

**Proceedings  
of the  
10th European Conference  
on Information Warfare and  
Security**

**The Institute of Cybernetics at the  
Tallinn University of Technology  
Tallinn, Estonia**

**7-8 July 2011**

Edited by  
Rain Ottis  
Cooperative Cyber Defence  
Centre of Excellence  
Tallinn, Estonia

Copyright The Authors, 2011. 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 Proceeding 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: 978-1-908272-07-2 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		<b>vii</b>	<b>iv</b>
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		<b>viii</b>	<b>v</b>
Biographies of contributing authors		<b>x</b>	<b>vi</b>
Legitimate Defenses Against Dangerous Archenemies. The Justifications by U.S. Presidents for the Initiation of Military Operations in the Persian Gulf and Kosovo, 1991-2003	<i>Kari Alenius</i>	1	1
Use of Compression Methods for Data Security Assurance	<i>Dominic Asamoah and William Oblitey</i>	1	6
Cyber Security: Time for Engagement and Debate	<i>Debi Ashenden</i>	2	11
This is not a Cyber war, its a...? Wikileaks, Anonymous and the Politics of Hegemony	<i>David Barnard-Wills</i>	3	17
Potential Threats of UAS Swarms and the Countermeasure's Need	<i>Laurent Beaudoin, Antoine Gademer, Loica Avanthey, Vincent Germain and Vincent Vittori</i>	4	24

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Developing Intelligence in the Field of Financing Terror - an Analytical Model of Anti-Terror Inter Agency and Cross Border Cooperation: The Security of Financial Systems Dimension	<i>Alexander Bligh</i>	4	31
A Secure Architecture for Electronic Ticketing Based on the Portuguese e-ID Card	<i>Paul Crocker and Vasco Nicolau</i>	5	38
Evaluation of the Armed Forces Websites of the European Countries	<i>Pedro Cunha, Parcídio Gonçalves, Vítor Sá, Sérgio Tenreiro de Magalhães and Miguel Pimenta</i>	6	50
Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security	<i>Christian Czosseck, Rain Ottis and Anna-Maria Talihärm</i>	7	57
An Usage-Centric Botnet Taxonomy	<i>Christian Czosseck and Karlis Podins</i>	8	65
User-Centric Information Security Systems - A Living lab Approach	<i>Moses Dlamini Jan Eloff, Marek Zielinski Jason Chuang<sup>1</sup> and Danie Smit</i>	9	73
Intrusion Detection Through Keystroke Dynamics	<i>João Ferreira, Henrique Santos and Bernardo Patrão</i>	9	81
The Computer Security of Public/Open Computer Spaces: Feedback of a Field Study in Europe	<i>Eric Filiol</i>	10	91
Perverting eMails: A new Dimension in Internet (in)Security	<i>Eric Filiol, Jonathan Dechaux and Jean-Paul Fizaine</i>	11	106

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Evaluating Cyber Security Awareness in South Africa	<i>Marthie Grobler, Joey Jansen van Vuuren and Jannie Zaaiman</i>	12	113
Missionaries of Peace – The Creation of the Italian Identity in the Representation of the Political Discussion in Favour of Italy’s Participation in the Iraq War in <i>Il Corriere della Sera</i>	<i>Marja Härmänmaa</i>	13	122
Thoughts of war Theorists on Information Operations	<i>Arto Hirvelä</i>	14	127
Live-Action Role-Play as a Scenario-Based Training Tool for Security and Emergency Services	<i>Sara Hjalmarsson</i>	14	132
Computer Games as the Representation of Military Information Operations – A Philosophical Description of Cyborgizing of Propaganda Warfare	<i>Aki-Mauri Huhtinen</i>	16	141
Information Security Culture or Information Safety Culture – What do Words Convey?	<i>Ilona Ilvonen</i>	17	148
Strategic Communication and Revolution in Military Affairs: Describing Actions and Effects	<i>Saara Jantunen</i>	18	155
A Case-Study on American Perspectives on Cyber and Security	<i>Saara Jantunen and Aki-Mauri Huhtinen</i>	18	163
Evolutionary Algorithms for Optimal Selection of Security Measures	<i>Jüri Kivimaa and Toomas Kirt</i>	19	172

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Botnet Detection: A Numerical and Heuristic Analysis	<i>Luís Mendonça and Henrique Santos</i>	20	185
Analysis and Modelling of Critical Infrastructure Systems	<i>Graeme Pye and Matthew Warren</i>	21	194
Modelling Relational Aspects of Critical Infrastructure Systems	<i>Graeme Pye and Matthew Warren</i>	21	202
A Study on Cyber Secured eGovernance in an Educational Institute: Performance and User Satisfaction	<i>Kasi Raju</i>	22	211
Steps towards Monitoring Cyberarms Compliance	<i>Neil Rowe, Simson Garfinkel, Robert Beverl, and Panayotis Yannakogeorgos</i>	22	221
Distributed Denial of Service Attacks as Threat Vectors to Economic Infrastructure: Motives, Estimated Losses and Defense Against the HTTP/1.1 GET and SYN Floods Nightmares	<i>Libor Sarga and Roman Jašek</i>	23	228
Legal Protection of Digital Information in the era of Information Warfare	<i>Małgorzata Skórzewska-Amberg</i>	24	237
Criteria for a Personal Information Security Agent	<i>Ewald Stieger and Rossouw von Solms</i>	25	245
International Criminal Cooperation in the Context of Cyber Incidents	<i>Anna-Maria Talihärm</i>	26	253
Methods for Detecting Important Events and Knowledge From Data Security Logs	<i>Risto Vaarandi</i>	27	261

<b>Paper Title</b>	<b>Author(s)</b>	<b>Guide Page</b>	<b>Page No.</b>
Locating the Enemy	<i>Marja Vuorinen</i>	28	267
Australian National Critical Infrastructure Protection: A Case Study	<i>Matthew Warren and Shona Leitch</i>	29	375
<b>PhD Papers</b>		<b>31</b>	<b>281</b>
Security Considerations for Virtual Platform Provisioning	<i>Mudassar Aslam and Christian Gehrman</i>	33	283
A Mobile and Quick Terrorism	<i>Anthony Desnos and Geoffroy Gueguen</i>	34	291
Regulatory Compliance to Ensure Information Security: Financial Supervision Perspective	<i>Andro Kull</i>	34	298
Behaviour Profiling for Transparent Authentication for Mobile Devices	<i>Fudong Li, Nathan Clarke, Maria Papadaki and Paul Dowland</i>	36	307
Description of a Practical Application of an Information Security Audit Framework	<i>Teresa Pereira and Henrique Santos</i>	37	315
Fight Over Images of the State Armed Forces and Private Security Contractors	<i>Mirva Salminen</i>	37	323
<b>Non Academics</b>		<b>39</b>	<b>331</b>
A Proposal for Domain Name System (DNS) Security Metrics Framework	<i>Andrea Rigoni and Salvatore Di Blasi</i>	41	333
<b>Work in progress</b>		<b>43</b>	<b>337</b>
Malicious Flash Crash Attacks by Quote Stuffing: This is the way the (Financial) World Could end	<i>Robert Erra</i>	45	339

<b>Posters</b>		<b>47</b>	
Assessment of Mission Risk; Role of Protection of Information and Communication Technology Resources	<i>Joobin Choobineh, Evan Anderson and Michael Grimaila</i>	49	
Constantly Evolving Cybercrime Forensic Challenges	<i>Abhaya Induruwa</i>	49	
Finding Patterns in the Alerts of Intrusion Detection Systems	<i>Francisco Ribeiro and Henrique Santos</i>	50	
<b>Presentation Only</b>		<b>53</b>	
The Image of the Afghan War Visual Strategic Communication Narratives of the Isaf-Operation	<i>Noora Kotilainen</i>	54	
Cloud-Based Shared Mental Model in Cyber Criminals	<i>Daniel Ching Wa Ng</i>	55	

## **Preface**

This year sees the 10th European Conference on Information Warfare and Security (ECIW 2011), which is hosted by the Institute of Cybernetics (IoC) at Tallinn University of Technology in collaboration with the Cooperative Cyber Defence Centre of Excellence (CCD COE) in Tallinn, Estonia. The Conference Chair is Vahur Kotkas from IoC and I am pleased to be the Programme Chair.

The Conference continues to bring together individuals working in the area of Information Warfare and Information Security in order to share knowledge and develop new ideas with their peers. The range of papers presented at the Conference will ensure two days of interesting discussions. The topics covered 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.

The opening keynote is given by Mr Raul Rebane from StratCom and the second day will be opened by Prof Enn Tyugu from CCD COE and IoC.

With an initial submission of 83 abstracts, after the double blind, peer review process there are 53 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.

I wish you a most interesting conference and an enjoyable stay in Estonia.

Rain Ottis, PhD  
July 2011

# Biographies of Conference Chairs, Programme Chairs and Keynote Speakers

## Conference Chair

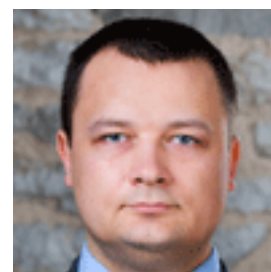


**Vahur Kotkas** is a Development Manager of the Institute of Cybernetics at Tallinn University of Technology, Tallinn, Estonia. His research and activities are mostly related to engineering, modeling and simulations where Knowledge- and Logic-Based techniques are developed and applied in order to achieve comfortable and efficient platforms for modeling and for simulations. During the past few years

Vahur has been active in Cyber Security related research under a contract with Estonian MoD to develop suitable tools for Cyber Defence.

## Programme Chair

Rain Ottis is a scientist at the Cooperative Cyber Defence Centre of Excellence. He previously served as a communications officer in the Estonian Defence Forces, focusing primarily on cyber defence training and awareness issues. He is a graduate of the United States Military Academy (BS, Computer Science) and Tallinn University of Technology (MSc, Informatics). He gained his PhD from Tallinn University of Technology, where his research focused on politically motivated cyber attack campaigns by non-state actors. Other research interests include cyber conflict and politically motivated cyber attacks



## Mini Track Chairs



**Debi Ashendeni** is a Senior Research Fellow within the Defence College of Management and Technology at Cranfield University. Prior to taking up this post she was a Managing Consultant within QinetiQ's Trusted Information Management Department (formerly the Defence Evaluation Research Agency). Specialising in information assurance in general, and risk assessment in particular, other specific

areas of interest include building trust for information sharing, governance processes for information assurance and information security awareness. Debi has worked extensively across government, defence and the finance sector as a consultant and her work concentrates on understanding the role of individuals in ensuring that security risks are mitigated. Debi has had a number of articles on information security published, presented at a range of conferences and has co-authored a book for Butterworth Heinemann 'Risk Management for Computer Security: Protecting Your Network & Information Assets'. Her current research examines the practice of information operations using discourse analysis.

**Eric Adrien Filiol** 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 and defense). 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 (especially computer virology and cryptanalysis) and cyber warfare with the attacker's mind.



**Dr. Marja Härmänmaa** is a university lecturer in Italian at the University of Helsinki. In addition to Critical Discourse Analyses and critical reading, her research interests include Italian literature and culture of the early 20th century.

**Professor, LTC(G.S), Aki Huhtinen, 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. He is also Docent of information security and information operations in the University of Tampere Technology. Aki works at the Department of Leadership and Military Pedagogy at the Finnish National Defence University.



**Saara Jantunen** has studied English language and culture in the University of Groningen in the Netherlands and English philology in the University of Helsinki. Her research interests are language & identity and military discourse. Jantunen currently works in education.

**Marja Vuorinen** is a social historian specializing in the study of elites and power within a theoretical framework of semiotics, text analysis and media studies. Marja holds a Doc. Soc. Sci. from the University of Helsinki





**Dr. Ken Webb** first career was in government special operations including command of strategic counter-terrorist, intelligence-gathering and unconventional warfare units. Operations in the international security field then followed where he developed a network of geostrategic relationships. Ken has completed an interdisciplinary PhD level government research project into enhancing national security from terrorist groups and has also been the counter-terrorism research leader for another Government initiative to identify and foster multi-disciplinary research into safeguarding countries from natural, human-caused, or accidental and terrorist acts. His exposure to and research experience is in special operations, information warfare, national security and emergencies, organised crime and counter-terrorism.

---

## Biographies of contributing authors (in alphabetical order)

**Kari Alenius** is Assistant Professor in the Department of History at the University Of Oulu, Finland. His research interests include the history of propaganda and mental images, the history of Estonia between the World Wars and the history of ethnic minorities.

**Dominic Asamoah** holds a 2009 M. Phil degree In Computer Science from the Kwame .Nkrumah University of Science and Technology. He is a lecturer of Computer Science at that University.

**Mudassar Aslam** is a researcher in Swedish Institute of Computer Science (SICS) since March 2010. He is also registered as a PhD student in Mälardalens University, Västerås. He has his Masters in Information and Communication Systems Security from KTH. Currently, he is working on Security and Trust establishment in virtualized environments and clouds.

