Proceedings

of the

11th European Conference on Information Warfare and Security

The Institute Ecole Supérieure en Informatique, Electronique et Automatique, Laval, France

5-6 July 2012

Edited by

Eric Filiol and Robert Erra

ESIEA, Laval

France
## Contents

<table>
<thead>
<tr>
<th>Paper Title</th>
<th>Author(s)</th>
<th>Guide Page</th>
<th>Page No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td></td>
<td>vi</td>
<td></td>
</tr>
<tr>
<td>Conference committee</td>
<td></td>
<td>vii</td>
<td></td>
</tr>
<tr>
<td>Biographies</td>
<td></td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>A Non-Militarised Approach to Cyber-Security</td>
<td>Andrew Adams, Pauline Reich and Stuart Weinstein</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Matching Attack Patterns to Security Patterns Using Neural Networks</td>
<td>Adetunji Adebiyi, Johnnes Arreymbi and Chris Imafidon</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Who are you Today? Profiling the ID Theft Fraudster</td>
<td>Olga Angelopoulou, Stilianos Vidalis and Ian Robinson</td>
<td>4</td>
<td>25</td>
</tr>
<tr>
<td>The Islamic Republic of Iran's Strategy Against Soft Warfare</td>
<td>Ebrahim Anoosheh</td>
<td>5</td>
<td>35</td>
</tr>
<tr>
<td>Recent Cyberwar Spectrum and its Analysis</td>
<td>Rabia Aslanoglu and Selma Tekir</td>
<td>6</td>
<td>45</td>
</tr>
<tr>
<td>Metrics Framework of Cyber Operations on Command and Control</td>
<td>Melanie Bernier, Sylvain Leblanc and Ben Morton</td>
<td>7</td>
<td>53</td>
</tr>
<tr>
<td>Attribution in the Future Internet: The Second Summer of the Sisterhood</td>
<td>Matt Bishop, Mina Doroud, Carrie Gates and Jeffrey Hunker</td>
<td>8</td>
<td>63</td>
</tr>
<tr>
<td>Paper Title</td>
<td>Author(s)</td>
<td>Guide Page</td>
<td>Page No.</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>Cloud Computing and Security</td>
<td>Abílio Cardoso and Paulo Simões</td>
<td>9</td>
<td>70</td>
</tr>
<tr>
<td>EU law and Internet Traffic Control Lost Between Privacy Rights and Freedom</td>
<td>Filipe Domingues Cerqueira Alves</td>
<td>10</td>
<td>78</td>
</tr>
<tr>
<td>of Individual and Corporate Enterprise</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Identification of Topics Targeted by Attackers</td>
<td>Manoj Cherukuri and Srinivas Mukkamala</td>
<td>11</td>
<td>84</td>
</tr>
<tr>
<td>Evaluation of Nation-State Level Botnet Mitigation Strategies Using DEMATEL</td>
<td>Christian Czosseck</td>
<td>12</td>
<td>94</td>
</tr>
<tr>
<td>From Perception Management to Communication Strategy</td>
<td>Arto Hirvelä</td>
<td>14</td>
<td>113</td>
</tr>
<tr>
<td>What Does the Concept of “Ambidexterity” Mean in the Current Military</td>
<td>Aki-Mauri Huhtinen</td>
<td>15</td>
<td>119</td>
</tr>
<tr>
<td>Planning Process?</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Susceptibility of the South African Media to be Used as a Tool for</td>
<td>Anna-Marie Jansen van Vuuren, Joey Jansen van Vuuren and Suna Venter</td>
<td>16</td>
<td>127</td>
</tr>
<tr>
<td>Information Warfare</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance of CyberSecurity in South Africa</td>
<td>Joey Jansen van Vuuren, Jackie Phahlamohlaka and Louise Leenen</td>
<td>17</td>
<td>135</td>
</tr>
<tr>
<td>Paper Title</td>
<td>Author(s)</td>
<td>Guide Page</td>
<td>Page No.</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>Security and Safety Education in the Czech Republic and eSEC-Portal User</td>
<td>Roman Jasek, Radek Vala and David Malanik</td>
<td>17</td>
<td>145</td>
</tr>
<tr>
<td>Requirements</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Explaining Politico-Strategic Cyber Security: The Feasibility of Applying</td>
<td>Eli Jellenc</td>
<td>19</td>
<td>151</td>
</tr>
<tr>
<td>Arms Race Theory</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Towards an Automated Security Awareness System in a Virtualized Environment</td>
<td>William Aubrey Labuschagne and Mariki Eloff</td>
<td>20</td>
<td>163</td>
</tr>
<tr>
<td>Information Security Model to Military Organizations in Environment of</td>
<td>José Martins, Henrique Santos, Paulo Nunes and Rui Silva</td>
<td>21</td>
<td>172</td>
</tr>
<tr>
<td>Information Warfare</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Simulation Approach for Military Cyber Operations</td>
<td>Ben Morton, Sylvain Leblanc and Melanie Bernier</td>
<td>22</td>
<td>180</td>
</tr>
<tr>
<td>A Taxonomy of Technical Attribution Techniques for Cyber Attacks</td>
<td>Andrew Nicholson, Tim Watson, Peter Norris, Alastair Duffy and Roy Isbell</td>
<td>23</td>
<td>188</td>
</tr>
<tr>
<td>A Vulnerability-Based Model of Cyber Weapons and its Implications for</td>
<td>Karlis Podins and Christian Czosseck</td>
<td>24</td>
<td>198</td>
</tr>
<tr>
<td>Cyber Conflict</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modelling Emergency Response Communication Systems</td>
<td>Graeme Pye and Matthew Warren</td>
<td>25</td>
<td>206</td>
</tr>
<tr>
<td>Digital Finland: Life at the Screen</td>
<td>Jari Rantapelkonen and Saara Jantunen</td>
<td>25</td>
<td>214</td>
</tr>
<tr>
<td>Finding Suspicious Activity on Computer Systems</td>
<td>Neil Rowe and Simson Garfinkel</td>
<td>26</td>
<td>221</td>
</tr>
<tr>
<td>Paper Title</td>
<td>Author(s)</td>
<td>Guide Page</td>
<td>Page No.</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>The Comprehensive Approach as a Strategic Design to run the Military-</td>
<td>Mirva Salminen and Aki-Mauri Huhtinen</td>
<td>27</td>
<td>230</td>
</tr>
<tr>
<td>Industrial Complex in Operations</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User-Side Password Authentication: A Study</td>
<td>Libor Sarga and Roman Jašek</td>
<td>28</td>
<td>237</td>
</tr>
<tr>
<td>Multi-Level Security Cannot Realise NEC Objectives</td>
<td>Harm Schotanus, Tim Hartog and Cor Verkoelen</td>
<td>29</td>
<td>244</td>
</tr>
<tr>
<td>From Kinetic Warfare to Strategic Communications as a Proactive and Mind-</td>
<td>Torsti Sirén</td>
<td>30</td>
<td>250</td>
</tr>
<tr>
<td>Centric Paradigm of the art of war</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cablegate Analysis of Likely Espionage of Nokia by the United States</td>
<td>Daniel Strmecki, Wilke Schwiedop, Emmanuel Oyo-Ita, Brigitte Kaagman, Pierre Leandre, Enrique Santos-</td>
<td>31</td>
<td>258</td>
</tr>
<tr>
<td></td>
<td>Brihuega, Lateef Kadiri and Jessica Dufmats</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Practical Application of Open Source Frameworks to Achieve Anti-Virus</td>
<td>Ignus Swart</td>
<td>32</td>
<td>265</td>
</tr>
<tr>
<td>Avoidance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overt Information Operations During Peacetime</td>
<td>Selma Tekir</td>
<td>33</td>
<td>272</td>
</tr>
<tr>
<td>Novel Tracking of Rogue Network Packets Using Danger Theory Approach</td>
<td>Solomon Uwagbole, William Buchanan and Lu Fan</td>
<td>34</td>
<td>277</td>
</tr>
<tr>
<td>Building an Ontology for Cyberterrorism</td>
<td>Namosha Veerasamy, Marthie Grobler and Basie Von Solms</td>
<td>36</td>
<td>286</td>
</tr>
<tr>
<td>Paper Title</td>
<td>Author(s)</td>
<td>Guide Page</td>
<td>Page No.</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td><strong>PHD Papers</strong></td>
<td></td>
<td>39</td>
<td>301</td>
</tr>
<tr>
<td>Proposal for a new Equation system Modelling of Block Ciphers and Application to AES 128</td>
<td>Michel Dubois and Eric Fillol</td>
<td>41</td>
<td>303</td>
</tr>
<tr>
<td>Cyber Threat at Management in Cognitive Networks</td>
<td>Anssi Korkkainen</td>
<td>43</td>
<td>320</td>
</tr>
<tr>
<td>A Framework for the Detection and Prevention of AQL Injection Attacks</td>
<td>Emad Shafie and Antonio Cou</td>
<td>43</td>
<td>329</td>
</tr>
<tr>
<td><strong>WIP Papers</strong></td>
<td></td>
<td>45</td>
<td>337</td>
</tr>
<tr>
<td>Information Systems Security Management (ISSM) Success Factor: Retrospection from the Scholars</td>
<td>Azah Anir Norman and Norizan Mohd Vasin</td>
<td>47</td>
<td>339</td>
</tr>
<tr>
<td><strong>Abstract Only</strong></td>
<td></td>
<td>49</td>
<td></td>
</tr>
<tr>
<td>CNA by Social Media , or is it 5th Generation Warfare</td>
<td>Hary Kantola</td>
<td>51</td>
<td></td>
</tr>
<tr>
<td>Paper Title</td>
<td>Author(s)</td>
<td>Guide Page</td>
<td>Page No.</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-----------------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>Critical Databases – Towards a Framework to protect</td>
<td>Mzukisi Niven Njotini</td>
<td></td>
<td>53</td>
</tr>
<tr>
<td>South Africa’s Key Information Infrastructure</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Preface

This year sees the 11th European Conference on Information Warfare and Security (ECIW 2012), which is hosted by the Institute Ecole Supérieure en Informatique, Electronique et Automatique, Laval, France. The Conference Chair is Eric Filiol from ESIEA, Laval, France and I am pleased to be the Programme Chair along with Laurent Beaudoin.

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 Rainer Fahs, Chairman of the European Institute of Computer Antivirus Research (EICAR) on the topic of "Cyber warfare: Prospective aspects from the EICAR perspective". The second day will be opened by Lieutenant-colonel Eric Freyssinet, head of the cybercrime division, Gendarmerie nationale in France. Eric will address the issue of the necessary continuum between fighting cybercrime and cyberdefense.

With an initial submission of 90 abstracts, after the double blind, peer review process there are 42 papers published in these Conference Proceedings. These papers come from around the world including Australia, Canada, Czech Republic, Estonia, Finland, France, Iran, Japan, Malaysia, Portugal, South Africa, The Netherlands, Turkey, United Kingdom and the United States of America.

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

Robert Erra and Eric Filiol

ESIEA, Laval, France

July 2012
Conference Executive

Eric Filiol, ESIEA, Laval, France
Robert Erra ESIEA, Paris, France
Laurent Beaudoin ESIEA, Laval, France

