## 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>v</td>
<td>iii</td>
</tr>
<tr>
<td>Committee</td>
<td></td>
<td>vi</td>
<td>iv</td>
</tr>
<tr>
<td>Biographies</td>
<td></td>
<td>ix</td>
<td>vi</td>
</tr>
<tr>
<td>Strategies for Combating Sophisticated Attacks</td>
<td>Chad Arnold, Jonathan Butts, and Krishnaprasad Thirunarayan</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Analysis of Programmable Logic Controller Firmware for Threat Assessment and Forensic Investigation</td>
<td>Zachry Basnight, Jonathan Butts, Juan Lopez and Thomas Dube</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>Top-Level Goals in Reverse Engineering Executable Software</td>
<td>Adam Bryant, Robert Mills, Michael Grimaila and Gilbert Peterson</td>
<td>3</td>
<td>16</td>
</tr>
<tr>
<td>An Investigation of the Current State of Mobile Device Management Within South Africa</td>
<td>Ivan Burke and F. Mouton</td>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>A Taxonomy of Web Service Attacks</td>
<td>Ka Fai Peter Chan, Martin Olivier and Renier Pelser van Heerden</td>
<td>4</td>
<td>34</td>
</tr>
<tr>
<td>DUQU’S DILEMMA: The Ambiguity Assertion and the Futility of Sanitized Cyber War</td>
<td>Matthew Crosston</td>
<td>5</td>
<td>43</td>
</tr>
<tr>
<td>Hacking for the Homeland: Patriotic Hackers Versus Hacktivists</td>
<td>Michael Dahan</td>
<td>5</td>
<td>51</td>
</tr>
<tr>
<td>Consequences of Diminishing Trust in Cyberspace</td>
<td>Dipankar Dasgupta and Denise Ferebee</td>
<td>6</td>
<td>58</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>Towards a Theory of Just Cyberwar</td>
<td>Klaus-Gerd Giesen</td>
<td>7</td>
<td>65</td>
</tr>
<tr>
<td>Defamation in Cyber Space: Who do you sue?</td>
<td>Samiksha Godara</td>
<td>7</td>
<td>72</td>
</tr>
<tr>
<td>Identifying Tools and Technologies for Professional Offensive Cyber Operations</td>
<td>Tim Grant and Ronald Prins</td>
<td>8</td>
<td>80</td>
</tr>
<tr>
<td>The Emergence of Cyber Activity as a Gateway to Human Trafficking</td>
<td>Virginia Greiman and Christina Bain</td>
<td>9</td>
<td>90</td>
</tr>
<tr>
<td>Deep Routing Simulation</td>
<td>Barry Irwin and Alan Herbert</td>
<td>10</td>
<td>97</td>
</tr>
<tr>
<td>Development of a South African Cybersecurity Policy Implementation Framework</td>
<td>Joey Jansen van Vuuren, Louise Leenen, Jackie Phahlamohlaka and Jannie Zaaiman</td>
<td>10</td>
<td>106</td>
</tr>
<tr>
<td>Replication and Diversity for Survivability in Cyberspace: A Game Theoretic Approach</td>
<td>Charles Kamhoua, Kevin Kwiat, Mainak Chatterjee, Joon Park and Patrick Hurley</td>
<td>11</td>
<td>116</td>
</tr>
<tr>
<td>Situation Management in Aviation Security – A Graph-Theoretic Approach</td>
<td>Rainer Koelle and Denis Kolev</td>
<td>12</td>
<td>125</td>
</tr>
<tr>
<td>SCADA Threats in the Modern Airport</td>
<td>John McCarthy and William Mahoney</td>
<td>14</td>
<td>141</td>
</tr>
<tr>
<td>Improving Public-Private Sector Cooperation on Cyber Event Reporting</td>
<td>Julie McNally</td>
<td>14</td>
<td>147</td>
</tr>
<tr>
<td><strong>Paper Title</strong></td>
<td><strong>Author(s)</strong></td>
<td><strong>Guide Page</strong></td>
<td><strong>Page No.</strong></td>
</tr>
<tr>
<td>--------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Copyright Protection Based on Contextual Web Watermark</td>
<td>Nighat Mir</td>
<td>15</td>
<td>154</td>
</tr>
<tr>
<td>Towards a South African Crowd Control Model</td>
<td>Mapule Modise, Zama Dlamini, Sifiso Simelane, Linda Malinga, Thami Mnisi and Sipho Ngobeni</td>
<td>16</td>
<td>159</td>
</tr>
<tr>
<td>A Vulnerability Model for a Bit-Induced Reality</td>
<td>Erik Moore</td>
<td>17</td>
<td>169</td>
</tr>
<tr>
<td>Results From a SCADA-Based Cyber Security Competition</td>
<td>Heath Novak and Dan Likarish</td>
<td>18</td>
<td>177</td>
</tr>
<tr>
<td>Design of a Hybrid Command and Control Mobile Botnet</td>
<td>Heloise Pieterse and Martin Olivier</td>
<td>19</td>
<td>183</td>
</tr>
<tr>
<td>Functional Resilience, Functional Resonance and Threat Anticipation for Rapidly Developed Systems</td>
<td>David Rohret, Michael Kraft and Michael Vella</td>
<td>19</td>
<td>193</td>
</tr>
<tr>
<td>What Lawyers Want: Legally Significant Questions That Only IT Specialists can Answer</td>
<td>Yaroslav Shiryaev</td>
<td>21</td>
<td>203</td>
</tr>
<tr>
<td>The Weakest Link – The ICT Supply Chain and Information Warfare</td>
<td>Dan Shoemaker and Charles Wilson</td>
<td>21</td>
<td>208</td>
</tr>
<tr>
<td>Thirst for Information: The Growing Pace of Information Warfare and Strengthening Positions of Russia, the USA and China</td>
<td>Inna Vasilyeva and Yana Vasilyeva</td>
<td>22</td>
<td>215</td>
</tr>
<tr>
<td>Investigating Hypothesis Generation in Cyber Defense Analysis Through an Analogue Task</td>
<td>Rachel Vickhouse, Adam Bryant and Spencer Bryant</td>
<td>23</td>
<td>221</td>
</tr>
<tr>
<td><strong>PHD Papers</strong></td>
<td></td>
<td>25</td>
<td>229</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 Potential Threat of Cyber-Terrorism on National Security of Saudi Arabia</td>
<td>Abdulrahman Alqahtani</td>
<td>27</td>
<td>231</td>
</tr>
<tr>
<td>Improving Cyber Warfare Decision-Making by Incorporating Leadership Styles and Situational Context into Poliheuristic Decision Theory</td>
<td>Daryl Caudle</td>
<td>28</td>
<td>240</td>
</tr>
<tr>
<td><strong>Work in Progress</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack-Aware Supervisory Control and Data Acquisition (SCADA)</td>
<td>Otis Alexander, Sam Chung and Barbara Endicott-Popovsky</td>
<td>31</td>
<td>249</td>
</tr>
<tr>
<td>Cyber Disarmament Treaties and the Failure to Consider Adequately Zero-Day Threats</td>
<td>Merritt Baer</td>
<td>33</td>
<td>251</td>
</tr>
<tr>
<td>Evaluation of a Cryptographic Security Scheme for Air Traffic Control’s Next Generation Upgrade</td>
<td>Cindy Finke, Jonathan Butts, Robert Mills and Michael Grimaila</td>
<td>34</td>
<td>259</td>
</tr>
<tr>
<td>Attack Mitigation Through Memory Encryption of Security-Enhanced Commodity Processors</td>
<td>Michael Henson and Stephen Taylor</td>
<td>35</td>
<td>265</td>
</tr>
<tr>
<td>Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia</td>
<td>Volodymyr Lysenko and Barbara Endicott-Popovsky</td>
<td>36</td>
<td>269</td>
</tr>
<tr>
<td><strong>Non Academic Papers</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Adam and Eve Paradox</td>
<td>Michael Kraft, David Rohret, Michael Vella and Jonathan Holston</td>
<td>37</td>
<td>274</td>
</tr>
<tr>
<td>Offensive Cyber Initiative Framework (OCIF) Raid and Respawn Project</td>
<td>David Rohret, Michael Vella, and Michael Kraft</td>
<td>40</td>
<td>284</td>
</tr>
</tbody>
</table>
Preface

These Proceedings are the work of researchers contributing to the 8th International Conference on Information Warfare and Security (ICIW 2013), hosted this year by The Regis University, Denver, Colorado, USA. The Conference Chair is Daniel Likarish and the Programme Chair is Dr. Doug Hart Regis both from Regis University, Denver Colorado, USA.

The opening keynote address this year is given by David L. Willson on the topic of “Active Defense: How to Legally Defend Beyond Your Network”. The second day will be opened by William Hugh Murray who will talk about “The Drums of War”.

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

With an initial submission of 74 abstracts, after the double blind, peer review process there are 29 research papers, 2 PHD papers, 5 Work in Progress and 2 Non academic papers published in these Conference Proceedings, including contributions from Belguim, Estonia, France, Greece, India, Israel, Netherlands, Russian Federation, Saudi Arabia, South Africa, United Kingdom, United States.

I wish you a most enjoyable conference.

Dr. Doug Hart
School of Computer & Information Sciences Regis University, Denver Colorado, USA
Programme Chair
Conference Committee

Conference Executive
Daniel M Likarish, Center on Information Assurance Studies, Regis University, Denver Colorado, USA
Dr. Doug Hart, Regis University, Denver Colorado, USA
Daniel T Kuehl, National Defense University, Washington, DC, USA
Leigh Armistead, Peregrine Technical Solutions LLC, USA
Andy Jones, Security Research Centre, BT, UK and and Khalifa University, UAE
William Mahoney, The Peter Kiewit Institute, University of Nebraska Omaha, Omaha, USA

Mini Track Chairs
Dr. Robert F. Mills, Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Dayton, Ohio, USA
Joey Jansen van Vurenen, Council for Scientific and Industrial Research (CSIR), South Africa
Dr Louise Leenen, Council for Scientific and Industrial Research (CSIR), South Africa
Dr Barbara Endicott-Popovsky, Center of Information Assurance and Cybersecurity, University of Washington, Seattle USA
Dr Volodymyr Lysenko, Center of Information Assurance and Cybersecurity, University of Washington, Seattle USA