**David Barnard-Wills** is a Research Fellow in the Department of Informatics and Sensors, Cranfield University. He has previously worked in the School of Political Science and International Studies, the University of Birmingham, and for the Parliamentary Office of Science and Technology. Research interests include the politics of technology, surveillance and privacy.

**Laurent Beaudoin** received a PhD from Télécom Paristech in image processing and remote sensing. He has worked in Ecole Supérieure d'Informatique d'Electronique et d'Automatique (ESIEA), a french engineering school, since 2001. He founded in 2004 the Image and Signal Processing R&D department (ATIS laboratory). His main research activities concern

Defence and Security, exploring robots (UAS, AUV), remote sensing and ICTs for persons with disabilities.

**Alexander Bligh PhD** (Columbia University, 1981) - Former advisor to the PM of Israel. President, *Strategic Objects*, an international strategic consulting firm. Former Chair of the Department of Political Science and Middle Eastern Studies, Ariel University Center, Israel, and visiting professor at Columbia University, U of Toronto, U of Notre Dame, etc.

**Jobin Choobineh** has a PhD from the University of Arizona. Research areas include Information Security, Management Information Systems, and Systems Analysis and Design. He has authored or been a coauthor of more than fifty (50) research articles. He is an Associate Editor of *INFORMS Journal on Computing* and serves on the editorial board of the *International Journal of Business Information Systems*.

**Paul Crocker** has a PhD in Mathematics from the University of Leeds, UK. After working in software development he joined the Computer Science Department at the University of Beira Interior, Portugal. His research and teaching interest include Parallel Computing, Security and Operating systems. He is a member of the Portuguese research Institute of Telecommunications.

**Christian Czosseck** is scientist at the CCD COE in Tallinn, Estonia. Serving in the German military for more than 12 years, he held several information assurance positions. Christian holds a M.Sc. equivalent in computer science and is currently PhD student at the Estonian Business School in Tallinn looking into cyber security and botnet related issues.

**Anthony Desnos** is currently a PhD Student at ESIEA (Operational Cryptology and Virology Laboratory) in Laval, France. He is involved in a number of open source security projects like Androguard. He had been speaker in various security/virology/information warfares conferences on different topics, including hack.lu, eicar, eciw, iawacs

**Moses Dlamini** received his BSc Computer Science and Mathematics at the University of Swaziland. He received his BSc Honours and MSc in Computer Science at the University of Pretoria, where he has now enrolled for a doctorate degree. Moses works at SAP Research Pretoria, as a PhD research associate.

**Salvatore Di Blasi** is an Information security professional with a solid track record in secure software design and development; he is a Certified Professional Engineer and qualified as a ISO 27001 Lead Auditor. He

currently works at Global Cyber Security Center (GCSEC) as an information security researcher.

**Robert Erra** is Professor of CS and Scientific Director of the Masters in Network & Information Security at ESIEA Paris and Laval. He is interested in developments of algorithms for information security, from cryptanalysis of asymmetric cryptography to malware analysis.

**João Ferreira** is an Informatics Engineering MSc student enthusiastic about Information Security, and the field of Biometric Security in particular. For his ongoing thesis, he is currently researching methods for strengthening the reliability of Data Centric Security solutions.

**Arto Hirvelä (Major)** is an instructor (leadership) in Research Group at the Finnish National Defence University. His research interests are information environment and information operations.

**Sara Hjalmarsson** is a security science honours student at Edith Cowan University of Perth, Western Australia. Her research revolves around the application of techniques from Live-Action Role-Play (LARP) to scenario-based training. Sara has 10 years experience as an educator, participant and organiser of LARP in Sweden and abroad. She currently resides in Sweden.

**Iloa Ilvonen** is a doctoral student at Tampere University of Technology, department of Business Information Management and Logistics. Her doctoral thesis topic is the management of knowledge security, and the thesis is due in 2012. She has published conference papers on information security management, knowledge management and relating topics since the year 2003.

**Abhaya Induruwa** PhD, FBCS, FIET, FIESL, HonFCSSL, CEng, CITP, Int. PEng, is the Programme Director for MSc Forensic Computing and MSc Cybercrime Forensics of the Canterbury Christ Church University, United Kingdom. His research interests include Pedagogic Issues in Cybercrime Forensics Education & Training. His PhD supervisions include the automation of mobile phone forensic investigation.

**Saara Jantunen** has studied English language and culture in the University of Groningen in the Netherlands and English philology in the University of Helsinki. Her research interests are language & identity and military discourse. Jantunen currently works in education.

**Saara Jantunen** has studied English language and culture in the University of Groningen in the Netherlands and English philology in the University of

Helsinki. Her research interests are language & identity and military discourse. Jantunen currently works in education.

**Toomas Kirt** is a post-doc researcher at University of Tartu. In 2007 he received a PhD from Tallinn University of Technology. Research interests include artificial intelligence, neural networks, pattern recognition and self-organization.

**Jyri Kivimaa** is a scientist at NATO Cooperative Cyber Defence Center of Excellence. He graduated from Tallinn University of Technology in 1972 and since 2009 he is a doctoral student at the Estonian Business School.

**Noora Kotilainen** (Master.Soc.Sci.) is a doctoral candidate at the Helsinki University social science history department, and is working as a visiting scholar at The Finnish Institute of International Affairs and as a researcher at Academy of Finland research project Ethics, Politics and Emergencies - Humanitarian Frame for Co-option and Collaboration in World Politics.

**Andro Kull** is a Doctoral student at the University of Tampere since 2005 and has graduated at University of Tartu in applied informatics and Tallinn University in IT management. Last academic conference experience is from annual Security Conference held in Last Vegas 2010. The practical side, he was linked to security issues, and more recently in relation to financial supervision. To ensure theoretical knowledge and practical experience, he has earned international certifications CISA, CISM, and ABCP.

**Fudong Li** is a PhD student within the Centre for Security, Communication and Network Research at the University of Plymouth, where he previously completed a MRes degree on the subject of Network Systems Engineering. His research interests are intrusion detection systems, mobile phone security, and user's behaviour within mobile device environment.

**Luís Costa Mendonça** is currently finishing the Master's degree in Communication Networks and Services Engineering (MERSCOM) in University of Minho. He has also been working in the IT industry for 12 year now in areas that span from software development to Datacenter design and maintenance. In the last years he has been digging deeper into network security.

**Daniel NG, Ching WA** started the career as computer programmer in 1990, and then progressing towards ICT Security, Computer Forensics, Financial Accounting and Auditing after millennium. Recently, he starts his PhD (Security & Forensics) in a UK reputable institute and The Hong Kong Daniel Polytechnic University, after earning a good stock options as a corporate director in a listed entity

**William Oblitey** holds a 1988 Ph. D. degree in Computer and Information Sciences from the University of Pittsburgh. He is a professor of Computer Science at the Indiana University of Pennsylvania.

**Kasi Raju** is a Technical Superintendent in the Department of Computer Science and Engineering, Indian Institute of Technology - Madras, India. Post graduation in Mathematics in Loyola college Madras (1981). Involved in Systems and Network administration. Recently acquired MBA( e-Governance ), PGD ( Cyber Laws ), PGD ( Cyber Security ) and DIP( Cyber Crime Prosecution and Defence ). Currently working in e-Governance, Cyber Forensics and Cyber Security.

**Francisco Ribeiro** is a student of Masters in Computer Engineering from the University of Minho. His specialization are "Network Engineering and Services" and "Encryption and Security of Information Systems". Also held a research fellowship in the field of bioinformatics.

**Andrea Rigoni** is Director General of the Global Cyber Security Center. With a working experience of 20 years in the Information Security field, he is an expert on Cyber Security, Threat Awareness, Information Sharing and Incident and Crisis Management. Member of different expert groups, and he is actively involved in many International and European initiatives.

**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). His main research interests are the modeling of deception, information security, surveillance systems, image processing, and data mining.

**Teresa Pereira** is an Assistant lecturer, Superior School of Business Studies, Polytechnic Institute of Viana do Castelo. PhD student, Department of Information Systems, University of Minho. Graduated in Mathematics and Computer Science, University of Minho (2002), obtained MSc degree in Information Technologies (pre-Bologna) 2006. 2002-2004 worked as researcher in OmniPaper project (IST-2001-32174) funded under 5th Fifth Framework Programme. Research interests: Semantic Web, Information management, ontologies, security audit, management information systems and information systems security.

**Vítor Sá** holds a five-year "licentiate" degree in Systems and Informatics Engineering and a Masters in Computer Science. Main activity has been teaching in higher education (currently at the Portuguese Catholic University). Lived for four years in Germany as a Guest Researcher at Fraunhofer IGD. He is doing his Ph.D. work in Biometric Authentication.

**Mirva Salminen** is a PhD student at the University of Tampere researching on outsourcing of the state's security functions. She has studied International Relations and Political Science at the University of Tampere, Military History and Strategy at the Finnish National Defence University, and Security Studies at Aberystwyth University in the United Kingdom.

**Henrique Dinis Santos** has a Degree in Electric and Electronic Engineering, University of Coimbra, Portugal, 1984, PhD in Computer Engineering, University of the Minho, Portugal. 1996. Currently Associate Professor, Information Systems Department, University of Minho, responsible for graduate/postgraduate courses. Supervision of several dissertations, in Information Security and Computer Architecture areas. President of a national Technical Committee (CT 136) related with information system security standards. 1990, under ERASMUS program, teaching at University of Bristol, UK, where recognized as University Academic staff.

**Libor Sarga** is a doctoral worker at Department of Statistics and Quantitative Methods, Faculty of Management and Economics, Tomas Bata University in Zlín. His dissertation work will focus on security and information technology applications and their effects on the virtualized economy. His personal interests include following technology, hardware and software trends, literature along with music.

**Malgorzata Skorzewska-Amberg** graduated from University of Warsaw (L.L.D) as well as Warsaw University of Technology (MSc IT). Appointed Assistant Professor 2009, Faculty of Law, Kozminski University Warsaw. For 17 years Senior IT Lecturer, Warsaw University of Technology. Research specialization combining two academic fields: digital data protection from legal as well as technical point of view.

**Ewald Stieger** is currently studying towards an MTech IT degree at the Nelson Mandela Metropolitan University in Port Elizabeth, South Africa. His subject of interest during the 4<sup>th</sup> year was Information Security and he decided to continue with research in that field. The research he is conducting is concerned with influencing users towards more secure.

**Anna-Maria Talihärm** is working in the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) Legal and Policy Branch, where her areas of research include European Union information society law, cyber terrorism and cyber crime. She is also currently striving for a PhD degree in Tartu University, specialising in legal aspects of cyber crime.

**Risto Vaarandi** received his PhD degree in Computer Engineering from Tallinn University of Technology, in June 2005. Since May 2006, he has been holding a position of a scientist at CCD CoE. Risto's research interests

include event correlation, data mining for event logs, network security, and system monitoring.

**Joey Jansen van Vuuren** Research Group Leader Cyber Defence for Scientific Research, CSIR South Africa, mainly involved in research for SANDF and Government sectors on Cyber Defence. MSc from UNISA and researcher for 25 years. Focuses research around national security and analysis of Cyber threat using non-quantitative modelling techniques. Actively involved in facilitating Cyber awareness programs in South Africa

**Matt Warren** is the Head of School at the School of Information System, 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.





# **Legitimate Defenses Against Dangerous Archenemies. The Justifications by U.S. Presidents for the Initiation of Military Operations in the Persian Gulf and Kosovo, 1991-2003**

**Kari Alenius**

**University of Oulu, Finland**

**Abstract:** This study will analyze how Presidents of the United States justified the initiation of military operations in three different cases: against Iraq in the Persian Gulf in the years 1991 and 2003 and against Yugoslavia/Serbia in Kosovo in 1999. It is evident that these justifications exploited the most classical elements of a general image of the enemy, and mainly only those. The justifications that Presidents offered the public for the initiation of military operations and the image that they attempted to portray of the enemy were thereby almost identical in all of the cases. Therefore, it can be concluded that speeches were for the most part built on a theoretical basis, and they did not necessarily have to be based on a reality of the actual country in question. Admittedly, similar features could be found in Iraqi and Serbian actions which it was possible to utilize in the construction of an image, but the identity of the image was first and foremost due to the identity of its use. The purpose was each time to justify why the United States took the offensive operation far beyond its own boundaries and without being attacked itself. In this case it was necessary to describe the actions, goals and the nature of the enemy in the most negative light, and one's own corresponding case was to be described in the best possible positive light. Only in this way was it possible to achieve sufficient justification for the initiation of one's own military operations. There was no room for bringing forth compromises or understanding the views of the other party.

**Keywords:** propaganda, rhetoric, enmity, United States, Iraq, Kosovo

---

## **Use of Compression Methods for Data Security Assurance**

**Dominic Asamoah<sup>1</sup> and William Oblitey<sup>2</sup>**

**<sup>1</sup>Kwame Nkrumah University of Science and Technology (KNUST),  
Ghana**

**<sup>2</sup>GhanaIndiana University of Pennsylvania (IUP), Indiana, USA**

**Abstract:** Organizations have documents that are not meant for public consumption. These documents provide the organizations with their competitive advantages. To maintain their respective competitive advantages and stay in business, the documents need to be secured and kept away from all unauthorized personnel. However, in this electronic age, protecting such

documents from copying or even browsing has become rather difficult. Computer technology has made copying so easy and yet difficult for people to become aware that such copying has been effected. To secure and protect such documents, various methods, including encryption techniques, have been employed. This paper suggests three methods that better ensure the security of such critical electronic data.

