

## **CURRICULUM VITAE OF PETER R. STEPHENSON, PHD, CISM, CISSP, FICAF**

### **Education**

2007 – MA Diplomacy (cum laude) - Norwich University, Northfield, VT (concentration in terrorism – Thesis: Information Dominance as an Affirmative Countermeasure against International Terrorism)

2004 – PhD Computing – Oxford Brookes University, Oxford, United Kingdom (Thesis: Structured Investigation of Digital Incidents in Complex Computing Environments)

2002 - MPhil Transition to PhD Program – Oxford Brookes University, Oxford, U. K.

### **Professional Experience**

#### **Current – Norwich University**

- Director, Norwich University Center for Advanced Computing and Digital forensics (<http://www.nuacc.org>)
- Chief Information Security Officer
- Lecturer, digital forensics, information assurance and network-centric warfare

#### **January 2005 – May 2009 – Norwich University**

- Chair, Department of Computing, School of Business and Management (2008 and 2009 school years)
- Associate Director, Master of Science in Information Assurance (MSIA) on-line program
- MSIA lead instructor 2004-2006
- Distinguished Faculty Award, School of Graduate Studies, 2009

#### **2003 - 2005 – CeRNS, Center for Regional and National Security, Eastern Michigan University**

- Associate Director for Research and Information Assurance

#### **2002 - 2003 – QinetiQ Trusted Information Management**

- Chief Technology Officer, US Operations
- Director of Research
- Director of Technology, US Operations

#### **1999 - 2001 – Netigy Corporation**

- Director of Technology, Global Security Practice

#### **1982 – 1999 – Private Practice**

- Consultant

#### **1980 – 1982 – Siemens Electric Canada**

- Intelligent Digital Analyzer Project Manager

#### **1978 – 1980 – Gould/Biomation, Inc.**

- Region Manager

#### **1976 – 1978 – ElectroRent Corporation**

- Region Manager

#### **1974 - 1976 – Tektronix, Inc.**

- Field Engineer

#### **1964 – 1974 US Navy**

- Cryptographic Technician

## **Publications**

### **Books**

- Information Assurance Essentials (editor) – in press Auerbach 2011
- Combinatorial Analytics – An Introduction to Advanced Quantitative Information Assurance Analytics – in press Auerbach 2012
- Computer Security Handbook (contributor) - pubWiley 2009
- Forensic Science – An Introduction to Scientific and Investigative Techniques - pub CRC Press - contributor 2002
- Investigating Computer-Related Crime - pub CRC Press 1999
- Introduction to Personal Computers - pub Wiley 1991
- The Novell Connection - pub Brady - co-author 1990
- SQL Self Teaching Guide - pub Wiley - co-author 1992
- PerForm Self Teaching Guide - pub Wiley 1991
- Novell NetWare 2.2 - pub Wiley Co-author 1992
- dBXL and Quicksilver Programming - pub Que - co-author 1988
- Using dBASE IV 1.1 - pub Que - contributed the programming section 1990
- Using dBASE IV 2.0 - pub Que - contributed the programming section 1993
- Werken Met dBASE IV 2.0 - pub Que - Foreign translation 1994
- Implementing Internet Security - pub New Riders - contributor 1995
- PC-Netze - pub Signum - co-author 1991
- Executive Guide to Local Area Networks - pub Compute! - co-author 1990

### **Peer Reviewed Papers**

- “Toward Cyber Crime Profiling: Cyberstalking”, *Proceedings of the 6<sup>th</sup> Annual Symposium on Information Assurance*. Stephenson, P., Walter, R. 2011
- “Building Information Modeling: Necessary but not Sufficient”, *Proceedings of the BIM-Related Academic Workshop*, BIMFORUM, buildingSMARTalliance, ecobuildamerica. Puddicombe, M., Lutz, M., Stephenson, P., (2010)
- *Towards a Theory of Cyber Attack Mechanics* – Presented at IFIP 11.9 Digital Forensics, 2005.
- *Forensic Analysis of Risks in Enterprise Systems*: Pending publication, “Auerbach Information Systems Security”, May, 2004
- *A Comprehensive Approach to Digital Incident Investigation*: “Information Security Technical Report”, Elsevier Advanced Technology”, Vol. 8 No. 2, 2004
- *Application of Formal methods to Root Cause Analysis of Digital Incidents*: Computer Forensic Educators Workshop August 2004
- *A Formal Model for Information Risk Management Using Colored Petri Nets*: CPN04, Aarhus Denmark. October, 2004
- *Structured Investigation of Digital Incidents in Complex Computing Environments*: “Auerbach Information Systems Security” – July/August 2003
- *Modeling of Post Incident Root Cause Analysis* “International Journal of Digital Evidence” (<http://www.ijde.org>) – Summer/Fall 2003, Volume 2, Issue 2

CV of Peter R. Stephenson, 4474 Castlewood Drive, Auburn Hills, Michigan, USA, 48326

+1-373-2813 (office) +1-802-498-4923 (mobile) <http://www2.norwich.edu/pstephen> pstephen@norwich.edu

- *S-TRAIS: A Method for Security Requirements Engineering using a Standards-Based Architecture* – Paper selected for presentation at the First Symposium on Requirements Engineering for Information Security, March 2001, Indianapolis, Indiana
- *Intrusion Management: A Top Level Model for Securing Information Assets in an Enterprise Environment* – Paper presented at EICAR 2000, Brussels, Belgium, March, 2000
- *The Application of Intrusion Detection Systems in a Forensic Environment* – Research Project Description presented at RAID 2000, Toulouse, France

### **Technical Reports and White Papers**

- *Class C-2: Controlled Access Protection - A Simplified Description*
- *Managing Intrusions*
- *Standards and Practices for Enterprise Network Vulnerability Certification*
- *Sample Standard Practice for Implementation and Management of a Computer Incident Response Team (CIRT)* - with Nanette Poullos
- *Information Security and Y2K*
- *Structured Investigation of Digital Incidents in Complex Computing Environments* (PhD Thesis)
- *Information Dominance as an Affirmative Countermeasure against International Terrorism* (Master's Degree Thesis)
- *Digital Investigation Process Language (DIPL) Syntax Manual*
- *Using Managed Decision Support for Tactical, Operational and Strategic Information Security*

### **Selected Invited Seminar Topics**

- *Information Conflict*
- *Implementing the Secure LAN*
- *Virus Control*
- *Implementing NetWare 4.X Security Controls*
- *Implementing a Secure Migration from NetWare 3.X to NetWare 4.X*
- *Implementing Secure Internetwork Communications*
- *Privacy on the Information Superhighway*
- *Implementing Secure External Network Access*
- *Third Party NetWare Security Tools*
- *Security Awareness for Computer Users*
- *Security Awareness for Banyan Vines Network Administrators*
- *Internet Security*
- *Security Incident Investigation*
- *Implementation of a Computer Incident Response Team (CIRT)*
- *Cyber Forensic Analysis*
- *Introduction to Computer Forensic Analysis*
- *Local Area Network Technology*
- *Introduction to Intrusion Detection*
- *Vulnerability Assessment Techniques*
- *Firewall Design and Implementation*
- *Wide Area Network Security*
- *Intrusion Management*
- *Standards-based requirements engineering*

## Selected Invited Talks and Seminars

- *Introduction to Information Warfare* (MISA Conference – 2007, 2008)
- *Digital Incident Investigation* (Combined Endeavor – 2007)
- *Defensive Information Warfare* (Combined Endeavor – 2007)
- *A Unique Approach to Attack Traceback* (COSAC – 2007)
- *Ensuring the Reliability and Admissibility of Digital Evidence* (CSI 31<sup>st</sup> Annual Conference - 2004)
- *Putting the Horse Back in Front of the Cart* (Keynote speech, DFRWS 2003)
- *End-to-End Digital Investigation* (NetSec 2003, CSI 30<sup>th</sup> Annual Conference - 2003)
- *Conducting Incident Post Mortems* (CSI 30<sup>th</sup> Annual Conference – 2003)
- *Introduction to the Digital Investigation Process Language* (CSI 30<sup>th</sup> Annual Conference – 2003)
- *Certification Wars* (CSI 30<sup>th</sup> Annual Conference – 2003)
- *Digital Post Mortems and Incident Response* (SCInfoSecurity News Security Round Table - 2003)
- *Forensic Readiness* (SecureWorld Detroit – 2003)
- *Future Directions in Forensic Digital Analysis* (CERIAS – Annual Symposium – 2003)
- *Post-Digital Incident Root Cause Analysis* (Purdue University – 2003)
- *A Structured Approach to Incident Response* (2 day seminar - CSI NetSec - 2004 and CSI 31<sup>st</sup> Annual Conference - 2004)
- *Forensic Analysis of Risks in Enterprise Systems* (CSI NetSec 2004, SecureWorld 2004, and CEIC 2004)

## Selected Invited Articles

- Products Section monthly opening column, *SC Magazine*, 2006-2011
- *Assessing Vulnerabilities*: “Auerbach Information Security Journal” - 2000
- *Hiring Hackers*: “Auerbach Information Security Journal” - 2000
- *Information Warfare*: “Auerbach Information Security Journal” - 2000
- *Where is the IDS?*: “Auerbach Information Security Journal” - 2000
- *France and the Art of Intrusion Detection*: “Auerbach Information Systems Security” Jan/Feb 2001
- *Standards or Best Practices – Conflicting Interests*: “Auerbach Information Security Journal” July/August 2000
- *Investigating a Computer Security Incident*: “Auerbach Information Security Journal”
- *On the Highway*: Opinion columns written for “SC InfoSecurity News” for 1998 through 2003
- *Security Library*: Computer security book reviews written for “SC Info Security News” from 1998 through 2001
- *Getting the Whole Picture*: Digital forensic tutorial appearing monthly in Elsevier’s “Computer Fraud and Security” Newsletter 2002 - 2003
- *A Structured Approach to Incident Post Mortems* “Auerbach Information Systems Security” – Sept/Oct 2003
- *The Right Tools for the Job*: “Digital Investigation” Elsevier Advanced Technology, Vol. 1 No. 1, 2004

## **Academic & Teaching Experience**

- **2002 – 2011 Norwich University – Lecturer, digital forensics, information assurance and network-centric warfare**
  - **Student evaluations (5-point scale)**
    - **Spring 2008: 4.89, Fall 2008: 4.25, Spring 2009: 4.38, Fall 2009: 4.42, Spring 2010: 4.31**
  - **MSIA - Master of Science in Information Assurance**
    - *GI510* – Foundations
    - *GI521* – Technical Defenses
    - *GI531* – Human Factors
    - *GI541* – Detection, Response and Hot Topics
    - *Elective* – Computer Forensic Investigations
    - *GI561* – Management Tools Master's Thesis Advisor (School of Graduate Studies)
  - IS100 – Foundations of Computer Science and Information Assurance
  - IS311 – Network Forensics
  - IS406B – Virtual Network System Administration
  - IS406C – Forensic Science of Sherlock Holmes
  - IS300 – Management Information Systems
  - CJ422 – Introduction to Computer Forensics (with lab)
  - IS411 – Digital Investigation
  - IS406A – Honeypots
  - IS340 – Fundamentals of Information Assurance
  - CJ341 – Cybercrime and Cyber Law
  - IS330 – Ethics in Computing and Technology
  - IS460 – Network Communications
  - IS440 – Software Engineering III: resilient and secure software development
- 2004 – 2005 Eastern Michigan University – Adjunct Professor**
- Information Security Vulnerability and Risk Analysis
  - Cyber Crime 1
  - Cyber Crime 2
  - Network Forensics for Law enforcement
  - Industry-Based Network Administration
  - Linux Server Security
  - PhD Committee and PhD candidate advisor (continued through 2009)
- 2002 - Walsh College – Adjunct Instructor**
- *BIT 672* – Business Systems Threat Assessment
  - *BIT 673* – Information Security Safeguards
- 1980 – 1981 - Grant MacEwan Community College (Edmonton, Alberta, Canada) – Visiting Instructor**
- *AP 242.2* – Marketing and Opinion Research Design
  - *AP 123.2* – Advertising; Its Role in Marketing

## **Specific Non-Academic Teaching Experience**

### **2002 – 2004 Norwich University *SecureIT* Symposium**

- Invited Lecturer on Digital Forensic Science and Digital Investigation, 16 contact hours per year

### **1999 – 2006 – Computer Security Institute - Faculty**

- Taught an average of 76 contact hours per year through 2004
- Developed at least 3 new courses per year through 2003, average 16 contact hours each

### **1995 – 1996 – MIS Training Institute - Faculty**

- Taught an average of 280 contact hours per year
- Developed 3 courses of 40, 22.5 and 17.5 contact hours respectively

### **2000 – 2004 – American Express - Contract Instructor in Digital Investigation**

- Taught an average of 64 contact hours per year & Developed 7 specialized courses of 32 contact hours each

## **Industry Certifications and Training**

- Member Upsilon Pi Epsilon, Honor Society for the Computing and Information Disciplines
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Fellow, Institute for Communications, Arbitration and Forensics (FICAF – UK)
- Digital forensic training certificate – NTI 1997
- Reid Interview and interrogation advanced certification - 2000

## **Current Research Interests**

- Cyber crime assessment, profiling cyber offenders
- Applications of theoretical digital forensic science

## **Editorial, Review and Advisory Boards**

- Program committee - CISSE
- Editor-in-Chief – Norwich University Press
- Editorial Review Board – “International Journal of Digital Crime and Forensics”
- Advisory Board Member - Digital Forensic Certification Board (DFCB)
- Technology editor – “SC Magazine”
- Referee - Research Council of Norway, 2004 digital forensics grant proposals
- Technical Program Committee, E-Forensics 2010 (3<sup>rd</sup> international ICST conference on forensic applications and techniques in telecommunications, information and multimedia)
- Faculty advisor, student chapter of the ACM

### **Pro Bono**

- IA advisor to the state of Vermont
- Testified before members of the Vermont Legislature
- IA advisor to Combined Endeavor 2007/2011, a 40 + nation NATO/US Army sponsored interoperability exercise held in Europe

### **University Committees**

- Academic integrity
- Committee on Academic Technology
- President's Advisory Council

### **Organizations**

- American Academy of Forensic Sciences – Associate Member
- Vidocq Society – Special Member
- Institute for Communications, Arbitration and Forensics (UK)
- Association for Computing Machinery (ACM)
- International Information Systems Security Certification Consortium (ISC<sup>2</sup>)
- Vermont Chapter, InfraGard
- International Federation of Information Processing, Technical Committee TC-11, Working Group WG 11.9: Digital Forensics – Regular Member
- Oxford Brookes University Alumni Association
- Norwich University Alumni Association
- Cyber Conflict Studies Association

### **Patents**

- A Formal Process for Information Systems Risk Analysis and Management (provisional - expired)
- An Improved Process for Information Systems Risk Analysis and Management (pending)