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

Abukari Abdul Hanan (University For Development Studies, Ghana); Dr William Acosta (University of Toledo, USA); Gail-joon Ahn (University of North Carolina at Charlotte, USA); Jim Alves-Foss (University of Idaho, USA); Major Todd Andel (University of South Alabama, USA); Dr Leigh Armistead (Edith Cowan University, Australia); Johnnes Arreymbi (University of East London, UK); Professor Richard Baskerville (Georgia State University, USA); Dr Alexander Bligh (Ariel University Center, Ariel, Israel); Dr Svet Braynov (University of Illinois, Springfield, USA); Dr Susan Brenner (University of Dayton, Ohio, USA); Dr Raymond Buettner (Naval Postgraduate School, USA); Dr Acma Bulent (Anadolu University, Eskisehir, Turkey); Ivan Burke (CSIR, Pretoria, South Africa); Dr Jonathan Butts (AFIT, USA); Dr Marco Carvalho (Institute for Human and Machine Cognition (IHMC), USA); Dr. Joobin Choobineh (Texas A&M University, USA); Prof. Sam Chung (University of Washington, Tacoma, USA); Dr Nathan Clarke (University of
Plymouth, UK); Dr. Ronen Cohen (Ariel University Centre, Israel); Earl Crane (George Washington University, USA); Geoffrey Darnton (Requirements Analytics., UK); Dr Dipankar Dasgupta (Intelligent Security Systems Research Lab, University of Memphis, USA); Evan Dembskey (UNISA, South Africa); Dorothy Denning (Naval Post Graduate School, USA); Jayanthila Devi (Anna university, India,); Dr Glenn Dietrich (University of Texas, Antonio, USA); Dr Hart Doug (Regis University, USA); Prokopios Drogkaris (University of the Aegean, Greece); Barbara Endicott-Popovsky (Center for Information Assurance and Cybersecurity, University of Washington, Seattle, USA); Prof. Dr. Alptekin Erkollar (ETCOP, Austria); Dr Cris Ewell (Seattle Children's, USA); Larry Fleurantin (Larry R. Fleurantin & Associates, P.A., USA); Kenneth Geers (Cooperative Cyber Defence Centre of Excellence, USA); Kevin Gleason (KMG Consulting, MA, USA); Dr Samiksha Godara (Shamshe Bahadur Saxena College Of Law, India); Prof. Dr Tim Grant (Netherlands Defence Academy, Netherlands); Virginia Greiman (Boston University, USA); Dr Michael Grimaila (Air Force Institute of Technology, USA); Daniel Grosu (Wayne State University, Detroit, USA, USA); Dr Drew Hamilton (Auburn University, Alabama, USA); Joel Harding (IO Institute, Association of Old Crows, USA); Dr Dwight Haworth (University of Nebraska at Omaha, USA); Dr Philip Hippensteel (Penn State University, Middletown, USA); Professor Bill Hutchinson (Edith Cowan University, Australia); Dr Berg Hyacinthe (Assas School of Law, Universite Paris Ill/CERSA-CNRS, France); Dr Cynthia Irvine (Naval Post Graduate School, USA); Ramkumar Jaganathan (VLB Janakiammal College of Arts and Science (affiliated to Bharathiar University), India); Joey Jansen van Vuuren (CSIR, South Africa); Dr Andy Jones (BT, UK); James Joshi (University of Pittsburgh, USA); Ayesha Khurram (National University of Sciences & Technology, Pakistan); Prashant Krishnamurthy (University of Pittsburgh, USA); Dr Dan Kuehl (National Defense University, USA); Takakazu Kurokawa (The National Defense Academy, Japan); Rauno Kuusisto (Finish Defence Force, Finland); Dr Tuija Kuusisto (Internal Security ICT Agency HALTIK, Finland); Arun Lakhotia (University of Louisiana Lafayette, USA); Michael Lavine (John Hopkins University's Information Security Institute, USA); Louise Leenen (CSIR, Pretoria, South Africa); Tara Leweling (Naval Postgraduate School, Pacific Grove, USA); Dan Likarish (Regis University, Denver, USA); Prof. Peter Likarish (Drew University, Madison, USA); Professor Sam Liles (Purdue University Calumet, USA); Cherie Long (Georgia Gwinnett College. Lawrenceville, GA, USA); Juan Lopez Jr. (Air Force Institute of Technology, USA); Dr Bin Lu (West Chester University of PA, USA); Volodymyr Lysenko (Center for Information Assurance and Cybersecurity, University of Washington, Seattle, USA); Fredrick Magaya (Kampala Capital City Authority, Uganda); Dr Bill Mahoney (University of Nebraska, Omaha, USA); Hossein Malekinezhad (Islamic Azad University of Naragh, Iran); Dr John
Biographies

Conference Chair

Dan Likarish is an assistant professor in the School of Computing & Information Sciences with responsibility for Information Assurance program coordination, students and research at Regis University. He is Director of the Colorado Front-range Center on Information Assurance Studies. His research and teaching interests are in the design and implementation of student cyber security competitions, security of critical SCADA infrastructure and virtualization of student lab exercises. He has installed and is calibrating a Radio Telescope for use as a K-Collegiate teaching instrument and directs the Rocky Mountain Collegiate Cyber Defense Competition. He is the recipient of various state, industry and federal grants and awards.

Programme Chair

Dr. Douglas Hart is a Professor in the School of Computer & Information Sciences. He is the Chair of the Information Technology Department and the Program Coordinator for the Software Engineering program in the School. Doug has over thirty years of experience in software development and scientific computing. His interests include signal processing and machine learning techniques for recognizing patterns in seismic data. His recent interests are in techniques for integration of software systems.

Keynote Speakers

David L. Willson is a leading authority in cyber security and the law. He is a licensed attorney in NY, CT, and CO, and owner of Titan Info Security Group, a Risk Management and Cyber Security law firm, focused on technology and the law, and helping companies lower the risk of a cyber-incident and reducing or eliminating the liability associated with loss or theft of information. He also assists companies with difficult legal/cyber-security issues. David is a retired Army JAG officer. During his 20 years in the Army he provided legal advice in computer network operations, information security and international law to the DoD and NSA and was the legal advisor for what is now CYBERCOM.
William Hugh Murray, CISSP. Bill is a management consultant and trainer in Information Assurance specializing in policy, governance, and applications. He is Certified Information Security Professional (CISSP) and has served as chairman of the Governance and Professional Practices committees of (ISC)2. He has more than fifty years experience in information technology and more than forty in security. He has been recognized by Information Security Magazine as a Pioneer in Computer Security.

Biographies of Presenting Authors

Otis Alexander is currently a student at the University of Washington, Tacoma. He is working towards a Bachelors of Science degree in Computer Science and Systems. His research interests include application level intrusion detection systems for Supervisory Control and Data Acquisition (SCADA) and artificial intelligence based solutions for cybersecurity.

Abdulrahman Alqahtani is a Special Forces officer rank of major, works as a lecturer at King Fahd Security College for 12 Years. Also, he served as Managing Editor of Security Research. Alqahtani holds a bachelor degree in Security Studies (2000), a Bachelor degree in Doctrine and Perverted Groups (2006), and a master's degree in Strategy and International Security, UK (2010). Currently studying a PhD in the field of Cyber-terrorism.

Chad Arnold, received a B.A. degree in computer science from DePauw University in 2006 and a M.S. in computer science from California Lutheran University in 2008. He is currently working toward a Ph.D. in computer engineering and computer science at Wright State University while participating in collaborative research with the Air Force Institute of Technology.

Merritt Baer is a graduate of Harvard Law School and Harvard College. She conducted cyberlaw research at Harvard's Berkman Center for Internet, and clerked at the US Court of Appeals for the Armed Forces. She focuses on the intersection of cybercrime, Constitutional Internet law and national security. She serves as a Legislative Fellow in the US Senate.
Zachry Basnight is currently an MS in Cyber Operations student at the Air Force Institute of Technology. He received his BS in Computer Science from the United States Air Force Academy in 2009. Zack is an active duty 1st Lieutenant in the Air Force and his research interests include critical infrastructure protection and information assurance.

Adam Bryant earned a BS in Social Psychology from Park University in 2001, an MS in Information Resource Management from the Air Force Institute of Technology (AFIT) in 2007, a second MS in Computer Science from AFIT in 2007, and a PhD in Computer Science from AFIT in 2012.

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

Dr. Daryl Caudle is a licensed professional engineer and career naval officer with over 27 years in the United States Submarine Force. He holds degrees from North Carolina State University, Chemical Engineering; Naval Postgraduate School, MS, Physics; Old Dominion University, MS, Engineering Management, and the School of Advanced Studies, University of Phoenix, Doctor of Management.

Peter Chan is a motivated MSc student with an interest in computer security and formalising approaches to negating security attacks. He is employed as a researcher in the Defence, Peace, Safety and Security (DPSS) department at the CSIR, South Africa.

Dr. Matthew Crosston is the Miller Endowed Chair for Industrial and International Security and Director of the International Security and Intelligence Studies program at Bellevue University. Crosston has authored two books, several book chapters and nearly a dozen peer-reviewed articles on issues covering counter-terrorism, corruption, democratization, radical Islam, and cyber-deterrence.

Dr. Dahan (Hebrew University of Jerusalem, 2001), is a veteran resident of the Middle East. His research interests focus on two primary areas – ICT usage and diffusion in the MENA area and Israeli and Palestinian politics. Currently permanent lecturer at the School of Public Policy and Public Administration, Sapir College, he is also Head of program in Political Communication at Tel Aviv-Yaffo College.
Dr. Dipankar Dasgupta is a Professor of Computer Science and the founding Director of Center for Information Assurance at the University of Memphis, Tennessee, USA. His research interests include application of Computational Intelligence in cyber security. He received research funding from various federal organizations and has more than 200 publications which are being cited widely.

Barbara Endicott-Popovsky is a Director for the Center of Information Assurance and Cybersecurity at the University of Washington, and Research Associate Professor with the Information School. Her academic career follows a 20-year career in industry marked by executive and consulting positions in IT architecture and project management. Barbara earned her Ph.D. in Computer Science/Computer Security from the University of Idaho.

Cindy Finke is currently an MS in Computer Science student at the Air Force Institute of Technology. She received her BS in Computer Science from the US Air Force Academy in 2005. Cindy is an active duty Air Force Captain assigned to Wright Patterson AFB, OH. As a KC-135 pilot, she has accumulated 1,700+ hours of operational flight experience.

Klaus-Gerd Giesen is professor of political science at the Université d’Auvergne in Clermont-Ferrand, France, and a visiting professor at the Université de Lausanne, Switzerland. He is a specialist of international ethics and of the international politics of technology. Previously, he has been professor in Germany and Belgium.

Dr. Samiksha Godara has done her B.A. (Law), LL.B., LL.M. (Criminal Law) & Ph.D. (Cyber Law) from the M.D. University, Rohtak, Haryana, India. She has experience of over 6 years as Criminal Lawyer in the District & Sessions Court, Rohtak. Presently, she is working as an Assistant Professor in SBS Law College, Rohtak.

Tim Grant is retired but an active researcher (Professor emeritus, Netherlands Defence Academy). Tim has a BSc in Aeronautical Engineering (Bristol University), a Masters-level Defence Fellowship (Brunel University), and a PhD in Artificial Intelligence (Maastricht University). Tim’s research spans the interplay between operational needs and ICT capabilities in network-enabled Command & Control systems, Identifying Tools and Technologies for Professional Offensive Cyber Operations.

Virginia Greiman is an Assistant Professor at Boston University in international law, cybercrime and regulation and project management and an affiliated faculty member at the Harvard Kennedy School in cybertrafficking. She has more than 20
years of experience in international development and legal reform and has held high level appointments with the U.S. Department of Justice.

**Major Michael Henson** is a PhD candidate in computer engineering at Dartmouth College where his work focuses on the security of mobile devices. He holds a masters degree in computer science (information assurance) from the Air Force Institute of Technology. He has developed and taught network security at the United States Air Force Academy.