**Keywords:** authentication; critical document; encoding; encryption; intellectual property; security assurance

---

## **Cyber Security: Time for Engagement and Debate**

**Debi Ashenden**  
**Cranfield University, Swindon, UK**

**Abstract:** This paper explores the issue of public engagement with cyber security issues and positions it as a key factor in ensuring cyber security. Reported incidents of vigilante hacking are given as examples of the role of the public in cyber security. The case is made that in order to ensure public engagement and to manage the potential threat from vigilante hackers we need more inter-disciplinary academic research and better quality journalism. The role of the public and the link between the state and the public as mediated through cyberspace is used as a case study to set the context. To explore the issue of inter-disciplinary research a brief review of current academic literature is outlined. The topic of better quality journalism is examined using content analysis of newspaper reports focusing on the Stuxnet worm. The paper concludes that at a very basic level without increased academic debate or better quality journalism we will have little to inform our public engagement programme. One area to be addressed that emerges strongly through the research is the need for a lexicon and framework for discussing cyber security. This is necessary, at least at a high level, in order to conceptualise the problems and to support work that crosses academic disciplines. A suggested high level lexicon is presented together with a simple framework to facilitate engagement and debate.

**Keywords:** cyber security, debate, engagement, lexicon, framework

---

# **This is not a Cyber war, its a...? Wikileaks, Anonymous and the Politics of Hegemony**

**David Barnard-Wills**

**Cranfield University, Shrivenham, UK**

**Abstract:** This paper conducts a political theory analysis using the conflict, attacks and 'hactivism' surrounding the WikiLeaks organisations following recent diplomatic cable releases, as a case study to demonstrate the complexity of contemporary cyber conflict. This complexity is reflected in the motivations, identities and values of a multiplicity of (often non-state) actors. Already termed 'the first visible cyber war' this is no simple two-sided conflict (having already drawn in states, media organisations, banks and payments companies, and loose coalitions of individuals) and it is one which traditional metaphors and analogies of war may occlude as much as they reveal. International Relations and critical security studies have developed a range of approaches to international conflict that focus upon the identities, values and normative frameworks of participants. These interpretative movements offer a productive way of understanding cyber conflict, and this paper therefore demonstrates their application. The theory of securitization is used to demonstrate the politics inherent in the act of labelling a conflict 'war' and how this applies to the cyber environment. The paper makes use of Antonio Gramsci's concept of Hegemony, and Ernesto Laclau's concept of democratic demands. These models allow us to examine the contested construction of meaning in cyber conflict, a contestation which applies to the very terminology of the discussion. From this perspective, activities such as distributed denial of service attacks on Mastercard, Visa etc, can be interpreted as an attempt to establish a dominant discursive position and to construct a coalition of sentiment and meaning around a set of political issues – in this case freedom of speech and internet censorship in conflict with state and commercial models of online activity. As a struggle for hegemony rather than a 'war' we can understand that hegemony is never total, nor permanent. The cyber conflict is not 'won' but instead something that is perpetually worked out.

**Keywords:** WikiLeaks, cyberwar, cyber conflict, language, international relations

---

## **Potential Threats of UAS Swarms and the Countermeasure's Need**

**Laurent Beaudoin, Antoine Gademer, Loica Avanthey, Vincent Germain and Vincent Vittori**  
**ESIEA, ATIS Dept., Paris, France**

**Abstract:** The rising capabilities and growing accessibility of recent Unmanned Aerial Systems (UAS) widen the risks of success of a terrorists attack through the current aerial defence systems. We will examine first the complexity of the threats from a single unmanned vehicle, to a team of unmanned vehicles and finally to a swarm of unmanned vehicles (and any other association of these three combinations). Then, from an operational point of view, we will see that early detection of danger - a critical stage in the development of counter-attacks - has become very difficult because small unmanned vehicles like UASs precisely possess the ability to take off directly within the sphere of attack. The next stage, equally critical, consists in elaborating the response that best fits the attack. We distinguish three general categories of active and passive countermeasures: destruction, incapacitation and jamming of the enemy UASs. We will then study several possible countermeasures appropriate to the type of attack (enemy's formation: isolated drone, team, swarm; weapon type: bomb, kamikaze, bacteriological etc.). We first present countermeasures that are rather conventional (they usually come from air defense systems) and others specific to the UAS case. We will finish by a case study in which we will tackle the use of simplified physical models for calculating positions in real time in an optimized way in a UAS swarm under constraints.

**Keywords:** unmanned aerial system, swarms, countermeasure, terrorism

---

## **Developing Intelligence in the Field of Financing Terror - an Analytical Model of Anti-Terror Inter Agency and Cross Border Cooperation: The Security of Financial Systems Dimension**

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

**Abstract:** This paper presents and analyzes the major challenges facing counter-terrorism players and proposes some ways to counter the always-present intelligence deficits in the field of financing terrorism and the threat of financing terrorism. However, this is in no way a recipe. The proposals introduced here are intended to raise awareness and to suggest new

approaches, and thus encourage fresh thinking on old issues, in the hope that this will shed light on a narrow angle of the free world's war on terror. This paper is based on the paper "Security through Science", presented at the 2005 NATO sponsored "Advanced Research Workshop" at the University of Konstanz, Germany, and later published (Bligh 2006). I have developed this model for a variety of uses, the issue of "dirty money" among them. It attempts to map the needs and major obstacles, and to offer possible solutions based on the integration of an analytical model with the most advanced technological hardware and software available to national entities at the present time. The approach adopted here integrates an existing computerized platform, used by the U.S. and NATO, with the SWIFT system, along with an original analytical model, proposed here, that can be used by all system members. The system will operate along lines similar to current agreements governing the global and national use of credit cards and ATMs. Nevertheless, it is worth noting that the conflict between privacy and security is particularly acute here because the possession of financial assets is one of the most sensitive types of personal data possible. The paper is divided to the following sections: the current map of terror and intelligence as related to the financial dimension; the main challenges and a possible approach to a partial solution; and a proposed methodology for developing intelligence.

**Keywords:** terrorism, security, intelligence, banking, money laundering

---

## **A Secure Architecture for Electronic Ticketing Based on the Portuguese e-ID Card**

**Paul Crocker<sup>1,2</sup> and Vasco Nicolau<sup>1</sup>**

<sup>1</sup>**University of Beira Interior 6201-001 Covilhã, Portugal**

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

**Abstract:** The current state of the art for electronic ticketing is based around a mobile concept, where the diverse players involved, clients, payment agents, mobile operators and merchants, often have different and competing needs in terms of technology and very often security. In this paper we shall discuss and analyse the security of current electronic ticketing, payment, delivery and authenticating systems and show that today's new payment system has the mobile operator as a central player and the mobile phone, giving its undisputed role in today's society, as a central agent. We shall then propose and describe a new innovative architecture for electronic ticketing that makes use of the Portuguese national electronic identity (e-ID) card as a fundamental aspect of the security of the ticketing architecture. This architecture is combined with the latest technologies such as NFC enabled mobile handsets. We shall describe the potentialities of our architecture to

store electronic tickets, in the form of QR-Codes, in a secure way. We shall also how the proposed architecture permits flexible authenticating scenarios for the eTickets based on the different levels of security which may be required for any given scenario. Different scenarios range from low level and rapid authentication for mass transit system to the stronger authentication level required for the delivery of high value items and to the stringent security required at border controls. The flexibility and secure authentication is made available due to the cryptographic PIN and biometric authentication available on national and in particular Portuguese National e-ID cards.

**Keywords:** electronic ticketing, identification cards, security, mobile authentication, cryptographic signatures

---

## **Evaluation of the Armed Forces Websites of the European Countries**

**Pedro Cunha<sup>1</sup>, Parcídio Gonçalves<sup>1</sup>, Vítor Sá<sup>1</sup>, Sérgio Tenreiro de Magalhães<sup>1</sup> and Miguel Pimenta<sup>2</sup>**

<sup>1</sup>Universidade Católica Portuguesa, Braga, Portugal

<sup>2</sup>Regimento de Cavalaria 6, Exército Português, Braga, Portugal

**Abstract:** The armed forces are a critical component of the national security strategy of several European countries. Despite the peace that has succeeded the cold war, several armies, in peacetime, have elements recruited with promises of individual opportunities. The countries have two forms of recruitment of their troops: by volunteering or by mandatory incorporation. Following the trends of the modern world, interconnected in a network, it becomes essential to the institutions to mark their presence on the Internet. The Armed Forces in their various branches are no exception; there are numerous sites with relevant information, being used as a channel for dissemination and fundraising. Since young people represent a large share of the population using the Internet, and this is the target population for recruitment, it becomes mandatory to use the internet as a communication channel between them. It was carried out a qualitative study of all sites of European armed forces, and their branches, in order to assess their quality and differences. The approach focused on the evaluation of sites for their ability to inform, update, quantity and quality of content, service availability, use and visual attractiveness, and ease of communication. The study has also tried to verify if the countries with volunteer incorporation were producing websites with higher levels of quality, reflecting the need to invest in order to recruit. On the other hand, countries with compulsive incorporation could have lower investments in their websites, once the satisfaction of the need for staff is guaranteed. We considered 38 countries, with an initial usability study

where data about the characteristics considered important for proper construction of a website as well as for a good and easy relationship with the user of this type of site were collected. This research defined the parameters to evaluate the sites and groups were created with the parameters of the different areas of analysis of those sites. The evaluation shows that there are differences in quality of sites for each of the countries evaluated in terms of graphics, usability and content, and that where there is a greater difference between the countries is on the number of existing sites by country. It is clear that there are countries that invest strategically in this area while others do not. It was also clear that there is a difference between Eastern and Western Europe in the quality and investment made in the sites of their armed forces. Dividing the countries by their incorporation system, the differences are smaller, both in terms of number of sites for the military, either as to the average assessment of each scheme. In countries where the incorporation is mandatory, investment in independent sites for each branch has not been neglected for a considerable part of the countries, a little more than half. But it is in countries where recruitment is made on a voluntary basis that there are more sites for the different branches, which may indicate an existing competitiveness for staff recruitment.

**Keywords:** armed forces, websites, recruitment, Europe

---

## **Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security**

**Christian Czosseck, Rain Ottis and Anna-Maria Talihärm  
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia**

**Abstract:** At the time of the state-wide cyber attacks in 2007, Estonia was one of the most developed nations in Europe regarding the ubiquitous use of information and communication technology (ICT) in all aspects of the society. Relying on the Internet for conducting a wide range of business transactions was and still is common practice. Some of the relevant indicators include: 99% of all banking done via electronic means, over a hundred public e-services available and the first online parliamentary elections in the world. But naturally, the more a society depends on ICT, the more it becomes vulnerable to cyber attacks. Unlike other research on the Estonian incident, this case study shall not focus on the analysis of the events themselves. Instead it looks at Estonia's cyber security policy and subsequent changes made in response to the cyber attacks hitting Estonia in 2007. As such, the paper provides a comprehensive overview of the strategic, legal and organisational changes based on lessons learned by Estonia after the 2007 cyber attacks. The analysis provided herein is based on a review of national security

governing strategies, changes in the Estonia's legal framework and organisations with direct impact on cyber security. The paper discusses six important lessons learned and manifested in actual changes: each followed by a set of cyber security policy recommendations appealing to national security analysts as well as nation states developing their own cyber security strategy.

**Keywords:** Estonia, cyber attacks, lessons learned, strategy, legal framework, organisational changes

---

## **An Usage-Centric Botnet Taxonomy**

**Christian Czosseck and Karlis Podins**

**Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia**

**Abstract:** Botnets have been a recognized threat to computer security for several years. On the timeline of malware development, they can be seen as the latest evolutionary step. Criminals have taken advantage of this new technology and cyber crime has grown to become a serious and sophisticated problem which law enforcement still finds difficult to deal with. In the past few years we are witnessing a movement away from cyber crime. Nation states become the target of attacks as well as actively using botnets to project their own power in the political or military domain. To study the new and emerging cases of botnet usage we propose an usage-centric botnet taxonomy. Although there are already a number of botnet taxonomies published, most of them have a technical viewpoint and often consider cyber crime as the major driver to use botnets. While it may be true for now, we believe that such approach might not be holistic enough to describe the current and future developments. Besides the trend of specialized botnets being developed, the number of botnet users is increasing, with new motivations coming along. The taxonomy proposed in this paper takes a different viewpoint by focusing less on technical attributes than on the actors using botnets and the functionality requested by them. Major difference from existing research is that proposed taxonomy classifies instances of botnet use. Based on existing taxonomies, case studies of recent botnet incidents and cyber warfare doctrines of selected nation-states, we explore theoretical and already seen ways of botnet usage. We propose new classification of botnets based on their technological attributes, the users and the intended effects on the target to provide a holistic picture of the current situation. We also test the proposed taxonomy on seven instances of botnet use.

