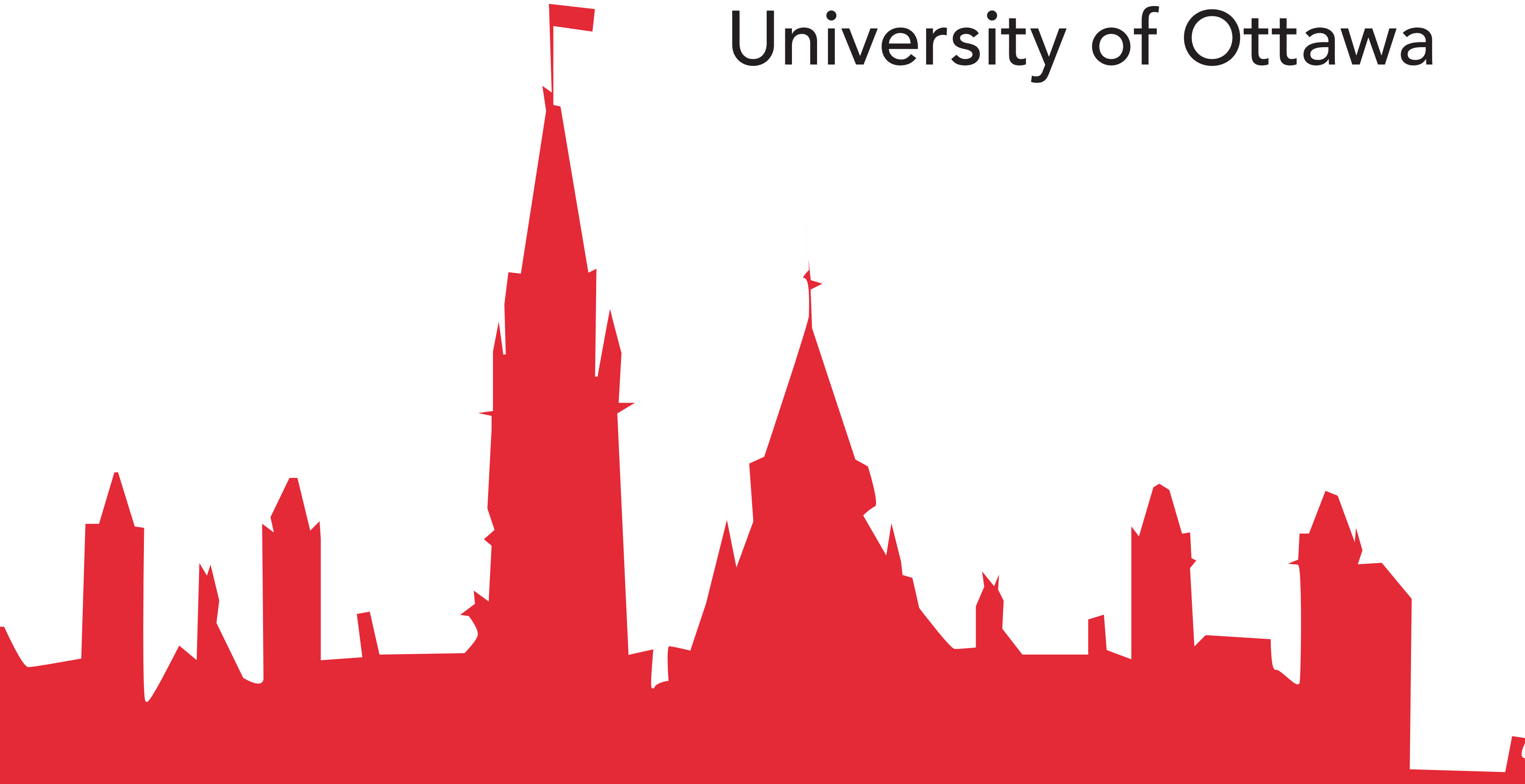
October 23-24, 2019
University of Ottawa



2019 SERENE-RISC Annual Workshop Program

serene
risc

NCE RCE

Université
de Montréal

Welcome to Our Workshop

On behalf of SERENE-RISC, it is my great pleasure to welcome you to Ottawa for our annual workshop, focused on public awareness initiatives and cybercrime prevention.

Over the years, the quality and diversity of SERENE-RISC's stakeholders and associates, along with the Networks of Centres of Excellence of Canada, have helped us reach a level of maturity and play a significant role in knowledge mobilization for the cybersecurity ecosystem.

Hence, I would like to thank the SERENE-RISC staff, session chairs, keynote speakers, panelists, poster presenters and attendees from academia, industry and governments for helping us build our network and this workshop.

We sincerely hope that you will enjoy our program and your time in Ottawa.