**Jonathan L. Holston**, CSC, Inc. Joint Information Operations Warfare Center (JIOWC). Mr. Holston served in the US Air Force as a vulnerability analyst assigned to the National Security Agency. His research interests include identifying third-world adversarial attack methodologies on communication networks and satellite communications and their associated vulnerabilities.

**Dr Barry Irwin** heads up the Security and Network Research Group (SNRG) in the department of Computer Science at Rhodes University. His research interests are in network modelling, and the application of network telescopes and honeypots for cyber security. He is also the Chapter lead for the South African Honeynet project.

**Joey Jansen van Vuuren** is the Research Group Leader for Cyber Defence at the CSIR, South Africa. This research group is mainly involved in research for the SANDF and Government sectors. Her research is focused around national security and the analysis of Cyber threats using non quantitative modelling techniques. She is also actively involved in facilitating Cyber awareness programs in South Africa.

**Dr. Charles A. Kamhoua** received his M.S. in Telecommunication and Networking and his PhD in Electrical Engineering from Florida International University in 2008 and 2011 respectively. He is currently a postdoctoral fellow at the Air Force Research Laboratory. His interdisciplinary research area includes game theory, cybersecurity, survivability, fault tolerant networks, and ad hoc networks.

**Rainer Koelle** is a Senior ATM Security expert with EUROCONTROL, Brussels. Rainer holds a PhD from Lancaster University, 2012, and a Diploma (MSc) in Electrical Engineering (Communication Systems) from the University of the German Federal Armed Forces, Hamburg, 1994. He is a researcher with Lancaster University, Aviation Security Group, in the field of Situation Management. For more than ten years Mr. Kraft has been deeply involved with Information Assurance and net-
work security. He holds a Master of Science in Information Assurance degree from Capitol College of Maryland. Mr. Kraft is a Certified Information Systems Security Professional (CISSP).

**Michael E. Kraft**, CSC, Inc. Joint Information Operations Warfare Center (JIOWC) For more than ten years Mr. Kraft has been deeply involved with Information Assurance and network security. He holds a Master of Science in Information Assurance degree from Capitol College of Maryland. Mr. Kraft is a Certified Information Systems Security Professional (CISSP).

**Dr. Andrew Liaropoulos**, Biographical Note Dr. Andrew Liaropoulos is a Lecturer in University of Piraeus, Department of International and European Studies, Greece. He also teaches in the National Security College, the Air War College and the Naval Staff Command College. He is also a Senior Analyst in the Research Institute for European and American Studies.

**Volodymyr Lysenko** is a research scientist at the Center of Information Assurance and Cybersecurity. He is a graduate of the Ph.D. program in Information Science at the Information School of the University of Washington, Seattle. He also has a degree in Physics. Volodymyr’s research interests are in the area of political cyberprotests and cyberwars in the international context.

**Dr. William Mahoney** received his B.A. and B.S. degrees from Southern Illinois University, and his M.A. and Ph.D. degrees from the University of Nebraska. He is an Associate Professor in the College of Information Science and Technology, University of Nebraska at Omaha, and is the Director of the Nebraska University Center for Information Assurance (NUCIA).

**Julie McNally** is a master’s student in the International Security and Intelligence Studies program at Bellevue University in Bellevue, Nebraska. She is an Intelligence Community Center of Academic Excellence IC Scholar.

**Nighat Mir** is working as an Assistant Professor, Computer Science Department, College of Engineering and as an Institutional Research Coordinator, Quality Assurance Department at Effat University, Jeddah Saudi Arabia. Her major is information security and the research focus is in the field of Digital Watermarking, Cryptography and Steganography.

**Erik Moore** has served as Co-Director of the Center for Information Assurance Studies at Regis University, as Associate Dean of Engineering and Information Sci-
ences at DeVry University, and is currently the Director of Academic Computing Services for Adams 12 school district in Colorado. His research is on security and virtualization have been presented at SEC2011, HICSS2010.

**Heath Novak** is a recent graduate from the Master’s of Information Assurance Program at Regis University and 2010 recipient of the United States Department of Defense Information Assurance Scholarship. Academic contributions include aiding Regis University faculty to design and implement cyber security competitions hosted by the university, most recently CANVAS 2011 and RMCCDC 2012.

**Heloise Pieterse** is a MSc student in the department of Computer Science at the University of Pretoria, South Africa. She is currently on a Studentship program at the Council of Scientific and Industrial Research and works within the Command, Control and Information Warfare research group. Research interests include information security and mobile devices.

**David M. Rohret**, CSC, Inc. Joint Information Operations Warfare Center (JIOWC). Mr. Rohret has pursued network security interests for over 20 years to include developing and vetting exploits for use with red teams and for adversarial research. He holds degrees in CS from the University of Iowa, 1981, and La Salle University, 1994. Mr. Rohret is a member of the IEEE Computer Society and is currently a Senior Principal Systems Engineer for the Computer Sciences Corporation (CSC).

**Yaroslav Shiryaev** is a PhD candidate at the University of Warwick. His doctoral research investigates the deficiencies of the existing international law regime in covering the threat of cyber-attacks and cyberterrorism. Yaroslav’s life experiences are quite diverse, and include e.g. compulsory military service, volunteering in Uganda and Kosovo, and traveling to the North Pole.

**Inna Vasilyeva** is currently a senior student at the Kuban State University of Technology, Faculty of Computer Security and Information Defense, Russia. Her research interests are: information security, information/cyber security awareness, intelligent systems and information operations. She is actively involved in the science life at her university, specializing in a field of Information Warfare.

**Michael P. Vella**, CSC, Inc. Joint Information Operations Warfare Center (JIOWC). For more than fifteen years Mr. Vella has been deeply involved with computer network security with specialty in pen-testing the last 5 years. Mr. Vella is a Certi-
fied Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and CompTIA Security+.

**Dr Jannie Zaaiman** is the Deputy Vice Chancellor: Operations of the University of Venda in the Limpopo Province, South Africa. Before entering the academic world, he was inter alia Group Company Secretary of Sasol, Managing Executive: Outsourcing and Divestitures at Telkom and Group Manager at the Development Bank of Southern Africa. His area of research is cyber security awareness especially in rural areas of South Africa.
Strategies for Combating Sophisticated Attacks

Chad Arnold², Jonathan Butts¹, and Krishnaprasad Thirunarayan²
¹Department of Electrical and Computer Engineering, Air Force Institute of Technology, Wright Patterson AFB, Dayton, Ohio, USA
²Department of Computer Science and Engineering, Wright State University, Dayton, Ohio, USA

Abstract: Industrial control systems (ICS) monitor and control the processes of public utility infrastructures that society depends on—the electric power grid, oil and gas pipelines, transportation and water facilities. Attacks that impact the operations of these critical assets could have devastating consequences. Yet, the complexity and desire to interconnect ICS components have introduced vulnerabilities and attack surfaces that previously did not exist. Cyber attacks are increasing in sophistication and have demonstrated an ability to cross over and create effects in the physical domain. Most notably, ICS associated with the critical infrastructure have proven susceptible to sophisticated, targeted attacks. The numerous communication paths, various ingress and egress points, diversity of technology and operating requirements provide myriad opportunities for a motivated adversary. Indeed, the complex systems enable both traditional and nontraditional attack surfaces. Current defense strategies and guidelines focus on defense-in-depth as a core component to protect critical resources. System security relies on multiple protection mechanisms to present an attacker with various challenges to overcome. This strategy, however, is not adequate for safeguarding critical assets against sophisticated attacks. This paper analyzes current ICS defense strategies and demonstrates that defense-in-depth alone is not a successful means for preventing attacks. Findings indicate that a paradigm shift is required to thwart advanced threats. As an alternative, cyber security for ICS is examined from the notion of weakest link as opposed to the current recommended strategies. Recent examples, including Stuxnet, are examined to shed light on the next-generation targeted attack in the context of current defensive strategies. The results demonstrate that current defense-in-depth strategies are necessary but not sufficient.

Keywords: ICS security, defense-in-depth limitations, critical infrastructure protection
Abstract: Modern industrial control systems (ICSs) regulate operations over a variety of different applications. Of most interest to national security is the role ICSs play in the management of critical infrastructure (CI) such as the national power grid, water treatment, and chemical industry. The control systems used in such sectors are developing into highly networked collections of distributed devices. Unfortunately, security has only recently become a topic of major concern for these devices. This leaves many implementations without secure configurations due to their long lifespan compared to the rate of advancing threats. In the paradigm of ICSs, programmable logic controllers (PLCs) represent the front line between the cyber world and physical systems. Attacks like Stuxnet have already proven the effectiveness of cyber-physical attacks by altering and disguising PLC programming, but the next generation of threats will likely focus on PLC firmware. Just as traditional computer malware evolved to hide itself using operating system-level rootkits, so will ICS attacks evolve to embed themselves in the PLC equivalent: the firmware. Since little research has been done in the area of PLC firmware security, this paper begins by addressing the related security concerns. One such concern is the application of digital forensics to a potential incident of ICS attack. Forensic investigations of digital devices have traditionally been limited to the analysis of typical computer systems like desktops or laptops. As forensic capabilities begin to expand into the scope of embedded devices like smartphones, parallels can be drawn to PLCs that will enable the development of more advanced forensic tools and processes. By performing a firmware analysis through reverse engineering, a PLC can be exploited for both malicious and forensic purposes. This paper discusses the techniques and procedures required to access, inspect, and manipulate firmware for an Allen-Bradley PLC to suit the purposes of the examiner. From this analysis, lessons can be learned not only about the capabilities and methods required by a potential attacker, but also about the accessibility and effectiveness of recovering PLC firmware for forensic investigation of a potential attack.

Keywords: industrial control system, programmable logic controller, firmware, embedded device, forensics, threat assessment
Top-Level Goals in Reverse Engineering Executable Software

Adam Bryant\textsuperscript{1, 2}, Robert Mills\textsuperscript{2}, Michael Grimaila\textsuperscript{2} and Gilbert Peterson\textsuperscript{2}
\textsuperscript{1}Riverside Research, Beavercreek, Ohio, USA
\textsuperscript{2}Air Force Institute of Technology, Wright-Patterson AFB, Ohio, USA

Abstract: People perform reverse engineering to discover vulnerabilities, to understand how attackers could exploit vulnerabilities, and to determine ways in which vulnerabilities might be mitigated. People reverse engineer executable programs to determine the structure, function, and behavior of software from unknown provenance that may not be trustworthy or safe to use. Reverse engineering also allows the investigation of malicious code to understand how it works and how to circumvent self-protection and stealth techniques used by malware authors. Finally, reverse engineering can help engineers determine how to interface with legacy software that only exists in executable form. Although each of these applications of reverse engineering provides part of an organization's defensive knowledge of their information systems, there has been relatively little work in understanding the human factors involved with reverse engineering software from executable code. Consequently, reverse engineering work remains a highly specialized skill, and many reverse engineering tools are difficult for analysts to use. To better understand the human factors considerations of reverse engineering executable software, we conducted semi-structured interviews with five nationally-renowned subject matter expert reverse engineers and analyzed the verbal data from the interviews using two analysis approaches. We used thematic analysis techniques borrowed from educational psychology to investigate themes from the interview responses, first at the idea level, then at the sentence level. We decomposed the responses into a set of main goals that we describe in this paper.