**Keywords:** botnets, taxonomy, incident categorization

---

## **User-Centric Information Security Systems - A Living lab Approach**

**Moses Dlamini<sup>1,2</sup>, Jan Eloff<sup>1,2</sup>, Marek Zielinski<sup>1,2</sup>, Jason Chuang<sup>1</sup> and Danie Smit<sup>1</sup>**

<sup>1</sup>SAP Research/Meraka UTD, Pretoria, South Africa

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

**Abstract:** For the past forty years, security experts have spent billions of dollars trying to improve security technologies. However, security systems are continually failing to protect end users' information systems and their information. Security experts claim that the end users are the weakest link in the security chain, and the end users claim that security features of systems are complex and full of gaping security vulnerabilities and they are an overhead that hinders their work. There is clearly a disjoint here. This paper introduces the concept of a Living Lab to help improve the current status and provide user-centric security systems.

**Keywords:** information security system, living lab, user-centric security

---

## **Intrusion Detection Through Keystroke Dynamics**

**João Ferreira<sup>1,2</sup>, Henrique Santos<sup>1</sup> and Bernardo Patrão<sup>2</sup>**

<sup>1</sup>University of Minho, Braga, Portugal

<sup>2</sup>Critical Software S.A., Coimbra, Portugal

**Abstract:** With the ever-increasing number of internal attacks towards information systems, Intrusion Detection Systems (IDSs) have become a necessary addition to the security policy of nearly every organization. An IDS is responsible for monitoring the events occurring in a computer system or network and analyzing them for signs of possible violation of security policies. At the Host level, current IDSs (Host-Based IDSs) typically perform file integrity checking, key file system objects monitoring, log analysis, among other functions capable of revealing malicious alterations of the system state. A major drawback of this approach is its natural limitation to detect "legal" operations when performed by an intruder after getting access through legitimate credentials, possibly causing considerable damage. Currently, authentication mechanisms are the only barrier to prevent these attacks. The most common means of authentication includes passwords, often used in conjunction with tokens or biometric readings, for increased security. However, these mechanisms do not offer continuous verification like IDSs do. One promising solution for this issue is to extend the IDS concept to the user authentication level, using *Anomaly-based detection* to distinguish benign

activity from malicious activity. Applying this concept with focus on the user requires tracking user profiles, leading us to biometric features. Keystroke Dynamics is a behavioral biometric technique that satisfies this goal. Besides being non-intrusive and inexpensive, keystroke analysis is also very attractive because typing patterns are continuously available after the authentication phase. The development of such IDS is the main motivation for the work described in this paper. In order to preserve the attractiveness of this technology, the solution will face a set of challenges. It should be transparent to the user, and therefore the execution (gathering typing rhythms, building user samples, computing comparison scores, and refining the stored profile through learning) will need to be performed without imposing restrictions to user input and without visual interface. It must also be generic concerning the keyboard type. Other important challenges come from the need to deal with unrestrained text input. Lastly, the security of captured data and the possibility of allowing future prevention measures by offering asynchronous detection capabilities are also considered.

**Keywords:** keystroke dynamics, biometrics, host-based intrusion detection, authentication, security, anomaly-based detection

---

## **The Computer Security of Public/Open Computer Spaces: Feedback of a Field Study in Europe**

**Eric Filiol**

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

**Abstract:** Many public places offer free or low-paying accesses to the Internet network: Internet cafes, hotels (especially high quality hotels). These places are experiencing a large attendance, especially near sites like railway stations, airports, international conference lounge....A number of questions then arises regarding the computer security aspects: what kind of users visit these places and use those internet accesses, what security risks do they face and especially how ill-intentioned actors (terrorists, organized crime, spies ...) could use those accesses to infringing users and possibly a company network. This article presents the results of a wide study conducted in Europe during the second half of 2010 in these "public/open Internet places". The report is alarming. Not only do users take an enormous risk to themselves but seriously jeopardize their businesses. This study reveals indeed that contrary to the popular belief – according to which most users of these sites are tourists or individuals only - the majority of users of these sites are professionals, employees of large firms who moreover are the custodians of high power or of high responsibility (CEO, CSO or CTO of large companies) or even of private data of third-party people (lawyers,

physicians...). Even worse, the lack of real security on all these Internet open-access can be exploited and perverted – after a suitable and necessary intelligence phase -- to conduct cyber attacks against companies, government offices and bodies, critical infrastructure...) thus causing an extreme prejudice.

**Keywords:** computer security, malware, intelligence gathering, computer network attack (CNA), computer network operation (CNO), computer terrorism

---

## **Perverting eMails: A new Dimension in Internet (in) Security**

**Eric Filiol, Jonathan Dechaux and Jean-Paul Fizaine**

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

**Abstract:** Electronic mail (or email) has not just changed the way we communicate in our daily life; it has transformed the way we do business today. Considered a convenient, powerful and a low cost tool, it is widely used to convey all kind of information including -unfortunately - sensitive or confidential information such as passwords, personal data, and private information. In recent times, two emerging technologies, referred to as the cloud computing and browser-based email technologies, have gained popularity among users and, along the way, also added a new significant layer of risk: It is common practice now from users to store their passwords into email folders and even worse, most of those browsers store and remember your password to open your email account automatically. Let's imagine the consequences of an attack launched by cybercriminals designed to resend and divert the original functionalities and features inherent to the browser for any malicious purpose, or worse - terrorist attempts. Let's take for example a US military officer operating in a country at war such as Afghanistan simply sending emails to his family to keep in touch with them. Whenever he sends an email, thousands of emails containing racial slurs against Muslim people are automatically sent to Afghan troops from his web account without him knowing it. The consequences of such an action would be unquestionably devastating. This above example, though fictitious, illustrates how efficient this kind of emails could be for both war propaganda and deception operations against US troops. Now imagine a company 's decision maker who daily exchanges large amounts of emails containing sensitive or confidential information within and outside his company ranging from trade secrets, contracts details, customer lists, research reports, financial information to staff's personal details. Modifying the browser-based email technology could enable any ill-intended person to wiretap and to eavesdrop any email directly at the browser's level to record any sent data

and to make them evade from the computer towards unscrupulous people. The collection of the daily flow of emails, both internally and externally, definitely provides a snapshot of a company's overall culture and is proving to be a powerful and efficient tool used for both industrial and economic espionage. As a last example, these technologies once modified, could be used to set up thousand of zombies in mail clients. For that purpose, a large number of email clients would simultaneously send thousands of mails to a single target – e.g. an email server -- to deny mail service for a limited period of time. We can easily imagine that this kind of attack launched on any stock exchange computer systems would entail damaging economic repercussions for the affected country and would probably plunge it into chaos for some time. In this paper, we will explain and show that email can be used as a ideal weapon for terrorism, cyber warfare, espionage, denial of service and can cripple all sectors of economy and nation states. We will address these issues both at the technical and operational level. In any case, we have considered systems with the most restricted user's privileges, but making those attacks really easy and powerful.

**Keywords:** eMail, terrorism, cyber-attack, espionage, email client, browsers, cyber warfare

---

## **Evaluating Cyber Security Awareness in South Africa**

**Marthie Grobler<sup>1</sup>, Joey Jansen van Vuuren<sup>1</sup> and Jannie Zaaiman<sup>2</sup>**

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

**<sup>2</sup>University of Venda, South Africa**

**Abstract:** In many ways, the internet and cyber world is a dangerous place where innocent users can inadvertently fall prey to shrewd cyber criminals. These dangers, combined with a large portion of the South African population that has not had regular and sustained exposure to technology and broadband internet access, expose local communities to cyber threats. Research done by the Council for Scientific and Industrial Research and the University of Venda shows that these local communities are not empowered to deal with these threats. To prevent innocent internet users from becoming victims of cyber attacks, an intensive awareness campaign is planned to educate novice internet and technology users with regard to basic security. The motivation for this awareness project is to educate all South Africans using the internet, in an attempt to strengthen the awareness level concerning the South African network - if there are local communities that are not properly educated, their technology devices may remain unprotected. This may leave the South African internet infrastructure vulnerable to attacks, posing a severe threat to national security. In this specific project, national

security will be promoted through awareness training focusing on the newly released broadband capability and knowledge transfer within rural communities. To evaluate the current level of cyber security awareness, a series of exploratory surveys have been distributed to less technologically resourced entities in rural and deep rural communities within South Africa. By analysing the results of the surveys, it is possible to benchmark the current level of awareness. These observations can then be extrapolated to the larger group of rural South African communities. The next stage of the awareness evaluation project is to develop cyber security awareness training modules for the local communities in their native tongue, aimed to improve the current level of awareness. This paper discusses the preparation, evaluation and training of South African rural communities with regard to cyber security awareness. Due to the networked nature of the internet, the level of awareness has an influencing impact on the global community. Thus, to ensure a safely protected South African network, it is necessary to target the communities that can inadvertently leave the network vulnerable.

**Keywords:** cyber security, awareness, rural communities, broadband, training, South Africa

---

## **Missionaries of Peace – The Creation of the Italian Identity in the Representation of the Political Discussion in Favour of Italy’s Participation in the Iraq War in *Il Corriere della Sera***

**Marja Härmänmaa**  
**University of Helsinki, Finland**

**Abstract:** Linguistics is not a traditional method used in the security studies. However, today’s world, and the information society are ever more based on texts and images. Also, both the sense of security and a threat are produced with language at the first place. For this reason, the study of a discourse used in a conflict is of vital importance. The present paper will deal with the political debate in favour of Italy’s participation in the Iraq war in the spring of 2003, as it is represented in one of Italy’s most important newspapers, *Il Corriere della Sera*. In using the term ‘representation’ I mean the interpretation of a given phenomenon with language. According to the method of critical linguistics elaborated by Roger Fowler, Robert Hodge and Gunther Kress, and based on the functional grammar of M.A.K. Halliday, I shall analyse the vocabulary and naming of different elements related to warfare, and transitivity; I will examine the choice of agents and affected participants and types of predicates to which they are related, as well as the argumentation strategies. In conclusion, I shall show how the representation of the Iraq war contributes to the creation of and/or emphasis on a specific national Italian identity.

**Keywords:** Italy's national identity; Iraq war; discourse analyses; political discourse; media discourse; right-wing coalition

---

## **Thoughts of war Theorists on Information Operations**

**Arto Hirvelä**

**National Defence University, Helsinki, Finland**

**Abstract:** Information operations (INFO OPS) increase in value as a means to reach ends in wars and lesser crises. Nowadays, the effectiveness of information operations depends on knowledge and the control of all of its different aspects as well as on the ability to utilize superior technology. Not all methods of INFO OPS require a significant technological advantage, nor are they generated by it even though a great many of the vulnerabilities are based on technology. Even some ancient war theorists have written about the value of some INFO OPS methods, e.g., psychological operations and military deception. Even though psychological operations as such were not included in war plans in the age of the war theorists covered in this article due to a lack of media, proper means and the slowness of communication, every theorist acknowledged the value of psychological operations. Revolution in military affairs (RMA) has been discussed at length by military researchers. INFO OPS is one of the concepts been used to rationalize RMA. Consequently the development of INFO OPS must be scrutinised. In this article the thoughts of war theorists Sun Tzu, Flavius Vegetius Renatus, Maurice de Saxe, Napoleon Bonaparte, Carl von Clausewitz and Sir Basil Liddell Hart are analyzed from viewpoint of various aspects of INFO OPS. The analysis concentrates on psychological operations, on military deception and on operations security. The analysis is based on a loose framework of content analysis.

**Keywords:** information operations, psychological operations, military deception, operations security, war theorist

---

## **Live-Action Role-Play as a Scenario-Based Training Tool for Security and Emergency Services**

**Sara Hjalmarsson**

**Edith Cowan University, Joondalup, Western Australia**

**Abstract:** Appropriate training and knowledge development is highly relevant to leaders and security professionals in the fields of information warfare and counter-terrorism. Scenario-based training methodology has a long history among military, law enforcement, emergency services and the private sector.

