Rene Willems

HSD Innovation in Security Process and Value Added

The Hague Security Delta (HSD) is the largest security cluster in Europe. Businesses, governments, and knowledge institutions work together on innovations and knowledge in the field of cyber security, national and urban security, protections of critical infrastructure, and forensics. They share a common goal: through innovation and education contribute to a more secure world and create more business activities and jobs. The HSD Campus, that was opened in February 2014, serves as cornerstone for the cluster.

In this presentation, Mr. Willem will address the initial development of HSD and present lessons learned in setting up such particular initiative of public-private partnership. With a brief discussion on the governance of HSD and the facilities that are offered to its stakeholders, Mr. Willem will conclude with HSD's innovation agenda and its collaboration with security clusters around the world. Particular emphasis will be given to the Cyber Security Agenda of HSD.

About the speaker

Rene Willems has a background in Military Operations Research. He worked as an analyst for TNO and for NATO (Saclantcen), mainly in the field of maritime and air defence studies, for operational planning and evaluation and for material procurement.

He held various TNO management positions, including Head of the Operational Research and Business Management Division at TNO Physics and Electronics Laboratory. He was involved in and responsible for a series of international cooperation programs in the field of Operations Research. He was chairman of the NATO Panel on Studies, Analysis and Simulation.

With Prof. R de Wijk, he set up the Hague Centre for Strategic Studies. He developed the concept of the Hague Security Delta and contributed to its development. The HSD Campus opened in February 2014.

Thanks to our SERENE-RISC Partners

CGI

DRDC | RDDC technologysciencetechnologie

ESET ENJOY SAFER TECHNOLOGY™

ITAC INFORMATION TECHNOLOGY ASSOCIATION OF CANADA

ACTI ASSOCIATION CANADIENNE DE LA TECHNOLOGIE DE L'INFORMATION

NCE RCE

Public Safety Canada / Sécurité publique Canada

Symantec

TRTech

Université de Montréal

VFAC

April 22 & 23, 2015 | Canadian Museum of Nature | 240 McLeod Street | Ottawa

Wednesday	
8:00 - 9:00	**Registration and continental breakfast** – Barrick Salon
9:00 - 10:00	**Opening session keynote** – Barrick Salon • *Our Phone Calls Are Insecure, And No One Is Doing Anything* Christopher Soghoian, American Civil Liberties Union (ACLU)
10:00 - 10:30	**Networking break** – Barrick Salon
10:30 - 12:00	**Session 1 – Government initiatives** – Barrick Salon • *CASL – More than SPAM* Lynne Perrault, Canadian Radio-television and Telecommunications Commission (CRTC) • *The Digital Age Creates One of the Greatest Challenges in the History of Policing* Bernie Murphy, Ontario Provincial Police (OPP)
12:00 – 13:30	**Networking lunch & Knowledge mobilization discussion group** – Barrick Salon
13:30 – 15:00	**Session 2 – Legal and regulatory options** – Barrick Salon • *Law + Document Security: Enterprise New Documentation Obligations* Vincent Gautrais, Université de Montréal • *The Future of the Emerging Cyber Regime Complex* Mark Raymond, University of Oklahoma
15:00 – 15:30	**Networking break** – Barrick Salon
15:30 – 17:00	**Session 3 – Information sharing in Canada** – Barrick Salon (registered participants only) • *CCIRC, Canadian Cyber Incident Response Centre & Cyber Security in Canada* Mark Matz, Canadian Cyber Incident Response Centre (CCIRC) – Public Safety Canada • *Know what is coming and be ready when it gets here* Gary Miller, CGI • *Information Sharing: a Key to Security* Colin Gilmore, TRTech **Followed by End of day remarks** (Barrick Salon) **& Networking reception** (Rotunda)
Thursday	
8:00 – 9:00	**Registration and continental breakfast** – Barrick Salon
9:00 – 10:30	**Session 4 – Technical solutions to cybersecurity challenges** – Barrick Salon • *Cyber Threat Intelligence Generation: Insights, Challenges and Opportunities* Mourad Debbabi, Concordia University • *Focusing on Trust and Security* Stephen Marsh, University of Ontario Institute of Technology • *Cybersecurity in a quantum world: will Canada be ready?* Michele Mosca, University of Waterloo
10:30 – 11:00	**Networking break** – Barrick Salon
11:00 – 12:30	**Session 5 – Innovative partnerships and developing a skilled cybersecurity workforce** – Barrick Salon • *How to create a Cybersecurity Workforce* Ida Haisma, The Hague Security Delta • *HSD Innovation in Security Process and Value Added* Rene Willems, TNO & The Hague Security Delta
12:30 - 14:00	**Networking lunch** – Barrick Salon

Opening session

Chair: Benoît Dupont, SERENE-RISC, Université de Montréal

Christopher Soghoian

Our Phone Calls Are Insecure, And No One Is Doing Anything

Some of the most widely used encryption algorithms that protect our cellular phone calls were designed in the 1980s and broken in the 1990s. In the decades since, computer security researchers have refined these attacks, ultimately demonstrating that phone calls and text messages can be intercepted with a few hundred dollars worth of off-the-shelf hardware and some open source soft-ware. Yet, in spite of the many research papers published and demonstrations at high-profile security conferences, little has been done. The phone companies in the US and elsewhere, continue to operate networks that use weak encryption. These companies and government regulators that are responsible for communications networks have neither warned the public about the insecurity of traditional phone calls, nor advised them about the ways in which they can more securely communicate. Moreover, efforts by activists to obtain documents showing how these flaws are being exploited for surveillance by law enforcement and intelligence agencies have largely been blocked, as agencies claim that publishing that information will reveal classified information.

This talk, in part, is about the sorry state of our cellular communications networks. But it is also about the total failure of the computer security community to influence public policy, particularly when opposed by law enforcement and intelligence agencies, who want nothing to change and the public to be kept in the dark.

About the speaker

Dubbed the "Ralph Nader for the Internet Age" by Wired and "the most prominent of a new breed of activist technology researchers" by the Economist, Christopher Soghoian works at the intersection of technology, law, and policy. A leading expert on privacy, surveillance, and information security, Soghoian is currently the Principal Technologist at the American Civil Liberties Union.

Workshop Facilitator

Conference Board of Canada

Dan Munro

About the facilitator

Daniel Munro is a Principal Research Associate in Public Policy at The Conference Board of Canada, and Lecturer in Ethics in the Graduate School of Public and International Affairs at the University of Ottawa. Prior to joining the Public Policy group, Daniel worked for the Conference Board's Centre for Skills and Post-Secondary Education, Centre for Business Innovation, and Industry and Business Strategy division.

Daniel has over ten years of experience in research and policy analysis on science, technology, innovation, education and skills issues. He also thinks, writes and speaks about ethics, decision-making, risk, and democracy for academic and public audiences. Daniel holds degrees from Toronto (B.A.), Western (M.A.), and MIT (Ph.D.).

Session 1

Government initiatives
Chair: Kerry Patterson-Baker, Symantec

Lynn Perrault

CASL – More than SPAM

Canada's Anti-spam legislation came into force on July 1, 2014. And while the name suggests that the CRTC's responsibilities under CASL focus on the sole issue of spam, it actually includes much more than that. The presentation will provide an overview of the CRTC's mandate, enforcement activities and its efforts to create robust partnerships to assist in supporting its mandate under CASL.

About the speaker

Lynne Perrault is the Director of Electronic Commerce Enforcement Division at the CRTC. She is responsible for ensuring that the CRTC enforcement responsibilities designated under the new Canadian Anti-Spam legislation are met. Mrs. Perrault previously held the position of Executive Director of the National Cyber-Forensics and Training Alliance Canada while concurrently working at the Competition Bureau of Canada in the Electronic Evidence Unit and previously in the Fair Business Practices branch. She has more than 25 years of rich experience in investigations and enforcement. In the past, Mrs. Perrault led the 2nd largest investigative firm in Ontario, expanding into three other provinces. As a respected leader and young entrepreneur, she was twice recognized as one of Ottawa's top 40 executives under 40 in 1997 and 1999 and nominated for Young Entrepreneur of the Year in 1998.

Michele Mosca

Cybersecurity in a quantum world: will Canada be ready?

Emerging quantum technologies will break currently deployed public-key cryptography which is one of the pillars of modern-day cybersecurity. Thus we need to migrate our systems and practices to ones that are quantum-safe before large-scale quantum computers are built. There are viable options for quantum-proofing our cryptographic infrastructure, but the road ahead is neither easy nor fast.

Impressive progress in developing the building blocks of a fault-tolerant scalable quantum computer indicates that the prospect of a large-scale quantum computer is a medium-term threat.

The transition to quantum-safe cybersecurity cannot wait any longer without risking a major cyber-catastrophe much broader and deeper in scope and impact than what has been witnessed in the world to date. Being global leaders in this transition presents Canada with a great opportunity, and Dr. Mosca will outline some of the steps needed to seize this opportunity.

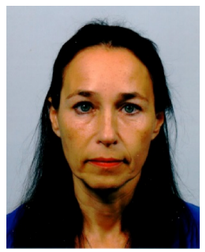
About the speaker

Michele Mosca obtained his doctorate in Mathematics in 1999 from the University of Oxford on the topic of Quantum Computer Algorithms. He joined the Waterloo faculty in 1999. He is co-founder and Deputy Director of the Institute for Quantum Computing at the University of Waterloo, a Professor in the Department of Combinatorics & Optimization of the Faculty of Mathematics, and a founding member of Waterloo's Perimeter Institute for Theoretical Physics.

His current research interests include quantum algorithms and complexity, tools for optimizing the implementation of quantum circuits, and the development of cryptographic tools that will be safe against quantum technologies. Dr. Mosca's work is published widely in top journals, and he co-authored the respected textbook "An Introduction to Quantum Computing" (OUP).

Session 5

Innovative partnerships and developing a skilled cybersecurity workforce
Chair: Joe Cummins, Red Tiger Labs



Ida Haisma

How to create a Cybersecurity Workforce

Security is an important prerequisite for social and economic development. It also is an innovative sector. The Hague Security Delta (HSD) has developed the Dutch National Innovation Agenda for Security. It directs the innovation processes and provides an overview of innovation needs and opportunities in the Dutch security sector, ensuring that innovation investments are used as efficiently as possible. With HSD's guidance, the Dutch government, businesses, and knowledge institutions are currently implementing the agenda. They focus on complex issues surrounding cyber security, sensor technology, identity issues, and secure critical infrastructures.

HSD Security Talent is the education and career platform for students and professionals in the fast-growing field of safety & security. The platform offers an up-to-date overview of vacancies, internships, courses, and trainings in security. This enables students to make informed study choices and employers can bring their vacancies directly to the attention of the currently scarce security talent. This way HSD Security Talent stimulates a career in security and contributes to employers' increasing need for security talent. It is only with qualified staff that the Dutch Security cluster will be able to realise more jobs, more business activity, and a more secure world.

About the speaker

In March 2014 Ida Haisma took up the position of Executive Director of the Hague Security Delta (HSD), www.thehaguesecuritydelta.com, the largest security cluster in Europe, in which companies, governments, and knowledge institutions work together on innovations and knowledge in the field of cyber security, national and urban security, protection of critical infrastructure, and forensics. They have shared ambition: a secure world and economic development. Ida directs the programmes of HSD and is responsible for further international positioning and developing the organization as well as the cooperation between the HSD partners. Previously she was Director Innovation Safety & Security at TNO.

Session 4

Technical solutions to cybersecurity challenges
Chair: Francis Fortin, SERENE-RISC co-Investigator, Université de Montréal

Mourad Debbabi

Cyber Threat Intelligence Generation: Insights, Challenges and Opportunities

In this talk, Dr. Debbabi will review some of his recent research and development initiatives in the area of cyber threat intelligence generation. In this respect, he will discuss his progress in software fingerprinting as well as the analysis of passive DNS, darknet and spam-trap streams. Moreover, he will highlight some of the interesting and challenging research directions and opportunities in this area.

About the speaker

Dr. Mourad Debbabi is a Full Professor at the Concordia Institute for Information Systems Engineering. He holds the Concordia Research Chair Tier I in Information Systems Security. He is also the President of the National Cyber Forensics Training Alliance (NCFTA Canada). He is the founder and one of the leaders of the Computer Security Laboratory (CSL) at Concordia University. In the past, he was the Specification Lead of four Standard JAIN (Java Intelligent Networks) Java Specification Requests (JSRs) dedicated to the elaboration of standard specifications for presence and instant messaging. Dr. Debbabi holds Ph.D. and M.Sc. degrees in computer science from Paris-XI Orsay, University, France. He published 3 books and more than 260 research papers in international journals and conferences on computer security, cyber forensics, privacy, cryptographic protocols, threat intelligence generation, malware analysis, reverse engineering, specification and verification of safety-critical systems, formal methods, Java security and acceleration, programming languages and type theory. He supervised to successful completion 21 Ph.D. students and more than 60 Master students. He served as a Senior Scientist at the Panasonic Information and Network Technologies Laboratory, Princeton, New Jersey, USA; Associate Professor at the Computer Science Department of Laval University, Quebec, Canada; Senior Scientist at General Electric Research Center, New York, USA; Research Associate at the Computer Science Department of Stanford University, California, USA; and Permanent Researcher at the Bull Corporate Research Center, Paris, France.

Stephen Marsh

Focusing on Trust and Security

It is becoming increasingly common to see trust featured insecurity milieu - mentioned, paid heed to, questioned and valued in equal measures. Indeed, the relationship between trust and computer security goes back many years (witness the Orange Book, for instance). Better security, it is asserted, brings trust. It's difficult to argue with this but the principles involved sometimes miss the fact that trust and security are orthogonal concepts with very different goals and outlooks.

They are both, for example, about control, but in very different ways. They both think about risk, but with very different lenses. They both work toward comfort, but along very different paths.

This talk will explore the relationships between trust and security in computational settings, bringing to the fore discussions of trusted computing, computational trust, reputation and foreground trust, topics which I've been working on for some time. It will examine how the concepts relate, where they should become closer, and where they should agree to differ and why. At the end of the talk, we hope a little light will be shed on the trust-security family, and that a little more understanding of when and how trust just might be helpful will be forthcoming.

About the speaker

Steve Marsh is a trust scientist who works with trust for computational systems. He is an Assistant Professor of Information Systems in Business and Information Technology, University of Ontario Institute of Technology. His PhD (University of Stirling) is a seminal work that introduced the first formalisation of computational trust. A milestone in multidisciplinary trust research, and still widely referenced.

Steve's current work builds on this model, applying it to mobile device security and privacy, protection of the user, device comfort and regret management. He is Secretary of IFIP Working Group 11.11: Trust Management, delegate to IFIP Technical Committee 11: Security and Privacy Protection in Information Processing Systems, and an adjunct professor at UNB and Carleton University. Steve lives in rural Ontario, Canada with dogs, cats, horses, chickens, and people, all of whom have their own things to teach us about trust.

Bernie Murphy

The Digital Age Creates One of the Greatest Challenges in the History of Policing

Digital technologies have impacted on police investigations in four key areas: 1) An overwhelming and unmanageable demand for the recovery of digital evidence from the myriad of devices entrenched in our lives; 2) The Internet provides a treasure trove of evidence, but one that comes with its own unique problems; 3) Communications technologies have and investigative techniques are not able to keep pace; 4) Police agencies are in possession of highly sensitive data and must ensure the highest security standards. Further, law enforcement has a key role to play in ensuring cybersecurity across society.

Some of the topics to be discussed in this presentation will expound on above illustrating the enormity of this problem and will discuss metrics related to police investigations such as numbers and measurements related to digital forensics (and the exponential growth in demand) and difficulties in measuring various types of cybercrime. Proposed strategies to address these problems will be discussed, including various forms of engagement with the broader community: academia, private sector, and other government agencies.

About the speaker

Bernie Murphy has been with the Ontario Provincial Police for 27 years. He started his career in Nipigon Detachment in Northwestern Ontario and has since worked in a number of specialized investigative roles including physical surveillance, forgery, major frauds and homicide. He has worked in management roles as a Major Case Manager in Criminal Investigation Branch, Director of Anti-Rackets Branch and as Director of Strategic Management at the Alcohol and Gaming Commission of Ontario. He is currently the Director of the OPP's Behavioural, Forensic and Electronic Services.

He is also a liaison with the OPP's Workplace Discrimination and Harassment Program and is a Deputy Aide de Camp for the Lieutenant-Governor of Ontario.

He sits on the Executive of the OPP Commissioned Officers Association and has been the Association's Director on the Board of the Friends of The OPP Museum since 2012.

Session 2

Legal and regulatory options
Chair: Laura Huey, SERENE-RISC co-Investigator, University of Western Ontario

Vincent Gautrais

Law + Document Security: Enterprise New Documentation Obligations

More and more, web players must document their data preservation practices. While in traditional evidence law, one must use documents produced by third parties to prove something (a signature, documents produced by the opposite side, etc.), digital evidence introduced in front of the courts must be accompanied by explanations of the conditions under which these documents were created, hosted, archived, transmitted. Whether it is an html page, a screen capture, a word file, or a Wikipedia entry, each new piece of evidence, to be admitted, must explain how the document was managed. A new major principle therefore emerges: documentation. Breaking somehow established legal traditions, each stage of a document's lifecycle must be considered beforehand. This process often rests on technical norms and standards designed by the industry (ISA, ARMA, COBIT). But these technical norms precisely require companies to adopt procedures and policies demonstrating their due diligence in how their protect their data.

About the speaker

Full Professor at the Université de Montréal's Faculty of Law, Vincent Gautrais is director of Centre de recherche en droit public. He teaches a number of courses on information technology law and business law and since June 2005, he has held the Université de Montréal Chair in e-Security and e-Business Law.

Prior to teaching at the Université de Montréal, he was a professor in the common law section at the University of Ottawa. Since 1992, he has been doing research, writing books and articles, giving conferences on electronic business law, electronic contracts, digital evidence, cyber-consumption, network security, dispute resolution by and for the Internet, intellectual property and privacy.

Mark Raymond

The Future of the Emerging Cyber Regime Complex

This talk examines emerging patterns of contention and assesses likely institutional trajectories in Internet governance and cybersecurity. In doing so it makes two primary arguments. The first is that a broader cyber regime complex is currently forming in response to externalities created by the increasing importance of the Internet. The second is that this ongoing process of regime complex formation is complicated by: (1) technological and social complexity; (2) uncertainty both about the governance implications of information technology, and about the distributional and other implications of particular governance arrangements; (3) the increasing number of stakeholders, with diverse (and rapidly-evolving) values and interests; and (4) lack of consensus on legitimate procedural rules. The collective result has been a degenerative shift from technocratic coordination to contention. The talk concludes by assessing theoretical and policy payoffs of these findings. Most notably, the speaker suggests the importance of: (1) crafting a procedural modus vivendi to ensure that it is possible to create and adapt institutions such that they will continue to enjoy broad legitimacy; (2) acquiring higher quality information both about the governance implications of ICTs and the distributional implications of different potential rule-sets; and (3) the virtues of patience and renegotiable soft law instruments.

About the speaker

Mark Raymond is the Wick Cary Assistant Professor of International Security in the Department of International and Area Studies at the University of Oklahoma. He holds a Ph.D. from the University of Toronto. His interests include International Relations theory, international law and organization, and international security.

He is the co-editor, with Gordon Smith, of Organized Chaos: Reimagining the Internet (Waterloo, Canada: CIGI, 2014). His work has also appeared in the Georgetown Journal of International Affairs and the Canadian Foreign Policy Journal.

Mark was previously a Research Fellow at the Centre for International Governance Innovation, where he contributed to research and programming on Internet governance, including the Global Commission on Internet Governance. He has spoken before the UN Commission on Science and Technology for Development, and at the Internet Governance Forum.

Session 3

Information sharing in Canada
Chair: Sylvain Leblanc, SERENE-RISC co-Investigator, Royal Military College of Canada

Mark Matz

CCIRC, Canadian Cyber Incident Response Centre & Cyber Security in Canada

CCIRC is Canada's National Cyber Emergency Response Team, or CERT. Learn what CCIRC services are and what areas of technical expertise on which it focuses as well as the role CCIRC has within the Canadian context. We will also share situational awareness of Canada's cyber security, elaborating on trends as well as how Canada is positioned in relation to other world leaders.

About the speaker

Mark Matz is Director of Policy and Issues Management within the National Cyber Security Directorate at Public Safety Canada. Mark has worked in various policy positions with the Government of Canada, including with the Privy Council Office and Canadian Heritage. Mark holds a Masters of Philosophy from the University of Oxford, which he attended as a Rhodes Scholar.

SERENE-RISC Workshop
Presenters bios and abstracts

Gary Miller

Know what is coming and be ready when it gets here

About the speaker

Gary Miller is a Global Director responsible for the business development and business engineering aspects of CGI's Global Cyber Security line of business. For 18 years Gary has been assisting government and industry across the globe shape appropriate cyber security strategies to support their changing business.

Having held executive leadership positions in cyber security strategy, general management, product management, and business development, Gary brings a diverse perspective to the modern cyber security challenge. Gary's unique balance of business and cyber security experience allows him to work with senior leaders to plot the most effective way forward in today's complex environment.

Colin Gilmore

Information Sharing: a Key to Security

About the speaker

Colin Gilmore is a currently the Program Leader for the TRTech Security Ecosystem, leading a technology development group in commercializing technologies for the cyber-security industry. He is a co-founder of a technology start-up (151Research) that is developing microwave imaging technology. He completed the M.Sc., and Ph.D. degrees in Electrical and Computer Engineering at the University of Manitoba in 2005 and 2010, respectively. He has received numerous national and international awards and scholarships, including the Gold Medal in Electrical Engineering for highest academic standing upon graduation, a Natural Sciences and Engineering Research Council (NSERC) of Industrial R+D Fellowship, NSERC Canada Post-Doctoral Fellowship, NSERC Canada Graduate Scholarship (Ph.D.), NSERC Post-Graduate Scholarship (MSc), and an International Union of Radio Science Young Scientist Award. He has authored and co-authored over 16 papers in peer reviewed international journals, and a US patent.

Thank you to our Gold Sponsor

The Conference Board of Canada | Le Conference Board du Canada