Keywords: reverse engineering, binary analysis, cognitive task analysis, knowledge engineering

An Investigation of the Current State of Mobile Device Management Within South Africa

Ivan Burke and F. Mouton
Council for Scientific and Industrial Research, Pretoria, South Africa
Abstract: In recent years mobile devices have become a critical part of employees daily lives. Mobile devices have greatly increase the speed at which information can be communicated within an organisation. These devices are continuously improving and offer an increasing number of features to the user. The user is often unaware of the potential risk the device might pose to the organisation. Due to the feature creeping of these devices, organisational policies designed to govern these devices become outdated with each new generation of mobile devices. This paper discusses some of the technological advances that increased the risk of mobile devices to organisations. It also covers a broad overview of how organisations strive to mitigate these risks by introducing Mobile Device Management policies. For this paper surveys were conducted to ascertain the current state of Mobile Device Management (MDM) policies within South African organisations. The results of these surveys are presented and the shortcomings of the organisational strategies are discussed. The authors also present a method to determine the prevalence of mobile devices on a network as well as propose actionable steps that can be added to MDM policies to reduce the risk mobile devices pose to the organisational security.

Keywords: mobile device management, bring your own device policies, mobile vulnerabilities

A Taxonomy of Web Service Attacks

Ka Fai Peter Chan ¹, Martin Olivier ² and Renier Pelser van Heerden ¹
¹Council for Scientific and Industrial Research, Pretoria, South Africa
²University of Pretoria, Pretoria, South Africa

Abstract: Web Services (WS) have become a popular application of Service Oriented Architecture (SOA) in many organisations for financial, governmental and military purposes. This is due to WS's ability to integrate seamlessly with other existing services and legacy systems in real time. This level of composition can create a chain of interdependencies between systems to address a complex transaction in real time. Such composition is possible using choreographies, orchestrations, dynamic invocations, and brokers. Messages are based on open standard web technologies, such as Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML). As a result, WS can be deployed on any existing internet protocol. Unfortunately, such capability does not come without disadvantages. In addition to being exposed to internet protocol attacks, they are exposed to attacks that specifically target WS technologies. In the event of an attack, multiple organisations in the chain can be affected, resulting in services not being available and possible financial loss. In order to build more effective
defence systems, one needs to understand the attacks and their effects. A taxonomy provides a way to understand attacks through its classification. However, there is a lack of standard classification of Web Service attacks. As such, a taxonomy of WS attacks is proposed. This paper begins by discussing possible WS attacks, supported by practical examples. The attacks are then grouped and classified based on three parameters: WS layer, attack methodology and effect. The resulting taxonomy helps to understand WS attacks. Furthermore, the proposed taxonomy provides the flexibility to classify new WS attacks in a SOA environment.

Keywords: web services, service oriented architecture, web service attacks, taxonomy

DUQU’S DILEMMA: The Ambiguity Assertion and the Futility of Sanitized Cyber War

Matthew Crosston
Bellevue University, USA

Abstract: There is an intense debate about the applicability of international law to cyber war and the need for a cyber-specific international treaty. The problem, however, might be that this debate is irrelevant. Both camps misread how the structure of the cyber domain likely precludes strategically ‘piggy-backing’ on conventional norms of war. There is a civilian/military ambiguity in the cyber domain that makes target differentiation unlikely if not impossible. Thus, Duqu’s dilemma: with the focus on establishing legitimate targets and setting limitations on allowable action the United States and its allies are engaged in a futile endeavor that cannot lead to improved cyber governance and likely only exposes them to vulnerabilities. Greater effort should be spent on accepting this structural ambiguity by developing strategy that aims to instill preemptive fear and produce reluctance to action.

Keywords: cyber war, cyber deterrence, cyber theory, law of armed conflict, attribution

Hacking for the Homeland: Patriotic Hackers Versus Hacktivists

Michael Dahan
Departments of Public Policy and Public Administration and Communication, Sapir College, Israel
Abstract: This paper discusses the phenomenon of "patriotic" hacking, i.e. cyber attacks that are mounted by hackers against states with which there is a pro-longed national conflict such as: India-Pakistan, China-Taiwan, Russia-Chechnya and of course Israel-Muslim countries. The paper does not look at hacking perpetrated by countries themselves (or their proxies) in the form of cyber warfare but rather by individual hackers and hacker groups. These hackers are then compared to cosmopolitan hackers or Hacktivists, active in global and national arenas. Political motivations and ideology of both groups are explored. Case studies for comparison are drawn primarily from the Israeli-Muslim cyber conflict, with an emphasis on the November 2012 (“Operation Pillar of Cloud”) conflict in Gaza, and its parallel arena in cyberspace. The Gaza case is unique in that patriotic hackers are joined by hacktivist groups such as Anonymous and LulzSec in mounting cyber attacks against Israeli institutions and individuals.

Keywords: patriotic hacking, hacktivism, cyberwar, Israel, Palestine, Middle East

Consequences of Diminishing Trust in Cyberspace

Dipankar Dasgupta and Denise Ferebee
Center for Information Assurance (CAE-R), Department of Computer Science, The University of Memphis, USA

Abstract: The cyberspace has become an integral part of modern day life—social, economic, political, religious, medical and other aspects. Without the availability of the Internet today’s businesses, government and society cannot function properly. Moreover, different online social media and blogosphere are bringing people together, providing platforms to share their ideas and allowing their voices to be heard. Ideally, the cyberspace has no political, geographical or social boundaries; as a result it is promoting globalization and uniting people from all over the world. While the potential benefits of this interconnectivity are unlimited, this virtual world is also becoming hackers’ playground, underworld’s marketplace, nation-states’ battle ground, and a vehicle for propaganda and misinformation. In this paper, we argue that with the growing threat of coordinated attacks, release of complex malware and gradually diminished trust in freely-available information, the openness of the web and its global connectivity will no longer exist. Specifically, if this trend continues, the Internet will be partitioned, users will rely on information and news only through membership-based services, the information flow will be limited to geographical and political jurisdictions and will be highly regulated by governments, online businesses and critical knowledge will only be shared among alliance of friendly nations.
Towards a Theory of Just Cyberwar

Klaus-Gerd Giesen
Université d’Auvergne, Clermont-Ferrand, France

Abstract: The text applies just war theory to cyberwar from a philosophical perspective. After defining the concept of cyberwar it discusses the ethical criteria of the traditional *jus ad bellum* and *jus in bello*, before emphasizing the need for a Kantian *jus post bellum*. The aim is to reach several ethical norms which may ultimately lead to new international legal norms (an international treaty inspired by *jus post bellum*) or allow to assess the adaptation of existing legal norms.

Keywords: cyberwar; just war, international ethics, jus post bellum

Defamation in Cyber Space: Who do you sue?

Samiksha Godara
Shamsher Bahadur Saxena College of Law, Rohtak, India

Abstract: - The right to freedom of speech and expression is probably the most important universally accepted human right in a democratic society. An extension of this right is the right to know i.e freedom of information which can be enjoyed only if there are sources from which the information can flow. Here comes into role the print media as well as audio-visual media. In the present era, with the advancement of Information and Communication Technology (ICT), there comes into picture machines like computers and facilities like internet. Nowadays, cyberspace is put to maximum use for exercising the freedom of expression. Due to anonymous nature of cyberspace one can exercise the freedom of expression to the extent of defaming another. But one must understand that this freedom is not absolute and reasonable restrictions can be imposed upon it on certain grounds like defamation, privacy, decency, public order etc. The law of defamation addresses harm to a person's reputation or good name through slander and libel.
The Internet has made it easier than ever before to disseminate defamatory statements to a worldwide audience with impunity. For quite some time, courts have been struggling with remedies for online defamation. The problem has been magnified by the difficulty in identifying the perpetrator, and the degree to which Internet Service Providers (ISP's) should be held accountable for facilitating the defamatory activity. This research paper contains a comprehensive study of laws of various countries dealing with cyber crimes in general and cyber defamation in particular. For example, Indian Information Technology Act, 2000 as amended by the IT (Amendment) Act, 2008; US Communication Decency Act, 1996; UK Defamation Act, 1996. An attempt has also been made to study the jurisdictional riddles involved in cases of internet defamation because internet is a global medium transcending across boundaries. It also focuses on the recent judicial pronouncements of High Courts and Supreme Court of various nations which have delivered landmark judgments for curbing the menace of cyber defamation.

Keywords: defamation, cyber space, internet service provider, online, jurisdiction

Identifying Tools and Technologies for Professional Offensive Cyber Operations

Tim Grant¹ and Ronald Prins²
¹R-BAR, Benschop, The Netherlands
²Fox-IT, Delft, The Netherlands

Abstract: Since 2008, several countries have published new national cyber security strategies that allow for the possibility of offensive cyber operations. Typically, national strategies call for the establishment of a cyber operations unit capable of computer network defence, exploitation, and, in some nations, attack. The cyber operations unit will be manned by professionals and operate under government authority compliant with national and international law. Our research focuses on offensive cyber operations (i.e. computer network exploitation and attack). The cyber unit must be provided with the right resources, in the form of accommodation, computing and networking infrastructure, tools and technologies, doctrine, and training. The open literature gives an unbalanced view of what tools and technologies a professional group needs because it emphasizes malware and, to a lesser extent, the delivery media used by cyber criminals. Hence, the purpose of this paper is to identify systematically the tools and technologies needed for professional, offensive cyber operations. A canonical model of the cyber attack process was enhanced by adding control inputs and mechanisms, and tools and technologies were extracted from these mechanisms. Both the enhanced model
and the set of tools and technologies have been checked by a subject matter expert.

**Keywords:** offensive cyber operations; attack; canonical process model; tools; technologies; SADT

---

**The Emergence of Cyber Activity as a Gateway to Human Trafficking**

**Virginia Greiman**\(^1,^2\) and **Christina Bain**\(^2\)

\(^1\)Boston University, Boston, USA
\(^2\)Harvard Kennedy School, Carr Center for Human Rights Policy, Program on Human Trafficking and Modern Slavery, Cambridge, USA

**Abstract:** Human trafficking is a worldwide crisis and the U.S. Department of State’s 2012 Trafficking in Persons Report highlights the critical need to address this issue both home and abroad. Today, it is estimated as many as 27 million people around the world are victims of trafficking into the sex trade and other forms of servitude known as modern slavery or trafficking in persons. “Trafficking in persons” and “human trafficking” has been used by the U.S. Department of State and other governmental and multinational organizations as umbrella terms for the act of recruiting, harboring, transporting, providing, or obtaining a person for compelled labor or commercial sex acts through the use of force, fraud, or coercion. Recent research reflects that the exploitation of people through trafficking, is being channeled heavily through cyber activity such as Internet service, local bulletin board service, or any device capable of electronic data storage or transmission including social networking sites like Craig’s List, Facebook, MySpace, and email instant messaging, text messaging, fictitious employment advertisements, immigration assistance and online bride websites. The goals of the research include: (1) identifying some of the key present challenges in cybertrafficking investigations, (2) understanding the impact of cybertrafficking in our society, locally, nationally and globally; and (3) assessing the role of the private sector in regulating the Internet for human trafficking activity. Presently, human trafficking scholarship and education is in its early stages particularly as it relates to
understanding victim protection and assistance, technological, evidentiary and surveillance issues and international legal frameworks for the prevention of human trafficking. Greater awareness and education is needed to assist in the challenges faced by our Executive and Legislative Branches as they address important issues of national security and the growing incidence of cybercrime. This paper will introduce common law legal doctrines, procedural and evidentiary tools, forensic analysis, and case studies that will assist in creating a deeper understanding of the impact of cyber activity on the human trafficking industry in the effort to find greater solutions for the prevention, prosecution and protection of the innocent from the growing incidence of cyber activity as it relates to human trafficking around the globe.

