

## **CURRICULUM VITAE OF PETER R. STEPHENSON, PHD, CISSP (LIFETIME)**

### **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 – Center for Digital Forensic Studies, Limited and Cyber Crime Research Lab**

- Next generation cyber security research
- Cyber criminologist and cyber jurisprudence subject matter expert
- Technology Editor, SC Magazine (retired 31 Dec 2017 after 25 years with the magazine in one form or another)

#### **2005-2015 – Norwich University (Vermont) – Retired June 2015**

- Director Center for Advanced Computing and Digital Forensics
- Associate Professor focusing on information security and digital forensics) and Chief Information Security Officer

#### **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 and 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

#### **1973 - 1976 – Tektronix, Inc.**

- Field Engineer

#### **1963 – 1973 US Navy**

- Cryptographic Technician

### **Duties and Assignments at Norwich Since Employment Began**

- Director, Norwich University Center for Advanced Computing and Digital forensics
- Associate Director, Department of Computing, School of Business and Management
- Chief Information Security Officer
- Associate Professor

CV of Peter R. Stephenson, 4474 Castlewood Drive, Auburn Hills, Michigan, USA, 48326  
+1-373-2813 (office) • +1-802-498-4923 (mobile) • <http://www.cdfs.us> • [pstephen@cdfs.us](mailto:pstephen@cdfs.us)

- 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
- Classes Taught (\*classes created)
  - *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
  - \*IS312 – Malware Forensics
  - \*IS399 – Cyber Criminalistics
  - \*IS406 – Advanced Digital Forensics Practicum
  - \*IS456 – Cyber Defense Practicum
  - \*IS406B – Virtual Network System Administration
  - 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

## **Professional Activities**

- Member of Vermont CybORG – Cyber Operations Readiness Group, sponsored by Vermont government initiative
- Submission Reviewer – HICSS-45 conference – Digital Forensics Mini-Track
- Program committee co-chair – Digital and Multimedia Section, American Academy of Forensics Sciences
- Program committee chair – Digital and Multimedia Section, American Academy of Forensics Sciences
- Session Chair – Symposium on Information Assurance: Data Privacy Protection
- Program committee chair – CISSE
- Member DC3 Academic Cyber Curriculum Alliance Board
- 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)
- Advisor to the Vermont AG office
- Consultant to local and Federal law enforcement agencies on cyber forensic matters

CV of Peter R. Stephenson, 4474 Castlewood Drive, Auburn Hills, Michigan, USA, 48326  
+1-373-2813 (office) • +1-802-498-4923 (mobile) • <http://www.cdfs.us> • [pstephen@cdfs.us](mailto:pstephen@cdfs.us)

- Advisor Combined Endeavor, international cyber interoperability exercise comprising over 40 countries
- Research collaborations with Prof. Ustijana Rechkoska Shikoska, of University for Information Science and Technology "St. Paul the Apostle"

## **Publications**

### **Books**

- Official Guide to the CCFP [Certified Cyber Forensics Professional] Certification (Editor in chief and contributor) – Auerbach 2014
- Investigating Computer-Related Crime, 2<sup>nd</sup> Ed - pub CRC Press 2013
- Criminalistics – An Introduction to Forensic Science 11<sup>th</sup> Ed (contributor) – Prentice Hall 2013
- Computer Security Handbook, 6<sup>th</sup> Ed (contributor –“Cyber Investigation”) – pub Wiley 2014
- Computer Security Handbook, 5<sup>th</sup> Ed(contributor– “Cyber Investigation”) - 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 and Conference Presentations**

- “*Adversarial Machine Learning – the Coming Legal Storm*” *Legal Issues Journal* – vol 8, issue 2 7/2020
- “Jurisdiction in Cyberspace: A Matter of Conflict of Laws?” *enfuse 2018 cyber security/privacy/forensics conference*
- “Digital Forensic Science – An Oxymoron?” *Legal Issues Journal* – vol 6, issue 2, 7/2018
- “Connecting Cyber and Physical Crime Scenes”, *Proceedings of the 65<sup>th</sup> Annual Scientific Meeting of the American Academy of Forensic Sciences*, Stephenson, P., Walter, R. 2013
- “The Facebook Faker”, *Proceedings of the 65<sup>th</sup> Annual Scientific Meeting of the American Academy of Forensic Sciences*, Stephenson, P., Walter, R. 2013
- “Cyber Crime Assessment”, *Proceedings of the 45<sup>th</sup> Hawaii International Conference on System Sciences*, Stephenson, P., Walter, R. 2012

CV of Peter R. Stephenson, 4474 Castlewood Drive, Auburn Hills, Michigan, USA, 48326  
+1-373-2813 (office) • +1-802-498-4923 (mobile) • <http://www.cdfs.us> • [pstephen@cdfs.us](mailto:pstephen@cdfs.us)

- “Toward Cyber Crime Assessment: 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: “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
- *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**

- “*Managing Next Generation Threats to Cyber Security*” – Best of the World in Security, virtual conference, 13 November 2020
- *An Update to the Cyber Threatscape – tracing threats to the financial services community* – ISACA Western New York Chapter

CV of Peter R. Stephenson, 4474 Castlewood Drive, Auburn Hills, Michigan, USA, 48326  
+1-373-2813 (office) • +1-802-498-4923 (mobile) • <http://www.cdfs.us> • [pstephen@cdfs.us](mailto:pstephen@cdfs.us)

- *Threat Hunting Workshop* - ISACA Western New York Chapter and SecureWorld Expo (multiple presentations)
- *(ISC)<sup>2</sup> CCFP Review Course –5-day master class*
- *Cybercrime Assessment and Offender Profiling*
- *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*
- *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**

- *Cybercrime Assessment* – full day seminar: SecureWorld Detroit Spotlight and Boston Spotlight
- *Cybercrime Assessment – an Introduction* – Keynote, HTCIA Training Day – summer 2011
- *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* (PurdueUniversity – 2003)

CV of Peter R. Stephenson, 4474 Castlewood Drive, Auburn Hills, Michigan, USA, 48326  
+1-373-2813 (office) • +1-802-498-4923 (mobile) • <http://www.cdfs.us> • [pstephen@cdfs.us](mailto:pstephen@cdfs.us)

- *A Structured Approach to Incident Response* (2 day seminar - CSINetSec- 2004 and CSI 31<sup>st</sup> Annual Conference - 2004)
- *Forensic Analysis of Risks in Enterprise Systems* (CSINetSec 2004, SecureWorld 2004, and CEIC 2004)

## Selected Invited Articles and Columns

*SecureWorld (WWW.SecureWorldExpo.com)* – “Is Hack-Back a Good Idea?” 16 Mar 2017

*SecureWorld (WWW.SecureWorldExpo.com)* – “Deception and Forensics for the Next Generation” – series of seven blogs starting 26 April 2020

*Cyber Defense Magazine*: Analysis and Deep Dive Review, Attivo BOTsink deception network – 21 May 2020

*Cyber Defense Magazine*: Analysis and Deep Dive Review, Infocyte, enterprise cyber forensic tool - 30 August 2020

*Security Library*: Computer security book reviews written for “SC Info Security News” from 1998 through 2001

*On the Highway*: Opinion columns written for “SC InfoSecurity News” for 1998 through 2003

*Getting the Whole Picture*: Digital forensic tutorial appearing monthly in Elsevier’s “Computer Fraud and Security” Newsletter 2002 - 2003

**The “SC Magazine” columns** below started in the mid 2000s and continued until my retirement at the end of 2017. This list includes a sampling only to show the breadth of topics covered.

- *Mobile and endpoints are where the action is*: “SC Magazine” July-August 2014
- *Mobile device management*: “SC Magazine” July-August 2014
- *Soft intelligence is important too*: “SC Magazine” July-August 2014
- *Bits and bytes in intelligence*: “SC Magazine” July-August 2014
- *Mitigating risk is not as simple as it seems*: “SC Magazine” June 2014
- *Risk & policy management*: “SC Magazine” June 2014
- *Digging deep with forensic tools*: “SC Magazine” May 2014
- *Digital forensic tools*: “SC Magazine” May 2014
- *The more things change...*: “SC Magazine” April 2014
- *SIEM*: “SC Magazine” April 2014
- *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”
- *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

## **University Committees and Other Assignments**

- Academic integrity
- Committee on Academic Technology
- Upsilon Pi Epsilon computing honor society Faculty Advisor
- Faculty Advisor ACM Student Chapter
- President's Advisory Council
- Principal Investigator for the DoD IASP (scholarship program)
- Principal Investigator for academic center of excellence programs
- Principle Investigator for NSF CyberCorps Scholarship for Service Program at Norwich

## **Professional and Scholarly Awards, Honors and Memberships**

- Received the Distinguished Faculty Award, School of Graduate Studies, 2009
- Certified Cyber Forensics Professional (CCFP) ID #1
- University award for excellence in research - 2013
- Faculty Member Upsilon Pi Epsilon, Honor Society for the Computing and Information Disciplines
- Certified Information Systems Security Professional (CISSP) – lifetime designation
- Certified Information Security Manager (CISM) – retired 2016
- Licensed Professional Investigator – Michigan - retired
- Digital forensic training certificate – NTI 1997
- Reid Interview and interrogation advanced certification - 2000
- IA advisor to the state of Vermont and the Vermont Attorney general's office
- Vidocq Society Member and chief information security officer
- Testified before members of the Vermont Legislature (House Commerce Committee and Senate Judiciary Committee) on the topic of breach disclosure laws
- IA advisor to Combined Endeavor 2007-2012, a 40 + nation NATO/US Army sponsored interoperability exercise held in Europe
- Fellow, American Academy of Forensic Sciences (retired in 2016)
- Patent: A Method for Evaluating System Risk – U.S. Patent Number 8539586
- Ponemon Institute – Distinguished Fellow
- Association for Computing Machinery (ACM) – Professional Member (retired 2016)
- International Information Systems Security Certification Consortium (ISC<sup>2</sup>)
- Albany Chapter, InfraGard
- Oxford Brookes University Alumni Association