Benoît Dupont
Scientific Director
SERENE-RISC

Table of Contents

About SERENE-RISC

About the Network

The Smart Cybersecurity Network (SERENE-RISC) is a knowledge mobilization network created to enable people to protect themselves against cyber threats and minimize their consequences. SERENE-RISC is a non-profit organization (NPO) funded by the federal Networks of Centers of Excellence and hosted by the University of Montreal.

To do this, SERENE-RISC relies on knowledge mobilization, a multidisciplinary approach to transfer knowledge from their point of creation to the end users. Knowledge mobilization thus reinforces the links between research, policy and practice.

SERENE-RISC brings together more than 40 academics from 9 disciplines and spread across 24 post-secondary institutions across Canada as well as more than 24 members from the public and private sectors and six NPOs.

Administrative Team

Benoît Dupont
Scientific Director

Nafi Niang
Executive Director

Michael Joyce
Knowledge
Mobilization Coord.

Fyscillia Ream
Scientific Coordinator

Jasmin Pilon
Comm. Adviser

Louis Couderc
Digital Media Assist.

Raphaël Hoarau
Digital Media Assist.

Find us on: /SERENE_RISC /COMPANY/SERENE-RISC/ /SERENERISC

Workshop Program

Day 1 – Wednesday, Oct. 23, 2019

8:00 - 8:45 **Registration and continental breakfast (Grande Salle)**

8:45 - 9:00 **Welcoming address**
Benoît Dupont, Université de Montréal,
SERENE-RISC Scientific Director

Sonia Chiasson, Carleton University,
SERENE-RISC Deputy Scientific Director

9:00 - 10:15 **Keynotes**
Dr. Michelle Mazurek, University of Maryland
Dr. David Maimon, Georgia State University

10:15 - 10:45 **Networking break**

10:45 - 12:15 **Session 1 – Demand-Driven Innovation in Cyber for Defence & Security**
Chaired by Eric Fournier, Defense Research and Development Canada

Brigadier-General Andrew Jayne, Canadian Armed Forces
Dr. Helen Tang, Defense Research and Development Canada
Allen Dillon, Sapper Labs, root9B

12:15 - 13:30 **Networking lunch**

13:30 - 15:00 **Session 2 – Election Cybersecurity**
Chaired by Dr. Holly-Ann Garnett, Royal Military College of Canada

Dr. Lisa Young, University of Calgary: "Spies, Lies and Election Law: Canada's Policy Response to Cyber-Threats to its Election Campaigns"

Dr. Anna Lennox Esselment, University of Waterloo: "Digital Campaign Threats in Canada: Party Responses in an Age of Disinformation"

Dr. Alexander Essex, University of Western Ontario: "Elephant in the Ballot Box: The Other Cyber Threats to Canada's Democratic Process"

Dr. Laura Stephenson – University of Western Ontario: "On Public Ppinion About Technology and Cyber-security in Elections"

15:00 - 15:30 **Networking break**

15:30 - 17:00 **Session 3 – Innovative Prevention Strategies: The Role of Insurance, Standards and AI**

Dr. Mathieu Charbonneau, Concordia University: "Constructing the Cyber-Insurance Market: Improving Cybersecurity Through Private Insurance?"

Dr. Jason Jaskolka, Carleton University: "Supporting Cyber Security Standards Development with Security Assurance Cases"

Isabelle Rochette, RCMP, and Dr. Helen Tang, Defense Research and Development Canada: "The Criminal Exploitation of Darknet Networks"

17:00 - 19:00 **Networking reception**

Day 2 – Thursday, Oct. 24, 2019

08:00 - 09:00 **Registration and continental breakfast**

09:00 - 10:30 **Session 4 – Updating Canada's Federal Data Protection Legislation for the 21st Century**

Deborah Hurley, Harvard University
Stephanie Perrin, Digital Discretion
Julien Bois, La Cité Collégiale: "Password Best Practices"

10:15 - 10:45 **Networking break**

10:45 - 12:15 **Session 5 – Investigating and Preventing Cybercrime**

Dr. David Hétu, Flare Systems Inc.: "The Low-Tech Communications of High-Tech Financial Fraudsters"

Alexis Dorais-Joncas, ESET: "Rotten Supplies — Supply Chain Attack Case Studies"

Alexandre Beaulieu, RCMP: "Partnership in Fighting Cybercrime"

12:15 - 12:30 **Closing remarks**

12:30 - 14:00 **Networking lunch**

Speakers Biographies

Welcoming address

Benoît Dupont, Professor, Université de Montréal

Benoît Dupont

Dr. Benoît Dupont holds the Canada Research Chair for Security, Identity, and Technology and the Research Chair in Cybercrime Prevention. He is a Professor at the Université de Montréal School of Criminology.