**Keywords:** human trafficking, cyberlaw, cybercrime, modern slavery

**Deep Routing Simulation**

**Barry Irwin and Alan Herbert**  
Department of Computer Science, Rhodes University, Grahamstown, South Africa

**Abstract:** This paper describes the implementation and testing of a flexible framework for near-real-time simulating the routing of IPv4 network traffic within the deep Internet. The purpose of this is to provide an improved degree of realism in cyber defence exercises. The most noticeable aspect of the tool, is the return of multiple hops when running link path discovery tools such as traceroute, although the correct handling of packets though decrement of IP TTL values is performed at each node. This allows for the better simulation of very large network topologies without the need for multiple discreet (or simulated) routing devices. Implemented for deployment on common open source unix-like platforms, the multi-threaded software scales on modern multi-core CPU platforms, and provides the simulation of thousands of network paths and intermediate nodes. Setup is simplified by providing a loading process that can consume real traceroute data, and optimize the internal network representations, an improvement over other simulation tools currently available. Additional functional aspects are the introduction of packet loss, corruption or delay at any point within the simulated paths. An instrumentation interface allows for the real-time monitoring, adjustment and reconfiguration of the network. This interface also provides a means for scripting automated packet insertion or configuration changes during the course of the simulation run. The initial implementation has been found to be stable, and offer adequate performance. The framework aims to provide a scalable and efficient means of providing this route simulation, and a number of future extensions are
discussed, most notably the intended porting to an embedded platform, and possibilities for increasing throughput rates.

**Keywords:** routing, simulation, cyberdefense

---

**Development of a South African Cybersecurity Policy Implementation Framework**

Joey Jansen van Vuuren\(^1\), Louise Leenen\(^1\), Jackie Phahlamohlaka\(^1\) and Jannie Zaaiman\(^2\)

\(^1\) Defence Peace Safety and Security: CSIR, Pretoria, South Africa
\(^2\) University of Venda, South Africa, Limpopo, South Africa

**Abstract:** National governments have the responsibility to provide, regulate and maintain national security, which includes cybersecurity for their citizens. Although South Africa has recently published its first draft cybersecurity policy, the implementation of the policy is still in its very early stages. In this paper, the authors propose and describe a possible cybersecurity implementation framework for South Africa. This implementation framework is based on previous analysis of structures in other countries, a cybersecurity awareness toolkit, guidelines for cybersecurity strategies in the literature, and an implementation framework proposed for Jordan.

**Keywords:** cybersecurity, national security, cybersecurity toolkit, policy framework, policy implementation

---

**Replication and Diversity for Survivability in Cyberspace: A Game Theoretic Approach**

Charles Kamhoua\(^1\), Kevin Kwiat\(^1\), Mainak Chatterjee\(^2\), Joon Park\(^3\) and Patrick Hurley\(^1\)

\(^1\) Air Force Research Laboratory, Information Directorate, Cyber Assurance Branch, Rome, New York, USA, \(^2\) University of Central Florida, Electrical Engineering and Computer Science Dept, Orlando, Florida, USA, \(^3\) Syracuse University, School of Information Studies (iSchool), Syracuse, New York, USA

**Abstract:** An effective defense-in-depth avoids a large percentage of threats and defeats those threats that turn into attacks. When an attack evades detection, it may disrupt the systems and networks, and then the need for survivability is more critical. In this context, mission assurance seeks to ensure that critical mission essential functions (MEFs) survive and fight through the attacks against the un-
derlying cyber infrastructure. Survivability represents the quantified ability of a system, subsystem, equipment, process, or procedure to function continually during and after a disturbance. US Air Force systems carry varying survivability requirements depending on MEF’s criticality and protection conditions. Almost invariably, however, replication of a subsystem, equipment, process, or procedure is necessary to meet a system’s survivability requirements. Therefore, the degree of replication within a system can be paramount for MEF’s survival. Moreover, diversity will prevent the same fault or attack from damaging all the replicas so that they can continue the mission. This research shows that the more dangerous vulnerabilities (that affect more replicas) in a system are sometimes less likely to be exploited. The attacker may be better off when exploiting small vulnerabilities because they will be less protected by the defender. In fact, diversity always gives extra challenges to attackers. This work uses the mathematical framework of game theory to show the significance of replica diversity for mission survival in cyberspace.

Keywords: cybersecurity, diversity, game theory, replication, survivability

Situation Management in Aviation Security – A Graph-Theoretic Approach

Rainer Koelle¹,² and Denis Kolev²
¹EUROCONTROL, Brussels, Belgium
²Lancaster University, Lancaster, UK

Abstract: This paper addresses support to aviation security incident management within distributed and highly interconnected system of systems like SESAR and NextGen. Explicitly, we address the problem of designing an information-centric approach to situation management. The management of an in-flight security incident requires the collaboration of various stakeholders with different information needs (e.g. national crisis cell, military, policy, airports, airlines, ATM). A graph-theoretic approach is chosen to model and investigate the design requirements for an aviation security incident management capability. Situation Management related information is modelled as information flows under associated network performance constraints. The network model is described as a feasibility and optimisation problem and the solution of a set of performance/constraint functions. These constraints represent resource limitations, capabilities of the agents, and the required infrastructure features (e.g. redundancy). The goal of this research is to develop a decision-support system for aviation security incident management. This paper presents the approach, initial modelling and design of such a capabili-
An algorithm for the corresponding feasibility and optimisation problem solution was developed. The model and algorithm are validated as part of a preparatory action for an upcoming European ATM security project. The results obtained demonstrate the feasibility of an information-centric approach to Situation Management, explicitly, its application to aviation security. This allows aviation security incident stakeholders to address the operational challenges in a more fine-tuned and timely manner. The graph-theoretical results were validated and proven through demonstration simulations. The approach and model discussed in this paper can be used for dynamic multi-agent coordination and collaboration and has the potential to systematically address information exchange requirements between distributed stakeholders in time-critical contexts, e.g. aviation security, critical infrastructure protection, and mission-critical systems.

**Keywords:** situation management, aviation security incident management, graph-theory, feasibility problem, optimisation problem

**Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction?**

Andrew Liaropoulos
University of Piraeus, Department of International and European Studies, Piraeus, Greece

**Abstract:** Cyberspace is erroneously characterized as a domain that transcends physical space and thereby is immune to state sovereignty and resistant to international regulation. The purpose of this paper is to signify that cyberspace, in common with the other four domains (land, sea, air and outer space) and despite its unique characteristics, is just a reflection of the current international system, and thereby is largely affected by the rules that characterize it. The issue of state sovereignty in cyberspace is critical to any discussion about future regulation of cyberspace. Although cyberspace is borderless and is characterized by anonymity and ubiquity, recent state practices provide sufficient evidence that cyberspace, or at least some components of it, are not immune from sovereignty. The increasing use of Internet filtering techniques by both authoritarian regimes and democracies is just the latest example of attempting to control information flows. Cyberspace is non-territorial, but in sharp contrast to the land, sea, air and outer space, cyberspace is not a part of nature, it is human-made and therefore can be unmade and regulated. States have continuously emphasized their right to exer-
exercise control over the cyber-infrastructure located in their respective territory, to exercise their jurisdiction over cyber-activities on their territory, and to protect their cyber-infrastructure against any trans-border interference by other states or by individuals. As a result, states are filtering and monitoring cyber-bytes. Over the past years, there is a growing number of states that is publishing national cyber-policies and establishing cyber-centers that aim to protect the national cyber-infrastructure and control their citizens’ access to information. The issue of state sovereignty in cyberspace raises critical questions about the need to regulate the cyber domain and gradually reach an international cyber-order.

**Keywords:** cyberspace, sovereignty, state sovereignty, international law, international cyber-order

---

**SCADA Threats in the Modern Airport**

John McCarthy¹ and William Mahoney²

¹Cranfield University, UK
²University of Nebraska at Omaha, USA

**Abstract:** Critical infrastructures are ubiquitous in the modern world and include electrical power systems, water, gas, and other utilities, as well as trains and transportation systems including airports. This work is concerned with Supervisory Control and Data Acquisition (SCADA) systems that are at the heart of distributed critical infrastructures within airports. Modern airports are highly competitive cost driven operations that offer a range of public and private services. Many airport systems such as car parking and building control systems are SCADA controlled. This is achieved with sensors and controllers monitored over a large, geographically disperse area. To increase efficiency and to achieve cost savings, SCADA systems are now being connected to information technology system networks using TCP/IP. The merging of SCADA systems into the main IT network backbone is presenting new security problems for IT security managers. Historically, proprietary solutions, closed systems, ad-hoc design and implementation, and long system life cycles have led to significant challenges in assessing the true security
posture of SCADA systems. To address this, this work seeks how SCADA systems are being integrated into the IT network within a modern airport. From this new standpoint we will be able to identify ways in which SCADA may be vulnerable to malicious attack via the IT network. The results of this work could offer solutions to increase security within airports.

**Keywords:** distributed security, airport terminals, control systems, SCADA

**Improving Public-Private Sector Cooperation on Cyber Event Reporting**

Julie McNally  
Bellevue University, Bellevue, USA

**Abstract:** A critical threat to US economic as well as national security lies in the inability of the private and public sectors to collaborate on cyber defence. Their competing interests, the profit motive and national security, have historically impeded any sharing of cyber attack information or defensive tools and strategies. As most critical infrastructure in the US is owned and managed by private companies, lacking access to corporate networks and being unable to compel companies to report cyber events prevents the government from collecting sufficient data on attacks to analyse and develop better defences. The cost of this inability is the continued rate of loss of monies from hacked financial data; loss of work product from billions of dollars of research and development loss; loss of future economic competitiveness as a result of lost future earnings on that work product; and threats to future military dominance and national security from the theft of intellectual property. To overcome the competing drivers of the public and private sector for a workable partnership on cyber defence, there must be better incentives for companies to share cyber event information. Lack of data is the leading impediment to meaningful analysis of trends and anomalies in cyber events. While industry-specific voluntary reporting associations have attempted to attract companies to report breaches in exchange for analytical products from that data, competition concerns lead companies to underreport, not report, and/or free-ride the system, resulting in a narrow pool of data. Market tools like insurance have been posed as a possible solution, but its purpose is primarily risk redistribution and indemnification of losses. Companies are only self-interested in reporting events for which there is coverage and resist full access to networks by insurance auditors for data breach assessment out of privacy and security concerns. Neither solution accounts for the desire of businesses to protect shareholder value and brand reputation by concealing data breaches. A potential solution would be a
national cyber event database to which companies could anonymously submit relevant cyber event information for analysis, without revealing identifying information that might compromise corporate interests. By decreasing the risk of information sharing by addressing privacy concerns, while offering the benefits of information sharing and analysis, this system could vastly increase the size and scope of data collection.