It is recognised as an effective method for preparing leaders to make critical decisions under pressure. Over time, several models have been developed to illustrate its components and characteristics. Live-Action Role-Play (LARP) has been defined as a unique art form that, like scenario-based training, can only be experienced as it is being created. It is an international phenomenon with a diverse range of styles and characteristics. The current leading-edge developments occur in the Nordic countries (Sweden, Denmark, Finland and Norway). Although LARP is primarily used for entertaining games, the art form bears significant resemblance to scenario-based training and could be adapted for authentic tasking exercises. LARP contrasts with scenario-based training in its use of persona within a variable narrative engine and a context that includes many layers of complexity. Educational Live-Action Role-Play, known as Edu-LARP, has been integrated into the Danish school system via Østerskov Efterskole, a boarding school for students aged 14-17 that follows the Danish national curriculum. LARP participants are already being used in training exercises for emergency services due to their dynamic improvisation skills and cost-effectiveness. Experienced organisers and participants could contribute their ability to generate scenarios, work with uncertainty and "think like the enemy, without becoming the enemy." to the design and execution of training exercises. Additionally, they could contribute to scenario generation for scenarios involving a high level of uncertainty, such as terrorist attacks and critical infrastructure incidents. LARP events themselves could also be adapted to the training needs and attributes of the audience, creating training that fully engages the trainee and results in improved learning outcomes. As in the case of scenario-based training, the use of LARP, LARP participants and LARP organisers must be implemented appropriately for them to be effective. This implies, for example, that participants and organisers must be experienced. It also implies that LARP used for training purposes would demand an appropriate narrative engine, educational framework and level of complexity suitable to the audience. Although this paper identifies that there is significant potential in the LARP art form, it also recommends that further research be conducted to explore the relevance of different styles, aspects relating to effective implementation and possible other uses of the art form.

**Keywords** authentic tasking, critical infrastructure protection, scenario generation, scenario-based training, live-action role-play, edu-LARP

---

# Computer Games as the Representation of Military Information Operations – A Philosophical Description of Cyborgizing of Propaganda Warfare

Aki-Mauri Huhtinen

Finnish National Defence University, Finland

**Abstract:** The history of combat is primarily the history of radically changing fields of perception. In other words, war consists not so much of scoring territorial, economic or other material victories but of appropriating the immateriality of perceptual field. The function of the eye has become the function of the weapons (Virilio 1989; 2009). To understand information age warfare we have to understand the concept of representation as a part of our process of violence. The idea of information warfare or an information operation is based on the process where the physical target is no longer destroyed with the kinetic systems, but the process where the non-kinetic systems, like information, scan the symbols-semiotics networks. Today, particularly the advanced mobile technology, the Internet and the entertainment industry immensely exploit the experiences from different wars and conflicts for example as ideas of computer games. In return the military industrial complex represents its own language for example in the concept of information operations with the help of applications particularly rising from the entertainment industry. The roles of Hector and Achilles, the teachings of Jomini and Clausewitz have an effect in the background of games and gaming. Opposite to Clausewitz's thinking, Jomini took the view that the amount of force deployed should be kept to the minimum in order to lower casualties and that war was a science, not an art. The most central genres in gaming are "strategy", "adventure", "shooter", "sports", "simulation", "music", "role playing" and "puzzle". All of these are related to warfare one way or another. Another interesting fact is that in the 1950's the first computer games were mathematic strategy based games that had been developed in universities (Czosseck 2009; Peltoniemi 2009).

**Keywords:** computer games, decision making, information operations, propaganda, representation

---

# Information Security Culture or Information Safety Culture – What do Words Convey?

**Ilona Ilvonen**

**Tampere University of Technology, Tampere, Finland**

**Abstract:** In the contemporary world of constantly changing information threats, information security culture is a concept that many organizations should emphasize on. Many threats cannot be countered only with sophisticated technical equipment. Instead, the attitudes and actions of employees gain significance each day, be the threat an urge to leak company confidential documents to Wikileaks or to competitors, or willingness to help a "colleague" with an unconventional request. Information security culture is a concept widely accepted in the field of information security research. It refers to the dominant understanding of how information security principles are manifested in the daily operations of a company. The culture implies what kind of behaviour of the employees is acceptable and encouraged. Literature about information security almost non-exceptionally uses the word security. However, in the field of organizational safety culture, the word security has little use. What is different? Is preventing human or material casualties really fundamentally different from preventing information casualties? This paper is triggered by the curiosity of how different literature streams discuss culture, be it called safety culture or security culture. Also the differences in approaches to security and safety are analysed. The term safety includes both the perspective of an object being protected from threats and the perspective of that object not causing threats. The term security includes only the perspective of an object being protected from threats. It is interesting to note, that both the words safety and security appear in the definitions for the term security. In information security the focus is for many organizations on the threats that come from outside the organization. This seems to justify the use of the word security. However, in many cases the biggest threats to the information of an organization come from inside the organization. Also, many organizations state that the information of customers is the most valuable to them and compromising customer information would not only harm the organization itself, but also its stakeholders. This would justify the use of the word safety in connection with information. This paper presents a literature review. The outcome of this paper is an understanding of the differences and similarities of the concepts under study. Discussion on the meaning of information security culture and implications to companies are presented.

**Keywords:** Information security, security, safety, information security culture, concept analysis, meanings

---

## **Strategic Communication and Revolution in Military Affairs: Describing Actions and Effects**

**Saara Jantunen**

**National Defence University, Helsinki, Finland**

**Abstract:** Changes in the concept of war are reflected by descriptions of military action. This article introduces a parameter system for analyzing strategic communication, which points out the division of military communication into tactical-operational and strategic levels. The system includes the parameter of legitimacy - whether an action is legitimate warfare or not. Second, it contains the good/bad parameter, which is manifested by the old tradition of glorification and demonization in war rhetoric. The focus of this paper is on discussing the third parameter: the exclusive parameter. It determines whether certain behavior is exclusive for 'us' or 'the other', and is often our only cue to deciding what is strategic communication, and functions on the strategic level. This approach links linguistics to strategy studies.

**Keywords:** strategic communication, linguistics, RMA

---

## **A Case-Study on American Perspectives on Cyber and Security**

**Saara Jantunen and Aki-Mauri Huhtinen**

**National Defence University, Finland**

**Abstract:** In 2009, the Cybersecurity Act of 2009 was introduced to U.S. Congress while the media were reporting about China's role in the Ghostnet-network. In 2010, WikiLeaks and selected newspapers published confidential documents, stirring up a cybersecurity debate. This article discusses these narratives in the context of securitization. The methodology consists of linguistic theory, namely the systemic functional language theory, and the securitization theory of the Copenhagen School. The analysis realizes as examination of the structures and evaluations of the action descriptions referring to the threat. As a result we can see that cyber discourse is a synonym to threat discourse. The agenda of cyber discourse is not purely about security, but is a reflection of the battle over cyber authority and the question of its status as a battle space.

**Keywords:** cyber, securitization, strategic communication, linguistics

---

# Evolutionary Algorithms for Optimal Selection of Security Measures

Jüri Kivimaa<sup>1</sup> and Toomas Kirt<sup>2</sup>

<sup>1</sup>Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

<sup>2</sup>University of Tartu, Tallinn, Estonia,

**Abstract:** A very important issue in IT Security or Cyber Security management is to provide cost-efficient security measures to achieve needed or required security goals (mainly CIA - Confidentiality, Integrity, Availability levels). For providing an optimal solution an optimization task with two goals have to be solved – to minimize needed resources and to maximize achievable security. The computational complexity of the optimization task is very high. In previous work a matrix based security model and an optimization framework based on the Pareto optimality and the discrete dynamic programming method has been used. But that solution has a quite important imperfection – there was required independence between security activity areas. That is not appropriate for IT security, as this solution does not follow the quite important principle in IT security – security is like a chain that is only as strong as the weakest link of layered security or defence in depth. The evolutionary optimization, as an alternative optimization tool, removed the independence restriction of the matrix based security model and the dynamic optimization method, but the first implementation of it was slightly slower than the other methods. For improving the performance of the evolutionary optimization we have performed a meta-level optimization of parameters of the algorithm and as a result the speed of optimization is comparable to other optimization techniques. As the evolutionary optimization is independent for all possible budget levels it lead to possibility to use a graph based security model. The graph based security model is a new and dynamical framework for security management. This paper presents how implementation of an evolutionary optimization technique removed the restrictions of independence of security measures and lead to implementation of an efficient graph based security model.

**Keywords:** graded security model, information security metrics, evolutionary optimization

---

# **Botnet Detection: A Numerical and Heuristic Analysis**

**Luís Mendonça and Henrique Santos**  
**Universidade do Minho, Braga, Portugal**

**Abstract:** Internet cyber criminality has changed its ways since the old days where attacks were greatly motivated by recognition and glory. A new era of cyber criminals are on the move. Real armies of robots (bots) swarm the internet perpetrating precise, objective and coordinated attacks on individuals and organizations. Many of these bots are now coordinated by real cybercrime organizations in an almost open-source driven development, which results in the proliferation of many bot variants with refined capabilities and increased detection complexity. Economical and reputation damages are difficult to quantify but the scale is widening. It's up to one's own imagination to figure out how much was lost in April of 2007 when Estonia suffered the well known distributed attack on its internet country-wide infrastructure. Among the techniques available to mitigate this threat, botnet detection emerges as a relevant solution. This technology has also evolved in recent years but it is still far from a definitive solution. New techniques, constantly appearing, in areas such as host infection, deployment, maintenance, control and dissimulation of bots are constantly changing the detection vectors thought and developed. In that way, research and implementation of anomaly-based botnet detection systems is fundamental to pinpoint and track the continuously changing botnets and clones, which are impossible to identify by simple signature-based systems. This paper presents the studies and tests made to define an effective set of traffic parameters capable of modeling both normal and abnormal activity of networks, focusing in botnet activity detection through behavior, numerical and heuristic modeling. Different types of botnets (IRC, P2P, HTTP, fast-flux among others) are initially analyzed followed by the study of some existing detection techniques and tools like Honeynet, Botsniffer and Botminner. Following this initial study, numerical and heuristic aspects of both normal and bot traffic are investigated. Finally, a set of traffic parameters is proposed aiming fast and precise botnet detection, with low false positive rate.

**Keywords:** Botnet detection, anomaly-based, heuristics, numerical, behavior

---

## **Analysis and Modelling of Critical Infrastructure Systems**

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

**Abstract:** The increasing complexity and interconnectedness of critical infrastructure systems, including the information systems and communication networks that support their existence and functionality, poses questions and challenges. Particularly, in terms of modelling and analysis of the security, survivability and ultimately reliability and continued availability of critical infrastructure systems and the services they deliver to modern society. The focus of this research enquiry is with regard to critiquing and modelling critical infrastructure systems. There are numerous systems analyse and modelling approaches that outline any number of differing methodological approaches, each with their own characteristics, expertise, strengths and weaknesses. The intention of this research is to investigate the merit of applying a ‘softer’ approach to critical infrastructure system security analysis and modelling that broadly views the systems in holistic terms, including their relationships with other systems. The intention is not to discuss or criticise existing research applying quantitative approaches, but to discuss a ‘softer’ system analysis and modelling approach in a security context that is adaptable to analysis modelling of critical infrastructure systems.

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

---

## **Modelling Relational Aspects of Critical Infrastructure Systems**

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

**Abstract:** The relational aspects for critical infrastructure systems are not readily quantifiable as there are numerous variability’s and system dynamics that lack uniformity and are difficult to quantify. Notwithstanding this, there is a large body of existing research that is founded in the area of quantitative analysis of critical infrastructure networks, their system relationships and the resilience of these networks. However, the focus of this research is to investigate the aspect of taking a different, more generalised and holistic system perspective approach. This is to suggest that that through applying network theory and taking a ‘soft’ system-like modelling approach that this offers an alternative approach to viewing and modelling critical infrastructure system relational aspects that warrants further enquiry.

**Keywords:** critical infrastructure, dependency relationships, systems modelling

---

# **A Study on Cyber Secured eGovernance in an Educational Institute: Performance and User Satisfaction**

**Kasi Raju**  
**IIT Madras, Chennai, India**

**Abstract:** It is widely acknowledged that eGovernance can be immensely useful in the efficiency of the functioning of the government and improving citizen service delivery. There are many areas of concern where the performance of eGovernance can be improved. A centralized security management system is installed for the secured access of the eGovernance service. The eGovernance approach will enable governments to achieve efficiency gains and improve service delivery levels, raise citizen satisfaction with government services, and enhance quality of life of citizens. This study attempts to find the performance and user satisfaction with eGovernance implemented in an educational institute. Further, the concentration of the analysis is to find what other areas can be brought under the eGovernance system. Studies have been made about the existing security measures deployed. From these studies, it was found that only computer science department students were aware of cyber crime and cyber security. Avoiding paperwork, 24x7 access and transparency were pointed out as advantages in the eGovernance system. Many respondents expressed concern about the security of their information both in transit and as well as in the databases of the eGovernance information servers. The aim of this study is to find the performance expectancy and evaluate user satisfaction in an eGovernance system and to provide secured eGovernance services by hardening the cyber infrastructures.

**Keywords:** eGovernance, cyber crime, cyber warfare, cyber security, stuxnet, DDOS, BAR,DCC,stratagem

---

## **Steps towards Monitoring Cyberarms Compliance**

**Neil Rowe<sup>1</sup>, Simson Garfinkel<sup>1</sup>, Robert Beverly<sup>1</sup>, and Panayotis Yannakogeorgos<sup>2</sup>**

**<sup>1</sup>U.S. Naval Postgraduate School, Monterey, USA**

**<sup>2</sup>Air Force Research Institute, Maxwell AFB, USA**

**Abstract:** Cyberweapons are difficult weapons to control and police. Nonetheless, technology is becoming available that can help. We propose here the underlying technology necessary to support cyberarms agreements. Cyberweapons usage can be distinguished from other malicious Internet traffic in that they are aimed precisely at targets which we can often predict in

advance and can monitor. Unlike cybercriminals, cyberweapons use will have political goals, and thus attackers will likely not try hard to conceal themselves. Furthermore, cyberweapons are temperamental weapons that depend on flaws in software, and flaws can get fixed. This means that cyberweapons testing will be seen before a serious attack. As well, we may be able to find evidence of cyberweapons on computers seized during or after hostilities since cyberweapons have important differences from other software and are difficult to conceal on their development platforms. Recent advances in quick methods for assessing the contents of a disk drive can be used to rule out irrelevant data quickly. We also discuss methods for making cyberweapons more responsible by attribution and reversibility, and we discuss the kinds of international agreements we need to control them.

**Keywords:** cyberweapons, cyberattacks, agreements, monitoring, forensics, reversibility

---

## **Distributed Denial of Service Attacks as Threat Vectors to Economic Infrastructure: Motives, Estimated Losses and Defense Against the HTTP/1.1 GET and SYN Floods Nightmares**

**Libor Sarga and Roman Jašek**  
**Tomas Bata University in Zlin, Czech Republic**

**Abstract:** With the number of nodes in the Internet's backbone networks rising exponentially the possibility of emergence of entities exhibiting outwardly hostile intents has been steadily increasing. The cyberspace is fittingly termed "the no man's land" because of an unprecedented growth pattern and lackluster control mechanisms. Distributed Denial of Service (DDoS) attacks take advantage of the current situation and primarily aim at destabilizing or severely limiting usability of infrastructure to the end-users in part or whole. A typical DDoS incursion exploiting heterogeneous base of personal computers consists of two phases: insertion of predefined set of instructions into the host systems via either self-propagating or non-reproducing malware and simultaneous execution of repeating queries to a destination unit. Generally targeted and deployed to impede functionality of a single or multiple servers with similar properties and utilizing substantial resources with little to no discernible selection criteria, DDoSes poses a significant threat. Moreover, effective and efficient countermeasures require experience, precision, speed, operational awareness, appropriate security protocols summarizing and alleviating potential consequences in case of failure to contain as well as proactive detection algorithms in place. Global response instruments (batch filtering, temporary IP address blacklisting) are

only suitable for SYN floods, whereas during GET DDoS the same tools can't be used due to presence of legitimate incoming requests. The article scrutinizes methodology and policies currently in effect as a part of Critical Infrastructure Protection initiatives. The examination allows to outline procedural decision-making trees in the event of a DDoS violation while maintaining predefined and consistent quality of service level. Furthermore, rationale of perpetrators' motives to instigate the attacks are hypothesized with preferential focus on economic infrastructure components. These hubs of virtualized economy are detailed and target selection probabilities in tactical and strategic perspectives are identified based on known facts. Financial losses, worst case scenarios and social repercussions following a successful intrusion are also investigated by means of inference from successful DDoS insurgences.

**Keywords:** distributed denial of service, economic infrastructure, potential losses, distributed attacks, network security, economic hubs, business continuity assurance, attack vectors analysis, botnet recruitment

---

## **Legal Protection of Digital Information in the era of Information Warfare**

**Małgorzata Skórzewska-Amberg**  
**Kozminski University, Warsaw, Poland**

**Abstract:** The danger of uncontrolled use of computers and computer networks has begun to be noticed in the last few years. Criminal acts committed in networks with the use of networks and against networks, reach beyond national borders. Since the 1990s, when the United Nations (UN) recognized computer violation as a form of transborder crime, profits originating in computer crime have surpassed those from drug trade. Organized crime is adapting to the environment of advanced technology, using thousands of computer networks to commit crimes on a global scale. Openness and anonymity is the strength of the Internet, but remains at the same time its greatest weakness. Among the network users, the group which aims at undesired or even unlawful accessing, distributing and exchanging information is growing. Technical solutions in information security have to be supported by demands to follow the rules of relevant procedures – assured through legal state obligations and sanctions in case of violation of such rules. To translate the language used by modern technology into proper legal language and catching behaviour seemingly unimportant or of minor consequence, but causing major damage, turned out to be most difficult. It is hence of great significance to adopt laws covering as much as possible of cyberspace behaviour. One of the most effective methods of securing digital

information is concealing it with the use of cryptography. It is true that communication using concealed information protects privacy and secrecy of mails to a high degree, but renders at the same time considerably more difficult accessing to information in cases when common good demands breaking such secrecy. Such procedures are most often carefully described and rigorously regulated by law since they interfere with the sensitive question of privacy of citizens. There is nevertheless still a need to specify i.a. how to use available cryptographic tools in order to access content of cryptographically concealed transmission without having access to the cryptographic keys. All efforts to exercise control over the Internet create controversy, raising questions about freedom of speech, stirring up protests about censorship, calling in question the intrusion of state authorities upon the private sphere of network users. At the same time, more countries introduce legal instruments of decree and prohibition in order to prevent law violation, something the Internet facilitates or even makes possible. In times of terrorism threats, efforts are intensified aiming at introducing measures which allow certain degree of control over the virtual space. It certainly requires a balance between the necessity of security regarding citizens and the need to guarantee their rights.

**Keywords:** computer network, legal interception, unauthorized access, cybercrime, anonymity, cryptography

---

## **Criteria for a Personal Information Security Agent**

**Ewald Stieger and Rossouw von Solms**

**Nelson Mandela Metropolitan University, Port Elizabeth, South Africa**

**Abstract:** Today's economy depends on the secure flow of information within and across organizations and information security is an issue of vital importance. Information security ensures business continuity and minimizes business damage by preventing and reducing the impact of security incidents. However, information security efforts are certainly not as effective as one would have wished for. A commonly accepted reason for this is the insecure behaviour of people. This insecure behaviour is often due to a lack of knowledge, awareness, education and training. In order to address this, many organisations provide security education, training and awareness programs to their employees. However, these programs often do not achieve a persistent change towards secure behaviour. The various reasons that contribute to the failure of security education, training and awareness programs and cause the trend towards insecure behaviour are briefly discussed. It follows that changing the behaviour of people is an inherently difficult task that requires the consideration of many factors. Similarly, a tool that intends to address

insecure behaviour needs to consider various technological elements that may contribute in its ability to influence behaviour. The aim of this paper is to propose the principles of a personal information security agent and explore a set of objectives and criteria that may contribute to its success in influencing and reminding individuals towards a more secure behaviour. The criteria stem from various domains such as persuasive technology and human computer interaction. Persuasive technology has been applied in various domains to shape, reinforce or change people's behaviour. We describe related work that has been done using persuasive technology, and build on it. The proposed criteria consists of functions such as "To motivate" and characteristics such as "Context sensitivity". To put the theory into practice, a prototype of a personal security agent has been developed that implements some of the criteria. Based on this, a discussion on the development and implementation of the prototype and its potential benefits has been included. The prototype was developed to test the proposed criteria in a practical experiment that will form part of future research.

**Keywords:** Information security, information security awareness, persuasive technology, human computer interaction, human behaviour

---

## **International Criminal Cooperation in the Context of Cyber Incidents**

**Anna-Maria Talihärm**

**Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia**

**Abstract:** The borderless and increasingly sophisticated nature of cyber crime calls for effective and timely responses from numerous stakeholders worldwide – including law enforcement agencies, international organisations, Computer Emergency Response Teams and Internet Service Providers. Therefore, the role of international criminal cooperation in the context of cyber incidents is becoming increasingly crucial. Cyberspace has challenged the fundamental principle of territorial jurisdiction and thus emphasises even more the burden on successful cross-border cooperation. Above and beyond the technical concerns of poor attacker attribution and the difficulties of acquiring digital evidence, some of the primary international legal obstacles include the lack of requisite procedural rules, determining jurisdiction and finding effective means of communication. Moreover, a cyber incident is not always recognised as a crime by both the victim nation and by the nation from which the attack originated. It is therefore clear that a thorough review of substantial and procedural law should be undergone on the national level before international cooperation could be effective, or even possible. This paper focuses on offences against data, property and infrastructure and

draws attention to the most relevant international instruments employed in prosecuting cyber crime. According to the firm belief of legal experts working in the area, awareness about such international instruments as well as guidance toward proper implementation are immediately required. Hence, this paper offers a brief introduction to the main challenges of judicial cooperation in the field of cyber crime and, looking toward the future, describes important trends in the domain of international criminal cooperation.

**Keywords:** cyber crime, international criminal cooperation, judicial cooperation, information exchange

---

## **Methods for Detecting Important Events and Knowledge From Data Security Logs**

**Risto Vaarandi**  
**CCD COE, Tallinn, Estonia**

**Abstract:** In modern computer networks and IT systems, event logging is commonly used for collecting system health information, in order to ease the system management process. For example, many sites are collecting events and network flow records from their applications, servers, and network devices over protocols like syslog, SNMP and Netflow, and analyze these data at central monitoring server(s). Among collected data, many events and records provide information about security incidents. Unfortunately, during the last decade security logs have grown rapidly in size, making the manual analysis extremely labor intensive task. This task is further complicated by the large number of irrelevant records and false positive alerts in security logs. For this reason, the development of methods for detecting important events and knowledge from security logs has become a key research issue during the recent years. In our paper, we propose some methods for tackling this issue in the context of IDS and Netflow logs from an organizational network. The first contribution of this paper is the study of important properties of IDS and Netflow logs. We have conducted our analysis on a number of production system logs obtained from a large financial institution, and some of our findings are supported by results from other researchers. The second contribution of the paper is the proposal of several data mining based and heuristic methods for event and knowledge detection from security logs. Our data mining methods are based on frequent itemset mining for identifying regularities in IDS alert sets and network traffic. These regularities are then used for finding unexpected IDS alert patterns and prominent network traffic flows. In this paper, we also discuss the implementations of the proposed methods in a production environment, and provide performance estimates for

our implementations. We conclude the paper with a short discussion on some promising directions for further research.

**Keywords:** data mining, security log analysis

---

## Locating the Enemy

**Marja Vuorinen, University of Helsinki, Finland**

**Abstract:** Enmity is structured discursively in several ways, focussing on different characteristics and producing various sets of concepts. Some of them relate to concrete geographical locations, while others refer to more abstract sociological and political notions. Some sets of concepts are completely separate from one another, while others are strongly interrelated and even form interesting combinations. An Enemy differs from an Other basically by being experienced as openly and actually threatening. When creating an Other the unwanted features unsuitable for the Good Self are moulded into a separate form, that is usually considered relatively stable, distant (not imminently threatening) and safe. An Enemy has a similar core, but it is considered actively menacing. Most often it is also imagined (or perceived) as approaching: drawing nearer and eventually closing in. To discover an enemy one thus has to define a) where it is supposed to be situated and whether or not it is moving closer, b) how close by it currently is, and c) whether it operates openly or under cover. This paper explores the location-related concepts that are used to define enmity in all their variety. It experiments with the idea of integrating them all into a single system, producing a mental map of all the possible locations of potential enemy types. These include first the enemies from outside: the traditional military enemies situated outside the borders of a sovereign state, easiest defined apart from one another by compass point. The second species of enemies are the so-called intimate enemies – a concept coined by Vilho Harle (2000) – residing within the same society but outside the defining group, and divided into sub-species such as the sociological enemies threatening ‘from above’ and ‘from below’, the enemies of a movement standing symbolically either behind or ahead of it, and the traditional political enemies from right to left. These sets of subtypes interrelate in many both obvious and unexpected ways. The third and most perilous enemy species is the internal enemy, lurking inside the defining group itself, weakening it, sponging on it, or threatening with sabotage, betrayal or desertion. Examples of each enemy type are discussed in the paper – the geographical ones, due to the author’s nationality, mainly from a Northern European perspective, but with excursions to a more general European and Western experience.

**Keywords:** enemy images, location, politics, sociology, geography

---

# **Australian National Critical Infrastructure Protection: A Case Study**

**Matthew Warren and Shona Leitch**  
**Deakin University, Australia**

**Abstract:** Australia has developed sophisticated national security policies and physical security agencies to protect against current and future security threats associated with critical infrastructure protection and cyber warfare protection. This paper will discuss some of the common security risks that face Australia and how their government policies and strategies have been developed and changed over time, for example, the proposed Australian Homeland Security department. This paper will discuss the different steps that Australia has undertaken in relation to developing national policies to deal with critical infrastructure protection.

**Keywords:** critical infrastructure, Australia and policy

---



# PhD Papers



# Security Considerations for Virtual Platform Provisioning

Mudassar Aslam and Christian Gehrman

Swedish Institute of Computer Science (SICS), Sweden

**Abstract:** The concept of virtualization is not new but leveraging virtualization in different modes and at different layers has revolutionized its usage scenarios. Virtualization can be applied at application layer to create sandbox environment, operating system layer to virtualize shared system resources (e.g. memory, CPU), at platform level or in any other useful possible hybrid scheme. When virtualization is applied at platform level, the resulting virtualized platform can run multiple virtual machines as if they were physically separated real machines. Provisioning virtualized platforms in this way is often also referred to as Infrastructure-as-a-Service or Platform-as-a-Service when full hosting and application support is also offered. Different business models, like datacenters or telecommunication providers and operators, can get business benefits by using platform virtualization due to the possibility of increased resource utilization and reduced upfront infrastructure setup expenditures. This opportunity comes together with new security issues. An organization that runs services in form of virtual machine images on an offered platform needs security guarantees. In short, it wants evidence that the platforms it utilizes are trustworthy and that sensitive information is protected. Even if this sounds natural and straight forward, few attempts have been made to analyze in details what these expectations means from a security technology perspective in a realistic deployment scenario. In this paper we present a telecommunication virtualized platform provisioning scenario with two major stakeholders, the operator who utilizes virtualized telecommunication platform resources and the service provider, who offers such resources to operators. We make threats analysis for this scenario and derive major security requirements from the different stakeholders' perspectives. Through investigating a particular virtual machine provisioning use case, we take the first steps towards a better understanding of the major security obstacles with respect to platform service offerings. The last couple of years we have seen increased activities around security for clouds regarding different usage and business models. We contribute to this important area through a thorough security analysis of a concrete deployment scenario. Finally, we use the security requirements derived through the analysis to make a comparison with contemporary related research and to identify future research challenges in the area.

**Keywords:** security; trust; virtualization; virtual private server; telecommunication networks, clouds

---

## **A Mobile and Quick Terrorism**

**Anthony Desnos and Geoffroy Gueguen**

**Operational Cryptology and Virology Laboratory (CVO), ESIEA, France**

**Abstract:** New technologies bring significant changes into our way of life, and mobile phone is one of them. It is an item which follows us everywhere, it has become somehow a part of our body. The fact is that nowadays mobile phones are like little and powerful computers. You can travel from a country to another one without your mobile phone being controlled by authorities, and that is an interesting characteristic. However your mobile phone can be turned into a new weapon for modern terrorism. It will not be use as a weapon to attack a target (it can be used in a bomb [Madrid, 2004]), but to synchronize an attack between different unknown terrorists who do not know each other. The idea is to follow a terrorist from his formation in an Al quaeda camp to the final attack. We will see how it is possible for a terrorist leader to perform and plan an attack by creating a mobile application, and by giving mobile phones (with an embedded application) to different “jihadists”.

**Keywords:** terrorism, mobile phone, android, cryptography

---

## **Regulatory Compliance to Ensure Information Security: Financial Supervision Perspective**

**Andro Kull**

**School of Information Sciences at the University of Tampere, Finland**

**Abstract:** The last financial crisis shows that more control is necessary for the financial sector. Controls should be planned and realized at the international, country and bank levels because everyone who has to use financial services wants to be sure that data about their assets are secure. Almost everyone use the electronic services of financial institutions and therefore information security issues can not be overemphasized. To increase security in computerized actions of financial institutions, a certain supervisory authorization must be established. In order to cleverly realize such questions as “How much security is necessary?”, “How much security is sufficient?” and “How to be shore that operations are secure”, a systematic approach to assess the state of security is necessary. In the current case, these questions should be answered by financial supervisors to provide assurances that people’s money is safe in banks and in other financial institutions. In this paper we shall propose a new compliance assessment and monitoring method for these purposes. The key concept presented and used through the research is named as technology assurance (TA), it is all which gives the feel

of security in using technology and this may be treated as synonym for the term information assurance (IA). To ensure technology assurance, the lowest steps have to be passed to go higher level. Technology assurance presumes that business processes are well organized, information assets and IT governance is well established and IT risks are managed to build up higher level assurance like information security measures, information systems/information security auditing and to reach highest levels like business continuity preparation. To answer to the main research questions mentioned above, the sub-questions like “How much to regulate?” should be answered. Considering some facts about Estonia and financial sector - Estonia is a member of European Union, the bigger banks in Estonia are the subsidiaries, we have launched Euro lately - it is essential to be in accordance with European practices in developing our standards to regulate the financial sector and IT field. During the research, survey about current arrangements in 29 European countries was studied and this paper describes the survey focusing on the results. The question was: how the European countries regulate financial sector IT field and what the requirements are the financial institutions should fulfill to ensure the security of electronic operations? The main results of survey show that the most important issue to cover with regulations was IT risk management, also business continuity process and information security policy were covered in most cases. About a half of respondents highlight the need to regulate IT outsourcing and access control management issues. In common, the survey confirms the trend for more strict regulation of IT in financial sector and Estonia tends to be top level regarding regulations.

**Keywords:** information technology, information security, business continuity, compliance assessment, financial sector

---

# Behaviour Profiling for Transparent Authentication for Mobile Devices

Fudong Li<sup>1</sup>, Nathan Clarke<sup>1,2</sup>, Maria Papadaki<sup>1</sup> and Paul Dowland<sup>1</sup>

<sup>1</sup>University of Plymouth, UK

<sup>2</sup>Edith Cowan University, Perth, Western Australia

**Abstract:** Since the first handheld cellular phone was introduced in 1970s, the mobile phone has changed significantly both in terms of popularity and functionality. With more than 4.6 billion subscribers around the world, it has become a ubiquitous device in our daily life. Apart from the traditional telephony and text messaging services, people are enjoying a much wider range of mobile services over a variety of network connections in the form of mobile applications. Although a number of security mechanisms such as authentication, antivirus, and firewall applications are available, it is still difficult to keep up with various mobile threats (i.e. service fraud, mobile malware and SMS phishing); hence, additional security measures should be taken into consideration. This paper proposes a novel behaviour-based profiling technique by using a mobile user's application usage to detect abnormal mobile activities. The experiment employed the MIT Reality dataset. For data processing purposes and also to maximise the number of participants, one month (24/10/2004-20/11/2004) of users' application usage with a total number of 44,529 log entries was extracted from the original dataset. It was further divided to form three subsets: two intra-application datasets compiled with telephone and message data; and an inter-application dataset containing the rest of the mobile applications. Based upon the experiment plan, a user's profile was built using either static and dynamic profiles and the best experimental results for the telephone, text message, and application-level applications were an EER (Equal Error Rate) of: 5.4%, 2.2% and 13.5% respectively. Whilst some users were difficult to classify, a significant proportion fell within the performance expectations of a behavioural biometric and therefore a behaviour profiling system on mobile devices is able to detect anomalies during the use of the mobile device. Incorporated within a wider authentication system, this biometric would enable transparent and continuous authentication of the user, thereby maximising user acceptance and security.

**Keywords:** mobile device, behaviour profiling, applications, transparent authentication

---

## **Description of a Practical Application of an Information Security Audit Framework**

**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:** Organizations are increasingly relying on information systems to enhance business operations, facilitate management decision-making, and deploy business strategies. This dependence has increased in current business environments where a variety of transactions involving exchange of information and services are accomplished electronically. The technological advances, the increases use of the Internet, the emergence of the Internet-enabled services and the current audit environment has promoted a growing interest in the continuously deployment of auditing information system security, in order to ensure the reliability of the organizational information systems. However the current approaches available to assist the auditor to perform a security audit is limited concerning the used concepts and it is increasingly dependence on the experience and knowledge of the auditor. This paper intends to present a developed framework, which is based on a conceptual model to assist the auditor to conduct an auditing in the information system security domain. The model developed contains the semantic concepts its relationships and axioms, defined in a subset of the information security domain. This conceptual approach promotes the standardization of the terminology used in the security information domain and to improve the information system security audit process within organizations. Comparisons of the current available approaches to audit information systems will be presented as well.

**Keywords:** auditing information system security, Information system security, ontology, COBIT, ITIL and concepts

---

## **Fight Over Images of the State Armed Forces and Private Security Contractors**

**Mirva Salminen**

**University of Lapland, Finland**

**Abstract:** Images of participants in conflicts held by military leaders, top politicians and administrators as well as the general public make a difference both in conflicts and in times of peace. The images do not only have practical implications in warfare, but also far reaching influence in people's shared

understanding. The shared understanding, again, is the arena on which suggested truths are either accepted or rejected and therefore, an arena for power struggles. Production and control over the emergence, existence and disappearance of different images of participants in conflicts have hence become goals of information warfare. The topic of this paper are the images produced firstly, of soldiers of the state armed forces and secondly, of employers of Private Security Contractors (PSCs). The production of these images is carried out both in discursive and non-discursive practices. This paper focuses on discursive production of the images with the help of descriptions given and pictures presented on the participants in conflicts. The two aforementioned imageries are examined for the reason that in the shared understanding they serve as a binary category: the armed forces functions as a norm against which the existence and conduct of private security contractors are evaluated. Data of the study consists of writings and pictures published in *The New York Times* (NYT) after a shooting in Baghdad in September 2007 and commenting on the shooting. In addition, the paper examines discussion in the US House of Representatives Committee on Oversight and Government Reform (HCOGR) hearing held 2<sup>nd</sup> of October 2007 which discussed the matter of PSCs operating in Iraq and in which CEO of the company accused of misconduct in relation to the aforementioned shooting witnessed. The questions under scrutiny are who has the right to speak and what kinds of images circulate in the data as well as how these images produce the binary category of the armed forces – private security contractors into the shared understanding. The role of PSCs is likely to grow in the complicated conflicts of the future and therefore, how political and military decision making and people's shared understanding manages them is important.

**Keywords:** images, collective meaning production, armed forces, private security contractors

---

# **Non Academics**



# **A Proposal for Domain Name System (DNS) Security Metrics Framework**

**Andrea Rigoni and Salvatore Di Blasi**  
**Global Cyber Security Center, Rome, Italy**

**Abstract:** The Domain Name System (DNS) is a fundamental and critical building block of the Internet. Not only, DNS represents one of the most critical services of information infrastructures, and the strong interdependency between critical infrastructures relying on information and communication technology makes DNS a likely, disrupting target in case of cyber conflict. Critical infrastructures are no longer independent from the Internet networks: electricity plants, telecommunications services, transportation systems, banks and financial institutions heavily rely on Information and Communication Technology (ICT). New risk scenarios for critical infrastructure protection are expected, in that newer threats propagate through the Internet networks and exploit Internet infrastructure vulnerabilities, making such threats as cyber espionage, cyber conflict and cyber terrorism a likely possibility every government should consider in its national security agenda. DNS is vulnerable to a series of threat agents, and these vulnerabilities might be exploited by coordinated groups of attackers to produce damages to national critical assets. A more secure DNS in terms of technology, processes, policy making and organizational structures is needed. The proposal presented in this paper represents a work in progress, whose main objective consists in the development of an accepted metric framework for DNS security and stability: this will be accomplished through a deep state-of-the-art analysis of current DNS metrics and KPIs, the proposal of a newer set of KPIs and consequential sharing of the results with the DNS community. We believe the definition and collection of these metrics will pave the way to the empirical definition of a DNS stability baseline, leading to the establishment of best practices, standards and acceptable service levels for a consolidated overarching DNS security policy making framework and raising awareness on DNS vulnerabilities and threats outside DNS community.

**Keywords:** DNS security, security policy, public key infrastructure, security, critical national infrastructure protection

---



# **Work in progress**



# Malicious Flash Crash Attacks by Quote Stuffing: This is the way the (Financial) World Could end

Robert Erra

Équipe S&IS, Esiea Paris, France

**Abstract:** Cybercrime and cyberterrorism use computers (well, softwares and networks) to attack targets like critical infrastructures. Computers, softwares and networks are necessary tools for a cyberattack but can also of course be targets. We propose here to describe a new form of cyberterrorism (or cybercrime) attack, theoretical but with a high probability of realization: *the cyberattack on the stock exchange market of some countries* but with legal cyberweapons. Consequences of such an attack could be devastating for the financial and the non financial world. How is such an attack possible ? Well, at the New York Stock Exchange, May 6th 2010, an astonishing fact has happened: all financial transactions during 20 minutes have been purely “deleted”. This is now called the *Flash Crash*. All details are not clearly understood, it seems that the so called “quote stuffing” (or *stub quotes* sometimes) used in conjunction with High Frequency Trading (HTF) is at the heart of this accidental incident. We have to point out that experts from SEC do not agree with this hypothesis. We propose in this paper here to describe a malicious version of the flash crash, this is a new cyberweapon that can attack a new target: Stock Exchanges places. More precisely, we propose to see this financial incident as it really is : a Denial Of Services (DOS) of a very new type that we will call a Denial Of Financial Services (DFOS). We remind that a DOS classical attack is simple to do and can be devastating, so it seems for the DFOS. The basic idea of the scenario of our malicious flash crash attack (MFCA) is simple: we propose to mimic the true flash crash of the New York Stock Exchange. So, a group of cyberterrorists, with just money and computers, following the mechanisms of the MFCA, could create an artificial but truly devastating flash crash. An quick evaluation of the legality of each step of our malicious flash crash attack shows that if the quote stuffing is considered as legal (the status of it is a little bit unclear) then the MFCA is absolutely legal. We propose also a illegal version of the MFCA. Is it possible to design a countermeasure against the MFCA ? Unfortunately, as long as HTF and quote stuffing will be legal, our scenarii are highly plausible, both the legal and the illegal version, and they are not so difficult if you have enough money, or enough cybercriminals.

**Keywords:** flash crash, quote stuffing, cyberwarfare, cyberterrorism, cyberattack

---



# Posters



## **Assessment of Mission Risk; Role of Protection of Information and Communication Technology Resources**

**Jobin Choobineh<sup>1</sup>, Evan Anderson<sup>1</sup> and Michael Grimaila<sup>2</sup>**

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

**<sup>2</sup>Air Force Institute of Technology, USA**

**Abstract:** The use of information and communication technologies (ICT) has become an integral component in the execution of modern combat operations. As a consequence, the ICT infrastructure is continuously subject to adversarial threats. Due to the complexity, scale, and interconnectedness of the ICT used in support of military operations, it is inevitable that security breaches will occur. When this occurs, the ability to quickly estimate the negative impact to mission objectives resulting from the cyber incident is of paramount importance for command decision making. In this paper, we present a methodology to assess the risk to mission resulting from cyber incidents and breaches. The methodology is based on the following broad steps: 1) Model the mission by its activities, 2) identify and document ICT resources used in the activities of the mission, 3) assign initial risk levels and then compute combined risk levels to ICT resources, 4) compute risk to the activities that use these resources, 5) identify protectors of ICT resources and adjust the configuration of the protectors to protect against the risks and reduce the negative outcomes. We demonstrate the application of the methodology with a typical and common ground movement of troops. The outcome of the methodology provides the commanders with an enhanced understanding and estimation of the impact of cyber attacks on their missions.

**Keywords:** risk assessment, mission modeling, security models, process modeling

---

## **Constantly Evolving Cybercrime Forensic Challenges**

**Abhaya Induruwa**

**Canterbury Christ Church University, United Kingdom**

**Abstract:** Digital consumer electronic market rapidly evolves as consumers demand for more performance and features, and as every manufacturer tries to capture a share of this lucrative market. Digital forensic investigators constantly face challenges as the industry continues to innovate and produce consumer electronic devices that are more and more powerful, contain enhanced features with increased performance and capacities. Among the

areas that are expected to throw the greatest challenges are constantly evolving Microsoft Windows operating systems, migration of the Internet to IPv6 protocol, Social engineering and social networking, increasing use of VoIP in IP telephony communication, smart mobile devices operating on a plethora of operating systems including Android, Apple iOS, Blackberry, Symbian, Windows Mobile, etc, virtualisation and cloud computing.

This paper concentrates on the devices and technologies that are relevant in forensic investigation and explores the challenges faced by digital forensic investigators when dealing specifically with the recent generations of Mobile Phones (Blackberry and iPhone), TomTom satellite navigation systems, Microsoft Xbox360, Nintendo Wii and Sony PS3 games consoles, and VoIP communications via Skype. It aims to serve as an overview of the state-of-the-art in digital forensic investigation and specifically concentrates on aspects of networks running IPv6, communication using Voice over IP (VoIP), smart mobile phones (BlackBerry, Apple iPhone), GPS navigation systems (TomTom) and games consoles (Xbox 360, Nintendo Wii and Sony PS3). The paper focuses on the recent developments of technologies, services and devices that today's digital forensic investigator should be aware of and provides an overview of products and processes based on contemporary work and material reported in the literature. The discussion on technical details is limited to a level that is essential for the understanding of the processes and tools but the paper provides adequate references to explore for further and more complete information on the topics treated. It is hoped that this should help the investigators to further develop their knowledge and skills.

**Keywords:** Forensic challenges, VoIP communications, games consoles, handheld devices, IPv6 forensics

---

## **Finding Patterns in the Alerts of Intrusion Detection Systems**

**Francisco Ribeiro and Henrique Santos**  
**Minho University, Portugal**

**Abstract:** With the growth and expansion of the Internet, the world has become global. Nowadays, when it comes to communication, we don't usually think about borders or distances because we can easily communicate with anyone anywhere in the world, using only an Internet connection. Obviously, given this flexibility, the Internet has become the primary method of communication between people in different countries or continents, and therefore an essential and indispensable asset. However, it is necessary to recall that the presence of sensitive data roaming the internet may lead to

attacks performed by ill-intentioned people who are trying to invade private networks hoping to capture important data or to take control of network devices. Most of that malicious activity is hidden in apparently legitimate traffic and can only be detected by sophisticated anomaly intrusion detection systems (IDS). Despite their evolution, IDSs still produce a huge number of false positives, lowering enormously their efficiency. To address this issue, the main goal of this work is to study patterns generated by IDS's false positives, and develop a methodology (system) that will automatically detect and ignore those patterns. With this in mind, we set up a system for intrusion detection using Snort, which monitored, for more than 30 days, a general purpose network used by students in a Campus. During this time, all anomalies were logged for future analysis. We later processed and analyzed all alerts using various tools and methods, both analytical and visual (using Base and ACID) to identify the significant characteristics. Therefore, using Data Mining techniques, with RapidMiner and MySQL, we were able to automatically generate outputs in Decision-Tree form. These outputs can be then processed, making it possible to create new and more reliable Snort rules. With this methodology we are able to meet the objective defined, and actively contribute to better deal with false alarms. Throughout this paper we present the reasons why we chose this subject, the Data Mining techniques used, and, through examples, how we made it possible to improve the detection of false positives by changing detection rules (Snort tuning).

**Keywords:** Security, intrusion, detection, internet

---



# **Presentation Only**

# The Image of the Afghan War Visual Strategic Communication Narratives of the Isaf-Operation

Noora Kotilainen

Finnish Institute of International Affairs/Helsinki  
University, Helsinki, Finland

**Abstract:** This paper examines the Information warfare of the Afghan war, or more precisely Nato's current visual strategic communications endeavour targeted to influence the western public opinion in very recent years. To track down what kind of means, messages and narratives the western strategic communications machinery typically uses, in order to more effectively convince and address the domestic publics, I concentrate on analyzing the communication and image building endeavour taking place in internet and new media surroundings, and namely bite into visual images constructed for the communication. As material I use-- "Isaf media's photostream" in Flickr – which is a frequently updated set of photographs presented by the ISAF in internet surroundings.

This paper seeks to analyze how the "imago fight of the Afghan war"-- the fight over the minds and perceptions of western population-- is waged today, and to explore what do the narratives utilized in communicating tell about the presenter and the audiences of the information, but also about the topical world order. The aim is to go beyond the official justifications tailored to explain and legitimize the war in Afghanistan. By analyzing the strategic communication images, the realms of western world views, dominant discourses and ways of perceiving ourselves, the "others" and the world of today emerge.

The paper at hand, I seek to deconstruct and examine what the discursive messages and narratives embedded in the visual representations tell, say and reveal about their presenter and audiences, and the values, morals and attitudes of their time, and of the world order they are presented in. By unravelling and deconstructing the visual narratives of today's war a clearer picture of the resources, messages and narratives used to address "us", in order to see conflicts of today in certain ways, can be brought into light; but also a clearer picture of who we are, and in what frames "we the westerners" are willing to see this war we are a part of come to light. Photographs presented on the Afghan war, ISAF operation and international coalition's activity on the ground in Afghanistan produce the frames of seeing the war of today. The visual narratives embedded in the images create a picture of how "we westerners" want to see our selves; as moral agents and international

actors. They also paint the picture of what we are not willing to encounter—thus the frames of seeing war come to light.

**Keywords:** Visual narratives, Afghan war, strategic communication, frames of war

---

## **Cloud-based Shared Mental Model in Cyber criminals**

**Daniel Ching Wa Ng**  
**C-PISA/HTCIA, Hong Kong**

The national level infrastructure penetration and server halts in both Estonia 2007 and Georgia 2008 sparked an rising concern in both Europe Council and Interpol on the vulnerabilities, integrity and sustainability of any government totally relying on computers and network, especially, opening up the whole national information assets to Internet. Further, the down counting of many countries' networking towards IPv6 actually has three empirical challenges to those financial-oriented internet hackers, and organized cyber criminals:

- 1) The removal of network address translation requirement in IPv6 alarms finding new ways to hide those malware payload, which is highly easily masked out through the current IPv4 routing limitation. A more simple BOTNET system could appear before end 2011 to exploit IPv6 feature for bigger exploit reward.
- 2) Mobile radio networks, like LTE and HSPA, are replacing fixed data and voice networks, remarkable in Nordic regions, and British Isles such that any cyber warfare, or cyber storms can be launched through handheld devices, such iPhone4, and other Android devices. The YouTube-available training kits to jailbreak handheld devices convert the mobile data networks into a team of hand-launched “cyber-missiles”.
- 3) Stuxnet outbreak in 2010 marks a new era in offline BOTNET control to shake up law enforcement in their Instance Response IR arrangement not solely on connected networks, but on SCADA weakness. Cyber criminals can hijack some intelligent building, like the IFC in Hong Kong, and Shanghai, or Petronas Twin Tower in Malaysia Kuala Lumpur to demand huge ransom from states' government. Even scarily, TGV could be a national cyber attack targets such that the stability of a key European Council member can rock the global financial flow overnight. This can recall famous “007 James Bond movie Royale Casino”.

Nonetheless, all computer attacks do not come from hardware or developed software themselves. It is the algorithm from human brains to trigger the evolutionary spread of cyber armed forces, such as Trojans, worms, BOTNET

agents and etc. The lesson learnt in Conficker 2009 debriefs the World's awareness of cyber criminals' diligence in using Public Key Infrastructure in Command & Controls centre. In this paper, an attempt is done to develop a cyber criminal's SHARED MENTAL MODEL (SMM) using public available information, like the arrest of Zeus personnel mid 2010, and the track down of Russian Business Network in 2008. China's Honker activities will be drilled, along with Nov 2010 scandal in China's QQ platform to install "legitimate spyware" to user's PC and GSM hand phones to pickpocket emails and other privacy infringement. This approach is a reference to latest criminology research in finding out the subconscious team building mechanism in cyber criminals.

Shared Mental Model could be something remote to technical expertises, especially those graduated from computer science, mathematics and electronics engineering. Fundamentally, mental modelling exists when a new baby is born. Human brain tickers few months after egg fertilized by sperm in mothers' womb. There is a thin layer of brain cells underneath human skull called Cortex Cerebrum. The interaction of parents with new baby helps the cell bidding. Logics and motor neuron reinforce all matter learnt.

The history of cyber crime does not have long history. A time line analysis on cyber criminal activity, with source information from US Council on Foreign Relations, explicitly states the 1<sup>st</sup> instance of Cyber Criminal happened in a US Bank's million dollar theft through a bogus modem transaction. Later, numerous national computer attack, says network lock down, or denial of services attack, are found in Baltic countries, Estonia and Georgia. The attack sources are labelled in Russia. Some accusations are made on PRC China relating to the leakage of critical defence weapon design, or the conspiracy acts against internet services providers, says Google. Interestingly, the report deliberately stresses no solid evidence is confirmed on PRC China originality.

In the arena of organizational learning, one great masterpiece is Cynefin Framework from David Snowden, the formal IBM Scientist on Knowledge Management. This is a high level abstraction model upon years of statistics on organizational failures and conflicts to define four quadrants of team learning and mentality sharing, i.e.:

1. Chaos for matters of inconceivable such that all happenings bearing NO cause and effect relationships. That is similar to earlier days of virus, says stones and pacmen.
2. Complex for many possibilities such that all casual relationship working coherently, as in worm spreading to exploit the weakness in network tcp port, like MS Blast. Still, no strong control is found to direct towards a

particular objective

3. Empirical Knowable for anything probable such that all instances are repeating over time, as in social engineering scandals. Those instances could be realized in different technologies, but the end result is still the same. Further, a strong central control in all distributed, as in social engineering outbreak in HB Gary or probable RSA breach through Advanced Persistent Threat.
4. Finally, the last domain of actuality drives the best practice such that all organized bandits can structure attack over timeline to circumvent security measures to seize sizeable financial goals, as in DDOS ransom.

Practically, the application of Cynefin Framework can be achieved through building of decision tree matrix. A quick example is quoted from PRC Police in detecting new, zero-day malware using the covariance analytics on decision tree.

Numerous contemporary cases are walked through, says latest list of malware domain list, twitter malware chronicles and facebook vulnerability. The well-crafted technicality inside the famous conficker worm is discussed to contrast against the latest development in HoneyNet and the outbreak of Lizamoon massive SQL injections.

Nonetheless, the best social engineering examples are the scandal in Societe Generale and Baring Banks, of which the covered-up fraud collapsed the whole organizations. The Advanced Persistent Threat against RSA SecureID, and the data leakage in Epsilon could be the beginning of a plot against giant financial institutes, but still in the prevailing technique of social engineering. The same old trick is found.

Upon this SMM, a cloud-based IR framework is to be constructed to embrace the widespread of social media. Case examples will be developed for Taiwan, PRC China, Korea, Germany, and some Nordic countries.

**Keywords:** Crowd computing, Team Memory, Cyber storm, Digital Defence, SCADA

---