Benoît researches the organizational and technological aspects of changes in the public and private security sectors, including identity theft, bank fraud, information pirating, telecommunications fraud and emerging cyber security policies. Professor Dupont's other research interests include governance of security, community policing and public-private networks of security. He also has an expertise in policing in Quebec and co-authored several books on the subject.

Sonia Chiasson, Associate Professor, Carleton University

Sonia Chiasson

Dr. Sonia Chiasson is the Canada Research Chair in Human Oriented Computer Security and an Associate Professor in the School of Computer Science at Carleton University. Her main research interests are in usable security: the intersection between Human-Computer Interaction (HCI) and computer security. Her current projects focus on user authentication, usable security for mobile devices, and improving end users' mental models of computer security, and collaborative security code reviews. Before moving to Ottawa, she was a full-time instructor in the Department of Computer Science at the University of Saskatchewan and a member of the HCI Lab.

Keynotes

"Interrogating Best Practices in Secure Operations and Development"

Security operations and secure development are critical requirements that receive significant personnel, resources, training and other kinds of attention. As best practices proliferate, there has been little empirical research as to which are most effective and why. In this talk, I will review recent empirical studies that examine in depth the utility of threat modeling, CTF contests as security training exercises and other topics. These studies highlight the benefits of academic-industry collaboration for evaluating and reconsidering best practices.

Michelle Mazurek, Assistant Professor, University of Maryland, College Park

Michelle Mazurek

Michelle Mazurek is an Assistant Professor in the Computer Science Department at the University of Maryland, College Park. Her research aims to understand and improve the human elements of security and privacy-related decision making. Recent projects include examining how and why developers make security and privacy mistakes; evaluating the use of threat-modeling in large-scale organizations; analyzing how users learn about and decide whether to adopt security advice; and contrasting user expectations with app behavior in Android apps.

Her work has recently been recognized with an NSA Best Scientific Cybersecurity Paper Award and a USENIX Security Distinguished Paper Award. She is Program Chair for the Symposium on Usable Privacy and Security (SOUPS) for 2019 and 2020. Mazurek received her PhD in Electrical and Computer Engineering from Carnegie Mellon University in 2014.

Keynotes

"Evidence Based Cybersecurity and its Relevance for Guiding Security Experts', Law Enforcement Agencies' and Policy Makers' Efforts in Cyberspace"

Evidence based cybersecurity is an approach aiming to support security professionals' and policy makers' decision-making processes regarding the deployment of security policies and tools, by calling for rigorous scientific investigations of the effectiveness of these policies and tools in achieving their goals in the wild.

This approach focuses on the human players who use cyberspace for various purposes, and seeks to guide the configuration and design of computer environments which could mitigate the consequences of cybercrime to targets and infrastructures. This talk will present concrete evidence from past and ongoing scientific efforts which the Evidence Based Cybersecurity Research Group in Georgia State University (ebcs.gsu.edu) has initiated, and which are aimed at understanding what works and what doesn't in preventing and mitigating cybercrime. Concrete examples to the relevance of this approach in the context of security experts', law enforcement agencies' and policy makers' efforts in deploying efficient and cost-effective security policies and tools will be provided.

Dr. David Maimon, Associate Professor, Georgia State University

David Maimon

David Maimon is an Associate Professor in the Department of Criminal Justice and Criminology at Georgia State University and the Director of the Evidence Based Cybersecurity Research Group. He has secondary appointment with the Computer Science Department at Georgia State University. He received his PhD in sociology from the Ohio State University in 2009. David's research interests include theories of human behaviors, cyber-enabled and cyber-dependent crimes and experimental research methods. In 2015, he was awarded the Young Scholar Award from the White-Collar Crime Research Consortium of the National White-Collar Crime Center for his cybercrime research. He is also the recipient of the Philip Merrill Presidential Scholars Faculty Mentor Award (from the University of Maryland) and the Best Publication Award in Mental Health (from the American Sociological Association).

His current research focuses on computer hacking and the progression of system trespassing events, computer networks vulnerabilities to cyber attacks and decision-making process in cyber space. He is also conducting research on intellectual property, darknet markets and cyber fraud.

Session 1 – Demand-Driven Innovation in Cyber for Defence & Security

Presentation

The Innovation for Defence, Excellence and Security (IDEaS) program was announced in Canada's new defence policy and commits to $1.6B of investment in innovations for defence and security over the next 20 years. IDEaS is looking for solutions to help resolve defence and security challenges. This informed panel will bring together the stakeholders, innovators and program managers to share their perspectives on the IDEaS program and innovations in Cyber.