Keywords: incident management; cyber security cooperation; data breach reporting

Copyright Protection Based on Contextual Web Watermarking

Nighat Mir
Computer Science Department, College of Engineering, Effat University, Jeddah, Kingdom of Saudi Arabia

Abstract: Interdependency of information, security and the advent of internet technologies bring more challenges to manage protection against threats like illegal copying, redistribution, tempering, reuse and forgery of online data. Web page is one of the main sources to trade online information and therefore require more protection. In this research a novel tamper proof web watermarking technique based on its textual content has been proposed. Watermarks are generated based on the context and have utilized the structural elements of HTML (Hyper Text Markup Language) to embed the watermarks into a webpage. Watermarks are further secured by a cryptographic technique before the embedding process to integrate more security. Experiments identify the tempered information without revealing any evidence of encrypted watermarks. Proposed system has been tested against different attacks to confirm the robustness and integrity.

Keywords: security, web watermarking, copyrights protection, cryptography, hash, HTML

Towards a South African Crowd Control Model

Mapule Modise, Zama Dlamini, Sifiso Simelane, Linda Malinga, Thami Mnisi and Sipho Ngobeni
Council for Scientific and Industrial Research, Pretoria, South Africa

Abstract: With the escalating number of incidents of service delivery, labour related protests and the increasingly violent nature of protests; crowd control is one of the major challenges facing South Africa today. Often these protests are cha-
racterized by violence stemming largely from clashes between the protesters and the law enforcement agencies, which results in property vandalism and even death. For this reason, there is a demand for greater understanding, modelling and simulating crowd control. In response, this project aims to develop a crowd control model that will be used to understand the interactions between different variables during the protest and subsequently a better crowd control approach. However, modelling a multidimensional social problem as complex as crowd control requires time, knowledge and experience from a wide range of disciplines. This is therefore a long-term project consisting of three main phases. Phase 1, identifies the most important variables concerning crowd control and how they relate to each other using general morphological analysis. Phase 2 of the project will be the verification and validation of the model by experts in the field, which will be followed by the identification of relevant tools and techniques. Phase 3, will be the development of decision support system for crowd control. This paper discusses Phase 1 of the project, which includes identification of various variables regarding crowd control and their relationships. During the Arab Spring Uprisings, social media was identified as one of the factors significant for the mobilization of the crowd. This phase will determine if social media is one of the major factors to consider in a South African context and the extent to which it affects the crowd. The role of social media or lack thereof has some implications on cyber defence in South Africa. The identification of variables and the relationships between them were carried out in a facilitated workshop. The result of this phase is a South African general morphological analysis crowd control model.

**Keywords:** crowd control, general morphological analysis, crowd control variables

**A Vulnerability Model for a Bit-Induced Reality**

**Erik Moore**
Academic Computing Services, Adams 12 Five Star School District, Thornton, Colorado, USA

**Abstract:** The increasing proliferation and psychological and physical embeddedness of the global digital infrastructure call us to reconsider traditional models of vulnerability, attack trees, and security auditing. The easy coordination of disparate digital means of attack suggests we should move to tighter coordination between digital information assurance, psychological operations, and physical security. Examples at the physical end of the spectrum includes embedded Floating Point Gate Array (FPGA) computer chips that can be configured on the fly to function as completely different chips, 3D printers that can be used to bypass traditional physical security, hypervisors that virtualize complexity previously instan-
tiated in hardware, and immersive communications environments where traditional physical facilities are being replaced. Digital technology also has a profound ability to monitor and induce behavior, opinion, and identity in ways that were not possible in previous eras. These include vivid multimedia production resources capable of inducing assumptions of events and facts in large populations, artificial intelligent systems capable of filtering of large volumes of communications for population behavior and also filter for patterns or persons of interest, and opportunities for highly engaging insertions of pseudonym contact and identity imprinting with low risk to operatives. Analyzing the behavior of a population and inducing behavior seem separate at first, but from the perspective of bit-induced reality and bit monitored reality, the two are ever closer. The author proposes that we re-assess vulnerability models to ensure that the natural integration occurring across a new Psy-BIR-Phys spectrum that tracks the level at which systems are a Bit-induced Reality (BIR) across a psychological-physical spectrum. The examples presented are particularly in reference to persistent threats and long-term security requirements. Traditional resources and functions are drawn by the author in a way that reflects changing vulnerabilities as they migrate within the author’s Psy-BIR-Phys Matrix model. Scenarios presented in this work, like an attack on a device with a speaker, are formulated by the author based on an analysis of recent incidents and technology trends that include mobile devices, cloud infrastructure, programmable logic controllers, internet-based surveillance, and social media.

**Keywords:** vulnerability threat attack virtual 3D

---

**Results From a SCADA-Based Cyber Security Competition**

**Heath Novak and Dan Likarish**  
**Regis University, Denver CO, USA**

**Abstract:** On April 1 2011, Regis University hosted the 7th Computer and Network Vulnerability Assessment Simulation (CANVAS) competition with a turnout of 68 event competitors and at least two dozen faculty and spectators. The event was a major success and provided Regis University with valuable recognition in the academic community focused on information assurance. The prevailing trends at the end of 2010, the interestingly-named Stuxnet malware, Critical Infrastructure Protection (CIP), and Smart Grid technology deployments, inspired the scenario for this cyber competition. Many government and industry-specific organizations
have been stepping up efforts to heighten awareness amongst national organizations managing critical infrastructure, as well as authoring guidelines and policies for moving progress forward on secure infrastructure. In recent times, CIP has received much greater awareness by the United States Congress and other governmental agencies, such as the General Accounting Office (GAO), due to the trend towards “connectedness”, with distribution and communications systems being increasingly connected over TCP/IP networks. CIP is especially important due to the far-reaching damage that can be suffered by businesses, industrial and government facilities, and the general populace in the event of a successful cyber attack. Simulating a true utility environment for the purposes of a cyber competition scenario is next to impossible due to resource constraints and unavailability of specialized equipment. However, the essence can be captured, and this is exactly what we strived for in the CANVAS cyber competition in 2011. Our primary goal was to introduce a CIP theme to a cyber competition in order to raise awareness of these types of attacks, especially since many power utilities across the nation are pushing Smart Grid infrastructure in order to offer value-added services to customers and increase efficiencies in power generation and distribution, which will inevitably increase complexity and connectedness of power utility operations and customer home area networks that can be exploited by motivated actors. This paper will discuss these goals as well as some of the intricacies of developing the CANVAS cyber competition, including technical details, extensibility of CIP-focused cyber competitions, as well as the continued development and value of CIP simulation infrastructure.

Keywords: CANVAS, CCDC, critical infrastructure protection, cyber competition, ICS, SCADA, virtualization

Design of a Hybrid Command and Control Mobile Botnet

Heloise Pieterse¹ and Martin Olivier²

¹Council for Scientific and Industrial Research, Pretoria, South Africa
²University of Pretoria, Pretoria, South Africa

Abstract: The increasing popularity and improvement in capabilities offered by smartphones caught the attention of botnet developers. Now the threat of botnets is moving towards the mobile environment. A mobile botnet is defined as a collection of compromised smartphones controlled by a botmaster through a command and control network to serve a malicious purpose. This study presents
the design of a hybrid command and control mobile botnet. It describes the propagation vectors, command and control channels, and topology of the design. The hybrid design explores the efficiency of multiple command and control channels against the following objectives: no single point of failure must exist in the topology, low cost for command dissemination, limited network activities and low battery consumption per bot. The objectives are measured with a prototype that is deployed on a small collection of Android-based smartphones. In addition, the prototype is evaluated against mobile security software and anti-virus software. The results indicate that current mobile technology exhibits all the capabilities needed to create a mobile botnet.

**Keywords:** mobile, botnet, command and control, hybrid

---

**Functional Resilience, Functional Resonance and Threat Anticipation for Rapidly Developed Systems**

David Rohret, Michael Kraft and Michael Vella
Computer Sciences Corporation, Inc., San Antonio, USA

**Abstract:** Traditionally, network-centric rapid-development teams primarily concentrate on functionality; integrating commercial off-the-shelf (COTS) and government off-the-shelf (GOTS) technologies to meet specific goals for a compressed development schedule. In most cases basic security measures will be implemented, but there is an assumption that the integrated COTS and GOTS systems are secure; despite the introduction of new development and integration into existing programs of record. Functional resilience for rapidly developed systems is rarely considered and can result in operational failure in real-world scenarios due to long recovery times following an attack or adverse effect. To compound the problem, techno-centric assessment teams approach their targets from one perspective (or technology) at a time, preventing discovery and mitigation of vulnerabilities that can be exploited by an adversary who is goal-oriented, not technology-centric or prohibitive. Sandia National Laboratory’s (SNL) Information Design Assurance Red team (formerly the Information Operations Red Team Assessment (IORTA)), lists eight separate red teaming methods, to include (SNL, 2007):

1. Design assurance red teaming
2. Red team hypothesis testing
3. Red team gaming (scenario play)
4. Behavioral red teaming
5. Red team benchmarking
6. Operational red teaming
7. Analytical red teaming
8. Penetration testing

20
Each of SNL’s methods are depicted as a separate action completed by multiple teams or subject matter experts. For rapid development or deployment technologies, this model of independent assessments presents three shortcomings that prevent an accurate portrait of a rapidly developed system’s security posture:

1. The inability to assess for functional resilience or resonance and anticipated threats due to disparate red teams and data collection methods, and collaboration
2. Time and resource constraints on rapidly fielded technologies
3. The inability to identify vulnerabilities created through cross-domain/technology integration.

SNL’s methodologies were developed based on traditional acquisition and development models that allow for extended testing, mitigation, and re-testing. Although SNL’s red teaming definitions have become widely accepted, it does not support current DoD acquisition processes for rapidly fielded systems and falls short in accurately identifying and mitigating vulnerabilities before a technology is deployed. Adaptive Red Teams (ART) research and employ adversarial techniques to exploit vulnerabilities that are overlooked by traditional assessment teams in the form of false negatives and/or false positives. ARTs employ all eight of SNL’s red teaming actions simultaneously, and use any means available to acquire their intended effects, including physical, environmental, and social factors combined with other technologies or methods that can be used to disrupt, attack or otherwise compromise a given technology. To accurately vet technologies and operational processes for vulnerabilities and shortfalls, an ART will emulate an adversary by using the adversary’s tools, methodologies, and tactics in an attempt to attain similar goals. This approach is an effects-based, goal-driven assessment and not a technology-centric approach to mitigating risk in experimental, rapidly developed, and deployed operational technologies and systems. This paper will briefly define a framework for adaptive red teams and introduce the processes necessary to integrate security and resiliency into development practices for rapidly developed systems and programs integrating COTS and GOTS technologies and systems.