Conference Committee

Nasser Abouzakhar (University of Hertfordshire, UK); Kari Alenius (University of Oulu, Finland); Colin Armstrong (Curtin University, Australia); Debi Ashenden (Cranfield University, Shrivenham, UK); Maumita Bhattacharya (Charles Sturt University, Australia); John Biggam (Glasgow Caledonian University, UK); Andrew Blyth (University of Glamorgan, UK); Martin Botha (South African Police, South Africa, South Africa); Svet Braynov (University of Illinois at Springfield, USA); Bill Buchanen (Napier University, UK); Catharina Candolin (Defence Command Finland, Finland); Joobin Choobineh (Texas A & M University, Texas, USA); Maura Conway (Dublin City University, Ireland); Michael Corcoran (DSTL, UK); Paul Crocker (Universidade de Beira Interior, Portugal); Josef Demergis (University of Macedonia, Greece); Moses Dlamini (SAP Research, South Africa); Geoffrey Darnton (Bournemouth University, UK); Paul Dowland (University of Plymouth, UK); Marios Efthymiopoulos (Political Science Department University of Cyprus, Cyprus); Ramzi El-Haddadeh (Brunel University, UK); Robert Erra (ESIEA PARIS, France); John Fawcett (University of Cambridge, UK); Eric Filiol (Ecole Supérieure en Informatique, Electronique et Automatique, France); Chris Flaherty (University of New South Wales, Australia); Steve Furnell (University of Plymouth, UK); Javier Garci’a Villalba (Universidad Complutense de Madrid, Spain); Kevin Gleason (KMG Consulting, MA, USA); Stefanos Gritzalis (University of the Aegean, Greece); Julio Cesar Hernandez Castro (Portsmouth University, UK); Ulrike Hugl (University of Innsbruck, Austria); Aki Huhtinen (National Defence College, Finland); Bill Hutchinson (Edith Cowan University, Australia); Berg Hyacinthe (Assas School of Law-CERSA-CNRS, La Sorbonne, France); Abhaya Induruwa (Canterbury Christ Church University, ); Ioannis Mavridis (University of Macedonia,
Greece); Hamid Jahankhani (University of East London, UK); Amit Jain (BenefitFocus Inc, USA); Helge Janicke (De Montfort University, UK); Andy Jones (BT, UK); James Joshi (University of Pittsburgh, USA); Nor Badrul Anuar Jumaat (University of Malaya, Malaysia); Maria Karyda (University of the Aegean, Greece); Vasilis Katos (Democritus University of Thrace, Greece); Auli Keskinen (National Defence College, Finland); Jyri Kivimaa (Cooperative Cyber Defence and Centre of Excellence, Tallinn, Estonia); Spyros Kokolakis (University of the Aegean, Greece); Ahmet Koltuksuz (Yasar University, Turkey); Theodoros Kostis (University of the Aegean, Greece); Prashant Krishnamurthy (University of Pittsburgh, USA); Dan Kuehl (National Defense University, Washington DC, USA); Peter Kunz (DaimlerChrysler, Germany); Pertti Kuokkanen (University of Helsinki, Finland); Takakazu Kurokawa (National Defence Acadamy, Japan); Rauno Kuusisto (Finish Defence Force, Finland); Tuija Kuusisto (Internal Security ICT Agency HALTIK, Finland); Michael Lavine (John Hopkins University's Information Security Institute, USA); Martti Lehto (National Defence University, Finland); Tara Leweling (Naval Postgraduate School, Pacific Grove, USA); Paul Lewis (technology strategy board, UK); Sharman Lichtenstein (Deakin University, Australia); David Llamas (University of St Andrews, UK); Hossein Malekinezhad, (Islamic Azad University, Naragh Branch, Iran); Mario Marques Freire (University of Beira Interior, Covilhã, Portugal); Rob McCusker (Teeside University, Middlesborough, UK); Durgesh Mishra (Acropolis Institute of Technology and Research, India); Yonathan Mizrachi (University of Haifa, Israel, Israel); Edmundo Monteiro (University of Coimbra, Portugal); Evangelos Moustakas (Middlesex University, London, UK); Kara Nance (University of Alaska Fairbanks, USA); Muhammad Naveed (IQRA University Peshawar, Pakistan); Daniel Ng (C-PISA/HTCIA, China); Rain Ottis (Cooperative Cyber Defence Centre of Excellence, Estonia); Tim Parsons (Selex Communications, UK); Andrea Perego (Università degli Studi dell'Insubria, Varese, Italy); Michael Pilgermann (University of Glamorgan, UK); Fred Piper (Royal Holloway, University of London, UK); Engur Pisirici (governmental - independent, Turkey); Jari Rantapalkonen (National defense University, Finland); Andrea Rigoni (for Booz & Company,, USA); Raphael Rues (DigiComp Academy, Switzerland); Filipe Sa Soares (Univer-
sity of Minho, Portugal); Henrique Santos (University of Minho, Portugal); Damien Sauveron (Mathematics and Computer Sciences, University of Limoges, France); Richard Sethmann (University of Applied Sciences Bremen, Germany); Paulo Simoes (University of Coimbra, Portugal); Jill Slay (University of South Australia, Australia); Anna Squicciarini (University of Milano, Italy); Iain Sutherland (University of Glamorgan, Wales, UK); Jonas Svava Iversen (Danish Broadcast Corporation, Denmark); Sérgio Tenreiro de Magalhães (Universidade Católica Portuguesa, Portugal); Peter Trommler (Georg Simon Ohm University Nuremberg, Germany); Theodore Tryfonas (University of Bristol, UK); Craig Valli (Edith Cowan University, Australia); Rudi Vansnick (Internet Society, Belgium); Richard Vaughan (General Dynamics UK Ltd, United Kingdom); Stilianos Vidalis (Newport Business School, Newport, UK); Paulo Viegas Nunes (Military Academy, Lisbon, Portugal); Natarajan Vijayarangan (Tata Consultancy Services Ltd, India); Teemupekka Virtanen (Helsinki University of Technology, Finland); Marja Vuorinen (University of Helsinki, Finland); Michael Walker (Vodafone, UK); Mat Warren (Deakin University, Australia, Australia); Kenneth Webb (Edith Cowan University, Australia); Trish Williams (Edith Cowan University, Australia); Simos Xenitellis (Royal Holloway University, London, UK); Omar Zaafrany (Ben-Gurion University of the Negev, Israel); Omar Zakaria (National Defence University of Malaysia,
Biographies

Conference Chair

**Eric Adrien Filiol** is the head of the Operational Cryptology and Virology at ESIEA a French Engineer School in Computer Science, Electronics and Control Science. He has spent 21 years in the French Army mainly as an ICT security expert (cryptanalysis, computer virology, cyberwarfare). He is also senior officer reservist in the French DoD. He holds an Engineer diploma in Cryptology, a PhD in applied mathematics and computer science and a Habilitation Thesis in Computer Science. His main research interest are Symmetric Cryptosystems analysis (especially from a combinatorial point of view), Computer virology (theoretical and experimental study of new form of malware and anti-malware technologies), Computer warfare techniques. He is also the Scientific Director of the European Institute in Computer Antivirus Research (EICAR) in Germany and the Editor-in-chief of the Journal in Computer Virology. He likes playing Bass Guitar (Jazz), running (marathon and half marathon) and good wine/food.

Programme Chairs

**Robert Erra** holds a PhD in Computer Science from the University of Rennes I and is currently Professor of CS Scientific Director of the Masters in Information & System Security at ESIEA Paris opened in 2004. He is interested in developments and analysis of algorithms for information security, from cryptanalysis of asymmetric cryptography to malware analysis and in secure programming.

**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. With his students, he regularly participates to national or international challenges (minidrone DGA-ONERA challenge, SAUC-E NATO.)

Keynote Speakers

Rainer Fahs is currently employed as Senior Information Systems Security Engineer at the NATO Air Command and Control Management Agency (NACMA) where he is responsible for the security architecture of the newly developed NATO Air Command & Control System (ACCS). In this capacity he is also the Chairman of the ACCS Security Accreditation Board which is responsible for the security accreditation of the ACCS system. In 2003 Rainer retired from the German Air Force where he spent most of his time in flight safety and flying operations inclusive many hours of F104 and Alpha Jet flying. His last active job was in HQ Air Force Ramstein (Germany) where he spent four years in tactical evaluation for offensive flying. Rainer has been with NATO in Brussels as NATO civil employee where he started as system/network administrator in an intelligence project and developed back in 1991 the first NATO Secret network based on PCs before he was hired by NACMA in 1995. In this new job he had to start over again and get back to school to learn the secrets of cryptography, formalization and the inner architectures of computers and networking. Part of his job is also to represent his agency at NATO Committees dealing with NATO Security Policy and in particular the INFOSEC Policy. Rainer joined the European Institute for Computer Anti-Virus Research (EICAR) in 1992 where he participated in the working group looking into the AV technology. In 1994 he was elected Board member and became the Director of EICAR Working Groups. In 1996 he was first time elected Chairman of the Board and has been in that position until today.

Lieutenant-colonel Eric Freyssinet, head of the cyber-crime division, Gendarmerie nationale. Chairman of the Expert group on IT Crime - Europe of Interpol. Education: Ecole Polytechnique (general engineering, X1992), Mastère spécialisé in Network and IT security from Telecom ParisTech (2000), and currently PhD student at Uni-
versity Paris 6 on the subject of the fight against botnets. Pour les horaires de train, dès que je les aurai fixés.

**Mini Track Chairs**

**Prof Kevin M. Gleason** has over 30 years of experience combining computers and education. A long-time student of computer hacks and information breaches his lectures introduced disaster recovery analysis and preparation. An author of technical textbooks and a 2001 NASA/ASEE Summer Faculty Research Fellow at the NASA—Goddard Space Flight Center in Greenbelt MD. In the aftermath of the 2001 terrorist attacks, was the principle investigator of ‘psycho-metrics’ (a method of identifying the author through written text). He is currently semi-retired working as an adjunct professor to several colleges and a consultant to business in the Greater Boston Massachusetts area.

**Professor Aki Huhtinen** LTC(G.S) PhD. is Docent of practical philosophy in the University of Helsinki and Docent of social consequences of media and information technology in the University of Lapland. The author is also Docent of information security and information operations in the University of technology in Tampere. Huhtinen works at the Department of Leadership and Military Pedagogy at the Finnish National Defence University.

**Amit Jain** is currently working in the R&D at BenefitFocus Inc, a Charleston, South Carolina based enterprise providing health benefits management platform for employers and insurance carriers. His current position involves researching and developing semantics enabled health care systems providing efficient and secure data management. Earlier he was a part of BeliefNetworks Inc, a startup company that sought to create tools for knowledge generation from structured and unstructured data. He holds a Masters and a PhD from University of South Carolina, Columbia. His disser-
tation focused on using semantics for authorizations on ontologies and syntax independent data. His research interests include security policies, ontology based enterprise systems, identity management, digital rights management and information warfare.

Dr. Helge Janicke is currently working as a Senior Lecturer in Computer Security at De Montfort University, Leicester (UK). He is leading the research theme on Computer Security and Trust within the Software Technology Research Laboratory and is working with De Montfort's Centre for Secure Computing. His research interests are in the area of computer security and formal methods for modelling security systems.

Jari Rantapelkonen LTC, D.Sc(mil) is a researcher and teacher in Finnish National Defence University. He works at the Department of Operational Art and Tactics.

Henrique Santos received his first degree in Electric and Electronic Engineering, by the University of Coimbra, Portugal, in 1984. In 1996 he got his PhD in Computer Engineering, at the University of the Minho, Portugal. Currently he is an Associate Professor at the Information Systems Department, University of Minho, being responsible for several projects and the supervision of several dissertations, mainly in the Information Security and Computer Architecture areas. He is the president of a national Technical Committee (CT 136) for information system security standards. In 1990, he was teaching at the University of Bristol, United Kingdom.

Dr Tim Watson is the Head of Department of Computer Technology at De Montfort University and the Director of its Centre for Secure Computing. Tim is a regular media commentator on information security and digital forensics and a member of various advisory groups, including DSTL's Cyber and Situational Awareness Information Exchange, the CESG Academ-
ic Advisory Group, the National Information Assurance Forum, the IAAC Academic Liaison Panel and the UK ISO 27000 series standards body.

**Peter Norris** is a teacher fellow and principal lecturer at De Montfort University where he leads the security strand of the Center for Secure Computing. Originally trained as an engineer, he spent nine years in industry, before joining academia. He has advised local government on identity management, supervised research on network security, helped develop the UK input to ISO standards on both digital forensics and network security, and is currently researching the security of motor vehicle digital systems. His overarching interest is in the security consequences of the practical interaction of heterogeneous systems.

**Biographies of Presenting Authors**

**Andrew Adams** is Professor of Information Ethics in the Graduate School of Business Administration and Deputy Director of the Centre for Business Information Ethics at Meiji University in Tokyo. He is the chair of ACM SIGCAS. He holds a BSc, MSC and PhD in Computing subjects and an LLM in Advanced Legal Studies.

**Adetunji Adebiyi** is a Doctoral student with the University of East London UK. His research focuses on integrating security into software design during SDLC. He is a member of the British Computer Society. His research has led him to give talks and presentations in conferences and seminars he has attended.

**Kari Alenius** is Associate Professor in the Department of History at the University of Oulu, Finland, since 1998. He also has Adjunct Professorship at the University of Oulu (1997). His research interests include the history of propaganda and mental images, the history of Eastern Europe between the World Wars, and the history of ethnic minorities.

**Olga Angelopoulou** is a lecturer in Digital Forensics at the University of Derby. She obtained a doctorate in Computing with the title: ‘Analysis of Digital Evidence in Identity Theft Investigations’. Her research interests
include Computer Forensics, Digital Evidence, Identity theft, Online fraud, Computer crime investigations and the Online Social Networking.

**Rabia Aslanoglu** got her B.S. degree from Izmir University of Economics, Department of Software Engineering in 2009. Currently, she is studying for her M.S. degree in Izmir Institute of Technology, Department of Computer Engineering, Izmir, Turkey. Her research interests are public-key cryptography and information warfare.

**Melanie Bernier** is a Defence Scientist with the Defence Research and Development Canada’s Center for Operational Research and Analysis. She has a Masters Degree in Electrical Engineering and experience in modelling and simulation, concept development and experimentation, joint C4ISR, and computer networks. She is currently leading studies in force development for the cyber environment.

**Matt Bishop** received his Ph.D. in computer science from Purdue University in 1984. His main research areas are the analysis of vulnerabilities in computer systems, security of electronic voting systems and election processes, and data sanitization, network security, and malware analysis. His textbook, *Computer Security: Art and Science*, was published in 2002 by Addison-Wesley Professional.

**Abílio Fernando Costa Cardoso**, Occupation or position held: Researcher in Cloud Computing, IT governance and computer networks, professor at Department of Innovation, Science and Technology, manager of IT area at Portucalense University. M Sc in Computer Science, 1995, B Sc in Applied Mathematics, 1987, Class teaching: Project planning and network management, Java advanced programming

**Christian Czosseck** is scientist at the NATO CCD COE in Tallinn, Estonia. Serving in the German military for more than 14 years, he held several information assurance positions. Christian holds a M.Sc. equivalent in computer scienceand is currently PhD candidate at the Estonian Business School, Tallinn looking into cyber security and botnet related issues.

**Michel Dubois** is teacher and researcher at the Cryptology and Operational Virology (C+V)* laboratory. Currently he is a PhD student in cryptography and works on a new approach of the cryptanalysis of the AES.
Tim Hartog graduated in 2005 at the Technical University of Twente, he has been active in the field of Information Security. During his work at TNO, the Dutch Organization for Applied Scientific Research, Tim has been working on topics like Trusted Computing, Trusted Operating Systems and Cross Domain Solutions.

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

Dr. Berg P. Hyacinthe (Ph.D., Florida State University; LLD Candidate, Assas School of Law, CERSA-CNRS, en Sorbonne) is Director of the “Centre de Recherche Scientifique et d’Études Cybernétiques” (CRESEC) at “l’Université d’État d’Haiti”. His research agenda is set at the intersection of law and technology, exploring legality/illegality of advanced digital technologies in armed conflicts.

Anna-Marie Jansen van Vuuren began her career as a journalist in 2004. She holds a Masters degree in Journalism and Media Management from the University of Stellenbosch and currently she is pursuing a Ph.D. at the University of Pretoria. Anna-Marie is a lecturer at the University of the Witwatersrand and freelances as a broadcast journalist and producer at the South African Broadcast Corporation.

Joey Jansen van Vuuren is the Research Group Leader for Cyber Defence at the CSIR South Africa, mainly involved in research for the Defence and Government sectors. She obtained her Masters from UNISA and her research is focussed on National Cybersecurity and the analysis of Cyber threads. She is also involved in Cyber awareness programs in South Africa.

Saara Jantunen has studied English language and culture in the University of Groningen, and English philology in the University of Helsinki. Currently she is writing her doctoral dissertation in the Finnish National Defence University, where she majors in leadership. Her research interests include language and identity, ideology in discourse, strategic communication and multimodal discourse. Jantunen currently works in education.

Roman Jašek is the head of Department of Informatics and Artificial Intelligence, Faculty of Applied Informatics, Tomas Bata University in Zlín. His
habilitation thesis focused on implementing information security paradigm into commercial organizations as well as tertiary education institutions. Professional interests include computer security auditing, knowledge protection, information systems, and informatics.

**Eli Jellenc** leads analysis of geopolitical cyber security and directs research operations in the EU and Japan for VeriSign-iDefense, where he previously created the International Cyber Intelligence unit. He holds an MA in International Security from Georgetown University, and has authored 3 cyber risk country-profiles in the “Cybercrime and Security” journal (Oxford University Press).

**Jeremy Julien** is an Engineering student at the ESIEA school in France. Jeremy has been responsible for the plotting of our keywords and related cables. Jeremy also assisted Nils by searching for related cables, keywords and other relevant sources.

**Harry Kantola** is working as a teacher at the department of tactics and operational arts in Finnish National Defense University (FNDU), teaching senior staff officers. Kantola has studied (Masters of arts) in Swedish National Defense College (SNDC) and to General Staff Officer at FNDU. His thesis at these schools dealt with CNO in general.

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

**William Aubrey Labuschagne** lectured programming, networking, and security subjects at Tshwane University of Technology (TUT) 2002-2009. Obtained Red Hat Certified Technician (RHCT - 2006) and is qualified SCRUM Master (Scrum Alliance). Qualifications consist of NDip: Computer System Engineering and BTech: Information Technology at Pretoria Technikon Currently completing MTech at UNISA in field of security awareness in rural areas and is technologist at CSIR.
Pierre Leandre is a student in his second year at ESIEA where he study in- formatics and electronics. At school he is part of the OCV lab (Operational Cryptology and Virology Laboratory).

Sylvain (Sly) Leblanc is an Assistant Professor at the Royal Military College of Canada. Sly was a Canadian Army Signals Officer for over 20 years, where he developed his interest in computer network operations. His research interests are in computer security and computer network operations.

Andrew Nicholson received his Masters degree in Computer Security in 2010 at De Montfort, University in England. In 2010 Andrew began PhD research looking into attribution of cyber attacks. He is a member of the De Montfort University Cyber Security Centre (CSC) research group. Andrews main interests are network security, cyber-conflict and online anonymity.

Mzukisi Niven Njotini is a currently working as a lecturer in College of Law at the University of South Africa (South Africa). Njotini has an LLB and LLM (Cum Laude) degree and is currently enrolled for an LLD or Phd degree. Njotini’s area of speciality is information technology law.

Azah Norman BA(Hons.) in Information Science from National University of Malaysia (UKM) (2000)and Masters in Secure e-Commerce from Royal Hol- loway University of London, United Kingdom (2003). Research focuses on information systems security and e-commerce. Worked as a consultant in a Malaysian premier security company under Malaysia’s national information & communication technology corporation (over three years). Research medals for research in Halal-RFID verification and currently pursuing PhD in information systems security management.

Karlis Podins has graduated University of Latvia with master degree in Computer Science, and is working for Cooperative Cyber Defence Centre of Excellence since 2008. Apart from dormant interest in Finite Automata and Natural Language Processing, his research has touched several areas re- lated to security.

Dr Graeme Pye is a Lecturer with the School of Information Systems, De- akin University, Australia. His research is continuing to focus on investigat-
ing the security and resilience aspects of Australian critical infrastructure and the relationships between associated infrastructures. Furthermore, he is also interested in modelling emergency management and disaster response systems, including resilience and security management aspects.

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.

Mirva Salminen (M.Soc.Sc.) is a doctoral candidate at the University of Lapland, Finland, researching on the outsourcing of the state’s security related functions. She has studied International Relations and Political Science at the University of Tampere, Finland; Military History and Strategy at the Finnish National Defence University; and Security Studies at Aberystwyth University, the UK.

Libor Sarga is a doctoral worker at the Department of Statistics and Quantitative Methods, Faculty of Management and Economics, Tomas Bata University in Zlín. His dissertation will be focused on computer and data security in the presence of unreliable human element as an exploitable attack vector. His personal interests include technology, hardware and software architectures.

Emad Shafie PhD student at The Software Technology Research Laboratory, in De Montfort University, I have achieved a master degree in Information technology 2009 from De Montfort University and bachelor degree in computer science 2000 from King Abdul-Aziz University. I have worked as leader of programming department for five years at Umu Alqura University in Saudi Arabia.

Torsti Sirén Lieutenant Colonel, General Staff, Ph.D. (Pol. Sc.), B.A. (Slavonic philology) Torsti Sirén is Head of Research Group in the Department of Leadership and Military Pedagogy at the Finnish National Defence University, Helsinki.

Ignus Swart obtained his masters degree in computer science at Tshwane University of Technology where he studied with a full scholarship. After
several years working as both a software developer and security professional, he is currently in the employ of the CSIR, Cyber Defence department and pursuing his PhD studies at Rhodes University.

**Selma Tekir** is working at Izmir Institute of Technology Department of Computer Engineering. In 2009, she worked as a visiting researcher at Faculty of Computer Science Chair for Databases, Data Analysis and Visualization at University of Konstanz-Germany. Tekir received a PhD in computer engineering from Ege University, Turkey in 2010.

**Solomon Uwagbole** is currently a full-time research student in the Centre for Distributed Computing, Networks, and Security at School of Computing, Edinburgh Napier University, Scotland. He is also a freelance Microsoft Certified Trainer (MCT). He holds B.Sc. in Zoology (Hons) from the University of Delhi, India and M.Sc. in Distributed Computing from Brunel University, UK.

**Professor 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.

**Stuart Weinstein** is Associate Head, University of Hertfordshire School of Law. Stuart earned his BA from Williams College, Massachusetts, his JD from Columbia University School of Law, and an MBA from University of Hertfordshire Business School. He is a member of the Bars of California, New York and DC and a Solicitor of Senior Courts of England & Wales.
A Non-Militarised Approach to Cyber-Security

Andrew Adams\textsuperscript{1}, Pauline Reich\textsuperscript{2} and Stuart Weinstein\textsuperscript{3}
\textsuperscript{1}Meiji University, Tokyo, Japan
\textsuperscript{2}Waseda University, Tokyo, Japan
\textsuperscript{3}University of Hertfordshire, Hatfield, UK

Abstract: In 2011 cyberspace came under highly visible military threat. This threat was not cyber-attack by governments or terrorists, but the threat of a militaristic approach to cyber-security. The US and UK military establishments (among others) made strong arguments about the need to expand their online presence from use of the Internet for their own information transmission and into cyber-attack capabilities. Responding to claims of the Russian and Chinese governments sponsoring cracking attacks against Estonia, Georgia and Google, cyberspace in 2011 became the fifth arena of warfare (land, (under)sea, air, space and now cyberspace). Although development of the basic concept and protocols of the Internet was funded by DARPA, a military research agency, the military and civilian uses of Internet systems rapidly diverged in the early days. This separation allowed the development of a free, generative and borderless Internet whose base flexibility and civilian orientation made it one of the core technologies of modern life by 2011. Just as it has become an essential platform for legitimate activity, illegitimate activity has also flourished online. The very automation which makes computers and the Internet so valuable can also be utilised for negative purposes such as Denial of Service Attacks, malware distribution and fraud. There are claims that some governments are sponsoring attacks and cyber-espionage against their enemies (other states or large corporations), and claims about the rise and dangers of cyber-terrorism. Military forces, faced with a diminishing role in preparations for large scale physical conflicts, have begun claiming that civilian cyberspace needs to be (re-)militarised and that the armed forces should be given both the technical tools and the legal rights to conduct not just cyber-defence activities, but offensive cyber-attacks. In this paper we argue from both philosophical and practical standpoints that a pacifist approach to cyber-security is more appropriate. Based on the constitutional pacifism of Germany and Japan, we argue that investment in cyber-defence would be better targeted at improving the physical and electronic infrastructure of the Internet in general (for example, by funding the free distribution of...
malware signatures to all users or research and development of better technological security tools). This would provide better cyber-security for the citizens of the world than an arms race to develop military cyber-attack capabilities. The borderless and non-geographic topology of the Internet provide little capacity for avoiding collateral damage which, we argue, is likely to prove more costly than the original dangers identified or forecast. Technological measures used within the parameter of laws protecting the privacy, civil rights and civil liberties of citizens and utilized for defensive purposes, along with further research on thwarting cyber-attacks on critical information infrastructures, would be more beneficial and are evaluated in this pacifist context.

**Keywords:** militarisation of cyberspace, cyberattack, cyberdefence, pacifism

---

**Matching Attack Patterns to Security Patterns Using Neural Networks**

*Adetunji Adebiyi, Johnnes Arreymbi and Chris Imafidon*

**School of Architecture, Computing and Engineering, University of East London, London, UK**

**Abstract:** The issue of information systems security and its consequences have raised so much concern in many public and private domains, and as hackers attacks on software continues to increase, the demand for secure software has also increased significantly. The industry has been looking at better ways of integrating security into every phase of software development lifecycle (SDLC). The use of security pattern is one of the ways that have been proposed in this research area to help software developers to integrate security into software application during development. However due to different types of security patterns and their taxonomy that have been developed, software developers are faced with the challenge of finding and selecting appropriate security patterns that addresses the security risks in their design. One of the solutions addressing this problem as proposed by Wiesauer, and Sametinger (2009), involves matching attack patterns identified in the software design to security patterns. This research investigated this area by matching attack patterns to security patterns using neural networks and finding how the outcome could be used to en-
hance software systems security at the design and development stages. The result of performance of the neural network and the advantage of this approach is presented in this paper. This study found that attack patterns can be matched to their corresponding security patterns using a neural network that has been trained for this purpose. Therefore, software developers using the trained neural network as a tool can easily be guided into selecting the appropriate security patterns meeting the security requirements of their software application.

Keywords: security pattern, attack pattern, neural network


Kari Alenius
Department of History, University of Oulu, Finland

Abstract: In the spring of 2007 Estonia became the victim of a large-scale cyber-attack. Estimates of the significance of these events vary both in and outside of Estonia. For those who regard the events as being exceptionally important, the cyber-attacks launched against Estonia are seen as a milestone of modern warfare. Sometimes the term “Web War One” has even been used. At the other extreme, the events have been underestimated and their distinctiveness has been disputed. This study does not attempt to answer the question of which perspective is “right” and which is “wrong”, especially when it is particularly difficult to provide an objective answer to this type of question. Instead, this study analyses Estonian interpretations of what occurred. The central elements of the Estonian main narrative crystallized during the summer and fall 2007. The narrative came to be composed of a few key elements describing the entire conflict in general and in a stereotypical way.

Keywords: rhetoric, narratives, cyber-attack, Estonia
Who are you Today? Profiling the ID Theft Fraudster

Olga Angelopoulou\textsuperscript{1}, Stilianos Vidalis\textsuperscript{2} and Ian Robinson\textsuperscript{2}

\textsuperscript{1}School of Computing and Mathematics, Faculty of Business Computing and Law, University of Derby, Derby, UK
\textsuperscript{2}School of Design, Engineering, Fashion and Technology, Faculty of Arts and Business, University of Wales, Newport, Newport, UK

Abstract: Online Identity Theft (ID theft) is a significant problem in our modern knowledge-based and social-driven computing era. This type of cybercrime can be achieved in a number of different ways; and more of the point, various statistical figures suggest it is on the increase. The target is individual privacy and self-assurance, while efforts and measures for increased security and protection appear inadequate to prevent it. While personal identities are increasingly being stored and shared on digital media in virtualised environments, the threat of personal and private information that is used fraudulently cannot be eliminated. This trend in crime can result in complex investigations that involve virtualised information technologies, both as a medium for analysis and as evidence at the same time. Fraudsters are obtaining more sophisticated technological ways and increase their capability not only for committing but also for concealing their crimes. It is believed that fraudsters of this kind of crime are not acting individually, but rather they operate in an organised and well-structured manner. Indeed ID theft is nowadays directly linked to drug trafficking, money laundering and terrorism. ID theft, like almost all different types of crime, involves two parts, at least one victim and at least one fraudster. We argue that the differentiation of the investigation procedure between the victim’s and the fraudster’s side, depends on the ownership and control of the digital media involved in the crime, and can provide results on a more crime-focused basis. In addition it provides information gathering, understanding and knowledge about the way the fraudster acts and could potentially assist in future investigations. Different pieces of evidence can be discovered on each side (victim-fraudster) concerning the techniques that have been used to perpetrate the crime. The online ID theft techniques can leave evidence on both the victim’s and the fraudster’s system. However, the evidence tends to contain different elements on each side that can reveal information about the fraudster and eventually profile him in relation to the attack. There is an approach of profiling the ID theft fraudster based on
the findings that arise during the forensic investigation process in this paper. We discuss the extent of ID theft as a problem and the role of the fraudster in different ID theft techniques. We aim to demonstrate processes that could assist the profiling of the fraudster under the forensic investigation of ID theft.

**Keywords**: identity theft, computer crime, fraudster profiling

### The Islamic Republic of Iran's Strategy Against Soft Warfare

**Ebrahim Anoosheh**  
Islamic Azad University, Rafsanjan, Iran

**Abstract**: New information and communication technologies in the emerging post-industrial society have led to new rules and concepts for politics and international relations. The notion of *soft warfare* is related to phenomena now in evidence in this changing environment. Today, various countries in the world – especially those challenging the present international order – are deeply involved deeply with this new concept. The Islamic Republic of Iran is among those countries which considered themselves as targets of *soft warfare*. Concepts such as *cultural invasion, cultural incursion* and *soft subversion* are commonly held by authorities of the Islamic Republic of Iran, indicating that the country believes itself to be involved in cyber and soft warfare. Iran’s authorities believe that the (imperialistic) West, and especially the USA, is targeting soft warfare against the cultural integrity, national identity and security of Iran. Thus, the Islamic Republic of Iran has attempted to defend itself on the cyber and virtual battlefield by installing a number of negative policies, such as censoring and filtering, but also through some positive measures including improvements in media and satellite infrastructures. This paper investigates positions, strategies and solutions the Islamic Republic of Iran is deploying against new communication and information technologies and, especially, the concept and subject of *soft warfare* and media war.

**Keywords**: The Islamic Republic of Iran; USA; soft warfare; media war; national security
Recent Cyberwar Spectrum and its Analysis

Rabia Aslanoglu and Selma Tekir
Izmir Institute of Technology, Izmir, Turkey

Abstract: War is an organized, armed, and often prolonged conflict that is carried on between states, nations or other parties. Every war instance includes some basic components like rising conditions, battlespace, weapons, strategy, tactics, and consequences. Recent developments in the information and communication technologies have brought about changes on the nature of war. As a consequence of this change, cyberwar became the new form of war. In this new form, the new battlespace is cyber space and the contemporary weapons are constantly being renovated viruses, worms, trojans, denial-of-service, botnets, and advanced persistent threat. In this work, we present recent cyberwar spectrum along with its analysis. The spectrum is composed of the Estonia Attack, Georgia Attack, Operation Aurora, and Stuxnet Worm cases. The methodology for analysis is to identify reasons, timeline, effects, responses, and evaluation of each individual case. Moreover, we try to enumerate the fundamental war components for each incident. The analysis results put evidences to the evolution of the weapons into some new forms such as advanced persistent threat. Another outcome of the analysis is that when approaching to the end, confidentiality and integrity attributes of information are being compromised in addition to the availability. Another important observation is that in the last two cases, the responsive actions were not possible due to the lack of the identities of the offending parties. Thus, attribution appears as a significant concern for the modern warfare. The current sophistication level of the cyber weapons poses critical threats to society. Particularly developed countries that have high dependence on information and communication technologies are potential targets since the safety of the critical infrastructures like; healthcare, oil and gas production, water supply, transportation and telecommunication count on the safety of the computer networks. Being aware of this fact, every nation should attach high priorities to cyber security in his agenda and thus behave proactively.

Keywords: cyberwar, Estonia attack, Georgia attack, operation aurora, stuxnet worm
Metrics Framework of Cyber Operations on Command and Control

Melanie Bernier¹, Sylvain Leblanc² and Ben Morton²
¹Defence Research and Development Canada - Centre for Operational Research and Analysis, Ottawa, Canada
²Computer Security Laboratory, Department of Electrical and Computer Engineering, Royal Military College of Canada, Kingston, Canada

Abstract: The reliance of modern military forces on networks and information systems makes them susceptible to cyber attacks and highlights the importance of cyber operations. This increased awareness of cyber operations has led to a need for concept development and experimentation. Concept development and experimentation work must be assessed, which requires measurement and metrics. To date, little work has been done to measure the impact of cyber operations on military command and control. This paper will address this requirement by putting forward a framework for the measurement of the impact of cyber operations on the effectiveness of the command and control of military missions. There have been many research efforts to describe measurement in the following capabilities: Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR), Network Enabled Operations (Net Enabled Ops), and Command and Control (C2). While these related fields have strong links to cyber operations, none of the associated measurement efforts specifically address the particular measurement requirements of the cyber realm. We propose a metrics framework for cyber operations that is adapted from the measures development work of the US Department of Defence Director of Operational Test and Evaluation, which recommends conducting the assessment at the mission, task and system level. We pay particular attention to the mission and task levels, which describe what is being done, why it is being done, and how well it is being done. The framework elements are “Mission Objective”, “Desired Effects”, “Functions”, “Attributes”, and “Metrics”. This paper will describe how the framework measures the cyber effects described in Simulation Approach for Military Cyber Operations (also submitted to this conference). The major contribution of the paper will be the application of the attributes and metrics discussed in the related capabilities of C4ISR, Net Enabled Ops, and C2 to the measurement of cyber effects.
Attribution in the Future Internet: The Second Summer of the Sisterhood

Matt Bishop¹, Mina Doroud¹, Carrie Gates² and Jeffrey Hunker³
¹Dept. of Computer Science, University of California at Davis, USA
²CA Labs, New York, USA
³Jeffrey Hunker Associates, Pittsburgh, USA

Abstract: Attribution is the binding of data to an entity. An attribution framework is an infrastructure for managing attributes and their values. It consists of four components: a set of entities (actors) having an interest in attribution with respect to a transaction; a set of data to be attributed; the level of assurance with which values of attributes can be determined, and with which they can be associated with an entity; and a policy negotiation engine that actors use to negotiate an acceptable set of attributes and levels of assurance for their values in order to conduct a transaction (the “policy”). The actors include the sender and recipient, the sender’s and recipient’s organizations, ISPs, backbones, and political entities. This paper assumes that such a general attribution framework has been implemented. It examines the implications of such a framework upon the Internet, and upon transactions (specifically, the sending and receiving of packets) among actors. The embedding of attribution requirements in policies controlling communications between parties raises the question of who can communicate with whom. Specifically, how does the use and enforcement of policies based upon attributes affect users of the Internet? We examine this question in two contexts: that of the societal revolution known as "Arab Spring", and that of elections in the United States. We present requirements and the attributes that must be supplied to meet those requirements. We then examine some of the implications of supplying the attributes from the point of view of servers, clients, and intermediaries (such as ISPs and governments). We conclude with a discussion of when attribution is desirable, and when the inability to attribute actions is desirable.

Keywords: attribution, attribution framework, policy, enforcement, security
Cloud Computing and Security

Abílio Cardoso¹ and Paulo Simões²
¹Portucalense University, Portugal
²CISUC-DEI, University of Coimbra, Portugal

Abstract: There is always a strong pressure on Information Technology (IT) to do more with fewer resources. Over the decades, this pressure to rationalize IT costs spurred a number of paradigms, technologies and buzzwords. Some of them failed to meet their promises, while others became successfully embed in IT practices and infrastructures, providing sizeable benefits. The paradigm of cloud computing is currently riding this wave, promising to be the next great revolution in IT. Cloud computing appears to have the right technological and market ingredients to become widely successful. However, there are some key areas where cloud computing is still underperforming – such as security. Availability, security, privacy and integrity of information are some of the biggest concerns in the process of designing, implementing and running IT services based on cloud computing, due to technological and legal matters. There is already an extensive set of recommendations for IT management and IT governance in general – such as the popular Information Technology Infrastructure Library (ITIL) guidelines and Control Objectives for Information and related Technology (COBIT) recommendations. However, the field of cloud computing remains poorly covered. ITIL and other general sources can be sometimes translated to the context of cloud computing, but there are many new challenges not addressed by those generic resources. Recognizing this state of affairs, a number of initiatives already started focusing on novel proposals specifically targeting cloud computing but, up to now, with no significant outcomes. In this paper, we discuss the security implications involved in the migration of IT services to the cloud-computing model, proposing a set of rules and guidelines to be followed in the process of migrating IT services to the cloud. This set of rules and guidelines largely builds on general ITIL recommendations, discussing how to extend/adapt them to the field of cloud computing and identifying which a number of novel areas not covered by current ITIL recommendations.

Keywords: cloud computing, security, ITIL
EU law and Internet Traffic Control Lost Between Privacy Rights and Freedom of Individual and Corporate Enterprise

Filipe Domingues Cerqueira Alves
Social Sciences Faculty – Portuguese Catholic University, Braga, Portugal

Abstract: The European Union is facing a shift of legislative paradigm as far as cyberspace is concerned. Recent legislative movements in EU countries have sought to prosecute presumed illegal activities, mainly associated to file-sharing communities violating principles of intellectual property law. As the attempt to regulate and coordinate legislation on specific Internet abuses takes place, boundaries of privacy rights as they were previously understood are questioned. Yet, as France implements an independent authority with specific traffic monitoring powers and a generality of countries moves towards an additional taxation of physical devices considered as potentially promoting copyright violation activities, the ECJ, in its recent ruling in Case C-70/10 (Scarlet vs. SABAM), has precluded an injunction made against an Internet service provider which requires it to install a system for filtering all electronic communications passing via its services, in particular those involving the use of peer-to-peer software, complying with special and particularly strict requirements, with a view to blocking the transfer of files the sharing of which infringes copyright. Such ruling deeply contributed to the establishment of a milestone on this enduring process as it is now secure that a general traffic monitoring filter cannot be applied by an ISP and at its costs. Moreover, the rationale of the decision had clear implications on two major areas of Law. On one hand, privacy rights are clearly at stake since traffic monitoring cannot, ab initio, distinguish licit from illicit traffic and will provide ground for multiple privacy violations and abuses if not carefully regulated. On the other hand, ISPs and industry companies are concerned as the costs, expenses and burdens of such monitoring are bound to run on their side. Nevertheless, several questions concern the audiovisual industry in particular and the community in general. How can illegal Internet activities – not only file sharing – be monitored? Who can monitor them? What can be defined as abusive vis-à-vis user’s privacy? How far can the monitoring obligations go so that they do not become an excessive restraint on freedom of individual and corporate enterprise? The quest for privacy rights’ defenders has just only begun. This
paper contributes for the answer of the previous questions while it attempts to approach a technical and legal crossed analysis of traffic monitoring alternatives, seeking to determinate whether the current legal establishment allows room for such strict regulation, as the audiovisual industry desires, or if intellectual property defense must be sought after by some means other than traffic monitoring.

**Keywords:** privacy rights; internet traffic control; fair balance; intellectual property rights; C-70/10

### Identification of Topics Targeted by Attackers

**Manoj Cherukuri and Srinivas Mukkamala**

*Institute for Complex Additive Systems and Analysis (ICASA), Computational Analysis and Network Enterprise Solutions (CAaNES), New Mexico Institute of Mining and Technology, Socorro, USA*

**Abstract:** The attackers often relied on using automated exploit kits to infect the legitimate websites with high traffic and inject malicious content into them. The compromised legitimate websites served the malicious content to its users who ended up getting infected. In this paper we present web crawling, inlink search, topic modeling and computational intelligent techniques to attribute the topics targeted by the attackers. We also identify the attack vector used by the attackers with respect to the topics, in targeting the internet users. A computational intelligent technique relying on Gibbs random sampling was used to extract the topics automatically from a set of webpages under study. The extracted topics are correlated with Google Trends to put forward some interesting properties that are helpful in detecting the malicious websites proactively. We identified the primary topics from the topic models generated by Gibbs random sampling across each month and analyzed the features of the targeted topics with respect to its importance then. We identified the words that were consistently targeted across the period of our study and analyzed the topics on which the attackers are always after.

**Keywords:** topic modeling, malicious websites, malware targeted topics, malware topic trends, malicious websites attribution, web security
Evaluation of Nation-State Level Botnet Mitigation Strategies Using DEMATEL

Christian Czosseck
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Abstract: Botnets have been recognised as a possible threat to national security, and over recent years national cyber security thinkers have started to draft national level strategies to reduce the threat posed. The steady increase in the number of infected machines and the damage caused by botnet-mounted attacks shows that the success so far has been limited. This research analyses nation-state and inter-state level botnet defence and mitigation strategies and ultimately evaluates their impact on the botnet threat by employing the Decision-Making Trial and Evaluation Laboratory (DEMATEL) method on empirical data collected via interviews from experts in the field. This paper develops and presents a system of nation-state level strategy groups and a simple model of effects they might have on the botnet threat. Based on this framework, the reciprocal influence of each element pair is identified, with the help of knowledgeable experts, and serves as the basis to conduct an analysis utilising the DEMATEL method. As a result we present a model of the influence that these strategy groups have on the botnet threat, identify strongly and weakly influential elements in this system and present a ranking based on these findings. This will lead to a recommendation as to which is the preferred strategy.

Keywords: botnets, DEMATEL, cyber defence, strategy evaluation
Abstract: During the year of 2010, a set of reports were released that contained important information regarding European multinationals and local governments. These reports were published by Wikileaks and were described as ‘cables’. These cables were sent from American embassies to the United States’ government. Suspicions were raised that the United States might have been spying on European countries, companies and their respective partners. One of the companies being mentioned in the cable files is Telefonica. Telefonica is a major Spanish telecom, television and Internet service provider operating in Europe and Latin America. The United States could have political and/or economic reasons to spy the Southern American continent. The main question during our research is to find out what reasons the United States might have to spy on Latin American countries and if the rumors were true that they have indeed spied upon Telefonica. And if these rumors are true, what profits there to be found within the cables and other relevant sources? During our research, we found relevant data containing possible evidence related to American espionage. The data found within the cables contain information about America’s interest in Telefonica and the pressure being put on their investments in Latin America. The cables contain quotes referring to America’s interest in Venezuela and Cuba. The cables contain messages being sent to an American official, stating that the United States should be aware of Telefonicas vast growing market share and influences in Southern American countries. Other relevant cables contain quotes referring to ‘informed sources’. Who are these sources and how did they obtain relevant information about Telefonicas expenses? Most of the other relevant cables refer to other investments being done in Latin America, especially in Brazil.
and Mexico. The United States have good knowledge about the investments being done in Latin America by Telefonica. Unfortunately, none of these cables contained actual proof that the US had directly spied on Telefonica. The cables only contain relevant information regarding America’s interest in Telefonica. Even though these cables contain shady and maybe suspicious quotes; this cannot be identified as evidence regarding possible espionage.

**Keywords:** e-Discovery, Wikileaks, EDRM, espionage, Telefonica, forensics

---

**From Perception Management to Communication Strategy**

Arto Hirvelä  
National Defence University, Helsinki, Finland

**Abstract:** Strategic communication is developing into an identified function of a successful information-age military operation. However, it is a concept which is still often misunderstood in the military. Leaders from strategic to tactical level must operate in an information environment to deliver the same message to the intended audiences. To address this challenge through unified action, a whole-of-government approach and concept known as strategic communication has emerged. Strategic communication is a concept which unites efforts of governmental organisations to influence intended key audiences in support of national interests. The concept tries to answer challenges posed by changes in the information environment; the increased flow of information; the increased number of networks and reach of media; the increased value assigned to information, and the greater impact of e-media. Governments have influenced key audiences in support of national interests throughout history. This influencing has had different names like propaganda, psychological warfare or operations and perception management. The question is, do we keep inventing the same things again and again or is there really a major difference? Have previous terms, such as perception management, gained negative status and need to be replaced as a result? Do we need a new term for describing how we affect the minds of others? According to Clausewitz, war is an act of policy. A strategic communication concept tries to get tactical level operators to work towards strategic level ends. Previously all different levels;
strategic, operational and tactical, has had their own objectives which were not necessarily related. Tactical level actions have even worked against political objectives. So, have we got back to Clausewitz’s theory of warfare as a continuation of politics? This theoretical paper clarifies the strategic communication concept and its relation to other similar terms and connection to the international politics.

**Keywords**: perception management, strategic communication, communication strategy, Clausewitz, international politics

**What Does the Concept of “Ambidexterity” Mean in the Current Military Planning Process?**

**Aki-Mauri Huhtinen**  
Finnish National Defence University, Helsinki, Finland

**Abstract**: How do organizations survive in the face of change? This is a key question for Western military organizations after the Iraq War and its consequences. All human crises are manmade because of we are human beings. The spreading of individual risk also increases systemic risk. The root cause of the problem is what has been termed “rational irrationality” – behavior that, on the individual level, is perfectly reasonable but that, when aggregated in a complex system, produces calamity (Alpaslan & Mitroff 2010, xvii). From the perspective of organizational adaptation and learning, March (1991) argues that a significant number of competencies needs to be learnt and unlearnt during each and every process of change. According to Birkinshaw and Gibson (2011, 2004), in many sports, ambidexterity is a competitive advantage. Footballers are encouraged to use both left and right foot; left-handed batsmen have a slight advantage against right handed bowlers; the southpaw boxer presents a rarely encountered challenge to a boxer with an orthodox stance; some ambidextrous tennis players even use both hands, separately, to play strokes during a rally. And while some individuals are naturally two-handed or two-footed, many work hard to gain an advantage by practising until they master ambidexterity. The challenge for public security and safety organizations is that with terrorism and changes brought on by cyber-security they are faced with their greatest challenge since the end of World War Two. Not only are the structures and operating procedures undergoing change
but also attitudes and values are pressed on by a changing society. Rational black and white thinking no longer functions when immigrants, various ethnic backgrounds, social media and the operating mechanisms and values of market economy force their way into the training grounds of military bases and battlefields. This article examines the usefulness of the concept of ambidexterity as part of the Comprehensive Approach planning and decision-making process adopted by Western military organizations.

**Keywords:** ambidexterity, planning process, comprehensive approach (CA)

### The Susceptibility of the South African Media to be Used as a Tool for Information Warfare

**Anna-Marie Jansen van Vuuren**¹, **Joey Jansen van Vuuren**² and **Suna Venter**³

¹University of the Witwatersrand, Johannesburg, ²Council for Scientific and Industrial Research, Pretoria South Africa, ³Private

**Abstract:** Many theorists refer to the “digital revolution” when they refer to social media and new media technologies. Internet use can also aid journalists in the mainstream media to improve their traditional reporting in terms of speed and feedback. However media practitioners should also recognize the negative consequences and ethical implications of these new media platforms, as the sources distributing information on social media sites such as Twitter may not be truthful and accurate. Journalists should be aware that these sites can be used by enemies of the state to distribute false information. The purpose of this article will be to investigate whether the South African media is at risk of being used as a tool for information warfare. The paper adopts an argumentative analytical approach on case studies with the intention to sensitize journalists to the possibility that different forces may try and exploit their weaknesses in order to influence social opinion with potentially destabilizing effects. In conclusion the paper ends with an overview of some challenges the mainstream broadcast media have to overcome to prevent being used as weapons by the enemies of the state.

**Keywords:** media influence; agenda-setting; Twitter; radio; social media; behaviour influencing
Governance of CyberSecurity in South Africa

Joey Jansen van Vuuren, Jackie Phahlamohlaka and Louise Leenen
Defence Peace Safety and Security: CSIR, Pretoria, South Africa

Abstract: It is each government’s responsibility to provide oversight on national security, which includes human security for its citizens. Recent declarations from the UK and USA governments about setting up new cybersecurity organisations and the appointment of cyber czars reflect a global recognition that the Internet is part of the national critical infrastructure that needs to be safeguarded and protected. South Africa still needs a national cybersecurity governance structure in order to effectively control and protect its cyber infrastructure. Structures need to be in place to set the security controls and policies and also to govern their implementation. It is important to have a holistic approach to cybersecurity, with partnerships between business, government and civil society put in place to achieve this goal. The aim of this paper is to propose an approach that South Africa could follow in implementing its proposed cybersecurity policy. This paper investigates different government organisational structures created for the control of national cybersecurity in selected countries of the world. The main contribution is a proposed structure that could be suitable for South Africa, taking into account the challenges of legislation and control of cybersecurity in Africa, and in particular, South Africa.

Keywords: cybersecurity, national security, governance, policy implementation. cybersecurity awareness toolkit

Security and Safety Education in the Czech Republic and eSEC-Portal User Requirements

Roman Jasek, Radek Vala and David Malanik
Tomas Bata University in Zlín, Zlín, Czech Republic

Abstract: Education in the field of security and safety is at different level in each country and it is divided into many distinct areas. Teaching of the certain fields of security is strategic due to countries’ geographical location, local business or cultural and social aspects. The European Union
countries are currently missing some kind of online public database, which would cover the security and safety field and bring together students, researchers and experts interested in the subject. The main aim of the preparation of portal “eSEC - Competency Based e-portal of Security and Safety Engineering” (eSEC-portal), is to establish a web system, which would serve as a new tool in the process of learning, for both students and professionals, in fields of security studies, safety studies and crisis management. One of the challenges, while establishing the web portal, was to analyse the conditions of teaching security and safety in the selected EU countries. That is why the first part of this paper focuses on current educational situation in the Czech Republic representing an EU member, however, it is above all intended for international audience such as students and teachers outside the Czech Republic. The second part introduces a qualitative SWOT analysis of education in security and safety and connection with services, which will be offered by the prepared eSEC-portal. The third part predicts and quantitatively analyses the profiles of potential future eSEC-portal users together with their possible requirements. Users are split into several groups such as students, pedagogues, scientists and experts. The analysis discusses the user requirements for content, interactivity, user-friendly extremity and graphical surroundings of eSEC-portal’s modules, all in the connection to their already existing ICT skills. Input data have been collected through on-line questionnaires and the sample has been represented by 144 respondents. The results of this user requirements analysis, enriched with similar data gathered in another five EU countries have been fundamental for functional design and final content of the eSEC-portal. The certain limitation of the study lies in the research sample, which consists mainly of respondents who are familiar with the Information security area. Conclusion discusses the other challenge for eSEC-portal developers and maintainers which is in keeping the portal alive.

**Keywords**: security safety education eLearning web portal eSEC
Explaining Politico-Strategic Cyber Security: The Feasibility of Applying Arms Race Theory

Eli Jellenc
Verisign (iDefense Security Intelligence), London, UK

Abstract: This paper applies existing theories of arms races to explain key problems of cyber security among nation-states. The motivating empirical problem (on which current theoretic approaches exhibit no grasp) is the rapid and pervasive increase in cyber security preparations and malicious activity in a politico-strategic context. Moreover, policy debates concerning cyber security are fragmented, often incoherent, and lack consensus on how even to judge the effectiveness of policies relative to problems. Primarily to blame for such confusion is the absence of a common, tested conceptual framework. To date, neither scholars, nor policymakers, nor industry professionals have succeeded in deriving robust theoretic approaches to unify various islands of useful empirical research on the geopolitics of cyber security. However, such theoretic models and approaches are not only available, but show promise for adaptation to specific cyber security problems. Cyber security is a new and complex class of issues, but it is, in the end, technologically mediated social behavior, and as such, it can be fruitfully studied as such. The increasing significance of cyber security to the international system makes such inquiry necessary to help inform the behavior of states, firms, and other stakeholders. The research effort summarized here hypothesizes that a cyber arms race is indeed underway, and all available findings provide no significant disconfirming challenge. In fact, the approaches to cyber security by the world’s major powers (and many minor ones) indeed exhibit all the features of a novel, multilateral arms race of hitherto unseen complexity: a global cyber arms race. Moreover it is improbable that anything short of revolutionary legal or diplomatic initiatives will prevent severe, near-term increases in cyber conflict activity. More generally, this research shows how existing theoretical work in political science, sociology, and communications theory can lend new rigor to the study of cyber security as a geopolitical issue.

Keywords: cyber warfare, cyber conflict, cyber espionage, cyber security governance, arms races, social science theory
Towards an Automated Security Awareness System in a Virtualized Environment

William Aubrey Labuschagne¹ and Mariki Eloff²
¹Defence, Peace, Safety and Security, Council for Scientific and Industrial Research, Pretoria, South Africa
²School of Computing, University of South Africa, Pretoria, South Africa

Abstract: A majority of African Internet users do not have access to the Internet. The lack of infrastructure in rural areas affects Internet usage. Since costs are high and the bandwidth low, these factors encourage users to access the Internet using shared resources. This is an efficient solution to access the Internet. However users might not be aware of the security threats that exist on using shared resources. Many companies provide security solutions to automatically protect resources on the network and security awareness training to users. This ensures that users are aware of the security threats and provide methods to mitigate them. These measures are useful in a corporate environment where funds exist to enable these security solutions. Public platforms, for example Internet Cafes and schools, allows multiple users to access the Internet using shared resources. This implies that multiple people will use the same computer to perform required tasks. Numerous security threats exist within the Internet sphere that could affect users utilizing shared resources these include but are not limited to viruses, keyloggers and phishing attacks. This shared environment could provide a platform that promotes the spread of virus infections. Users using these platforms should be made aware of these threats and monitor the effectiveness of the security awareness campaign. This paper proposes a system used to address these issues from a single platform. The Shared Public Security Awareness (SPSA) system is an automated virtualized system used to determine the current security awareness levels of users on a shared platform accessing the Internet. The system uses virtual machines to provide users with access to the Internet, assess the security awareness levels of the users, determines if any web browser components were infected by web based malware during browsing sessions, provides users with access to security related material affecting the users and provide reports on online behaviour. This paper evaluates the proposed SPSA system as a mechanism to conduct a security awareness campaign in a shared resource environment while providing a
capability to analyze the online behaviour of users that affects the security of this environment.

**Keyword:** internet cafes, security awareness, security training, virtualized environments, cyber literacy, internet

---

**Information Security Model to Military Organizations in Environment of Information Warfare**

José Martins¹, Henrique Santos², Paulo Nunes³ and Rui Silva⁴

¹, ³Military Academy – CINAMIL, Lisboa, Portugal  
²University of Minho - Department of Information Systems, Guimarães, Portugal  
⁴Lab UbiNET/IPBeja, INESC-ID, Lisboa, Portugal

**Abstract:** This article proposes a model to maximize the information security within military organizations, inserted in environment of Information Warfare. It attempts to answer three fundamental questions, *what to do, why and how?* to protect the information and Information Systems of possible incidents related to the information security that may affect confidentiality, integrity and availability of information. The main variables to be considered are defined and their possible values are proposed. These variables are obtained by means of an interpretative epistemological approach, through a literature review, the use of research methods of Contents Analysis, Focus Group and the General Morphologic Analysis method. To respond in an integrated manner to the three questions above, the model considers the possible incidents of information security in Information Systems, taking into account primarily the main components of the security risks of Information Systems that collect, store, process, transmit and disseminate the information. Its operation is guided by the military concepts of Information Warfare, Information Assurance, the most important principles of war applied to Defensive Operations and the military doctrine of Information Operations. Given the type of problem identified in the study, focusing primarily on the analysis of scenarios of information security incidents and interconnection with the planning and selection of security controls, the method used is the General Morphological Analysis. This method allows for the prediction of possible scenarios of incidents related to information security at the organizational level, which results in
the selection of the most efficient solution of security controls, to max-imize the security of information. Information security must guarantee con-fi-dentiality, integrity and availability of information and seeks to contribute, by means of the operational implementation of the military concept of Information Assurance, to achieve the information superiority.

**Keywords:** information security management, information assurance, in-formation security model, general morphological analysis, information warfare

Simulation Approach for Military Cyber Operations

Ben Morton¹, Sylvain Leblanc¹ and Melanie Bernier²
¹Royal Military College of Canada, Computer Security Laboratory, Kingston, Canada
²Defence Research and Development Canada, Centre for Operational Research and Analysis, Ottawa, Canada

**Abstract:** Cyber operations are expected to become more important, and thus military commanders and staff will need to be trained in these operations. The aim of this paper is to describe an approach for simulating the effects of cyber operations in constructive simulations used for training by modern military forces. The paper argues that it is not currently possible to realistically simulate military cyber operations in a cost-effective manner, due to of the lack of existing data on the subject and the fact that it is not possible to validate available data from the civilian realm against military cyber operations. However, we argue that to educate senior military leaders, it is more important to simulate the effects of cyber attacks than to simulate the actual attacks themselves with a high degree of fidelity. The paper will discuss a set of cyber effects, and introduce an attack taxonomy that focuses on these effects. This taxonomy will discuss the effects of various attack types, along with the level of access to the target computing resource that is required to prosecute the attack. The effects of attacks will be described in terms of their impact on the computing network, computers or other devices. From this, we will derive impacts on mission capabilities, and discuss how these could be implemented inside constructive simulations. For example, to demonstrate the effects of a denial-of-service (DoS) attack, it is not necessary to carry out the attack itself; it may be suf-
ficient to disconnect the server that is the target of the DoS attack. When prosecuting an attack, adversaries must always contend with limited resources and time. In order to integrate cyber operations in constructive simulations with a measure of realism, the paper will discuss a mechanism to limit the cyber attacks available to an attacker in terms of available resources and time. The approach will also introduce the concept of stochastic attack success by assigning probabilities of attack success against known defences. Finally, the paper will discuss avenues of future and related work, including the relationship of this work with the Metrics Framework for Cyber Command and Control paper, (Bernier et al. 2012) also presented at this conference. **Keywords:** cyber operations, constructive simulation, education, cyber effects, military operations

### A Taxonomy of Technical Attribution Techniques for Cyber Attacks

**Andrew Nicholson, Tim Watson, Peter Norris, Alistair Duffy and Roy Isbell**  
*De Montfort University, Leicester, UK*

**Abstract:** In recent years the number of cyber-attacks has dramatically increased, affecting military, government, business and home users. For example, the UK Ministry of Defence claims to have blocked and investigated over 1000 serious cyber-attacks in 2010 while in 2011 Detica reported that the cost of cybercrime in the UK is estimated to be £27 billion per annum. In cyber-attacks numerous methods exist that can be used to discover information about the attacking entity, otherwise termed as attribution. Attribution is a desired quality to counter a variety of attackers. Cyber-crime attribution can aid police investigations in identifying cyber criminals. In cyber warfare and conflict an attribution capability is desired to enhance decision making of Computer Network Operations (CNO). Attribution of terrorist cyber-attacks may help to prevent future attacks. Highly publicised attacks such as Stuxnet and Night Dragon have been subject to intense analysis, yet published attribution of these attacks has been minimal. The complexity of reliable attribution is increased by an attacker’s ability to route attacks through compromised systems, anonymised networks, proxy servers and various jurisdictional boundaries. There are numerous technical attribution techniques ranging from traceback, malware inspection and honeypot deployment. In this paper we present a taxonomy
A Vulnerability-Based Model of Cyber Weapons and its Implications for Cyber Conflict

Karlis Podins and Christian Czosseck
Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Abstract: Throughout history, mankind has developed and employed novel weapons systems and equally novel countermeasures. Naturally, both offensive and defensive systems are limited by the laws of nature. Consequently, military concepts and doctrines were designed by implicitly taking into account those same limitations. The digital age has introduced a new class of weaponry that poses an initial challenge to our common understanding of conflict and warfare as for their different characteristics: cyber weapons. Cyber weapons and other terms like hacking are used frequently, commonly without giving clear definitions in the given context. We propose a restricted definition of cyber weapons as consisting primarily of data and knowledge, presenting themselves in the form of prepared and executed computer codes or a sequence of user interactions with a vulnerable system. This article explores the crucial differences between the conventional weapons and cyber weapons domains, starting a debate on to which extent classical concepts and doctrines are applicable to cyber space and cyber conflict. This motivates a discussion on the role of vulnerabilities in IT systems and their impact to IT security and cyber attacks. The authors describe a vulnerability-based model for cyber weapons and for cyber defense. This model is then applied to describe the relationship between cyber-capable actors (e.g. nation-states). The proposed model clarifies important implications for cyber coalition-building, and disarmament. Furthermore, it presents a general solution for the problem of the destruction of cyber weapons, i.e. in the context of cyber arms control.

Keywords: cyber weapons, cyber defense, disarmament, coalition, vulnerabilities
Modelling Emergency Response Communication Systems

Graeme Pye and Matthew Warren
School of Information Systems, Faculty of Business and Law, Deakin University, Geelong, Australia

Abstract: Subsequent to the Australian ‘Black Saturday’ bushfires there were a number of issues arising from investigations with regard to the functional stability and resilience of communications systems and the flow of information between emergency response organisations, and their ability to provide relevant information to the general public. In some cases, the transference of information failed or was late or ineffective with regard to decisions, advice and information broadcasting during the crisis. This was particularly evident in terms of managing emergency organisational information requests and field situational advice both to and from emergency response management teams and the delivery of informative advice to the public. This paper analyses one such case study with a view of applying a systems modelling technique to determine the viability of the communication systems and information exchange structures associated with an emergency response agency.

Keywords: communication, resilience, emergency response, systems modelling

Digital Finland: Life at the Screen

Jari Rantapelkonen1 and Saara Jantunen2
1Department of Tactics and Operations Art, National Defence University, Helsinki, Finland
2Department of Leadership and Military Pedagogy, National Defence University, Helsinki, Finland

Abstract: This article aims to critically engage the Finnish cyber narrative from the perspective of human life. It discusses the representation and the narrative of future 'cyber life', as presented by the Finnish authorities through the Digital Finland document written in 2010. Digital Finland is a
It proposes three alternative government programs for managing Finnish communication services and labels them as "progressive", "dynamic" and "decisive". These proposals make rhetorical claims and narrative assumptions about what is noteworthy in cyberspace, providing empirical data for analysis. The analysis discusses the actors and the actions reported in the document in the spirit of critical discourse analysis: Who are the participants in cyber life, and what are their actions and responsibilities? What do these narratives reveal of the authorities' perceptions of the cyberspace and its actors? The results show that the alternative programs are not only positive metanarratives of imagined future, but arbitrary and vague descriptions of the use of political power: without any reference to what is meant by "digitalizing", it remains unclear what makes the program labeled as "Decisive Finland" decisive. By choosing the terms "progressive", "dynamic" and "decisive" to describe the options, the authorities impose a desired image that corresponds with the promotion of the Nordic welfare model. What is listed under these definitions remains political. The "decisive" program proposes most funding and government control, and presents the most concrete and detailed plan for future cyber life. In contrast, the "dynamic" program is discussed in highly abstract terms and lacks indication of the roles and responsibilities, making it an unattractive option. In terms of content, *Digital Finland* fails to recognize the interrelationship between information technology and social life as complex questions about the nature of society, and ignores how networks, technology and society co-constitute each other.

**Keywords**: cyber strategy, cyber policy

---

**Finding Suspicious Activity on Computer Systems**

Neil Rowe and Simson Garfinkel  
U.S. Naval Postgraduate School, Monterey, California, USA

**Abstract**: When computer systems are found during law enforcement, peacekeeping, counter-insurgency or similar operations, a key problem for forensic investigators is to identify useful subject-specific information in a sea of routine and uninteresting data. For instance, when a computer is obtained during a search of a criminal organization, investigators are not as
much interested in the machines used for surfing the Internet as the machines used for accounting of drug deals and emailing to co-conspirators. We are doing research on tools to enable investigators to more quickly find such relevant information. We focus on the directory metadata of a computer drive, the listing of the stored files and directories and their properties, since examining it requires much less time than examining file contents. We discuss first what ways people try to hide things on drives. We then discuss clues that suggest concealment or atypical usage of a drive, including encryption, oddities in file names, clusters of deletions, atypical average values, and atypical clusters of files. We report on experiments we have conducted with a corpus of drives purchased from a range of countries. Processing extracted the directory metadata, classified each file, and calculated suspiciousness metrics on the drives. Experimental results showed we could identify some suspicious drives within our corpus but with a certain number of false alarms.

**Keywords**: digital forensics, law enforcement, drive classification, metadata, suspicion

---

**The Comprehensive Approach as a Strategic Design to run the Military-Industrial Complex in Operations**

Mirva Salminen and Aki-Mauri Huhtinen

1Department of Social Sciences, University of Lapland, Finland
2Department of Leadership and Military Pedagogy, National Defence University, Finland

Abstract: How to steer the 21st century military actions that are concurrent both in the real world and in virtual networks? The 20th century saw immense struggles between nation states that contained a level of unprecedented material and human destruction. After the great wars, the Cold War and nuclear weapons paralysed the application of military plans in the organisation. The new wars and global threats that emerged towards the change of the millennium required the re-thinking of military organisation, planning and conduct. Simultaneously, the information revolution penetrated the battle space. These developments have lead to an increasingly complex security space, in which the military-industrial complex influences both virtual and material aspects of warfare, politics and economy. The
21st century introduced the general public with so far undetected actors in conflict zones, that is, with private military and security contractors (PMSCs). The policy of outsourcing warfare and security related functions that were seen primarily, at times even solely, as state functions raised heated discussion; especially, when an increasing number of scandals related to PMSCs’ conduct as well as to the governmental contracting practices was discovered. Despite the strong rhetorical opposition to PMSCs, they have become codified as a steady part of the military-industrial complex. This paper scrutinises the basic principle and key concepts of the new western politico-strategic level military planning model called the Comprehensive Approach (CA). It is a Wikileaks type of open door policy: everyone operating in the same real space can participate in the shared virtual planning space in order to fill in the comprehensive picture of the parallax and the narrative gap. The model’s usability in a new military atmosphere in which private contractors operate alongside public soldiers and attend the planning is under scrutiny. Challenges that the open planning creates to the military organisation are highlighted.

**Keywords**: comprehensive approach, strategic planning, military-industrial complex, private military and security contractors

---

**User-Side Password Authentication: A Study**

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

**Abstract**: Researchers have for a time been struggling to change inert mindset of users regarding passwords as a response to advances in processing power, emergence of highly-scalable computing models, and attackers prioritizing human element for attacks. Recommendations regarding security are ignored as documented by recent corporate database breaches and releases of unencrypted password caches which corroborated lacking security awareness in vast majority of Internet users. In order to educate users about computer security, terms such as hashing, cipher systems and their weaknesses, brute-force attacks, social engineering, multi-factor authentication, and balance between usability and ease of use must be clearly explained. However, academia tend to focus on areas requiring deep mathematical or programmatic background, clear communication of
these security elements while minimizing scientific rigor thus remains challenging. The article aims to provide a concise, comprehensive research overview and outline of authentication, including information entropy, hashing algorithms, reverse password engineering, importance of complexity and length in passwords, general-purpose attacks such as brute-force and social engineering as well as specialized ones, namely side-channel interception. Novel ways of increasing security by utilizing two- and multi-factor authentication, visual passwords, passphrases, mnemonic-based strings will be considered as well along with their advantages over the traditional textual password model and pitfalls for their widespread propagation. In particular, we hypothesize that technological developments allow vendors to offer solutions which limit unauthorized third parties from gaining windows of opportunity to exploit weaknesses in the authentication schemes. However, as infrastructure becomes more resilient, attackers shift their focus towards human-based attacks (social engineering, social networking). Due to largely unchanging short-term behavior patterns, institutions need to lecture employees over extended periods about being vigilant to leaks of procedural and organizational information which may help attackers bypass perimeter-level security measures. We conclude the article by listing emerging threats in the field, specifically social networks-distributed malware and mobile devices targeting.

**Keywords**: authentication, security, hash, password, mnemonic, visual, multi, factor, social, brute-force, attack, engineering, passphrase, side-channel

---

**Multi-Level Security Cannot Realise NEC Objectives**

**Harm Schotanus, Tim Hartog and Cor Verkoelen**

**Information Security Dept., TNO Information and Communication Technology, Delft, The Netherlands**

**Abstract**: Multi-Level Security (MLS) is often viewed as the holy grail of information security, especially in those environments where information of different classifications is being processed. In this paper we argue that MLS cannot facilitate the right balance between need-to-protect and duty-to-share as required for a Network Enabled Capability (NEC) based military operations. This is due to the fact that MLS is deemed rigid in its re-
restrictions; it obstructs the flow of information towards lower classifications by definition and thus influences duty-to-share; furthermore MLS results in a set of rigid preconditions for the physical environment to guarantee the required need-to-protect. The focus of a security solution instead should be on flexibility towards information sharing and reducing risks to be useful in a NEC environment. This can be achieved by firstly reducing the size (and complexity) of the systems that contain the classified information systems, using Multiple Independent Levels of Security (MILS) to create these smaller, separated compartments; and secondly controlling the information flow between the (different) classified compartments by dynamic policies. Moreover, the realignment of classification provisions can make management of information much more flexible and efficient. Hence, we can finally forget MLS.

**Keywords:** MLS, MILS, information security, classified information, policies

**From Kinetic Warfare to Strategic Communications as a Proactive and Mind-Centric Paradigm of the art of war**

**Töstti Sirén**
**National Defence University, Finland**

**Abstract:** Traditionally, the purpose of war has been to influence the Other’s behaviour, or even to destroy the existence of the Other. In this article, war has been referred to as the violent, or killing-prone, state of the human mind. The art of war, for its part, involves an understanding of ideational possibilities and restrictions along with future-oriented open-mindedness to reach grand-strategic ends set by political authorities. If the fundamental maxim of the art of war is understood as the proactive avoidance of kinetic wars without losing peace as it has been understood in this article, then individual and collective minds should be recognised as the essential targets to be influenced, not by kinetics, but by incentives for cooperation. Methodologically, this article focuses on both Social Constructivism (habituation and reification theses) and Critical Realism (emancipation thesis) as social theories and abductive content analysis as a method. While we may be habituated into the past contexts of war and the art of war, which may even be reified in their nature, there is still space
for emancipation – the power of new ideas. This article argues that during
the past decade the mentioned maxim of the art of war has found promin-
ience in the comprehensive, proactive and mind-centric paradigm of the
art of war, Strategic Communications (StratCom), which is based on the
theory of positive recognition. The theory of positive recognition assumes
that human societies may reconstruct their domestic structures (identities,
interests and social systems) in order to earn ‘universal recognition’ in the
eyes of other human societies. The challenge of liberal democratic human
communities and societies is then to seduce intolerant human communi-
ties and societies to reconstruct their constitutive identity structures by
‘being wonderful and acting accordingly’.

Keywords: war, the art of war, paradigm, strategic communications,
emancipation

Cablegate Analysis of Likely Espionage of Nokia by the United States

Daniel Strmecki¹, Wilke Schwiedop², Emmanuel Oyo-Ita, Brigitte
Kaagman⁴, Pierre Leandre⁵, Enrique Santos-Brihuega⁶, Lateef Kadiri³ and
Jessica Dufmats⁷
¹University of Zagreb - Faculty of Organization and Informatics, Croatia
²University of Applied Sciences Bonn-Rhein-Sieg, Germany
³University of Salford, UK
⁴Hogeschool van Amsterdam, Netherlands
⁵ESIEA, France
⁶Universidad de Alcalá, Spain
⁷Mid Sweden University, Sweden

Abstract: In recent years computing has shown an increasing shift towards
mobile devices. Smartphones and similar devices such as tablets are be-
coming more powerful and less expensive every day and as such are be-
coming more widespread not only in developed, but also in developing
countries. Alongside the development of the mobile devices, the internet
offers an increasing amount of services for these devices. This evolution of
mobile devices from simple telephones to portable computers as well as
their increased interconnectivity however also made them more prone to
security issues. As such secret services around the world are given more
possibilities and opportunities to use these mobile devices for espionage and widespread surveillance. The recent leak of cables sent by US embassies around the world also known as the 'cablegate' gives us an opportunity to get a better understanding of this issue. In the light of these events we tried to measure to which extent US have spied on European companies, especially one of the leading manufacturers of mobile devices around the world, Nokia. We set up a database and preprocessed the embassy messages to allow us to search through the huge amount of data in short time. We then investigated Nokia's fields of business to find possible contact points to special agencies. Additionally we looked for other reasons why special agencies might have a specific interest in Nokia. With this information we analyzed the data. The analysis clarifies two major key points: Firstly it validated the assumption that mobile devices, even civil ones, play an important role in modern warfare. They are used not only by US special agents, but also by guerrilla forces to coordinate military operations. Secondly Nokia is a main competitor to American companies in the fastest growing markets worldwide, such as India and China. This paper intends to present the results and the main conclusion of our analysis.

**Keywords:** Wikileaks, cablegate, Nokia, espionage, mobile devices, smartphones

---

**Practical Application of Open Source Frameworks to Achieve Anti-Virus Avoidance**

*Ignus Swart*

**CSIR, Pretoria, South Africa**

**Abstract:** A common aim of malware creators is to have the ability to spread their software undetected through various networks until the required goal is completed. In response to this, anti-virus vendors have implemented various strategies to detect viruses as they attempt to execute and propagate from one target to the next. Some of the anti-virus vendors claim to achieve impressive success rates as high as 98.7% that indicates the problem of spreading viruses and malware is well taken care of. Yet, despite the impressive detection rates, a proliferation of open source tools, frameworks and utilities are being introduced that claim to have the ability to avoid anti-virus detection. As an example, the very popular
Metasploit framework has several encoders available that can alter the virus signature in such a way that it will avoid the anti-virus engine and allow the malicious code to be executed. This approach has been implemented and simplified in the Social Engineering Toolkit (SET) as part of a menu driven approach that is accessible to people with a relatively low skill level. The SET framework, implemented in Metasploit, is only one such framework and several more specialised open source tools exist, that does not only focus on encoding but on other common anti-virus avoidance techniques such as binary editing, packing and encryption. Open source packages such as UPX compress the data in the selected virus executable to such an extent that it will most likely completely circumvent the anti-virus and similarly so for a program that is encrypted with a common encryption product such as TrueCrypt. Should the anti-virus still detect the offending executable after either packing or encryption a combination of the two applications might yield superior results. The aim of this paper is to experiment on a common executable that is classified as malware e.g. the meterpreter module of Metasploit, and make use of the various open source frameworks and utilities to document the techniques and success rate of anti-virus avoidance. By presenting the results of this research, it will contribute to the understanding of security personnel / researchers on what can be achieved with open source frameworks and how to better protect against the virus threat. Paper Relevance: While great strides have been made in anti virus detection it is not nearly perfect and many open source tools can be used to effectively hide even old executables flagged as malicious. The question is how difficult is it to use these tools and how effective are they?.

**Keywords:** antivirus avoidance, open source packer, protector, binder

---

**Overt Information Operations During Peacetime**

Selma Tekir  
Izmir Institute of Technology, Izmir, Turkey

**Abstract:** Information superiority is the most critical asset in war making. It directly addresses the perception of the opponent and in the long term the will of him to act. Sun Tzu's classical text states this fact by the concept of deception as the basis of all warfare. The success in warfare then is de-
pendent on being aware of what’s happening, accurately realizing the context. This is the intelligence function in broad terms and mostly open source intelligence as it provides the context. Competitive intelligence is based mainly on open sources and day by day the open source share in the intelligence product is increasing. Present diversified open sources & services represent a methodology shift in war. The two preceding ways have been overt physical acts against military targets in wartime and covert information operations conducted throughout peacetime against even non-military targets respectively. The present methodology must be overt (open) information operations during peacetime. This coincides with a metaphor change as well. It proposes a transformation from a war metaphor into a game metaphor in which there are some playing rules. In fact, the existence of such rules helps in drawing the boundary of the field of competitive intelligence and thus making it a profession. Game metaphor is safer to adopt than war as it’s easier to take responsibility in public disclosure scenarios in this case. By following this metaphor, you continue to stay in the boundary of legitimate competition. In other terms, you make a conscious preference in terms of war intensities by choosing to avoid the more intense war forms limited conflict, and actual warfare respectively. Finally, this preference is in accordance with the fundamental point of the Sun Tzu's entire argument: The vision of victory without fighting. To summarize, open source domination in the competitive intelligence lays the ground for the game metaphor that represents a transformation in warfare. The apparent outcome is overt information operations during peacetime. It emerges as the most important tool to fight against deception, thus success in information warfare in the contemporary world. **Keywords:** information warfare, information operations, competitive intelligence, open sources, ethics

**Novel Tracking of Rogue Network Packets Using Danger Theory Approach**

**Solomon Uwagbole, William Buchanan and Lu Fan**  
Centre for Distributed Computing, Networks and Security, Edinburgh Napier University, Edinburgh, UK

**Abstract:** Recently there has been heightened, continuous, and intrusive activity by remotely located rogue hacking groups, such as Anonymous and
Lulzsec. These groups often aim to disrupt computer networks and gain access to private confidential data. A typical method used to steal confidential data is by SQL Injection (SI). This problem is likely to increase as Cloud Computing gains popularity, thereby moving organisations’ network security boundaries, firewall, deeper into the internet cloud environment. There is thus a strong requirement for a real-time framework that detects and mitigates any intrusion activities as, and when, they occur. Conventional firewalls lock down ports and applications, but often does little against malicious packets stealthily concealed in legitimate network packets payload, thus a framework that solely depends on network packets payload analysis for malicious fingerprint, rather than traditional system calls and processes is required. This paper thus presents a novel framework that introduces the vaccination of Danger Theory’s Dendritic Cell Algorithm (DCA) for the real-time detection and mitigation of network intrusions. The proposed framework draws an inspiration from the active and passive biological immune systems in which the human body has an efficient autonomous response to fight infections on encountering danger signals to indicate anomalies in cellular activities. This immunological principle is widely adopted in the computational field of study of Artificial Immune Systems (AISs). To achieve this novel bio-inspired computational framework of detection and response, there is research work in progress using .NET Framework implementation of DCA. There are two stages to this implementation which are creating detecting receptors input data to train DCA, and finally, using the trained DCA in real-time for detecting anomalous network packets payload. Take an example of database security exploit of SI that is discussed in this paper. Stage one involves creating detector precursor (receptors) by subjecting a database to be protected to a controlled SI scripts or code with the network packets payload of such exploits captured in real-time by using .NET custom built packets analyser. Stage two involves real-time monitoring of protected databases for anomaly (antigens) through the trained DCA by using r-contiguous rule to match receptors with antigens in the data pre-processing stage when immature Dendritic Cell (DC) is transformed to semi-mature or matured. The structure of SI packets is now constructed to easily isolate SI malicious packets from legitimate network packets payloads between known source and destination of confidential data request. The approach in brief is: protected data or assets are modelled as cells in tissues to be monitored; while rogue network packets triggers the computational modelled DCs to co-stimulate B and T Cells as to provide detection feedback to the protect-
ed cells. The outcome of this paper can be practically applied in: detecting an attempt to steal protected data and applications by a rogue remote intruder; and detection of man-in-the-middle attacks on applications that sit in cloud. The proposed bio-inspired approach to resolving SI computer systems security challenges is a research work in progress by this paper’s author. The research proposes an easy adaptation of the system to any domain as the finger-print required for detection and training the system is now introduced by vaccination method. **Keywords:** intrusion, detection, immunised network, danger theory

**Building an Ontology for Cyberterrorism**

**Namosha Veerasamy**¹, **Marthie Grobler**¹,² and **Basie Von Solms**²

¹Council for Scientific and Industrial Research, Pretoria, South Africa

²University of Johannesburg, South Africa

**Abstract:** Cyberterrorism and the use of the Internet for cyberterrorism is an emerging field. Often cyberterrorism activities overlap with traditional hacking and Information and Communication Technology (ICT) Infrastructure exploitation. As a result, the defining and differentiating characteristics of cyberterrorism can easily be misunderstood. The use of an ontology specifically developed for cyberterrorism, will provide a common framework to share conceptual models. By using an ontology, the internal and external environment of a field (in this case, cyberterrorism) can be captured together with the relationships between the environments. This paper proposes an ontology to identify whether a cyber event can be classified as a cyberterrorist attack or a support activity. The role of the cyberterrorism ontological model will be to provide a better structure and depiction of relationships, interactions and influencing factors by capturing the content and boundaries in the field of cyberterrorism. The ontology will be developed using a cyberterrorism framework covering influencing factors, together with a compiled network attack classification ontology. Classes will be drawn from research carried out on the use of ICT in the support of cyberterrorism. As defined in this research, a cyberterrorism attack consists of a high-level motivation that is religious, social or political. The individual/group can furthermore be classified as having a specific driving force depending of the level of extremism or revolutionary thinking. Thus, the ontology will take into consideration the motivating charac-
Characteristics that play a significant role in contributing towards the definition of cyberterrorism. Overall, this paper promotes the understanding of the field of cyberterrorism and its relation to ICT manipulation, together with the use of the Internet to support terrorism in general. Ontologies enable a common view on a specific domain to generate knowledge that can be shared and reused. Ontologies can further be populated with specific dynamic instances of information and therefore can be used to generate real-world scenarios. In this paper, the proposed ontological model will form a knowledge base for the field of cyberterrorism and will provide instances that aim to convey realistic cyberterrorism situations and support examples.

**Keywords:** anti-forensics, Internet, terrorism, ICT, propaganda, social-networking

---

**Swarm UAV Attack: How to Protect Sensitive Data?**

Robert Erra, Vincent Guyot, Loica Avanthey, Antoine Gademer and Laurent Beaudoin
SI&S and ATIS Lab, ESIEA, Paris, France

**Abstract:** We consider the following scenario: a swarm of UAVs has a mission and a UAV from it has been captured: is it possible to secure (in a broad sense) the sensitive data and software in such a way as to avoid any information leak in this situation. In this article we study a possible solution using in a complementary way: an embedded secure token (a smartcard); Shamir's secret sharing algorithm associated to k-ary goodware.

Either of these tools can bring a very high level of security.

**Keywords:** military swarm, secret sharing scheme, secure token, k-ary goodware
PHD Papers
Proposal for a new Equation System Modelling of Block Ciphers and Application to AES 128

Michel Dubois and Eric Filiol  
Laboratory of Operational Virology and Cryptology, Laval, France

Abstract: One of the major issues of cryptography is the cryptanalysis of cipher algorithms. Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is normally required. Some mechanisms for breaking codes include differential cryptanalysis, advanced statistics and brute-force. Recent works also attempt to use algebraic tools to reduce the cryptanalysis of a block cipher algorithm to the resolution of a system of quadratic equations describing the ciphering structure. As an example, Nicolas Courtois and Josef Pieprzyk have described the AES-128 algorithm as a system of 8000 quadratic equations with 1600 variables. Unfortunately, these approaches are, currently, deadlocks because of the lack of efficient algorithms to solve large systems of equations. In our study, we will also use algebraic tools but in a new way: by using Boolean functions and their properties. A Boolean function is a function from $F_2^n$ to $F_2$ with $n>1$, characterized by its truth table. The arguments of Boolean functions are binary words of length n. Any Boolean function can be represented, uniquely, by its algebraic normal form which is an equation which only contains additions modulo 2 -- the XOR function -- and multiplications modulo 2 -- the AND function. Our aim is to describe a block cipher algorithm as a set of Boolean functions then calculate their algebraic normal forms by using the Möbius transforms. After, we use a specific representation for these equations to facilitate their analysis and particularly to try a combinatorial study. Through this approach we obtain a new kind of equations system. This equations system is more easily implementable and could open new ways to cryptanalysis. To test our approach we first apply this principle to the mini-AES cipher and in a second time to AES-128 algorithm.

Keywords: block cipher, Boolean function, cryptanalysis, AES

Berg Hyacinthe
Assas School of Law, CERSA/CNRS, Université Paris II, Sorbonne; France

Abstract: When computers and computer systems are treated and utilized as weapons of war, it becomes more difficult to deny legal implications under domestic and international laws. In effect, many legal scholars have called for Rules of Engagement that would govern i-Warfare conducts, while taking into consideration the applicable notions of the laws of armed conflicts (LOAC). However, even the most powerful military in the world is still struggling with i-Warfare’s legal ambiguities and technical challenges. As U.S. Army Gen. Martin Dempsey, chairman of the Joint Chiefs of Staff, acknowledged, during his Senate confirmation hearings, he is “not particularly well versed” on the subject of cyber warfare — a lacuna shared with his predecessor, Navy Adm. Mike Mullen. Nonetheless, they both agree on the need to combine diplomatic, military and economic prowess, in order to neutralize one of the most challenging threat to U.S. national security today: asymmetric cyber warfare. Several indicators continue to show that the U.S. strategic agendum aimed at “information dominance” would fail, if it does not include a competent level of knowledge of the laws that should — and will likely govern — the use of digital information technologies in warfare during this millennium onward. To acquire such knowledge, the most basic concepts found in such solid legal doctrines as Thomas Hobbes’s positive law paradigm or/and John Locke’s moral obligation principle may be helpful. Hence, this article highlights the danger associated with the introduction of new “high tech” weapons of war on the battlefield, in the absence of appropriate legal measures as required by laws of armed conflicts, military field manuals of modern States, and under Article 36 of 1977 Additional Protocol I to the Geneva Conventions of 1949. Furthermore, it discusses how and under what conditions military drone strikes may be conducted, to comply with domestic laws as well as international conventions and treaties. The author concludes with the following call to U.S. and NATO officials: protect your cyber warriors against obvious cybercrimes of war and “cyber-boosted” crimes against humanity by enacting appropriate and consensus-driven legislations.

Keywords: space sovereignty, information operations in space, space laws & treaties; ASAT & communications satellites; military drones; computers-as-weapons
Cyber Threat Management in Cognitive Networks

Anssi Kärkkäinen
Defence Command Finland, Helsinki, Finland

Abstract: Threats and attacks in cyberspace are growing in number and sophistication, originating different sources and encompassing intentional attacks as well as inadvertent causes. Despite ongoing development of security products, many organizations feel their infrastructure is inadequate for combating rapidly evolving threats. Next generation information and communication technology provides cognitive networking capabilities which also are challenging from security point of view. The cognitive network is defined as a network with a cognitive process that can understand current conditions, plan, decide, act on those conditions, and learn from the results of actions. This adaptive and self-acting behavior of the network requires new approaches to cyber threat management. Risk management and security mechanisms of the network must adapt to cyber threats and dynamically provide a coordinated response in real-time. The paper presents a framework for cyber threat management system for the cognitive networks. The framework consists of three layers. The first layer includes a single network node, the second one contains a cluster of nodes and the third one covers the entire network. The framework describes a risk assessment process, and includes also security policy aspects. Also, implementation challenges of the proposed framework are discussed in this study.

Keywords: cyber threat, cognitive network, threat management

A Framework for the Detection and Prevention of SQL Injection Attacks

Emad Shafie and Antonio Cau
Software Technology Research Laboratory (STRL), Faculty of Technology, De Montfort University, Leicester, UK

Abstract: The use of Internet services and web applications has grown rapidly because of user demand. At the same time, the web application vul-
Vulnerabilities have increased as a result of mistakes in the development where some developers gave the security aspect a lower priority than aspects like application usability. An SQL (structure query language) injection is a common vulnerability in web applications; it has been classified as the most dangerous type of vulnerability according to OWASP (Open Web Application Security Project) statistics (OWASP, 2010). An SQL injection vulnerability allows the hacker or illegal user to have access to the web application’s database and therefore damage the data, or change the information held in the database. This paper will discuss a framework for the detection and prevention of common types of SQL injection attacks. The framework consists of three main components; the first component will check the user input for existing attacks, the second component will check for new types of attacks, and the last component will block unexpected responses from the database engine. Additionally, our framework will keep track of an ongoing attack by recording and investigating user behaviour. The framework is based on the Anatempura tool, a runtime verification tool for Interval Temporal Logic properties. Existing attacks and good/bad user behaviours can be specified using Interval Temporal Logic. Moreover, this paper will discuss a case study where various types of user behaviour are specified in Interval Temporal Logic and show how these can be detected.

**Keywords:** SQL injection, user input checker, runtime verification, database observer
Work In Progress Papers
Information Systems Security Management (ISSM) Success Factor: Retrospection From the Scholars

Azah Anir Norman and Norizan Mohd Yasin
University of Malaya, Kuala Lumpur, Malaysia

Abstract: Information System Security Management (ISSM) studies today have presented remarkable solutions in addressing security management (SM) problems. Many companies have designed SM procedures to protect their businesses from threats. Often, ISSM implemented by these businesses are based largely on common practices, current understanding and business requirements which seldom reach optimum levels. This presents risks as such practices often lead to resource wastage and security abuse. This paper attempts to review previous studies on ISSM implementation. This retrospection study aims to determine the most influential factors for successful ISSM implementation in a business. The study reviewed selected journal articles and conference papers in the field of information systems security. The three main classes of success factors in ISSM comprise technology characteristics, organizational structure and environmental influences. The success factors were collated from the ISSM success theoretical model which is based on selected IS theories. Fundamentally, technology, process and human elements that form the management mechanism were found to be vital for successful ISSM implementation. Retrospection of various scholars’ practical-theoretical-experimental researches and views enables better understanding and the subsequent assimilation of success factors that influence successful ISSM implementation in a business context.

Keywords: information system security management, success factor, security management, information systems security
Abstracts only
CNA by Social Media, or is it 5th Generation Warfare

Harry Kantola
Finnish National Defense University, Helsinki, Finland

Abstract: Society today uses information to handle daily matters. Both civilian and military actors are dependent on the cyber network. In order to be able to protect these networks, one has to understand how to attack them. The purpose of this paper is to discuss level of ambition and methods within the Computer Network Attack (CNA) environment that a military force can deal with in a small state. What kind of technological CNA capability is recommended and how can this operational capability be achieved? Study results show that a state with an advanced technological level should aim to have high qualifications in the field of testing and defending their own critical systems and infrastructure. Such a qualification is the ability to perform Computer Network Exploitation (CNE) activities. A military force that can perform CNE activities can, with help of strategic partners such as universities and high-tech industries, conduct needed CNA actions. The level of ambition does not need to exceed the ability to perform CNE activities. Even though the CNE activities are mainly technological, the information-psychological effect can be achieved through thorough coordination within information operations. To achieve a goal through CNA activities can be reached multiple ways. One way to reach wanted effects can be through causing destruction or malfunctionalities in equipment, command and control or in SCADA (supervisory control and data acquisition) -systems. These methods require extensive knowledge of the targeted system, information about the weaknesses in it and access to high performance simulation systems. By attacking different material systems may the attacker influence the target audience by not letting them have reliable systems in use for their needs. Another way to reach the same effect can be done through social media and by influencing the information that leaders and decision makers need for their mission. The interesting question is in what level or combination of these methods are suitable for small states in order to create suitable CNA capabilities in a cost efficient way. Should a small state concentrate in the use of social media or does it also need some proficiency in attacking technical systems also. Is computer network attacks which are conducted through social medias a fifth generation of warfare together with unmanned fighting systems, such as un-
manned aerial vehicles (UAV) and unmanned ground vehicle (UGV) or is there tougher demands that needs to be filled up. Preliminary study shows that a cost-beneficial way conducting CNA-activities would be through social media, but will that change in conjunction to more extensive use of 5th generation warfare principles? To elaborate further on these issues there is a need to evaluate the effect that can be achieved through CNO. Can this kind of warfare or activity alone accomplish desired effects or do they have to be accompanied with other traditional means of warfare? If it can be used as a standalone method, what kind of effects can it reach and what are the limitations in that case or does it always need to be in conjunction to other means of warfare? If CNO has to be used in conjunction with other military when answering to the requirements from the political elite, what are these means in that case? Does this mean that an act of CNO alone will always be considered an incident of criminality, not a state driven action? What elements are to be found so that a CNO attack will be classified as a stat driven happening? Another interesting point of view is how to evaluate the measure of effectiveness (MoE) CNO activities can bring to operations. Is it even possible to measure the effectiveness or is it only measurement of performance (MoP) that can be evaluated? If there is a possibility to evaluate measurement of effectiveness, then there is certainly a possibility to decide what level of ambition a nation needs in the different aspects of CNO-related warfare technics. These criteria can then be used to describe the capability of different nations. The ability to evaluate effectiveness will also bring the possibility to establish ratings for different types of CNO-activities. But how can the psychological influences be measured and what academic value will that bring to solve this question? Then again, if there is no or limited possibilities to evaluate the measurement of effectiveness, is the only way to evaluate achieved results through evaluating the measurement of performance. This leads to the question, will the method how effects are measured in cyber networks automatically focus on then technological abilities, because there limitations in evaluations or can all aspects be taken in consideration with either of these methods of evaluation or do we need to have both? By evaluating measurement of performance the whole system focuses on the methods and technics used to achieve effects, but can these evaluations be transferred to the psychological level or is it only the amount of destroyed or disabled equipment that matters, as in traditional warfare. This gives us the interesting question of “how to measure the effect of CNO-activities” – technological, measurement of effectiveness or measurement of performance, or
could there be a combination of these and in that case, what kind? Is there any reliable method to measure effectiveness in the cyber domain? And if there is, what are the limitations in these evaluations? All these small questions are aimed to find an answer to what kind of CNO-activities can be used by a mediatorate state and what effects they can accomplish with different ambitions. By focusing on the method of measurement there will probably be different kind of answers to how to conduct CNA. Some abilities can only be measured with numbers and others only by cognitive understanding of the human nature and way of thinking. How can these two different methods bring additional value to the quest of finding the optimal way of conducting CNA from a state perspective?

**Keywords:** cyberwar, cyber, mediatorate state, computer network attack

---

**Critical Databases – Towards a Framework to Protect South Africa’s key Information Infrastructures**

Mzukisi Niven Njotini  
University of South Africa, Pretoria, South Africa

**Abstract:** South Africa has made great strides to protect critical information infrastructures (CIIs). South Africa uses its national key points protection framework as a model to secure CIIs. National key points are places or areas of strategic interest to South Africa. These include any soil or water surface, installation or structure, premises or industrial complexes. The criterion for protection is that the places or areas must be in need of security. The need for security is evidenced by facts demonstrating the critical nature of the places or areas. The risks associated with recent information and communication technologies (ICTs) bring about the need to safeguard CIIs. ICTs facilitate the assembling of large quantities of information into databases. The information can extend to key or critical information. Critical information is *inter alia* information the disclosure of which could weaken the security and stability of a country. Examples of critical information are state secrets. Availability and the interdependency of ICTs contribute to the need to safeguard CIIs. Consequently, the security and protection are no longer limited to physical or stationed places or areas. Security is extended to places or areas that exist in mechanical circles. In view of the foregoing, South Africa adopts measures against acts of sabotage or
cyber-attacks that weakens the integrity and safety of CII s. The measures
distinguish between the necessity to safeguard critical data and database.
Critical data encompasses data that are essential to the protection of the
national security of South Africa or the economic and social well-being of
its citizens. Critical databases include data collected in electronic format.
The measures furthermore prescribe rules to preserve the integrity and
security of critical data and databases. The rules enjoin South Africa to
identify and classify critical data; to register the full names, address and
contact details of the administrator (person who manages critical data-
bases); to identify the location of critical databases or their component
parts, and to outline the general descriptions of information stored in criti-
cal databases. The rules also assist in determining data and databases that
are fundamental to the protection of the national security of South Africa
or the economic and social well-being of South African citizens. This paper
reveals the shortcomings to the South African approach to safeguard CII s.
More specifically, this paper argues that the South African approach fa-
vours a one-size-fits-all method of identifying and classifying critical data
and databases. The aforementioned method assumes that a generalised
approach of identifying and classifying critical data and databases can be
and/or is applicable to all scenarios. Furthermore, the South African ap-
proach acknowledges that critical data and databases protection is aimed
at alleviating direct or indirect attacks to CII s. However, the measures to
secure data and databases in South Africa omit to enunciate critical data
and databases recovery plans and/or strategies in cases where attacks
have occurred.

**Keywords:** CIF, ICT, critical information