Session chaired by Eric Fournier, Director General, Innovation for the Assistant Deputy Minister (Science & Technology)

Eric Fournier

Mr. Fournier is presently the Director General, Innovation for the Assistant Deputy Minister (Science & Technology). He is a Scientific Advisor to the Department of National Defence and to the Canadian Armed Forces.

His role is to ensure that the Canadian Armed Forces / Department of National Defence (CAF/DND) have access to the most cutting-edge solutions for their challenges from Canadian Innovators. Eric began his career with Defence Research & Development Canada (DRDC) as a Defence Scientist in the Flight Mechanics Group of the Precision Weapons Section at the Valcartier laboratory in August 1992. He spent most of his scientific career in that establishment, where he held a number of positions in the weapons field of study.

In May 2006, he was appointed Director for Science & Technology Air, in Ottawa, where he managed the Air Force S&T Program portfolio. He was then appointed Director of Defence Research and Development Canada's Centre for Operational Research and Analysis (CORA), and was responsible for the delivery of a science and technology program in the areas of operational research, strategic analysis, and scientific and technical intelligence. In 2014, Mr. Fournier took up the position of Defence R&D Counsellor at CDLS (London) where he was responsible for liaison in defence science and technology between Canada and the United Kingdom, Germany, the Netherlands, Sweden, Norway and Denmark.

Upon returning to Canada in July 2017, he was appointed DG, Innovation, and also selected to develop and lead the implementation of the Innovation for Defence Excellence and Security (IDEaS) initiative.

Session 1 – Demand-Driven Innovation in Cyber for Defence & Security

Brigadier-General Andrew Jayne, Director General, Cyberspace, Canadian Armed Forces

Andrew Jayne

Brigadier-General Jayne grew up in Bridgewater, Nova Scotia and joined the Canadian Forces in 1987 under the Regular Officer Training Plan. He graduated from the Royal Military College in Kingston, Ontario in 1991 with a Bachelor's in Civil Engineering.

After completing his training as a Military Engineer Officer in Chilliwack, British Columbia he went on to complete Regimental duties with 4 Engineer Support Regiment, 22 Engineer Regiment in the UK, and 1 Combat Engineer Regiment. During this time, he served in various command and staff positions and completed one operational tour in Croatia and two tours in Bosnia.

Over the years he served in staff and training positions with 1 Canadian Mechanized Brigade Group, the Canadian Forces School of Military Engineering and within the Chief of Force Development. In 2006 he attended the Canadian Forces College in Toronto, Ontario, graduating with a Master's in Defence Studies. In 2008, Brigadier-General Jayne deployed to Afghanistan as the Chief Engineer of Regional Command South and then became the 21st Commandant of the Canadian Forces School of Military Engineering in 2009. Following his time in command, he went to Ottawa to work on the Army Staff in various positions.

Promoted to Colonel in December 2012, he took over the position of Director Land Requirements. He completed the National Securities Program at the Canadian Forces College in 2015 and then returned to the position of Director Land Requirements before being appointed Base Commander of CFB Kingston in October 2016. He was promoted to his current rank in November 2017 and deployed as the Commander, Joint Task Force Iraq on December 16, 2017. Brigadier-General Jayne is currently serving as Director General, Cyberspace.

Session 1 – Demand-Driven Innovation in Cyber for Defence & Security

Dr. Helen Tang, Senior Defence Scientist and Portfolio Manager, IDEaS, Defence R&D Canada (DRDC)

Helen Tang

Dr. Helen Tang is a senior Defence Scientist and Portfolio Manager with Innovation for Defence Excellence and Security (IDEaS), Defence R&D Canada Ottawa.

She received her PhD in Electrical Engineering from Carleton University in 2005. From 1999 to 2005, she worked in several R&D organizations in Canada and USA including Alcatel-Lucent, Mentor Graphics and Communications Research Center Canada. She joined DRDC in 2005 to conduct cyber security research. She received the Outstanding Achievement Award at DRDC-CSS in 2017, and at DRDC-Ottawa in 2009 and 2016. She has published over 100 journal and conference papers related to cyber security and communications networks.

She is a senior member of the IEEE and she received the Best Paper Award at IEEE/IFIP TrustCom 2009 and the Outstanding Leadership Award at IEEE/IFIP TrustCom 2010.

She has been an Adjunct Professor at the Department of System and Computer Engineering of Carleton University since 2009, where she is the supervisor of many graduate students, conducting research on cyber security for critical infrastructure.

Session 1 – Demand-Driven Innovation in Cyber for Defence & Security

Allen Dillon, Sappers Lab, COO, root9B

Allen Dillon

Allen Dillon (Al) is well known in the security community in Canada, as both a former military officer of the Canadian Forces and a seasoned hi-tech innovator in industry. Al's roots in technology and cybersecurity started in the military. He is a 4th generation decorated soldier with entrepreneurial spirit. Al's experience includes the development of advanced electronic warfare assets, communications intercept, intelligence systems and cyberwarfare capabilities for use on the battlefield and in the global security community.

In industry, Al's contribution to innovation for the defence, security and aerospace industries earned him the 2013 CDR Defence and Security Executive of the Year in Canada. Notably in 2015, he led a team cooperating with a national security agency that exposed international media fraud perpetrated by organized criminals who leveraged social media and mobile systems to steal an estimated $350M annually from global advertisers. Al is also the Founder and visionary of CyberNB, the only Canadian Provincial Special Operating Agency dedicated to cybersecurity protection frameworks in Canada. He is currently the COO of root9B Canada and his team is actively engaged in several programs in the defence of Canada and the United States.

Session 2 – Election Cybersecurity

Presentation

Cybersecurity was undoubtedly on the public radar during the 2019 Canadian federal election, particularly as evidence of cybersecurity breaches, fake-news and disinformation campaigns in other countries have made the news in recent years. This roundtable will bring together academics who have researched the 2019 Canadian federal election to provide immediate reactions on cybersecurity issues that emerged during the 2019 campaign.

Included are participants working on research considering issues including political parties' use of new medias, public opinion on election technology, policy solutions to major threats and other insights into other cyber-issues during the campaign.

Session chaired by Dr. Holly Ann Garnett, Assistant Professor, Royal Military College of Canada

Holly Ann Garrnett

Holly Ann Garnett is an Assistant Professor of political science at the Royal Military College of Canada in Kingston, Ontario. Her research examines how electoral integrity can be strengthened throughout the electoral cycle, including the role of election management bodies, electoral assistance, voter registration, convenience voting measures, election technologies, civic literacy and campaign finance.

She is a co-convener of the Electoral Management Network and contributes to the Electoral Integrity Project. Holly Ann was an Endeavour Research Fellow at The Australian National University (2017), a Visiting Fellow at the Åbo Akademi, Finland (2017), a Visiting Researcher at the University of Sydney (2014) and a Killam Fellow at Cornell University (2009).

Session 2 – Election Cybersecurity

"Spies, Lies and Election Law: Canada's Policy Response to Cyber-Threats to its Election Campaigns"

Compelling evidence of foreign cyber-interference in the 2016 US Presidential election campaign has prompted a robust policy response in Canada at the federal level. This presentation will review legislative changes, the critical incident contingency plan, and initiatives to promote voters' resiliency, and offer an early evaluation of their implementation in the 2019 campaign.

Lisa Young, Professor, University of Calgary

Lisa Young

Lisa Young is Professor in the School of Public Policy and Department of Political Science at the University of Calgary. Her research has focused on election finance law, political party organization and women's involvement in Canadian politics. She is author of *Feminists and Party Politics*, co-author of *Rebuilding Canadian Party Politics* and *Advocacy Groups* and co-editor of *Money, Politics and Democracy: Canada's Party Finance Reforms*.

"Digital Campaign Threats in Canada: Party Responses in an Age of Disinformation"

Threats to parties, leaders, and candidates via digital platforms are on the rise. Disinformation about leaders and parties can be spread through bots on Twitter and Facebook, and they can take the shape of news articles, #hashtags that trend, or altered videos. For example, the fake ads purporting NDP Leader Jagmeet Singh owned a multimillion-dollar mansion during the February 2019 by-election in Burnaby is an instance of disinformation infecting campaigns in Canada. Interference can also occur through accessing information about voters stored in party databases or hacking into a campaign's e-mail server. Disinformation and misinformation undermine meaningful deliberation during the most important exercise in a democracy – an election. Notably, Canada's federal election will not be immune to these sorts of attempts to destabilize the integrity of its electoral system.

Session 2 – Election Cybersecurity

This talk will report on results from examination of interference using disinformation through digital platforms. Its methods will rely on media monitoring (both traditional media and social media) and interviews with party strategists.

The aim is to detail the main instances of disinformation and other digital threats, and analyze how each of the major parties responded to combat them (such as through a party news release, a Twitter counter-attack, a party ad, employing social media influencers, discussing the incident with journalists, and so on). The analysis will include an assessment of the effectiveness of these party / leader responses and how these methods might be improved for future elections.

Anna Lennox Esselment, Associate Professor, University of Waterloo

Anna Lennox Esselment

Anna Lennox Esselment is Associate Professor in the Department of Political Science at the University of Waterloo. She is co-editor of *Permanent Campaigning in Canada* (UBC Press, 2017) and publishes in the fields of campaigns and elections, political marketing, political parties, partisanship, and federalism.

"Elephant in the Ballot Box: The Other Cyber Threats to Canada's Democratic Process"

The Communication Security Establishments's *Cyber Threats to Canada's Democratic Process* has been an important and influential series of reports providing the public with an invaluable snapshot of challenges facing our elections in the digital age. But for an agency with a predominately outward view toward foreign intelligence, the reports are also noteworthy for the threats they do not describe. For a country that is quickly becoming a world leader in the use of election technology, we must also take an inward-facing view to acknowledge the degree of privileged access to highly sensitive democratic data this technology provides. Drawing on recent national and international events and observations, this talk will explore some of the other threats to Canada's democratic process.

Session 2 – Election Cybersecurity

Aleksander Essex, Associate Professor, University of Western Ontario

Aleksander Essex

Aleksander Essex is an Associate Professor of software engineering at Western University. His research specializes in cybersecurity, cryptography and has focused on electronic and online voting to develop technical methods for evidence-based elections. He has presented his research findings at the federal, provincial, territorial and municipal levels and has made over 80 television, radio and print appearances speaking on the topic of election security.

He is a member of the Election Verification Network, a U.S. based professional society of election experts and is a licensed professional engineer (P.Eng.) in Ontario.

"On Public Opinion About Technology and Cyber-Security in Elections"

Dr. Laura Stephenson, Professor, University of Western Ontario

Laura Stephenson

Laura Stephenson is a Professor of political science at the University of Western Ontario. She co-directs the Consortium on Electoral Democracy (C-Dem). She specializes in the study of political behaviour, both Canadian and comparative. Her research is focused on understanding how institutions and context influence attitudes, electoral preferences and engagement with politics. She is one of the investigators of the 2019 Canadian Election Study and part of the Canadian Municipal Election Study team.

Session 3 – Innovative Prevention Strategies: The Role of Insurance, Standards and AI

"Improving Cybersecurity Through Private Insurance?"

While dealing with interconnected and global risks, the cyber-insurance market is intensely growing. This market is a creature of privacy and data security regulations, and mandatory breach notifications have shaped its business model. Market stakeholders suggest that cyber-insurance provides incentives and resources to insured organizations for improving cybersecurity.

This presentation seeks to empirically test this claim, using academic and grey literatures, official statistics and ethnographic interviews. First, it describes cyber-insurance in the US and Canada, showing that the market faces major obstacles. Second, it presents the benefits and limits of private insurance as a cybersecurity policy instrument. Keeping in mind the market's lack of maturity, this presentation concludes that cyber-insurance generates massive uncertainties, risks, increasing cyber-risks, and could even contribute to systemic risk.

Mathieu Charbonneau, Postdoctoral Fellow, Concordia University

Mathieu Charbonneau

Mathieu Charbonneau is Postdoctoral Fellow at Concordia University's Karl Polanyi Institute of Political Economy (Montreal, Canada), and holds a joint PhD from Carleton University (Ottawa, Canada) and Université Paris-Sorbonne (Paris IV, France). His research focus, from an institutional economic sociology and public policy perspective, on climate change and the insurance industry, the cyber-insurance market, and prescription drug insurance and high-cost specialty drugs.

Session 3 – Innovative Prevention Strategies: The Role of Insurance, Standards and AI

"Supporting Cyber Security Standards Development with Security Assurance Cases"

The existence of well-defined or documented sets of standards, guidelines, or best practices for developing secure systems is limited. Those that are available often lack focus and specificity, making compliance either too difficult or too easy. As a result, many practitioners are never quite sure what needs to be done to demonstrate that they have taken appropriate measures to adequately secure the systems they are developing. Without readily available guidance documents, assuring the security and trustworthiness of critical systems will remain challenging.

As demonstrated by both Canada and the United States in their recent national cyber strategies, further research efforts in developing more rigorous standards, guidelines and best practices is needed. In particular, better guidance for practitioners to incorporate suitable security measures at all stages of system development, and to generate and gather the evidence needed to support assurance claims can help to improve system security.

In this presentation, I will discuss the need for more rigorous, outcome-oriented cyber security standards, guidelines and best practices based on sound technological principles. I will present recent research efforts in the development of security assurance cases and describe the role they can have in the understanding and development of such cyber security standards.

Jason Jaskolka, Assistant Professor, Carleton University

Jason Jaskolka

Jason Jaskolka is an Assistant Professor in the Department of Systems and Computer Engineering and the Director of the Cyber Security Evaluation and Assurance (CyberSEA) Research Lab at Carleton University, in Ottawa, Canada. He received his PhD in Software Engineering in 2015 from McMaster University (Hamilton, Canada). He is a licensed Professional Engineer in Ontario.

His research interests include cyber security evaluation and assurance, threat modeling, security-by-design, and formal methods and algebraic approaches for software and security engineering. He is interested in applying his research to critical infrastructures, cyber-physical and distributed systems, and the Internet of Things (IoT).

Session 3 – Innovative Prevention Strategies: The Role of Insurance, Standards and AI

"The Criminal Exploitation of Darknet Networks"

A darknet is a purposefully hidden network that is accessible with specific software or protocols and that is meant to provide its users with anonymity. The criminal exploitation of darknet networks is a major obstacle to digital evidence and allows countless criminals to conduct their illicit activities without being detected by law enforcement agencies. Darknet technologies facilitate criminality and provide offenders with a platform to acquire and supply illicit goods and services. Europol, who dedicated a team to tackle darknets' criminal activities, stated in 2018 that many of these illicit commodities, such as cybercrime toolkits or fake documents, are enablers for further criminality.

This session will give an overview of what kind of crimes are facilitated by this technology, of different darknets used by criminals such as Tor, I2P and Zeronet, their technical architecture and how they are used to avoid identification. We will discuss how public safety agencies could address these threats while acknowledging that these networks can provide legitimate users with freedom and personal privacy.

Isabelle Rochette, Research and Development Project Manager, RCMP

Isabelle Rochette

Isabelle Rochette has been a civilian member of the Royal Canadian Mounted Police (RCMP) since 2000, where she is a Research and Development Project Manager for the Technical Operations. Her principal interests and research priorities are data science and cybersecurity solutions for policing operations. She also has extensive experience consulting on investigations as a technical advisor.

Dr. Helen Tang, Senior Defence Scientist and Portfolio Manager, IDEaS, Defence R&D Canada (DRDC)

(See Helen Tang's biography on page 12.)

Session 4 – Updating Canada's Federal Data Protection Legislation for the 21st Century

The modern era of privacy and personal data protection corresponds with the rise of computing, leading to today's ubiquitous information environment and the massive collection and use of personal data. The current Information Age is characterized by dynamic shifts in privacy and personal data protection. This rapid evolution occurs, however, on a solid foundation of fair information practices. This panel explores updating Canada's federal data protection legislation to meet the demands of the 21st century. It will also address Canada's important international leadership roles in this domain.

Deborah Hurley, Fellow, Harvard University

Deborah Hurley

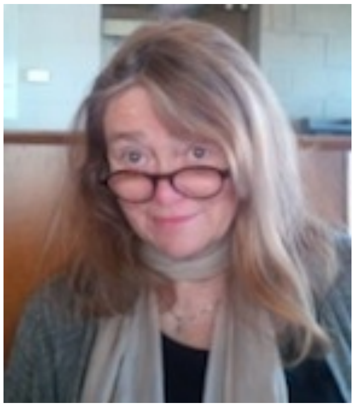
Deborah Hurley is Principal of the science and technology policy consulting firm she founded in 1996. She is: Fellow, Institute for Quantitative Social Science, and Global Innovation Policy Fellow, Technology and Entrepreneurship Center at Harvard (TECH), both at Harvard University; Associate Faculty Director, Data Privacy, and Adjunct Professor of the Practice of Computer Science, Brown University; Adjunct Faculty, Information Ethics and Privacy Law, Boston College; Senior ICT Expert, Pacific Region Infrastructure Facility, Sydney, Australia; and Arbitrator, US-EU Privacy Shield.

At the Organization for Economic Cooperation and Development (OECD) in Paris, France, Hurley identified emerging technological, economic, social, and legal issues related to science, technology, and innovation policy, information and communications technologies, biotechnology, environmental and energy technologies, privacy and personal data protection, cybersecurity, nanotechnology, encryption, and other advanced technology fields. She has been a Fulbright scholar in Korea.

Hurley has received the Namur Award of the International Federation for Information Processing in recognition of outstanding contributions, with international impact, to awareness of social implications of information technology.

Session 4 – Updating Canada's Federal Data Protection Legislation for the 21st Century

Stephanie Perrin, President, Digital Discretion



Stephanie Perrin

Stephanie Perrin established Digital Discretion in 2003, producing reports on matters ranging from identity theft to RFID, conducting risk assessments and training sessions, and developing privacy impact assessments and audits.

She has worked for most of her career in information and privacy issues, having started in 1984 as one of the first federal Access to Information and Privacy Coordinators at the then Department of Communications. In 2005, she returned to the federal government as Director of Policy and Research at the Office of the Privacy Commissioner, before moving to Service Canada as a Director of Risk Management Policy. Now retired from the Canadian public service, she has re-launched Digital Discretion as a top-tier privacy and transparency consulting firm.

"Password Best Practices"

A quick reminder on current best practices for password selection and password expiry. Discussion on how Cloud and blockchain are evolving the password cracking threat. Existing solutions to ensure password randomness and uniqueness.

Julien Bois, La Cité Collégiale (P.Eng., MBA, CISSP, CISA)

Julien Bois

Bois is a cybersecurity professional specializing in Identity and Access Management architecture. He has worked for more than 12 years for large organizations in France, India, Quebec and Ontario, such as Société Générale, BNP Paribas, Mouvement des Caisses Desjardins, Laurentian Bank, the Université de Montréal, the Canadian Revenue Agency, Shared Services Canada and the Bank of Canada. Registered as an engineer in Ontario (PEO) and France (IESF), he also holds specialized certifications such as CISSP-ISSAP, CISA, CISM, CEH, CASP, AWS Certified Solutions Architect and PMP. He teaches ethics and the management of security systems in the cybersecurity program at La Cité Collégiale.

Session 5 – Investigating and Preventing Cybercrime

“The Low-Tech Communications of High-Tech Financial Fraudsters”

Much case has been made of the use of sophisticated anonymity tools by financial fraudsters that hack financial institutions and steal personal and financial information. Our past research has shown that these technologies were used to protect the fraudsters’ privacy and to facilitate their attacks against financial institutions. Our latest interactions and analysis of the cybercrime underground has shown however that many financial fraudsters are still using low-tech communications methods to connect with each other.

The aim of this presentation is to analyze how low-tech communication tools such as ICQ are still being used by Canadian financial fraudsters. We demonstrate that thousands of actors appear to use daily the low-tech communication tools even though a handful of fraudsters appear to control the sale of personal and financial information. We also demonstrate the type of intelligence that can be gathered on these communication tools and that fraudsters go as far as posting videos of themselves pushing the sale of their illicit services. This presentation will highlight the need to have a holistic approach when analyzing financial fraud in Canada and that different sources of open data complement each other to enhance our understanding of financial fraud.

David Hétu, Chief Scientist, Flare Systems Inc.

David Hétu

David Hétu is Chief Scientist at Flare Systems Inc. He has a PhD in Criminology with a specialization in the study of illicit markets on the Internet and the darknet. David has developed massive data collection tools on online illicit activities and threat actors as well as cryptocurrency flow analysis. His research has been published in major scientific journals and has helped to understand the social structure of delinquent communities on the Internet as well as the performance of offenders.

Session 5 – Investigating and Preventing Cybercrime

"Rotten Supplies – Supply Chain Attack Case Studies"

We have seen an increase in supply chain attacks in the past few years. Some of these attacks have something in common: they involve a compromised Linux server to distribute malware or act as C&C server. This presentation will use real world case studies: the Transmission BitTorrent client distributing OSX/Keydnap; the M.E. Doc compromise responsible for the famous Petya outbreak; the VestaCP administration panel used to distribute Linux/ChachaDDoS; and the Winnti Group, famous for attacking the gaming industry and high profile targets such as Asus and CCleaner to create botnets of millions of victims. In some of these cases, our team was in the field and was able to witness how attackers compromise the infrastructure of the suppliers to inject malware into the build system and infect all their users when they install or update their software.

We will demonstrate that these attacks are mostly performed manually, with a mix of of-the-shelf and custom tools, both on Linux and Windows. We will display the different mitigation and remediation techniques to prevent Linux servers from becoming the next low hanging fruit. Finally, we will discuss the trust problem when vendors push automatic updates and how it is hard, if not impossible, to inspect all code contained in updates.

Alexis Dorais-Joncas, Head of Montreal Branch R&D, ESET

Alexis Dorais-Joncas

Alexis Dorais-Joncas started his career in cybersecurity in 2010 when he was hired by ESET as a malware researcher. In 2015, Alexis was appointed Head of ESET's R&D branch office located in Montreal, where he and his team focus on cutting edge malware research, network security and targeted attack tracking. Their goal: shed light on the latest trends and developments in the malware ecosystem and implement efficient and innovative countermeasures to allow ESET customers to be safe online.

Session 5 – Investigating and Preventing Cybercrime

"Partnership in Fighting Cybercrime"

Cybercrime knows no border and traditional techniques need to evolve in order to succeed in fighting this problem. This includes looking at how we traditionally investigate crimes and increasing everyone's capacity through partnerships whether domestic, international, public, private and / or academic. Partnerships and information sharing will be discussed through concrete examples and considerations will be highlighted.

S/Sgt. Alexandre Beaulieu, NCO/ic RCMP National Division Cybercrime Investigative Team

Alexandre Beaulieu

S/Sgt. Alexandre Beaulieu joined the RCMP in 2003 and began his career in New Brunswick, first working general duty and eventually as an investigator within federal policing. In 2009, S/Sgt. