specifying the progression of the attack. We claim that such a methodology of attack modeling provides a more effective analysis in the fields of threat modeling and secure software development.

**Keywords:** conceptual model, attacks, information flow, security, threat risk

# **Towards Symmetrization of Asymmetric air Dominance: The Potential key Role Playing by Home-Made low Cost Unmanned Aerial Systems**

**Laurent Beaudoin and Antoine Gademer, ESIEA, Paris, France**

**Abstract:** Unmanned Aerial Systems could play a crucial role in tactical intelligence. Until recently, as the cost of developing UAS was high, only military UAS were flying. But recent improvements in NTIC and model aircraft technologies allow the development of very low cost Unmanned Aerial Systems with very interesting operational performance characteristics. And this is a new equation to solve: new performance + low cost = potentially new threats. In this article, we start by briefly presenting the UAS world: history, classification, present main performances and missions. Then we focus on the mini/micro (i.e. tactical) UAS and describe briefly some of the more promising ones. To demonstrate that developing efficient low cost mini-UAS with operational possibilities is possible, we developed a Vertical Take Off and Landing one and tested it in an international contest organized by the French DGA/ONERA agencies and achieved very high resolution (centimetric) cartographic missions. We have faced practical and technical issues to be able to perform these missions. Thus, we will describe the tools we developed to improve its ability for operational mapping like, for instance, how to pilot a flight in immersion with a customizable HUD taking video broadcasts from the UAV and adding vector information in real-time on virtual reality glasses; how to combine satellite and vector data with a path optimization algorithm to design relevant flight plans and update them in real time to ensure data completeness, how to generate relevant geolocalization meta-data to be able to navigate in the database of produced images a few minutes after the landing and, finally, how to employ home-made open-source mosaicer to take advantage of the three simultaneous on-board digital cameras. To perform a low cost UAS, we have hacked an off-the-shelf digital camera to allow an efficient on-board geo-localization in real time. As a conclusion, we talk about some potential threats possibly arising from our experience and how these threats could be a first step towards balancing asymmetric air dominance.

**Keywords:** Unmanned aerial system, quadrirotor, air dominance

# **Electronic Digital Passport as a Means of Partial Response to the Lack of Intelligence in the Field of Border Control**

**Alexander Bligh, Ariel University Center, Ariel, Israel**

**Abstract:** International travel has been involved in a significant way in the preparation and execution of terrorist activities. The challenge facing international actors fighting terror and Organized Crime (OC) is twofold: how to better inspect the movement of persons and still impose as little inconvenience on the travelers as possible. This paper deals with the formal and intelligence dimensions: travel documents and their makeup, the border crossing travel documents inspection and the sharing of information among concerned parties. The following discussion deals with some of the more acute areas in this field and offers a model designed to further narrow down the net and yet admitting that it will only add to the necessary security but will not produce the ultimate solution. After observing some of the current pitfalls of the system the paper presents the concept of a credit card size electronic digital passport. The idea is not new, however since it is not yet in use this is the time to characterize the product. Therefore, perhaps the initial element, the one which involves decision on cabinet level should be that all citizens must carry one official identification document. That move will obviously contribute to enhanced security. The only difference between an ID/ED passport and a credit card is not in its appearance, but in its contents. It hides a radio frequency identification, or RFID, chip and many counter forfeiting elements. It is unique in that it is a driver's license, national ID and a national passport at the same time. It does not only say that on the cover and back of the card but it includes on its chip all the necessary data. This card, given the authority in charge, can be read and enact different types of mechanism: the police officer's cruising car terminal, a voting machine, a passport control terminal etc. Obviously, the encryption procedure and the access protocols are distinctive for each level. However, access to changing the contents should be encrypted in a way that several authorities may have access to their own information but never to any other information entered by other bodies. This approach will undoubtedly make forging travel documents expensive and time consuming beyond the usual means of most terror and OC organizations. Moreover, on top of safeguarding the re-writing process the data should be protected by security features embedded in the software and unknown to the officer feeding the machine with the necessary details. Many current national travel documents depend on two elements: a bulky paper document and an RFID chip. The desired end result proposed here will be a new concept of a travel document: a small multipurpose card. The technology alluded to in this paper does exist. Moreover, it is partially in use

in the present. It is a matter of further developing the abilities of the embryonic software and integrating many elements into one system.

**Keywords:** passport, border control, intelligence, Interpol, Schengen, WHTI, terror, organized crime

## **Zero-Sum Games of Deception**

**Sviatoslav Braynov, University of Illinois at Springfield, USA**

**Abstract:** The paper proposes a simple 2x2 zero-sum deception game in which one of the players (Deceiver) can partially manipulate and misrepresent the game to the other player (Target). The abilities of Deceiver to misrepresent the game are limited in the sense that he can misrepresent only one out of the four outcomes of a game. Target expects deception and applies countermeasures to reduce its adverse consequences. Despite the limited abilities of Deceiver and the active response of Target, we show that every 2x2 zero-sum game is vulnerable to deception. More specifically, we found a universal deception strategy which works for all 2x2 zero-sum games. We also show that the deception strategy is in equilibrium with Target's response. Moreover, the value of the deception game is greater than the value of the corresponding game without deception. In other words, deception always pays itself off even when Target expects it and acts accordingly. Therefore, it should be carried out whenever possible.

**Keywords:** deception, zero-sum games, denial, counterdeception

## **Developing Strategic Perspectives for Enterprise Risk Management Towards Information Assurance**

**Aristeidis Chatzipoulidis<sup>1</sup>, Ioannis Mavridis<sup>1</sup> and Theodoros Kargidis<sup>2</sup>**

**<sup>1</sup>University of Macedonia, Thessaloniki, Greece**

**<sup>2</sup>Alexander Technological Educational Institute, Thessaloniki, Greece**

**Abstract:** Information is an important key business asset, which can exist in many forms, it involves various risks and it is essential that it is suitably protected. Therefore, it requires the involvement of proper management ensuring that information assets are sufficiently secured and controlled. Truth is that the risk management discipline has received increasing attention in recent years due to increased regulations, ongoing changes and greater economic volatility that all affect the business environment. The purpose of a proper risk management action is to ensure transparency at all levels of the organization by taking the appropriate measures to reduce costs and manage financial, organizational and personal risk all at once, satisfying business

objectives. However, due to misleading fallacies around its concept and the complexity that derive from governance, risk and compliance (GRC) activities, risk management falls short of assuring information assets. In this paper the results of our work on studying government, compliance and human factors in information security risk management are presented. The scope is to develop strategic perspectives around risk management implementation related to the concept of information security, helping minimize risks and cost. Sustaining security value over long term necessitates the realization of the information security lifecycle and the recognition of an imperative factor, the human involvement. Security spending remains a main concern despite the current economic crisis showing challenges that need to be confronted. Such challenges include maintaining a strong IT workforce, addressing growing foreign and domestic competition, developing critical infrastructure protection, balancing automated and manual controls and controlling intellectual property rights. The road ahead is the recognition of an enterprise risk management (ERM) strategy able to maintain security assurance and challenge ongoing changes that impact on the effectiveness of risk management. In addition, it is high time to consider a wider risk management approach, that of the societal risk management. For optimized results, the organization should foster a culture based on communication and feedback, recognizing training and security awareness a top priority. Creating a holistic picture of an enterprise as part of risk management and compliance efforts, it will provide a comprehensive platform for capturing and integrating multiple perspectives on processes, thus controlling information flow. Information assurance depends on the level of collaboration across internal and external parties and the correlation of disperse information. To avoid unpleasant circumstances, the risk management principle should engage into a dual approach of operability, that is maintaining performance and periodically re-evaluate itself to tackle with upcoming trends and risks.

**Keywords:** information security, risk management, compliance, human factor, strategy

## **Sniffing With the Portuguese Identify Card for fun and Profit**

**Paul Crocker<sup>1,2</sup>, Vasco Nicolau<sup>1</sup> and Simão Melo de Sousa<sup>1</sup>**

**<sup>1</sup>University of Beira Interior Covilhã, Portugal**

**<sup>2</sup>Institute of Telecommunications, Covilhã, Portugal**

**Abstract:** In this paper we describe a case study of the re-engineering process used to discover the low-level application protocol data units (APDUs) and their associated significance when used in communications with the Portuguese e-id smart card. This was primarily done simply to learn the

processes involved given the low level of documentation available from the Portuguese government concerning the inner workings of the Citizens Card. However it was also done in order to produce a generic platform for accessing and auditing the Portuguese Citizen Card and for using Match-on-Card biometrics for use in different scenarios. Given that no documentation is available concerning the use of the Match on Card capabilities of the e-id card this is a challenging procedure.

**Keywords:** smart card, e-id, reengineering, sniffing, authentication, biometrics

## **Information Warfare in Greece and Rome: Cryptography and Steganography**

**Evan Dembskey, Tshwane University of Technology, South Africa**

**Abstract:** The ancient Greeks and Romans were fully aware of the necessity of obtaining, protecting and communicating military intelligence. The timely delivery of information often turned the tide of battle to advantage, and the lack of it to disadvantage and even disaster. The ancient Greek and Roman literature is replete with examples of intelligence gathering, analysis and communication. Intelligence failures are not ignored, but recorded and discussed. In this paper we examine the ancient primary sources to understand what role cryptography and steganography played in Ancient Greece and Rome. A brief discussion of ancient Greek and Roman intelligence techniques and some modern examples (drawn from secondary literature) of intelligence failures are included in the discussion. This serves to demonstrate that the ancient Greeks and Romans were sophisticated in their use of technology, and faced many of the same problems we face today. The question in this ongoing research project is then asked, is it possible to draw lessons that are applicable to modern intelligence and information warfare activities? It is concluded that of the incidents and technologies analysed, the failures are the result of non-technological factors, and that we can profit from a more detailed study of ancient primary sources.

**Keywords:** Ancient Greece, Rome, cryptography, steganography, information warfare, intelligence

# **Anti-Forensic Techniques Based on Malicious Cryptography**

**Eric Filiol**

**ESIEA - Operational virology and cryptology laboratory, Laval, France**

**Abstract:** In the field of forensic analysis, encrypted data are particularly interesting when found on a hard disk. They are clear proof that a person has intended to protect data against analysis. When the analyst succeeds in one way or another to decrypt those encrypted data, the underlying plaintext clearly becomes very strong evidence for the judge. This means that in the process of digital proof, cryptography has a status of extremely high confidence. In this article we show how an attacker can use cryptography in order to manipulate both the forensic analyst and the judge and thus fool them to incriminate an innocent people wrongly. Our approach mainly lies in malicious cryptography techniques. The aim is to undermine a judge's blind faith in the value of cryptographic evidence and fool all those who rely heavily upon it. We show from a fictional scenario how such an attack and manipulation can be performed. The goal of this paper is to show that the concept of proof must be considered very cautiously and has no absolute value. In particular, we show and thus prove that any plaintext can be obtained from a given encrypted text just by designing or using an encryption algorithm in a suitable way. Even the secret key can be used to fool the judge. In this context, our scenario explains how to use such an algorithm in a real case.

**Keywords:** cryptography, digital evidence, data counterfeiting, anti-forensics, malicious cryptography, rogue cryptography

# **Exploiting the Hutu/Tutsi Divide: The Relationship Between Extremist Propaganda and Genocide in Rwanda**

**Sarah Gendron, Marquette University, Milwaukee, USA**

**Abstract:** Before the advent of colonization, Rwanda was fundamentally a unified country comprised of people who shared geographical borders, a god (Imana), and a language (Kinyarwanda). For centuries, the names "Hutu" and "Tutsi" were known as social distinctions. Hutus were understood to be agriculturalists and Tutsis pastoralists. Under colonial rule, these once social and mobile identities became racialized. Thought to have physical characteristics resembling those of Europeans, the Tutsi people were given both public and private privileges denied to the Hutus. These newly constructed ethnic identities and the inequalities that resulted from the privileging of one group over the other prompted the beginning of the hatred that ultimately resulted in the devastation of 1994. This paper explores how

Hutu extremists further exploited the colonial Hutu/Tutsi divide for the purpose of inciting genocide. Of particular interest are the propagandistic images related to the Tutsis which were made manifest by way of popular culture, including in magazines, talk radio, and pop music. The essay continues by examining issues that could impact any culture or country. Specifically, it will consider the relatively recent attempts to prosecute those responsible for the creation and dissemination of these images as well as the repercussions that such legal action could have on the notion of freedom of expression. Finally, the work concludes with an exploration of the ways in which the same modes of popular culture have since been employed in Rwanda for the purposes of reconciliation.

**Keywords** Rwanda, propaganda, genocide, popular culture

## **Smart Card, the Invisible Bullet**

**Vincent Guyot, ESIEA, Paris, France**

**Abstract:** Information leakage is a major issue for homeland security. When entering and leaving certain countries which are particularly concerned by their national security, electronic devices such as PDAs, mobile phones and laptops are examined, as well as data storage devices such as USB sticks and mobile hard disks. Technical investigations can be more or less thorough, and might lead up to confiscation of the material in case of doubt. In the same time, the use of smart cards is spreading over the world, mainly as a mode of payment, in public transportation or as SIM cards in mobile phones. These usages are widely adopted, in particular due to the security benefits delivered by these systems. But smart card technologies can also be used in an unconventional way to efficiently hide information in order to cross national borders. Smart cards have been designed as objects which ensure security in an untrustworthy environment. Their major function is to protect from the outside world and to hide its ways of working. A smart card is a programmable device, close to a very small computer, in which it is possible to hide functionalities impossible to detect. We demonstrate that is nowadays possible to use a smart card in an unconventional manner, by using its storage and cryptographic capacities to transport information in an undetectable way, under the cover of a harmless common object.

**Keywords:** smart card, information leakage, undetectable hidden data

# Cyber Antagonism Between Hacker Groups Develops new Challenges

Roland Heickerö, Swedish Defence Research Agency (FOI), Stockholm, Sweden

**Abstract:** The rapid development of information technology does not only change the way to interact, communicate and distribute information between people and organisations. It also creates new possibilities for conducting antagonistic, criminal and hazardous activities by using the Internet. A qualified cyber attack against an opponent's critical information infrastructure can within very short period of time lead to effects in a country's security policy. One area of great concerns is malicious hacking and hacktivism. The paper discusses the escalation of conflict on the Internet between different kinds of hacker groups fuelled by political, religious and national manifestations that tend to increase over time. The level and intensity of the activities are governed by recent incidents whereas conflicts are spreading from the physical sphere into cyber space. Symbols of different kinds are often used as tools for escalating conflicts. Whenever a cyber conflict is initiated a situation develops where different parties are willing to help either side. Unholy alliances form between disparate groups of people that could come from all over the world. The conflicts boost on various internet forums with everything from rumours and accusations from one part towards another to directed cyber attacks on a large scale. Misleading information is continuously disseminated with the purpose to create antagonism. In the text several examples are given on cyber antagonism with malicious hackings and defacement attacks that has developed from the physical sphere. For instance the infected debate of the Mohamed Cartoons as well as the publishing of the Swedish painter Lars Vilks "Roundabout dog", the second Intifada between Israelis and Palestinians and the ongoing quarrel between Pakistani and Indian hacker groups, all with implication on security policy level. The paper ends with a short discussion on the risk for cyber escalation and the need to improve both information security and international cooperation in order to hinder or reduce the negative effects of antagonistic cyber operations.

**Keywords:** cyber conflicts, hacker groups, defacement attacks, hacktivism, Indian-Pakistan hacker conflict, cyber escalation

# **The Malicious Insider Problem: An Integrated View on Individual, Organizational and Contextual Influencing Factors**

**Ulrike Hugl, University of Innsbruck, Austria**

**Abstract:** Malicious insider misuse continues to be an important security event. Such breaches may cause enormous threats to an organization drawing diverse and huge negative consequences. Recent research has recognized that technological-oriented efforts are not the only key factor to avoid malicious insider acts. However, additionally there is a need to understand the impact of the human factor and surrounding social issues. To approach the malicious insider problem in an organization it is argued that individual and psychological as well as diverse organizational and contextual factors play a crucial role to avoid misuse. The aim of this paper is to present a literature-based framework of such influencing factors on the malicious insider problem. Thus, the paper reviews definitions, characteristics and motivational aspects of insiders, presents specific triggers for misuse, influencing issues of trust and trustworthiness, organizational culture and refers to contextual factors like the current market downturn. Finally, an analysis of related managerial implications offers potential starting points to 'catch' the insider problem.

**Keywords:** malicious insider, characteristics/motivation of insiders, trust/trustworthiness, organizational culture, contextual factors, managerial implications

# **The Way of Warfare in Three Possible Worlds – From art of war to Information Warfare**

**Aki-Mauri Huhtinen**

**National Defence University, Helsinki, Finland**

**Abstract:** In the 17th century the compiling of statistics on groups of people - military, children, the sick, the workers - started. In order to achieve this, a "box" had to be created for everyone to measure man in time and place. Hospitals, barracks, children's homes, schools and factories were all divided into spaces so that compartmentalizing and controlling individuals would be easier. Also soldiers were enclosed in barracks. The modern soldiers and military systems state that compartmentalizing the soldier enabled the idea of observing a larger military formation, first on the map and then (now) in computer screen. They started to use different colours to mark forces (both own and the enemy's.) The individuality of the soldier was removed for good. (eg. Zizek 2006) Now the top of this geometric (jominian) school of thought is

represented by EBO (Effects Based Operations) or Comprehensive Approach (CA) model in NATO and generally in western style armed forces. Operational Net Assessment (ONA) is based on system-of-system thinking, PMESII (political, military, economic, social, infrastructure, Information) on the all seeing eye of God on the battlefield. Technology has come between the combatants in battle. Today, maps and colours are no longer used but acronyms and concepts so abstract that the whole universe fits into the staff's situation picture. All those people who previously fought physically man to man are now committed to maintaining this situation picture. (eg. Krips 2010) It is not correct only annihilate the geometric school, but what happens when the officers committed to and knowledgeable of the maintenance of the situation picture have to run again, when they get out of breath and have to use a knife, fight in close combat etc. Or is it so that warfare is now permanently and finally a cyber thing? This article attempts to view the change of war from the Art of War to Military Sciences, especially Information Operations. The argument is that the current technology based theory has become permanently detached from the everyday practicalities of warfare. A special focus is on observing the development of warfare into information warfare through three possible worlds.

**Keywords:** rational world, complex world, postmodern world, information warfare, art of war

## **Changing Security Speech and Environment: From Nation States to Corporation Security**

**Aki-Mauri Huhtinen<sup>1</sup> and Kari Laitinen<sup>2</sup>**

**<sup>1</sup>National Defence University, Helsinki, Finland**

**<sup>2</sup>Police College of Finland, Tampere, Finland**

**Abstract:** Security in organizations is embedded in texts and speech that influence our understanding on it. Furthermore, texts dealing with security and threats influence our security environment, like organizations, and the way security is managed. All in all, the concept of security is very problematic. The faith in and search for security are evident in nearly all sectors of society and also in organizations. Security is something we can swear to. By definition, security is a good thing – who would want to promote insecurity? Due to the problematic conceptual foundation, security should be seen as a process. At the level of politics, this would lead to the question of which direction the process is to be steered towards and which goals are to be set for the process, knowing that complete security can never be achieved. Consequently, our notions of security vary constantly. This article addresses the concept and speech of security and its consequences to society and

security organisations. The main focus of the article is on security organisations that are run by governments, but the increase of private security sector is also noted. This context brings up the concept of securitisation. In brief, securitisation means seeing various matters and phenomena, as well as social problems, as security issues, which alters the political take on them and the means used to resolve them. Security operators, or organisations, at the national and international levels compete regarding data, knowledge, information, resources and power of speech in the social discussion. These "gatekeepers" of security – security authorities and the political elite – also determine what constitutes a threat, while simultaneously deciding on resource allocation and means to be deployed. This speech of security is neither innocent nor free of consequences, which is why it should be taken into consideration.

**Keywords:** security, securitization, terrorism, organization, information, discourse

## **Influence Operations and Behavioural Change**

**William Hutchinson<sup>1,2</sup> and Matthew Warren<sup>2</sup>**

<sup>1</sup>SECAU, Edith Cowan University, Western Australia

<sup>2</sup>Deakin University, Victoria, Australia

**Abstract:** The intended outcome of Information Operations appears to be a favourable change (to the instigator) in attitudes or belief systems of the target, however, the relationship between attitude and behaviour is tenuous. Propaganda and other methods of 'influence' are difficult to assess as the cause and effect relationship is complicated. The short term effects of psychological warfare where force is used in conjunction with influence techniques can be easily assessed; at least at a superficial level. Even in the latter case, the actual causes and effects could be solely the force used or some other factors rather than the psychological techniques per se. Influence Operations attempt to win the hearts and minds of the target audience but, even if successful, the lasting effects of a campaign are problematic. It is further complicated because if a person has a particular view, it does not mean that the ensuing behaviours will reflect that view. Also, there is evidence that the use of force on one set of people produces attitudes and behaviours that instigate radical beliefs and behaviours in another set. So psychological warfare techniques on one group that may or may not produce compliant behaviour stimulates another group to empathise with the victims thus producing an overall practical negative influence. Influence campaigns cannot be separated from the physical environment in which they are executed. If good politics requires good influence campaigns then good

influence campaigns require good politics to back them up. This paper will examine the relationships between short term influence campaigns and compare them with the more long term socialising effects such as early education, family and physical attributes that have on attitudes and beliefs which result in the development of such behaviours as terrorism.

**Keywords:** influence campaigns, power, psychological warfare, propaganda, beliefs, behaviour

## **Identities, Anonymity and Information Warfare**

**Stuart Jacobs, Lou Chitkushev and Tanya Zlateva  
Boston University, USA**

**Abstract:** We discuss the primarily role of anonymity and identity manipulation in information warfare. We contend that those who engage in information warfare have very similar goals as those involved in cyber crime and cyber terrorism. Today Internet-based commerce has become global, representing a significant component of the world market. Network-based personal communications services are rapidly becoming the method of choice for many nations. In fact many critical infrastructure components are managed and controlled remotely. Yet these various capabilities are usurped by cyber warriors, terrorists or other criminals. A number of networking issues contribute to the current state of Information Warfare. Historically, security capabilities (e.g., authentication, authorization and confidentiality services), had not been considered a high priority in the original design of the critical Internet protocols still in use. Further complicating the security problem is the lack of consistency in name scheme adopted for network-related objects (hosts, applications, interfaces). Mapping of object names continues to be a trial-by-error exercise, which is frequently misused by malicious actors, as in the case of Address Resolution Protocol (ARP). Moreover, the lack of authentication facilitates the use of ICMPv4 and UDP as protocols of choice for Distributed Denial-of-Service attacks. Dynamically used transport protocol port numbers are now common: negating the effectiveness of classic firewall type packet filtering. Regrettably, mapping of device domain names to IP addresses via DNS continues with no major efforts to prevent invalid updates or query responses. Many of the aforementioned protocols rely on data-origin authentication via secret key and message digests, yet, secret key management is non-existent. IEEE 802.1X, used in newer wireless networks, is routinely avoided for wired infrastructures. Although IP security (IPsec) is widely available, it is rarely deployed beyond secure virtual private networks (VPNs), especially given that its availability in IPv4 is optional and usage optional with IPv4 and IPv6. DNS security (DNSSEC) has existed for over 10

years yet serious discussion for its deployment are only now occurring. The standards for Public Key Infrastructures (PKIs) and Digital Certificates are extensive but the majority of organizations find excuses to avoid its use and most PKI-enabled applications cannot even check for revoked certificates. In conclusion, we contend that given the security threats associated with current and future Information Warfare activities, the inter-networked global community should focus on more rapid implementation and deployment of the existing security mechanisms. As such, mandatory, robust authentication as well as several key network security services should be adopted. The necessary mechanisms already exist, now is the time for network administrators to recognize the need for prompt deployment of these capabilities as a proactive defense/mitigation against malicious attacks at reasonable level.

**Keywords:** identification, authentication, anonymity, federated identities, next generation networks, information warfare, cyber-crime, cyber-terrorism

## **How to Grasp Emerging Futures of Information Wars?**

**Auli Keskinen, National Defence University, Helsinki, Finland**

**Abstract:** In industrial war, the objective was to win the trial of strength and thereby break the enemy's will. In the information age military force is used to influence the intentions of people. Globalisation and networking of operational environments constantly change the traditional order of management. Military organisations are challenged to behave more dynamically and to enhance the knowledge base being more multidisciplinary and agile. The societies today are "systems of systems", i.e. complex interactive human-technological systems forming various dynamic multidimensional networks. Thus, the complexity of interactions can only be tracked using conditional probabilities. This makes the decision-making of operations all the more dependent on tacit knowledge of the officers all through the various levels of command-and-control. Human behaviour cannot be forecast in detail, since people can change their rules of interaction thus changing expected outcome. In the past, the general understanding of ontology has been that there are two - order and chaos. Recently the third ontology - complexity - has emerged in scientific approach. In complex systems there is order, but it is emergent rising from the local interaction of independent actors, each of whom behaves according to its own principles, logic and knowledge. The behaviour of complex evolving systems and organisations arises from the intricate interconnectivity of elements - independent actors - within the system and between the system and its operational environment. In this paper, the futures research methodology for creating alternative futures images of information wars is

presented. There are recent major efforts to upgrade foresight methodologies available for the global community, such as organisational complexity, six-to-seven pillars of futures methods, HIF-analysis (Hindsight/Insight/Foresight), sense-making and Futures Signals Sense-making Framework (FSSF). Furthermore, to enhance the understanding of network-centric behaviour the new network theories are discussed. In particular, the varying error tolerance of networks is of interest.

**Keywords:** futures, complexity, sense-making, networks, robustness, warfare

## **Future Requirements for Deception in Naval Defence**

**Theodoros Kostis<sup>1</sup>, Athanasios Goudosis<sup>1</sup>, Konstantinos Galanis<sup>2</sup> and Ioannis Koukos<sup>3</sup>**

<sup>1</sup>University of the Aegean, Karlovassi, Greece

<sup>2</sup>Ethnodata S.A., Greece

<sup>3</sup>Hellenic Naval Academy, Greece

**Abstract:** Military naval targets are difficult to hide. For radar wavelengths they are extended targets to a surveillance Inverse Synthetic Aperture Radar (ISAR) system that can resolve their superstructure details and provide classification and even identification tasks from a very far distance. But the need to hide from adversary threats is always there. We focus on finding such an effective soft-kill countermeasure for ISAR systems. The principle is that since a naval target cannot be directly hidden from an ISAR system then a simulation-defined virtual world could furnish multiple false targets around and away from the real vessel under protection. The advantage of the simulation approach is improved flexibility when constructing the false naval target images because the heading, velocity and position vectors of the threat platform must always be taken under consideration. In other words the verisimilitude of the stratagem requires the provision of appropriate false target permutations that correspond to the changing aspect and depression angles of the threat signal. The proposed solution is a Simulator-defined Radar Countermeasure System (Sim-dRCS). We have already developed a relevant proof of concept that provides the ISAR side view of a battleship class false naval target for threat signals that expect such a real naval target to be on a dominant roll motion and at zero depression angle. In this paper we further verify and validate the involved requirements and data model by using a simple parallelogram target that is easy to extract conclusions by pictorial inspection according to the prevalent ISAR theory. The novelty in this paper is the provision of the ISAR top view of the simple false naval target for threat signals that expect such a simple real naval target to be on a dominant yaw motion and at zero depression angle. Also the previously available ISAR side

view is revisited for verification and validation purposes now using the simple model instead of the more complicated battleship class model. In conclusion the ISAR side view or the ISAR top view of the false naval target can be presented to the high range resolution threat sensor according to its current position (aspect and depression angles) enhancing the belief of the adversary radar operator that a real target is indeed at that position. Future work involves the programming of the intermediate states between ISAR top and ISAR side views of the false naval target.

**Keywords:** ISAR, countermeasure, naval target, deception, soft-kill protection

## **Detecting XML Data Irregularities by Means of Lexical Analysis and Parsing**

**Dirk Kotze and Martin Olivier**  
**University of Pretoria, South Africa**

**Abstract:** Irregular activities such as fraud often lead to recurring, identifiable patterns in the meta-information. Such patterns may be automatically identified by means of a grammatical rule set which uses compiler construction techniques to identify the origin of the irregularity and the pattern associated with it. The eXtensible Modelling Language (XML) is often used to facilitate inter-operation of applications. Extensible Business Reporting Language (XBRL) is based on the concept of XML and is an open, human readable format designed for the sharing of financial information. Due the ease of editing and modifying human readable information, it is comparatively easy to manipulate the information contained in XBRL in a fraudulent way. An example might be to edit the totals of a transaction or to add a bogus transaction to the data. Our research addresses this problem by applying compiler construction techniques on the XBRL information. In doing so, we hope to extract useful forensic information from the patterns in the meta-information which may in turn be used for prosecution in case of irregularities (such as fraud). Our techniques can be further applied to other XML based applications (such as command and control XML specifications) to detect irregularities in a post-event analysis. The paper reports on a prototype that was constructed using standard compiler construction tools such as `Lex` and `Yacc` under Linux. We have used these tools to construct a grammar and to compile the grammar into an executable. The executable was then run on a set of XBRL inputs, where it performed pattern matching on the meta-information in the XBRL input. The parser was generated to parse correct XBRL; the 'normal' productions that form part of correct XBRL were augmented by error productions to deal with a few examples of fraudulent

actions. The prototype was able to identify pre-defined fraud patterns in the XBRL-file. It is thus possible to conclude that grammar rules and compiler construction can be used to successfully parse meta-information and extract forensic information.

**Keywords:** digital forensics, XBRL, lexical analysis, grammar, Lex and Yacc

## **Operations Management of Information Security at Enterprise Levels**

**Pertti Kuokkanen**

**Defence Command Finland**

**Abstract :** This research paper has been prepared to present an outline of operations management at enterprise levels and to produce a framework of operations management for information security management. Operations management is a mediation between, first, the strategic planning and the guidance of work, and second, the different functions of an organization's reporting, in which every activity area can be systematically checked. The key idea is to have the organization managing in the whole information security operation be a positive management of change. To be a viable part of operations management, the information security management is resourced and supported in all enterprise levels by decisions at the top level. There are three types of operations management. The first, structural operations management, deals with restructuring and systemizing important areas such as management features. The second, resource information operations management, is based on the real-time registered information of selected organizations. And for the third, events reporting operations management, it is essential to actively report the organization's successes and, therefore, the knowledge of their utilization. Also, there are the three main types of management decision making and control processes, which are strategic planning, management control, and work control. Strategic planning contains the organization's overall strategies, goals, and change. Under management control, consistent results will be monitored to ensure the effectiveness of the organization's resources and the achievement of objectives. Work control directs attention to the daily performance of the functions. All of these actions can be linked to the plans and objectives of the higher performance of the organization. The main contribution of this study is based on the conceptual approach, which intends to construct systems of conceptions. The research has been done to combine previously presented dimensions of management and to develop a framework process for operations management which is useful for the actions of information security at different enterprise levels.

**Keywords:** strategic leadership, security management for enterprises, information security governance and management

## **The Finnish air Surveillance Radar System Evolution – From war Time Experience to Network Enabled Warfare System**

**Martti Lehto<sup>1</sup> and Juha-Antti Lamberg<sup>2</sup>**

**<sup>1</sup>National Defense University, Helsinki, Finland**

**<sup>2</sup>Aalto University School of Science and Technology, Finland**

**Abstract:** This article analyzes the evolution of Finnish Radar System Development. The Air Surveillance system is inherently a combination of human communities and technical systems. The objective of this paper is to outline the empirical framework for the evolution of the Air Force's radar system and analyze why the radar systems are identical to various countries from institutional logic / global convergence but they develop at the same time as a result of nation- specific processes (the logic of path dependence). The evolution of radar systems in Finnish Air Force can be seen as divided into phases, each with a different focus area. The objective during the 1950s was to build an indigenous radar system since Western high technology was unavailable. Buying Western equipment became possible during the 1960s. In the 1970s Finland developed indigenous radar systems. A major evolutionary change began during the 1980s. The final decade of the Cold War saw the attainment of operational capability of the last radar system of Finnish design so far. Programs for the acquisition from abroad of long- and short-range surveillance radar systems were launched as the decade was drawing to a close. The article provides patterns, discourse, and analyses of radar evolution from the standpoint of institutional logic and path dependence.

**Keywords:** radar system, evolution, institutional logic, the logic of path dependence

## **War and Ethics in Cyberspace: Cyber-Conflict and Just war Theory**

**Andrew Liaropoulos**

**University of Piraeus, Greece**

**Abstract:** Over the last two decades there is a growing body of literature over exploiting cyberspace for offensive and defensive purposes. Cyber-conflict is after all the newest mode of warfare and cyber-weapons have been described as weapons of mass disruption. Although the attention on the technical and military dimensions of cyberspace is justifiable, one needs also to look into the legal and ethical aspects of cyber-conflict, in order to

comprehend the complex nature of cyberspace. Conflict in cyberspace raises many ethical questions for both theorists and practitioners of warfare. In particular, the lack of an international legal framework that defines the use of force in cyberspace, operational difficulties in deterring and identifying cyber-attacks as well as the asymmetric dimension of cyber-conflicts pose without a doubt, great pressure on the just war tradition. This paper applies just war theory (*jus ad bellum*, *jus in bello* and *jus post bellum*) in cyberspace and explores when and how states may justly resort to cyber-conflict, operate during such a conflict and terminate it. Cyberspace is accessible to all and there are no rules or norms providing guidelines for the use of force. In addition to that, cyber-conflict appears to be less lethal and has a global reach. As a result, cyberspace makes conflict more thinkable, but that does not mean that it must also be unjust.

**Keywords:** war, ethics, cyberspace, cyber-conflict, just war theory, law

## **She Wolves and Russian Brides – Women Enemies in war Propaganda”**

**Tiina Lintunen**

**University of Turku, Finland**

**Abstract:** In this paper I will scrutinize how Red women were stereotyped by the enemy during the Finnish Civil war in 1918. Women acted both in service troops and as soldiers in the Red Guard. These women who participated actively in the war provided their opponents a useful way to distance all Red women as 'the others' who are threatening 'us'. During the war, the Whites spread rumours and strengthened propagandistic stereotypes about the Red women, which affected the public opinion on the White side. There were four types of mythical stereotypes that were related to the Red Women, which described them as threatening, unfeminine, indecent and unfit for mothers. The propagandistic images had an influence on the way women were treated after the war. By supporting the revolution Red women had erupted the *status quo*. These women challenged the traditional women's role, which the conservative opponents perceived as threatening, confusing and reprehensible. The defaming of political women opponents has also been widely used in connection with other wars and revolts.

**Keywords:** war propaganda, women enemies, stereotypes, civil war, Finland

# **Towards a Framework for the Generation of Enhanced Attack and Background Network Traffic for Evaluation of Network-Based Intrusion Detection Systems**

**Owen Lo, Jamie Graves and William Buchanan  
Edinburgh Napier University, UK**

**Abstract:** There are a multitude of threats faced in computer networks such as viruses, worms, trojans, attempted user privilege gain, data theft and denial of service attacks. To combat such threats, multiple lines of defence are applied to a network including firewalls, malicious software scanners and intrusion detection systems (IDS). IDSs are generally considered a last line of defence for the detection of attacks; therefore, it is vital for users to assess how well an IDS will perform through means of testing. Although various methodologies have been proposed for the evaluation of IDSs in the past there is still no widely agreed upon standard. A framework which is capable of carrying out an evaluation of network-based intrusion detection systems (NIDS) is presented in this paper. The paper shows that such a framework requires the need for both realistic real-time network traffic and meaningful metrics when carrying out an evaluation of IDSs. Automation of the testing process is also emphasised - which provides for ease-of-use and simplicity in repetition when carrying out an evaluation. The framework is evaluated against the NIDS Snort in order to show its capabilities. Through the use of pre-existing programs and utilities, the aim of generating real-time attack traffic is achieved whilst benign background traffic is generated using static data sets. The metrics of efficiency, effectiveness, packet loss, CPU utilisation and memory usage are derived and, finally, the goal of automation is achieved by implementing the framework as a singular application. The results of the evaluation show that, whilst Snort is highly effective in the detection of attacks (true-positives), its main weakness is the dropping of network packets at higher CPU utilisations due to high traffic volume. Finally, the conclusion to this paper illustrates that the main weakness with current IDS evaluation methodologies is in the approaches used in the generation of benign background traffic. Whilst using static data sets is viable, the main argument against such an approach is that an IDS under evaluation will not react to the traffic in a real-time manner. Furthermore, the use of synthetic traffic generators also has limitations due to the fact that such traffic may not accurately reflect traffic seen on a live network. This paper proposes that further research and development must be applied in the area of benign traffic generation in order to achieve the aim of providing real-time generation of background traffic which realistically mirrors real-life networks when carrying out an evaluation of IDSs.

**Keywords:** intrusion detection, evaluation framework, attack traffic, background traffic, evaluation metrics

## **Towards a Risk Management Based Approach for Protecting Internet Conversations**

**Dimitrios Michalopoulos<sup>1</sup>, Ioannis Mavridis<sup>1</sup> and Vasileios Vitsas<sup>2</sup>**

**<sup>1</sup>University of Macedonia, Thessaloniki, Greece**

**<sup>2</sup>Alexander Technological Educational Institute of Thessaloniki, Greece**

**Abstract:** During recent years the number of online communication means between teenagers has been growing rapidly. However, the hazards that follow these new types of communication are growing as well. Predators use Internet conversations to attract minor users, usually resulting in catastrophic consequences. In this paper, a new risk management based approach is proposed, which aims to monitor internet-based conversations and identify possible attacks. In particular, a wide research on the area of children exploitation is first conducted, in order to identify the methods and the techniques that are used. Then, the implementation of a system capable of capturing and analyzing chat dialogs is proposed. The proposed system is under development and has not been implemented yet. It is based on three different sensors. The first one performs text analysis on captured traffic, as an attempt to look for known patterns that may indicate a possible attack. The Naive Bayes classifier method then follows, based upon the initial training set. In addition, this training set is enhanced and adopted to specific users' needs via the proposed "supervised learning technique". The second sensor captures files or web links that are sent through the chat conversation, indicating possible personal information leak or exposing unwanted material to minors. The third sensor counts how many times the same users talk with a particular child. As a result, a total risk factor is calculated as a weighted sum of the three risk factors, through applying the proper weight coefficients. In case the risk factor is above the predefined threshold, a warning signal is sent in order to warn on time that there is a possible grooming attack. The main challenge in the proposed system implementation is related to natural language processing, due to the fact that teenagers use their own acronyms and idioms when chatting, creating their own language. A deep research on these dialogs might result into different linguistic sets. Another important challenge is related with the privacy in internet related communications.

**Keywords:** cybercrime, grooming, risk assessment, attack recognition

# **Analysis of Malicious Affiliate Network Activity as a Test Case for an Investigatory Framework**

**Mathew Miehling<sup>1</sup>, William Buchanan<sup>1</sup>, John Old<sup>1</sup>, Alan Batey<sup>2</sup> and Arshad Rahman<sup>3</sup>**

<sup>1</sup>**Napier University, Edinburgh, UK**

<sup>2</sup>**Detective Sergeant, Computer Crime Unit, Northumbria Police, UK**

<sup>3</sup>**Financial Services Authority, London, UK**

**Abstract:** Currently there is a great deal of literature surrounding methods that can be used to detect click-fraud, but there is very little published work on actual cases of click-through fraud. The aim of this paper is to present the details of a real-life fraud, in order that lessons may be learnt to overcome this type of fraud in the future. The paper outlines a fraud that is suspected to have included both PPC and PPS from fraudulent affiliates. This paper describes a methodology for the investigation process of affiliate network scams, including the anonymisation of personal and location details, while providing an analysis of an actual crime. In total, the case examined resulted in an estimated loss of around £200,000 with a further estimated loss of over £200,000 if further transactions had not been cancelled. The methods used within the scam are outlined using anonymised data, and presented to highlight the malicious activity. This included both pay-per-click and pay-per-sale scams most likely using stolen identity information. It concludes with the methods that may be helpful in possibly identifying malicious activity with affiliate networks and how a framework can be setup to investigate these crimes. The current work involves developing an investigatory framework focused on the early detection of electronic fraud, and the work done for this paper will be used as a test case on affiliate fraud data. The future aim of the research is to completely automate the investigatory framework that will allow incident data to be processed so that the context of a crime is not lost, but that it anonymises and protects the identity of those involved.

**Keywords:** affiliate advertising, click through, fraud, financial services, eCrime

## **Block Based Steganography**

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

<sup>1</sup>**Helwan University, Cairo, Egypt**

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

**Abstract:** Steganography is the art and science of hiding communications. In contrast to cryptography, which aimed at encrypting messages such that it is infeasible to an attacker to decrypt the messages, Steganography aimed at

hiding the presence of communication in a medium that is used to carry secret messages (image, audio, or video). This has to look innocuous to an attacker, so it will not raise suspicion from an eavesdropper. Most steganographic systems can be attacked visually or statistically (steganalysis). Systems that are resistant to such attacks, provides a relatively small capacity for steganographic messages. In this paper, a new technique is introduced to hide data in the least significant bit (LSB) of the discrete cosine transform (DCT) coefficients of JPEG image blocks. This technique exploits the ratio of even to odd coefficients in each image block and embeds data bits in a way that preserves the ratio between even and odd DCT coefficients of each image block. A Block Based Steganography (BBS) algorithm offers high capacity with statistically minimal changes compared to current steganographic algorithms. A comparison between BBS algorithm and current steganographic systems will be introduced.

**Keywords:** steganography, steganalysis, information hiding, JPEG hiding

## **Hacking for fun and Education: ELearning on Network Security**

**Alexander Ott and Richard Sethmann**

**University of Applied Sciences, Bremen, Germany**

**Abstract:** In a world where security agencies recruit their security experts, a fundamental and affordable education is needed to address these high demands. Security experts need to understand the hacker view to be able to secure a network or an IT system. Therefore hacking skills are needed to protect the 24 / 7 availability of an IT system which is crucial for successful business in the connected world. Only reading about a security flaw can't cope with the feeling of exploiting it. Exploiting by oneself can enhance the ability to comprehend the full extend of a security flaw. The Network Security eXperience (NetS-X) eLearning environment is able to provide a fully controlled hacking environment, with on demand guidance and an optimized learning process. The hands on experience combined with the ongoing encouragement through instant feedback on request are delivering an interesting learning experience. NetS-X is setup on top of an existing enterprise like, sandbox network, to provide a suitable learning environment. Nothing is simulated or emulated. Therefore the experience of the practical learning module (scenario) is "the real deal,,". Special scenario deployment, controlled by the game engine is the key to the multiuser capability of NetS-X. This deployment is realized by the implementation of different setup types for environment and user. The user knows every fault is reversible with the click of a button, and therefore encouraged to play around as he likes, exploring the environment in his own way. Multiple choice tests before and after a scenario are introduced to help understanding & remembering even better.

The game motivated eLearning environment helps the player to extend the knowledge on his own and is supported by the game engine counselling. The build in framework technologies maintainable through admin interfaces are allowing tutors as well as the learner himself to add content to the education process. Students of the University of Applied Sciences Bremen become capable of developing even more scenarios respectively learning modules to the game after passing it. Now NetS-X is deployed initially with 4 Levels and 31 scenarios from brute force and man in the middle attacks to SQL injections and buffer overflows.

**Keywords:** education, information, hacking, network, security

## **Proactive Defense Tactics Against On-Line Cyber Militia**

**Rain Ottis**

**Cooperative Cyber Defence Centre of Excellence**

**Abstract:** There is a developing trend of “popular” cyber campaigns that mirror political, economic or military conflicts in cyberspace. The Estonian case from 2007 showed that a whole nation-state can be affected by cyber attacks, whereas the Georgian case of 2008 is an illustration of a cyber campaign that mirrors an armed conflict. In both cases at least part of the attacks were likely committed by patriotic hackers – volunteers who use cyber attacks to take part in intra- or international conflicts. In such cyber conflicts usually only the targets are known while the aggressors remain anonymous. It is often difficult to discern where state capability ends and independent patriotic hacker groups begin. Furthermore, it is relatively easy to form a new cyber militia from people who have little prior experience with computers. I define *cyber militia* as a group of volunteers who are willing and able to use cyber attacks in order to achieve a political goal. I further define *on-line cyber militia* as a cyber militia where the members communicate primarily via Internet and, as a rule, hide their identity. What the newly-minted cyber warriors may lack in skill and resources, they can often compensate with numbers. However, even an ad-hoc cyber militia that is not under direct state control can be a useful extension of a state’s cyber power. On the other hand, they can also become a threat to national security. Due to the global nature of the Internet, this threat is most likely coming from multiple jurisdictions, which limits the law enforcement or military options of the state. Therefore, other approaches should be considered. In order to understand the potential threat from cyber militias, either ad-hoc or permanent, we need to explore how they are organized. I provide a theoretical overview of a specific type of on-line cyber militia and then propose tactics to neutralize it. The tactics are based

on a proactive defense posture and primarily use information operation techniques to achieve the effect from within the cyber militia itself.

**Keywords:** cyber conflict, cyber militia, proactive cyber defense, information operations, hactivism

## **The Necessity of Implementing a Long-Term Security Strategy in Public Administration Organizations From Romania**

**Marius Petrescu, Ionut Barbu, Gabriela Popa and Valentina-Ofelia Robescu**

**Valahia University from Targoviste, Romania**

**Abstract:** Information and Information Technology is at the heart of the modern economy - and at the heart of the modern organization. Governance and management of security are most effective when they are systemic, woven into the culture and fabric of organizational behaviors and actions. In this regard, culture is defined as the predominating shared attitudes, values, goals, behaviors, and practices that characterize the functioning of a group or organization. Culture thereby creates and sustains connections among principles, policies, processes, products, people, and performance. Effective security should be thought of as an attribute or characteristic of an organization or a project. It becomes evident when everyone proactively carries out their roles and responsibilities, creating a culture of security that displaces ignorance and apathy. One manifestation of this is that everyone proactively considers the attacker perspective throughout the software development life cycle and how the software can fail when under intentional attack or unintentional actions of users or developers. An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification. Security must come off the technical sidelines as activities and responsibilities solely relegated to software development and IT departments. Today, boards of directors, senior executives, and managers all must work to establish and reinforce a relentless drive toward effective enterprise, information, system, and software security. Because security is now a business problem, the organization must activate, coordinate, deploy, and direct many of its core resources and competencies to manage security risks in concert with the entity's strategic goals, operational criteria, compliance requirements, and technical system architecture.

**Keywords:** information, effective security, security classification, organization

## **An Applied Framework for Modelling a Critical Infrastructure System Incident**

**Graeme Pye and Matthew Warren**  
**Deakin University, Geelong, Australia**

**Abstract:** The research applies the TARDIS system security analysis and modelling framework to an adverse critical infrastructure system incident. This paper reports on the practical application of the framework to a case study based on an actual critical infrastructure system failure and the resultant implications for the system and the wider regional community. Then a reflective discussion is undertaken reviewing the TARDIS framework approaches employed within the blended hybrid approach incorporated into the framework, before speculating on future research areas of framework development and application.

**Keywords:** critical infrastructure, security analysis, systems modelling

## **Towards Reversible Cyberattacks**

**Neil Rowe**  
**U.S. Naval Postgraduate School, Monterey, California, USA**

**Abstract:** Warfare without damage has always been a dream of military planners. Traditional warfare usually leaves persistent side effects in the form of dead and injured people and damaged infrastructure. An appealing feature of cyberwarfare is that it could be more ethical than traditional warfare because its damage could be less and more easily repairable. Damage to data and programs (albeit not physical hardware) can be repaired by rewriting over damaged bits with correct data. However, there are practical difficulties in ensuring that cyberattacks minimize unreversible collateral damage while still being easily repairable by the attacker and not by the victim. We discuss four techniques by which cyberattacks can be potentially reversible. One technique is reversible cryptography, where the attacker encrypts data or programs to prevent their use, then decrypts them after hostilities have ceased. A second technique is to obfuscate the victim's computer systems in a reversible way. A third technique is to withhold key data from the victim, while caching it to enable quick restoration on cessation of hostilities. A fourth technique is to deceive the victim so that they mistakenly think they are being hurt, then reveal the deception at the conclusion of hostilities. We also discuss incentives to use reversible attacks such as legality, better proportionality, lower reparations, and easier ability to use third parties. As an

example, we discuss aspects of the recent cyberattacks on Georgia. This paper appeared in the Proceedings of the 9th European Conference on Information Warfare and Security, July 2010, Thessaloniki, Greece.

**Keywords:** cyberweapons, cyberattacks, reversibility, damage, cryptography, deception

## **Reconfigurable Radio Systems: Towards Secure Collaboration for Peace Support and Public Safety**

**Johan Sigholm**

**Swedish National Defence College, Stockholm, Sweden**

**Abstract:** As military priorities are shifting from invasion defense to crisis management and peace support operations, the capability to partake in efficient inter-organizational collaboration is becoming increasingly important for armed forces across Europe. The “solidarity clause” of the Treaty of Lisbon, which entered into force on December 1<sup>st</sup> 2009, dictates that all EU member states shall act jointly if another member state is the target of a terrorist attack or the victim of a natural or man-made disaster. Sweden has gone even further, stating that it will not remain passive if a member state or another Nordic country is attacked, and expects these countries to act in the same manner if Sweden is attacked. This declaration obligates Sweden to be able to collaborate successfully with allied partners, both within own territories and abroad. Application-based collaboration tools for use in unpredictable settings, requiring high user mobility and network survivability, put high demands on the underlying ICT systems in order to function correctly. Networks employing the TERrestrial Trunked RAdio (TETRA) standard are becoming pervasive as platforms for interagency collaboration in crisis response. Although these networks provide many benefits compared to legacy technology they lack the possibility to offer secure, infrastructure-less and disruption-tolerant communication in challenging environments. Emerging ICT such as MANET-based Reconfigurable Radio Systems (RRS) shows potential for overcoming these problems, in addition to resolving issues of technical heterogeneity. The Common Tactical Radio System (GTRS) is an RRS being developed by the Swedish Armed Forces, intended to be the future ICT system for all parts of the forces, used both in national and international mission settings. However, remaining challenges include threats of node compromisation and adversary network infiltration, as well as the safeguarding of confidential information shared by collaborating parties and preventing information leakage. This paper contributes by (i) giving a summary of recent work in mechanisms for achieving information security in tactical MANETs and Hastily Formed Networks for disaster response. The

paper also (ii) presents in-progress work towards the design of a gossip-based cross-layer Distributed Intrusion Detection System (DIDS) for the GTRS system, which takes resource constraints of portable devices into account, and offloads traffic analysis and anomaly detection to more powerful “Big Brother” nodes. An outline of the proposed DIDS architecture is presented, and the paper (iii) suggests future work towards offering a dependable and trustworthy communications platform for efficient and secure inter-organizational collaboration.

**Keywords:** reconfigurable radio systems, MANET, distributed intrusion detection, hastily formed networks, disaster response collaboration, emergency management communication

## **An Alerting System for Interdependent Critical Infrastructures**

**Paulo Simões<sup>1</sup>, Paolo Capodiecì<sup>2</sup>, Michele Minicino<sup>3</sup>, E. Ciancamerla<sup>3</sup>, S. Panzieri<sup>4</sup>, M. Castrucci<sup>5</sup> and Leonid Lev<sup>6</sup>**

<sup>1</sup>**CISUC - DEI, University of Coimbra, Portugal**

<sup>2</sup>**Selex Communications S.p.A., Italy**

<sup>3</sup>**ENEA, Italy**

<sup>4</sup>**Università di Roma Tre, Italy**

<sup>5</sup>**University of Rome – La Sapienza, Italy**

<sup>6</sup>**Israel Electric Corp., Israel**

**Abstract:** In the last few years we have witnessed a strong interest in the protection of Critical Infrastructures (CIs) such as power distribution networks, power plants, refineries, water distribution, transportation systems, hospitals and telecommunication networks. Despite their relevance for public safety and security, these infrastructures are highly exposed to a large number of threats, including natural hazards, component failures, criminal actions and terrorism. Several research projects address this topic. Many of them focus on building CI simulators for preventive analysis of system vulnerabilities, while others try to proactively strengthen partial sections of the CIs (such as fault tolerant components or secure control networks). Nevertheless, despite their positive results, those projects seldom provide mechanisms to assess, in real time, the risk level associated with each of the services provided by the addressed CI. Moreover, they do not take into account the high level of interdependency between heterogeneous CIs (power distribution failures, for instance, have a direct impact on telecommunication networks, which also affect other critical infrastructures and so on) or, when they do, they have to make compromises at the level of scalability, performance, or privacy of sensitive information. In this paper we present a CI alerting system that takes a step further, when compared to those approaches, by estimating in real

time the risk level associated with each service provided by the CI (i.e. the current likelihood of service degradation or service shutdown induced on a given CI by "undesired" events occurred in that CI and/or in other interdependent CIs).

**Keywords:** Critical infrastructure protection, online alerting systems, CI interdependence

## **Hard Disk Storage: Data Leakage**

**Iain Sutherland and Gareth Davies**  
**University of Glamorgan, UK**

**Abstract:** The hard disk drive remains the most commonly used form of storage media. The concerns relating to the correct sanitisation of user data, in particular when the hard drive is recycled or discarded have been well documented. However, it is possible that even when a user effectively overwrites data from the operating system, user data can still remain on the hard disk drive as a result of the normal operation of the hard disk drive. We highlight the risk of inadvertent data leakage as a result of the firmware processes present in a hard disk, in particular the error-handling component of the hard disk drive firmware. Where an area of the drive becomes unreliable due to natural wear and tear, the disk firmware which monitors data access will instruct the drive to copy the data from the failing area to a specially designated reserved area. The system remaps this data shift so the old data area and the original copy of the data are no longer accessible to the user. However, this does not erase the original copy of the data. This will therefore remain on the drive although the 'failed' portion of the drive will no longer be accessible by the operating system. This paper discusses the potential problem generated by this process with certain disk drives potentially retaining substantial amounts of data after being wiped by the operating system or other security tools. In conclusion this paper will propose best practice for data disposal and disk reuse.

**Keywords:** hard disk, steganography, data disposal, firmware

## **Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons**

**Eneken Tikk and Kadri Kaska**  
**Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia**

**Abstract:** To investigate and prosecute the 2007 cyber attacks against its governmental and critical private information infrastructure, Estonia requested

legal cooperation from the Russian Public Prosecutor's Office. This paper looks into the anatomy of this request and the Russian refusal to cooperate and suggests that in situations like the Estonian events in 2007, the lack of a legal mechanism or political willingness to cooperate equally result in the inability of the victim state to prosecute the cyber incidents. The paper also concludes that situations where a nation is depending on another sovereign's mercy may, in combination with the persistent trend of politically motivated cyber attacks, lead to a sense of fearlessness among patriotic hackers.

**Keywords:** State responsibility, criminal cooperation, cyber attacks, prosecution

## **Information Security Education in the Greek Universities and Technological Education Institutes**

**Theodosios Tsiakis, Technological Educational Institute of Kozani, Greece**

**Abstract:** A plethora of universities departments, especially those applied to the field of Computer/Informatics studies, observing the current need for information security, have incorporated courses of information/computer/network/communication security to their undergraduate curricula. This paper illustrates the academic courses in the subject area of security, which are available/teach in the Computer/Informatics departments of Greek Universities and Technological Education Institutes (TEI). It discusses and evaluates the different didactic methodologies that are followed, the learning process, the teaching material and methods, the structure of the module. Also it compares the syllabus, the theoretical and practical contents that taught, the offered books, as well as whether it is a compulsory or optional course and if it is a single course or an entire set of coursework.

**Keywords:** information security, curriculum development, information security education

# **RIDICULING THE DEMON: The Comical Image of Lazy, Stupid, Ineffective, Helpless, Uncultured Russians During the Winter War 1939–1940 in Finland**

**Vesa Vares, University of Turku, Finland**

**Abstract:** Most enemy images concentrate on hatred, and they are usually based on very permanent national stereotypes. During the Second World War, and even before that, there was only one proper enemy image for the vast majority of the non-Socialist Finns: that of the Russians. The Russian enemy image filled all the criteria of being the "Other", and it was also actively produced especially by the right-wing radicals and the student organization Academic Carelia Society between the World Wars. This phenomena - the so-called "ryssänviha", hatred of Russians - has also been academically studied quite a lot in Finland, like International Russophobia in general. However, although the Russian was a "natural" enemy because of historical reasons and obvious differences in the way of life historical wars, religion, language, Russian serfdom, political culture etc.) In the minds of many Finns, "ryssänviha" as such touched only a fraction of the Finnish society. There existed also another image, which was not positive, but not totally hostile or ideological either. This image can be seen, for example, in the Finnish movies during the 1930's: The Russian was a stupid, irresponsible, lazy, drunken and lustful good-for-nothing rather than a violent demon, contrasted to the steady, reliable, hard-working and self-sacrificing Finns. During the Winter War between Finland and the Soviet Union, the hateful enemy image was evident, but also the comical side was used to boost the Finnish fighting spirit. This was done precisely by reviving the image of the Russian who was stupid, oppressed and terrorized by his own Commissars and could not achieve anything but was sometimes also very cunning and asked the Commissars the awkward questions. Primus inter pares in this genre was one of the editors with a permanent column in the conservative daily Uusi Suomi (the New Finland), who had created the image "Muzik Ivan Petrovitsh" already in the 1930's and carried on ridiculing the Russians during the Winter War. Thus he created such an "Other", against whom it was not hopeless to fight, disregarding the materially overwhelming power of the Russians during the war. Another of his themes was ridiculing the Russian war propaganda. It is also possible to find many anti-Russian stereotypes which were in fact typical among other Europeans in his texts as well. Other nations he left largely alone. I shall go into these articles and analyze how a comical image of the Russian was produced in order to encourage especially the Finnish homefront and to advance the values of home, religion and fatherland - In the Conservative sense of the words

**Keywords:** war propaganda, comical propaganda, Finnish-Russian War 1939-40, Winter War, Russophobia, homefront

## **Motivation and Requirements for Determining a Network Warfare Capability**

**Namosha Veerasamy and Jan Eloff, University of Pretoria, South Africa**

**Abstract:** Computers and networks have provided for increased connectivity, ease of use and convenience. Other advantages include the ability to communicate across borders, have access to information at your fingertips and the huge capacity for storage and transport. However, there also arises the need to properly protect these vital resources. At a computer security level, there exists the underworld community of hackers and crackers who seek to cause damage. From a military point of view, offensive actions are part of the warfare mode of operation. Thus, the attack, together with the protection of information, can take place for various reasons ranging from recreational pastimes, to skilful challenges, as well as military requirements. Networks and cyberspace have become the battleground as attacks are launched to disrupt, destroy or deny access to valuable resources. Network Warfare can thus be seen as the branch of Information Warfare that deals with the utilisation of Information and Communication Technology (ICT) to carry out various exploits of information, as well as the various defensive mechanisms that are deployed in order protect information against attack. Individual users and organisations need to be warned about the latest face of warfare that is not only being played out in the military networks, but also on the Internet and cyberspace. Consequently, Network Warfare has various facets which are often difficult to distinguish between. This paper builds on the field of Network Warfare and contains the motivation for determining a Network Warfare Capability. The motivation and requirements for determining a Network Warfare Capability are explored in this paper. This helps to recognise important considerations for determining a Network Warfare Capability. Some of the requirements are intricate and required further discussion. The extended discussion served to describe some of the requirements in greater detail. A noteworthy requirement of portraying offensive and defensive techniques is elaborated on through the use of UML diagrams. This paper, thus describes the importance of determining a Network Warfare Capability and serves as an introduction to future work in which a model to determine a Network Warfare Capability is proposed.

**Keywords:** network warfare capability, offensive, defensive

# ***Mein Kampf* Revisited: Enemy Images as Inversions of the Self**

**Marja Vuorinen**

**University of Helsinki, Finland**

**Abstract:** Adolf Hitler's (1889-1945) best-selling ideological tome, *Mein Kampf* (My struggle), established the National Socialist political program. Hitler began working on it while in the Landsberg prison, after his first, failed attempt to seize power, the Munich revolution in 1923. In prison he was visited by fellow Nazis-to-be, with whom he contemplated his ideas. He intended to make the book a financial success as well as an ideological one, hoping thus to pay his debts and gain capital for further political projects. After being released, in 1924, he moved to Obersalzberg, where he continued working on the book. The first volume was published in 1925, the second in 1926. After Hitler's rise to power in 1933, his book became the "Nazi Bible". It was the official wedding gift, presented by the state to newlyweds. During the war it was given to every soldier leaving for the front. By the end of the war, about 10 million copies had been distributed in Germany alone. The book was available in several editions, ranging from the inexpensive paperback to the wedding edition. It was translated into many languages, including Swedish, Italian and French (1934), English and Dutch (1939) and Finnish (1941). After the World War II it has not been published in Germany, but is sold internationally and available online via the internet. Lately it seems to have gained new popularity in the Arab world, for obvious reasons. *Mein Kampf* is a highly controversial, notorious book. It is known by name to almost everyone, but has been read by few. With its flagrant racist and otherwise hateful content it has well earned its reputation as an "evil" book. One of its main features is an assortment of perceived enemies: imagined counter-forces threatening to curb the success of the German nation. Political movements create enemy images basically to define their own group identity. What cannot be included into the good Self is projected away, to create an image of an Enemy. To know who they are, what they strive for, whom they protect and what they cherish, it is necessary also to know who doesn't belong, what will not be tolerated, who is to blame and who will have to be destroyed. The "enemies" listed in *Mein Kampf* include the Bolsheviks, the Jews, Austrian royal house, parliamentarians, (Jewish) Viennese journalists, intellectuals and international (Jewish) capitalists. Most of these negative images were not created by Hitler, but came from a much older European stock. Actually, Hitler's most effective innovation may well have been to bring the Self back to the foreground. Imagining the "superior" Aryan German nation as the eventual historical winner, and himself as its messiah, was the recipe for his temporary success. The enemy-images were perhaps originally

introduced as inversions, to accentuate this heroic self-image. It did not prevent them from being lethal.

**Keywords:** enemy images, propaganda, nationalism, National Socialism, Hitler

## **Development of a Security Chain Management Security Risk Management Method: A Conceptual Model**

**Matthew Warren and Shona Leitch**

**Deakin University, Melbourne, Victoria, Australia**

**Abstract:** This paper continues the prior research undertaken by Warren and Leitch (2009), in which a series of initial research findings were presented. These findings identified that in Australia, Supply Chain Management (SCM) systems were the weak link of Australian critical infrastructure. This paper focuses upon the security and risk issues associated with SCM systems and puts forward a new SCM Security Risk Management method, continuing the research presented at the European Conference of Information Warfare in 2009. This paper proposes a new Security Risk Analysis model that deals with the complexity of protecting SCM critical infrastructure systems and also introduces a new approach that organisations can apply to protect their SCM systems. The paper describes the importance of SCM systems from a critical infrastructure protection perspective. The paper then discusses the importance of SCM systems in relation to supporting centres of populations and gives examples of the impact of failure. The paper proposes a new SCM security risk analysis method that deals with the security issues related to SCM security and the security issues associated with Information Security. The paper will also discuss a risk framework that can be used to protect against high and low level associated security risks using a new SCM security risk analysis method.

**Keywords:** critical infrastructure, security risk analysis and supply change management

## **Behavioural Profiling for Impostor Detection in Mobile Networks**

**Ibrahim Zincir, Steven Furnell and Andy Phippen**

**University of Plymouth, UK**

**Abstract:** The object of this research is to propose a new approach, using behavioural profiling as the basis of an Intrusion Detection System (IDS) to detect impostors who masquerade as legitimate users in mobile networks. In behaviour-based IDS, historical user profiles are created and then compared

with the real-time ones in order to detect malicious activity. If a user changes behaviour this results in alerting the system since it is highlighted as an anomalous activity that might suggest an impostor is at work. To assess this approach C4.5 machine learning algorithm is applied over Massachusetts Institute of Technology's Reality Mining Dataset and successful results are achieved.

**Keywords:** mobile devices, authentication, behavioural profiling, intrusion detection systems, machine learning



# **Research in Progress Papers**



## **Legal Issues and Challenges Involved in Cyber World Business**

**Shubhangi Sunil Bhatambrekar, Modern College, Ganeshkhind, Pune, India**

**Abstract:** The exponential growth of the Internet and online activity raise a number of cyber world business issues and legal questions. The power of the Web to reach the world carries with it a variety of legal issues, often related to intellectual property concerns, copyright, trademark, privacy and security etc., particularly in the context of doing business on the Internet. Authorities seeking to apply their laws in traditional ways or to expand legal control over international links face many challenges due to the global nature of the Internet. Today, there are more questions on cyber law than answers. Also it poses a challenge for technology and the criminal justice system. There is general misunderstanding that the entire Indian cyber law is encapsulated in IT Act 2000. Whereas IT Act 2000 defines and punishes only a few cyber crimes. Therefore, it is necessary to know the relevant aspects of several other laws and their interplay with IT Act which directly or indirectly affect transactions in the cyber world since the cyber crimes such as hacking planting computer viruses and online financial frauds have the potential of shaking economics of the country. This paper provides an overview of the cyber crimes and cyber-legal issues related with IT Act 2000 in INDIA and challenges in eCommerce.

**Keywords:** cyber crime, cyber law, IT Act 2000, eCommerce

## **Knowledge Management and Knowledge Security – A Conceptual Comparison**

**Ilona Ilvonen, Tampere University of Technology, Finland**

**Abstract:** Taking care of knowledge is important for every company nowadays. Knowledge is acknowledged as an important asset along with traditional resources such as money and raw materials. The discipline of knowledge management seeks answers to questions such as how to make the best use of knowledge within an organization. As well as every asset, also knowledge needs to be protected so that it is properly secured from outsiders and other threats. Knowledge security addresses the protection of knowledge in organizations. However in the real world, the knowledge management efforts and the knowledge security efforts have little to do with each other, even though both aim to nurture the same assets. The people that plan and implement knowledge management strategies are not necessarily the same people who plan for security. Thus literature on the topic of these concepts is

written for different audiences with different interests. This paper explores the literature for knowledge management and knowledge security management. Both management books and scientific articles are reviewed. Common goals and common incentives are searched for, as well as grounding differences in approaches. The approach of this paper is theoretical. The paper comprises conceptual examination of two concepts; knowledge management and knowledge security. Especially knowledge security is a relatively new concept, so study of relating concepts from the field of information security is needed. The paper also takes a deeper look into the concept of knowledge and its role in both of the concepts under study. The aim of the paper is to find out the common factors and main differences of knowledge management and knowledge security. Common factors of the concepts include for example a close connection to strategic planning and the aim to codify important knowledge. Implications for the practitioners are presented and discussed.

**Keywords:** knowledge security, knowledge management

## **A Conceptual Model Approach to Manage and Audit Information Systems Security**

**Teresa Pereira<sup>1</sup> and Henrique Santos<sup>2</sup>**

<sup>1</sup>**Polytechnic Institute of Viana do Castelo, Valença, Portugal**

<sup>2</sup>**University of Minho, Guimarães, Portugal**

**Abstract:** Speed and accessibility operations promoted by information and communication technologies, particularly the Internet, leads organizations to become heavily dependent of their information systems. Further, the rapid technological advances have also created significant risks to organizations and government operations. The risks are expected to continue to escalate as new technologies and new Internet-enabled services emerge. As a result, the security strategies of these organizations need to evolve as well, in response to the evolving information security requirements. In short, there is a need for a proper information security management, within the context of the organization's structure, objectives and activities. One way to achieve this goal is to plan regular audits to evaluate the information systems security. The current available resources are typically guidelines and checklists, more or less linked to particular views. To address this issue, it was developed a framework based on a conceptual model approach. This solution introduces a new perspective to model information in security domain. It allows the description of the data semantics and enables to firm up and unify the concepts and terminology defined in the information security domain, based on the ISO/IEC\_JTC1 standards. This paper presents the preliminary stage of

the framework development, in particular, the adoption of the ontological approach for the information security management.

**Keywords:** information security management, information system security, information systems security auditing, audit, ontology, conceptual model

## **IST: Improved Steganography for Html**

**Khan Farhan Rafat and Muhammad Sher**  
**International Islamic University, Islamabad, Pakistan**

**Abstract:** Who could have thought that the digitization of electronic communication would unwittingly open gate for covert channel communication which is now being exploited for good as well as illicit motives by electronic and computer persons/agencies all over the world. Every now and then we come across new digitized ON and/or OFF-Line, information security products, enabling us to communicate without compromising our confidentiality, integrity and authorization. Among the various solutions proposed; Cryptography and Steganography having their origin from Greek, are the most promising. The purpose of cryptography is to eradicate the sense out of information thereby rendering it useless for an intruder. Steganography on the other hand, focuses on hiding the existence of information. These two, though opposite of each other, go well when used together as elaborated in the subsequent sections. This paper proposes an enhancement in existing steganographic techniques suggested and discussed respectively by Mohammad Shirali Shahreza (2005) 'A New Method for Steganography in HTML Files', In: Proceedings of *IETA Computer, Information, and Systems Sciences, and Engineering*, EIAE 2005, Springer, p. 247-251. and K. Bennett (2004), 'Linguistic Steganography: Survey, Analysis, and Robustness Concerns for Hiding Information in Text', Purdue University, CERIAS Tech. Report 2004-13, for hiding information inside HTML TAGs.

**Keywords:** steganography, steganalysis, covert channel, information hiding, data hiding, conceal

## **Proactive Cyber Initiative: An Expert System Framework**

**David Rohret**  
**Computer Sciences Corporation, Inc., San Antonio, USA**

**Abstract:** Cyber warfare is often depicted as pertaining only to malicious hacking, network attacks, denial of service attacks, data theft, and data manipulation. Only recently has cyber warfare been considered a major

component of the modern warfare battle space. But while resources are expended on tools development for defensive and offensive methodologies, they are rarely, if at all, combined with strategies and parallel capabilities that would provide military decision makers the ability to react to real-world scenarios in milliseconds rather than minutes or hours. With no clear framework encapsulating all necessary cyber warfare components, adversaries are able to use non-traditional means of cyber-attacks against targeted national interests with a low risk of retaliatory defensive measures being applied. Furthermore, the lack of a cohesive framework prevents a cyber-warfare commander from actively engaging the enemy by initiating an offensive cyber action or implementing an active cyber defense in real-time. Additionally, the rapidly changing cyber warfare environment is further complicated as more powerful open-source and publically available tools can be easily obtained and utilized by organizations and states once seen as incapable of conducting cyber warfare against more sophisticated nation states. If a nation state is to maintain a strategic advantage in protecting critical assets, infrastructure, commerce, and military operations, they must develop the capability to defend and dominate their cyberspace. Further amplifying the problem is an acute shortage of skilled computer scientist and network defense specialist able or willing to work for governments and militaries. Recent calls for increasing the size of cyber task forces have been met with scepticism as the demand greatly out-weighs the available human resources (Nakashima and Krebs, 2009). An approach for an offensive cyber initiative that includes cyber intelligence, trends and predictive analysis, tools development, integration of supporting technologies, continual reconnaissance, and implementation plans (integrated into offensive and defensive cyber frameworks), will be necessary to provide decision makers and planners the ability to incorporate cyber warfare actions into an overall concept of operations. This capability will allow action officers to implement cyber warfare in support of mission goals in the same manner air, sea, and ground actions are currently implemented. Central to this approach is a flexible and interchangeable offensive operations framework used to organize, coordinate, and integrate offensive technology, while reducing human error and providing the ability to align cyber actions with kinetic mission objectives. An operational prototype will implement a framework using technology from publically available and open-source tools that include intelligence collection, threat/target determination, custom and open-source weaponized exploits, covert infrastructures, and code obfuscation (anonymity). The offensive cyber framework, developed within expert systems, will support all facets and levels of cyber offensive, defensive, and covert actions. The goal of this paper is to develop an understanding for an advanced offensive cyber warfare framework that allows system control of hostile networks in support of national interests and military objectives,

regardless of an adversary's network topology, security counter-measures, and retaliatory capability.

**Keywords:** offensive cyber warfare, pro-active defense, expert system

## **Cyber Warfare: Virtual war Among Virtual Societies**

**Anthimos Alexander Tsirigotis**  
**Hellenic Air Force, Athens, Greece**

**Abstract:** The purpose of this paper is to offer for further discussion a view of cyber warfare which for some governments and military organisations, during last years, seems to be a point of serious concern. The core of the article is far away from presenting a monolithic militaristic analysis focusing on how cyber attacks are waged or what should be the military response to them. Instead, the focal point is to prove that in the 21<sup>st</sup> century the structure of societies is heading to a new model of order in which cyber warfare will constitute the war paradigm. Cyber warfare, as part of Information warfare, it is not conceived by governments as a real danger against the security of their societies even it has already shown its potentials at the recent attack against Estonia (2007). Defacements of governmental sites do not seem to have the same impact on societies as, for instance, life losses of air strikes, do have. The central analytical axis will be to examine past Military Revolutions in conjunction with the respective historical social trends proving that in each era, societies wage their wars in harmony with their system of values. This is the thesis of Military Revolution theory that will be concisely described and which examines how in early modern Europe changes in military organisation did fuel social reordering and vice versa. In the 21<sup>st</sup> century, respectively, networking of people around the world offers innovative ways not only for socializing but for every aspect of human activity to be expressed through them as well. Warfare, as society, is mainly based on the impeccable use of networks through which information flows undisturbed to every operational level: to the higher command echelon and to fighting squadrons, as well. This constitutes the kernel of Information warfare and which has already been implemented in real life battlefield heralding fundamental changes to war paradigm. Post modern military is already a reality and it is definitely in accordance with the general social trends of our century. Trying to foresee in what ways military organisation will be transformed we should first take a look of the future warriors. Young people pass a great deal of their day “surfing” into a virtual world rather than a real one. They are interlocutors in a worldwide chatting room of a society without borders, without limitations and with free information flow. Citizens of a virtual society with no or limited physical touch. In what way do virtual societies fight each other? Cyber

warfare may be the answer. Is it high time we resigned the idea of any other type of war other than cyber warfare? What are its potentials and where to draw the line? The virtual war lends credence to the theory of Clausewitz about war? These are some of the questions that this paper will try to reveal and to offer for further discussion.

**Keywords:** cyber warfare, military revolution, virtual society, virtual war

## **Novel Information Sharing Syntax for Data Sharing Between Police and Community Partners, Using Role-Based Security**

**Omar Uthmani<sup>1</sup>, William Buchanan<sup>1</sup>, Alistair Lawson<sup>1</sup>, Christoph Thuemmler<sup>1</sup>, Lu Fan<sup>1</sup>, Russell Scott<sup>2</sup>, Anne Lavery<sup>2</sup> and Chris Mooney<sup>3</sup>**

<sup>1</sup>Edinburgh Napier University, UK

<sup>2</sup>Scottish Police College, Kincardine, UK

<sup>3</sup>Glasgow Community & Safety Services, Glasgow, UK

**Abstract:** The exchange of information between the police and community partners forms a central aspect of effective community service provision. In the context of policing, a robust and timely communications mechanism is required between police agencies and community partner domains, including: Primary healthcare (such as a Family Physician or a General Practitioner); Secondary healthcare (such as hospitals); Social Services; Education; and Fire and Rescue services. Analyses of numerous criminal investigations have frequently highlighted the requirement for a robust information-sharing framework. This paper presents a novel syntax that supports information-sharing requests, within strict data-sharing policy definitions. Such requests may form the basis for any information-sharing agreement that can exist between the police and their community partners. It defines a role-based architecture, with partner domains, with a syntax for the effective and efficient information sharing, using SPoC (Single Point-of-Contact) agents to control information exchange. The application of policy definitions using rules within these SPoCs is inspired by network firewall rules and thus define information exchange permissions. These rules can be implemented by software filtering agents that act as information gateways between partner domains. Roles are exposed from each domain to give the rights to exchange information as defined within the policy definition. This work involves collaboration with the Scottish Police, as part of the Scottish Institute for Policing Research (SIPR), and aims to improve the safety of individuals by reducing risks to the community using enhanced information-sharing mechanisms.

**Keywords:** information sharing syntax; intelligence model; security policy implementation; role-based security; police and public services; community risks

# Practitioner Papers



## **BinThavro: Towards a Useful and Fast Tool for Goodware and Malware Analysis**

**Benjamin Caillat, Anthony Desnos and Robert Erra**  
**ESIEA, Paris, France**

**Abstract:** We present our tool *BinThavro*, which helps to solve the following general problem : given two programs, how can we compare them? More precisely, how can we understand the similarities, but also the dissimilarities between both files? The most difficult but the most interesting case seems to be the case of executable (binary) files and this problem has an important application: the malware analysis. A malware is one of the main tools used by information warfare warriors, "bad guys" commonly called "cyberwarriors". *Hélas*, there are so many new malwares that appears quite each day that we need *automatic* tools to make the analysis faster, and more sure. In the *Microsoft Security Intelligence Report* it is pointed out that, for the first half of the year 2009, around 116 million malicious samples were detected "in the wild" while this number was around 95 million in the second half of the year 2008. Of course, there does not exist 116 million of *dissimilar* malwares, a lot of them are clones, similar or quite similar. This proves clearly that the "malware industry" is flourishing, and it is an important arm for the cyberwarriors involded in the information warfare. But of course, a lot of "new" malwares share large portions of codes with existing and already known malwares (a lot of malwares contains small or large parts of code that has been *copied* from another). Here, *known* means *analyzed*, *i.e.* we have understood for example what the malware does, how it is programmed, how we can detect him with the help of a static signature in an antivirus software and so on. Why does someone wants to analyze a malware? There are (at least) three reasons: we want to understand how we can be protected against it, with or without a antirus software; or, we want to understand how we can modify to create a new variant (possibly with new functionalities for example); we want to "name" a new malware (see (Gheorgescu 2005)); So, at the first glance, any tool that can be used to analyze a malware can have bad consequences because it will probably be used also to create new malwares. Yes, but this is true for any new language, any new compiler etc. So, beyond the basic idea of searching for a signature of a malware, is there an interest to develop new of better tools for malware or goodware analysis? Yes, for at least two reasons: 1.a new view is emerging the last years: if we have better tools to analyze quickly new malwares that are variants of known malwares, the malwares programmers have to work harder (and so, hopefully, longer) to create new malwares that are difficult to analyze; 2.in the few last years, a new threat has appeared in the tools used for the information warfare:

*Targeted Malware Attacks*, i.e. malwares that are developed to attack a specific target. This is really a serious problem because the reaction of the AV community faced to a new malware depends a lot of the impact of this new malware. And there are so many new malwares that the analyze of new malwares is prioritized, resources has to be managed in a balance between the importance of the threats and the ability to analyze a lot of files. There are some reasons why this problem is interesting also for goodwares, for example: we want to detect plagiarism or copyright infringement (mostly for goodwares); we want to understand the evolution of a software (both for goodwares and malwares); we want to detect vulnerabilities in an old version by comparing the patched and unpatched versions (mostly for malwares) we want to detect redundancy into a software (mostly for goodwares). The malware analysis problem has clearly close relations with the clone detection problem and so, techniques for comparing goodware files can be used to compare malwares. We can of course also think to the *reversed* view: new techniques to compare malwares can be used to compare goodwares. For example, the last five years a lot of works has been done about the problem of the *dynamic analysis* of malwares; we can use these techniques of dynamic analysis to analyze goodwares. Another example is the visualization of a software to help its analyze: if you have such a tool, you can use it for goodwares or malwares. We are interested here to present what problems we have to develop a tool that could help to analyze goodwares and malwares: for goodwares: we will suppose we have a unique file or a few file to compare and analyze; for malwares: we will suppose we have a unknown malware and a large database of (already) known malwares, we want to understand how we can be protected against it (for example we want to ding a signature for AV softwares). We focus mainly on this work on the global *malware filtering* problem. Let us suppose we have: an unknown malware  $A$ , possibly new, this is our "target"; a (large) database of known malwares  $M = \{M_1, \dots, M_n\}$ ; our problem is : how can we choose quickly, from a set of known files  $\{M_1, \dots, M_n\}$ , the subset of the files the "most similar" to a target  $A$  ? We propose to use *filtering* tactics to select the better files of the malware set  $M$ . We propose to use two different but similar tactics, using the *Normalized Compression Distance* (NCD) for a first filtering tactic to filter the set  $M$  and the entropy for a second filtering tactic. We also use the NCD and the entropy at two different levels of granularity using the Control Flow Graphs (CFG) and the Call Graph (CG). With these tools we will define local filtering tactics and we will show how to use them to define our *global filtering strategy*. The tool *BinThavro* is not yet available, it is a set of tools, but *asap* we will likely make it available when we will have a nice GUI.

**Keywords:** malwares binaries comparison CFG algorithm

## Forensic and Software (UN) Obfuscation

Anthony Desnos and Eloi Vanderbéken  
ESIEA, France

**Abstract:** The computer security problem in a computer war is a more general problem, and actually, memory forensic and reverse engineering having growing usage in computer security, and allow to fight against malwares, but also to override the intellectual property of some software. Before doing the reverse engineering, you must be able to do forensic, to get information and data allowing to do an analysis with tools like IDA PRO [Hex-Rays], Olly [Oleh Yuschuk], Immunity Debugger [Immunity], but also with automatic software like BinDiff, BinAvi [Zynamics], or else Anubis [Iseclab] which is more specific to malware. The protections offered to protect software intellectual against these analysis can also be used for malicious software, and vice versa. It is therefore necessary to evaluate and quantify the various protections, allowing a ranking of these, and seeing on a scale if a protection ask to needs of a user. It has been shown mathematically that the total obfuscation is not possible [Barak, 2001], and a  $\tau$ -obfuscation [Beaucamps and Filiol, 2007] can be determined, but we must see this study in an operational context to qualify this formalization, and provide new protection systems based on software or materials techniques and that meet clearly a need, and respecting a time of protection sought. In a first part, we will explain briefly the state of the art of forensics' techniques, and we will subsequently illustrate techniques on Linux system for recovering and rebuilding process with a simple memory dump, because Linux system isn't generally evoke in forensic paper but it is necessary to know these methods. Then in a second part we discuss the problems arising from new programming languages like Java, then we propose an analyze of famous packers, and next we will do a simple quantification of obfuscation techniques (and therefore deobfuscation), and finally we will try to bring new ideas to protect software more effectively.

**Keywords:** forensic, memory, linux