**Keywords:** adaptive red team, functional resilience, functional resonance, preliminary threat assessment, security posture

---

**What Lawyers Want: Legally Significant Questions That Only IT Specialists can Answer**

Yaroslav Shiryaev  
University of Warwick, Coventry, UK
Abstract: For the last decade international lawyers and IT specialists are brought together to conferences on issues of cyber-security. With various topics covered from such different perspectives, a clash of educations occurs. Lawyers are rarely able to understand the deep technological discussions, while legal presentations might seem too philosophical for the IT professionals, leaving them wondering, what do lawyers want and why. In this environment legal questions that cannot be answered without the deep technological knowledge possessed by the computer experts, should be formulated carefully and very precisely. Therefore, with emphasis on the jus in bello, this article aims to outline a list of issues that inevitably require joint lawyer-IT specialists dialogue and explain their significance from the point of view of international law. These issues include possibilities for digital “marking” of internationally protected objects online required under the existing humanitarian law, developing a “distinctive sign” for cyber-combatants, forewarning the enemy of incoming attacks (“carrying arms visibly”) and re-evaluating the concept of “vicinity” to dangerous installations in the context of cyber-space.

Keywords: jus in bello; armed conflict; cooperation; cyber-combatants; cyber-attacks; cyber warfare

The Weakest Link – The ICT Supply Chain and Information Warfare

Dan Shoemaker and Charles Wilson
University of Detroit Mercy, USA

Abstract: This paper proposes a unified model of best practice for ICT supply chain risk management (SCRM). Ensuring proper ICT-SCRM practice is an important national priority because of the vulnerability of current supply chains to attack by nation states and other adversaries. This paper presents a comprehensive set of standards based lifecycle practices designed to address ICT product integrity concerns in the global marketplace.

Keywords: national security policy, ICT product integrity, risk management, threat mitigation, federal program response, security training and certification, malicious software, counterfeiting

Thirst for Information: The Growing Pace of Information Warfare and Strengthening Positions of Russia, the USA and China
Inna Vasilyeva and Yana Vasilyeva  
Kuban State University of Technology, Krasnodar, Russian Federation  

Abstract: The progress of modern information technologies makes any society very vulnerable. Each breakthrough of mankind into the future fails to release it from the weight of past mistakes and unresolved problems. When economic wars due to the integration of national economies become too dangerous and unprofitable, global military conflict is capable of leading to the extinction of all life on the planet. The war gets new directions and qualities: information warfare with a great thirst for comfort in it. Today information resources have become the wealth of the country like its minerals, production and human resources. The rapid development of informatization worldwide, specifically in the USA, China and Russia, and its penetration into all spheres of the vital interests of an individual, society and the state, have caused, besides doubtless advantages, the emergence of a number of significant problems. The urgent necessity to protect the information along with being protected from it has become one of them. Considering that nowadays economic potential is increasingly defined by the level of development of the information structure, the potential vulnerability of economy from information influences grows in proportion. Turning information into a commodity has led to a sharp aggravation in international competition for possessing the information markets, technologies and resources; the information sphere considerably determines and greatly affects the economic, military, social, political and other components of the national security of the country. Information has become a global, inexhaustible resource and mankind has entered a new era of civilization - the era of serious exploitation of this resource. This is no longer the world where the material base was the subject of fierce rivalry. Now the key to success will be in the proper management of information capacity, i.e., strategic planning. Information is truly the foundation of life! The geopolitical confrontation and information warfare between the United States and China will be a major factor in world politics in the twenty-first century. This increasing tendency is pushing Russia towards further increasing the development of information warfare along with ensuring national security; the formation of an open dialogue between civilizations; and resistance to the threat of conflict in the field of information. Exhaustion of natural resources of the planet, their consumption and growth of the population do not contribute to the reduction of information warfare. Therefore, the positions of Russia, the United States and China will be strengthened due to deeper integration into the world information space. This paper has highlighted the quintessence of what causes the great thirst towards reaching information comfort and leadership, along with information warfare terrifying serious threats and modern global geopolitical tendencies.
Keywords: information, information warfare, Russia, the USA, China.

Investigating Hypothesis Generation in Cyber Defense Analysis Through an Analogue Task

Rachel Vickhouse\textsuperscript{1}, Adam Bryant\textsuperscript{2} and Spencer Bryant\textsuperscript{1}
\textsuperscript{1}711th Human Performance Wing, Wright-Patterson Air Force Base, Ohio, USA
\textsuperscript{2}Riverside Research, Beavercreek, Ohio, USA

Abstract: Sensemaking refers to the process of constructing a mental representation of a situation, that includes the objects, data, events, intentions, and inferences involved in a situation. Our previous work in studying reverse engineers’ mental models revealed that their sensemaking activities can be decomposed into seven core processes that appear in a regular pattern. In this pattern, people work through the seven processes in a “sensemaking cycle” to interpret and understand situations by refining, confirming, and disconfirming a number of hypotheses about what the information in the environment means. The processes in the sensemaking cycle are: creating a goal representation, planning an approach, carrying out the plan, sensing information, interpreting information, updating knowledge, and generating a hypothesis. Many tasks associated with cyber defense, such as malicious software analysis and network intrusion monitoring involve making sense and connecting background knowledge to information from complex displays. By investigating the last process in the sensemaking cycle, hypothesis generation, we can better understand how it supports sensemaking and how to best design tools to aid cyber analysts in making sense of the displays. In this study we investigated hypothesis generation to discover the processes by which people generate the guesses that guide them in their interaction with the environment. Ultimately this supports their sensemaking in the task. To do this, we developed an abstract hypothesis generation task to aid in our analysis of interactive sensemaking work and conducted a verbal protocol study in which participants completed the task. We collected verbal and performance data from 13 participants, who were shown a display in which eighteen cards were presented, each with a different face and combination of character arities. The participants were then able to ask a variety of yes or no questions about the arities displayed and use that information to refine their hypothesis. The participants’ goal was to accurately identify the character that was selected by the computer. We collected concurrent verbal protocols and had multiple raters code the protocols according to Bryant’s sensemaking cycle taxonomy and observed that participants demonstrated the same pattern that was observed from Bryant’s previous study of sensemaking in reverse engineering.
Keywords: sensemaking, reverse engineering, cognitive task analysis, verbal protocol, cyber defense
PHD
Research
The Potential Threat of Cyber-Terrorism on National Security of Saudi Arabia

Abdulrahman Alqahtani
Department of Politics and International Studies, The University of Hull, UK

Abstract: Throughout history, there have been many events and dangers that threaten state security, causing heavy loss of life, disease, injuries, destruction of property, displacement of large numbers of people and heavy economic losses. Political unrest on international and local levels and recent technological developments increase the seriousness of threats against national security. The concept of security has evolved gradually, especially since the disintegration of the Soviet Union, and end of the Cold War. The lingering impact of the policy of the bipolar world has blurred the image of relations between states. However, it provides an opportunity to understand and identify new threats and emerging conflicts, in addition to many unsolved problems. Simultaneously, globalisation has changed international rules and norms, in order to facilitate the rapid flow of capital and technology, with a weakening of national barriers. Non-governmental actors now play key roles in international politics, some as a threat, and others bridging the gap between communities and nations. In these circumstances, the role of the state began to suffer and the accepted traditional concept of power was challenged.

Today, a major issue of such concern worldwide, arousing heated debate at both national and international levels, is terrorism. The threat of terrorism has never been as prominent as it seems to be at the present time. Terrorism is an old phenomenon that has existed since the emergence of human societies, but the threat of terrorism has increased steadily over the past 30 years. With technological and technical progress, the actions of terrorists have become more dangerous and destructive, while the perpetrators of such acts have become more elusive. There are few parts of the world that have escaped terrorism since late 1960s (Mythen and Walklate 2006). The phenomenon of terrorism is changing, while the motives of terrorism remain the same. The world today faces new and unfamiliar kinds of weapons. The international system, intelligence systems, security procedures and tactics which are expected to protect people, nations and governments, are not able to meet this new and devastating enemy. The methods and strategies developed to combat terrorism over the years are providing ineffective, as the enemy no longer attacks only with hijacked plans, truck bombs or suicide bombers. Terrorists may engage in cyber-terrorism, the use of cyberspace to launch attacks. The integration of the virtual and physical worlds, is a weakness confronting secu-
rity agents (Collin 1996). This paper outlines a PhD proposal, which seeks to design an effective framework for the potential threat of cyber-terrorism on national security, compared with conventional terrorism by addressing three main themes: awareness - vulnerabilities – response, important in assessment of any security threat. According to Denning (2000) to understand the potential threat of cyber-terrorism, we should consider two factors: first, whether there are targets that are vulnerable to attack, and, secondly, whether actors have the ability and motivation to attack them. In this proposal a preliminary review of relevant literature will be introduced, followed by the research questions to be addressed and the proposed methods to address them. Then the expected time frame will be considered.

Keywords: terrorism, cyber-terrorism, national security, Saudi Arabia

Improving Cyber Warfare Decision-Making by Incorporating Leadership Styles and Situational Context into Poliheuristic Decision Theory

Daryl Caudle
Advanced Education Concepts, Wilmington, USA

Abstract: Cyber attacks on a global scale increasingly continue to threaten critical infrastructures, information networks, and digital control systems that fundamentally support our national security and improve our quality of life. The ability to respond appropriately to a cyber attack in a timely and effective manner has never been more important. Unfortunately, decision-making uncertainty following a cyber attack can hinder and delay critical response options including the use of force. A review of the literature indicated the decision-making uncertainty experienced by senior military officers was described by five interdependent characteristics: response process, human factors, governance, technology, and environment. Furthermore, the response decision-making process used by military officers following a cyber attack was best characterized by poliheuristic, noncompensatory decision theory. The literature also suggested that poliheuristic theory as originally formulated failed to incorporate two key elements of the decision-making process, specifically leadership styles and situational context. Accordingly, this qualitative, directed content analysis was used to validate published research findings that certain leadership characteristics and situational variables affect the poliheuristic decision-making process that senior military officers use when determining the appropriate response to a cyber attack. A directed content analysis was used to examine previously collected interview data from 21 senior military
officers who served for the Chairman of the Joint Chiefs of Staff in cyber warfare divisions in Washington, DC. The results of this research study supported and triangulated the findings in the literature that leadership styles and situational context are necessary additions to a more comprehensive poliheuristic theory that has improved predictive and explanatory power. The research study also showed that senior military officers’ leadership styles are more *use of force* oriented than *politically* oriented with adversarial distrust and military assertiveness being the predominate themes. Finally, the research study results revealed generational and organizational cultural effects, ethical considerations, and anticipatory skills influence leadership style and decision-making following a cyber attack.

**Keywords:** decision-making, cyberspace, warfare, poliheuristic, leadership, situ
Work in Progress
Attack-Aware Supervisory Control and Data Acquisition (SCADA)

Otis Alexander, Sam Chung and Barbara Endicott-Popovsky
Institute of Technology – University of Washington, Tacoma, USA
Center for Information Assurance & Cybersecurity – University of Washington, Seattle, USA

Abstract: SCADA systems are used for geographically distributed process control. These systems are used in national critical infrastructure such as transportation, power grid, water facilities, etc. Malfunctions in these systems can be catastrophic and can potentially cause harm to the environment and even human beings. As a result, SCADA systems are high value targets for attackers and need to be able to detect intruders within the system before they can exploit vulnerabilities. In this paper, we propose an architecture that makes SCADA systems attack-aware. The architecture builds on several existing methodologies and works to improve application level intrusion detection. This goal is accomplished by helping to make sense of the vast amounts of log data that SCADA systems produce daily and over time also refining them.

Keywords: attack-aware, SCADA, log mining, snapshots, baselining, anomaly detection

Cyber Disarmament Treaties and the Failure to Consider Adequately Zero-Day Threats

Merritt Baer
Harvard Law School, Cambridge, USA

Abstract: Because the Internet carries a borderless aspect, it is unsurprising that international solutions to cybersecurity problems have become an increasingly insistent area for debate. The notion of a cyber disarmament treaty is appealing as we begin to wrap our minds around the destructive possibilities in cyber, including the potential for civilian casualties of cyber dimensions of recognized armed conflicts—a traditional arena for treatymaking. In this paper, I argue that calls for cyberwarfare treaties miss the mark because they conflate traditional forms of force with the avenues that nation-state cyber actors are exploiting. In this, I differ from existing cyber treaty skeptics because my rationale hinges on the substantive nature of the cyber threat as one ill-suited to treaties. I agree with others’ critiques that definitions in the cyber world remain vague, often haphazard or poor adjustments of kinetic world definitions. Yet the search for terminol-
ogy to best address cyber threats and behaviors is not a problem particular to
cyber disarmament. Another common critique of cyber disarmament is that we
have no enforcing body. Similarly, I find this critique true but not necessarily
unique—international law of all sorts faces problems in law enforcement. I con-
tend that the reason a cyber disarmament treaty is not an appropriate tool to
address the threat of cyberwarfare is that it fails to recognize that the most
threatening cyber warfare concerns involve quiet but lucrative zero-day threats. A
zero-day threat is a foundational “hole” in software or hardware that can be ex-
plotted before its existence is even known. Emerging research shows that zero-
day exploitations last longer and the payload is significantly higher than that of
traditional hacking. Because a cyber disarmament treaty could only effectively
bind countries to behavior that is known to the other players, it would not bind
zero-day hacks or the deliberate installation of zero-day vulnerabilities in prod-
ucts. The notion of a treaty derives from a sense that violence is knowable at the
moment when a defector acts. Cyber warfare simply acts outside of that assump-
tion much of the time.

**Keywords**: zero-day threat, cyber disarmament, supply chain integrity

**Evaluation of a Cryptographic Security Scheme for Air Traffic Control’s Next Generation Upgrade**

Cindy Finke, Jonathan Butts, Robert Mills and Michael Grimaila
Air Force Institute of Technology, Wright Patterson AFB, USA

**Abstract**: The United States’ national airspace system (NAS) is reliant on legacy
systems and technology that stems from the 1970s. Indeed, the Air Traffic Control
(ATC) radar surveillance system is antiquated, the controller communication pro-
tocol is unreliable, and the traffic management process is heavily dependent on
human perception of conflict. As a result, the safety margin incorporated into the
ATC separation standards artificially limits air traffic capacity. With the demand
for air transportation increasing each year, the Federal Aviation Administration
(FAA) has introduced the Next Generation (NextGen) upgrade to modernize ATC
capabilities. Automatic Dependent Surveillance-Broadcast (ADS-B), a key compo-
nent of the NextGen upgrade, enables an aircraft to generate and broadcast digi-
tal messages that contain the aircraft’s Global Positioning System (GPS) coordi-
nates. Ground stations and other aircraft within range will be able to interpret the
sender’s location, trajectory, and identification. The incorporation of ADS-B sur-
veillance is intended to provide enhanced surveillance accuracy, efficiency, and
safety. The open design of the system, however, introduces inherent security
concerns. Currently, ADS-B messages can be received and decoded by any receiver within range that is tuned to the operating frequency. Additionally, recent research has demonstrated aircraft position and tracks are surprisingly simple to fabricate—making it possible for malicious spoofing to flood the ATC system. In each instance, the ability to intercept and fabricate authentic ADS-B messages was accomplished using inexpensive, store-bought equipment. Such key vulnerabilities could be mitigated using encryption, providing message confidentiality and aircraft authentication. However, implementation of a large-scale, distributed encryption scheme is nontrivial. This paper evaluates limitations of the legacy systems currently associated with the ATC and explores the feasibility of employing Format Preserving Encryption (FPE), specifically the FFX algorithm, within ADS-B communication. Based on the analysis, recommendations are provided that highlight areas that should be examined for inclusion in the ADS-B upgrade plan.

**Keywords:** format preserving encryption, FFX, ADS-B, FAA NextGen security

**Attack Mitigation Through Memory Encryption of Security-Enhanced Commodity Processors**

**Michael Henson and Stephen Taylor**

**Thayer School of Engineering at Dartmouth College, USA**

**Abstract:** Modern computer systems exhibit a major weakness in that code and data are stored in the clear, unencrypted, within random access memory. As a result, numerous vulnerabilities exist at every level of the software stack. These vulnerabilities have been exploited to gather confidential information and inject malicious code into device drivers, operating system kernels, and user processes. Encrypting memory would mitigate the vulnerabilities but the CPU-memory bottleneck presents a significant challenge to designing a usable system with acceptable overheads. Recently, security hardware, including encryption engines, has been integrated on-chip within commodity processors such as the Intel i7, AMD bulldozer, and multiple ARM variants. This paper describes on-going work to develop a clean-slate operating system -- Bear -- that leverages on-chip encryption to provide confidentiality of code and data. The system currently operates on the Intel X86-based multi-core blade servers and ARM M3, A8, and A9 processors. Work on memory encryption is focused on the Freescale i.MX53 using its integrated encryption engine.

**Keywords:** memory encryption, mobile platform security, security-enhanced commodity processors, secure microkernel
Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia

Volodymyr Lysenko and Barbara Endicott-Popovskey
University of Washington, Seattle, USA

Abstract: In this work in progress we investigate, what tactics and strategies are employed by the main opposing stakeholders in the current Russian politically-motivated local cyberwar. Particularly, we found further evidence which can indicate active Kremlin involvement in cyberattacks against its political opponents. Our results suggest that modern cyber-arms can be effective means of conducting contentious politics in (semi)authoritarian countries. We show that the technically well-prepared protesters can successfully withstand even highly sophisticated and powerful cyberattacks, and are able to retaliate accordingly.

Keywords: hacktivism, cyberwar, Russia, “patriotic” hackers, anonymous, e-
Non Academic
The Adam and Eve Paradox

Michael Kraft, David Rohret, Michael Vella and Jonathan Holston
Computer Sciences Corporation, Inc., San Antonio, USA

Abstract: Individuals working in the Information Technology (IT) industry are familiar with Moore’s Law and its guiding principle: exponential improvement every 18-24 months where computer technology is concerned (Brock, 2006). This principle has been proven generally accurate and is routinely used for long term planning by the computer industry, which has led to an explosion in computing power and technologies that have catapulted computing into every aspect of human’s lives in the 21st century. However, while new technologies increase the quality of life for the current generation, they also provide avenues for nefarious individuals to take advantage of others using the same new technologies. To help counter this, the IT industry has made great strides in its efforts to protect users by developing security appliances to include firewalls, intrusion detection systems, encryption, passwords, two-factor authentication methods, and a layered approach to security; to name just a few. It is because of this effort by the IT industry to help protect users, the authors have identified unique cyber attack trends, that could be referred to as a new “Moore’s Law” (as it pertains to cyber security). As computer technologies become more sophisticated and robust, malicious actions have become less sophisticated, and in many instances, cyber exploitation and attacks occur without the use of technology. The authors have penned this concept as the “Adam & Eve Paradox”. The paradox construct being, as technologies improve and network perimeters are hardened preventing direct attacks against systems, users and systems are being exploited at an exponentially increased rate by methods contrary to the technological improvements. Cyber criminals and hackers will always first attempt attacks against the easiest targets, known as the low-hanging forbidden fruit described in the biblical Adam & Eve story. While the IT industry continues to spend billions of dollars (US) annually to create appliances and develop software to protect its resources, data, and users; attackers are increasingly focusing their attention on the lowest hanging fruit, whether it be an unsuspecting user who clicks a link in an email, to a helpful administrator who provides information to a false authority. As the IT industry moves in the direction of complex defensive tactics, attackers are moving towards less complex – softer targets that are more difficult to detect, block, and mitigate. It is the authors’ intention to define and substantiate the “Adam & Eve Paradox”.

Keywords: malware, social engineering, Moore’s law, cyber-attack, perimeter defense, Adam & Eve
Offensive Cyber Initiative Framework (OCIF) Raid and Re-Spawn Project

David Rohret, Michael Vella, and Michael Kraft
Computer Sciences Corporation, Inc., San Antonio, USA

Abstract: During the 2010 European Conference on Information Warfare (ECIW) the authors unveiled their Offensive Cyber Initiative Framework, which outlined an approach for an offensive cyber initiative that included cyber intelligence, trends and predictive analysis, in-line exploit tool development, integration of supporting technologies, continual reconnaissance, and implementation plans (integrated into a single comprehensive offensive cyber framework (Rohret, 2010)). The unique aspect of the OCIF project was the autonomy in which, once released, the program would complete a mission or set of goals without user intervention or support through traceable proxy services. One requirement not addressed was identified by the author that would be required to allow such a system to be successful; the ability to recover from a counter attack or adverse affect and re-spawn as a viable system. In the following paper the authors review the OCIF framework, requirements for resiliency, and outline their solution for this additional capability that will provide autonomous functional resiliency for an OCIF-based tool. Advancements in cyber security, to include the ability for network security companies and government agencies to identify and mitigate new or legacy attacks, have significantly decreased the life span of exploits and attack tools. Coupled with more robust operating systems, and a generation of better educated system administrators, the longevity of any attack tool can be measured in hours rather than days. If a unique attack exploit or methodology is developed it is often withheld; for once it is released it will rapidly be countered or defeated. Furthermore, the releasing organization engaging in cyber warfare will wish to remain anonymous in order to prevent political fallout or a retaliatory attack. Polymorphism and code mutation have been key components in successful attacks, but for a tool to continue a specific mission, resiliency will need to be developed into the tool’s framework. Often touted as a system requirement, resiliency is rarely achieved in software projects due to the cost in time and other resources. The least complicated and least expensive method of resiliency is achieved through redundancy of systems, providing immediate failsafe measures should an adverse condition arise at an alternate operating location (AOL). Unfortunately, an autonomous system with the requirement to remain anonymous cannot afford to be duplicated throughout the World Wide Web or be linked to multiple AOLs, as multiple instances (especially static instances) would amplify the systems’ exposure to an adversary. The author’s solution is a cloud-based non-traditional
redundant array of independent disks (RAID) that will allow an autonomous tool to replicate itself using concatenation of a large span of disks. The necessary disk space is acquired through easily exploited systems throughout the cloud. Each span or node is separated from other nodes and wholly contained, allowing one node to be corrupted or discovered without affecting other nodes. In this way an OCIF-based system will survive counter attacks, reconstitute, and the new instance will continue the mission. The authors will discuss the various methods of RAID and demonstrate through a simulated cloud environment their solution and results.

**Keywords:** cloud RAID, RACS, RAIC, re-spawn, functional resiliency, autonomous cyber warfare
Research Jotter

Research ideas can happen at any time – catch them in writing when they first occur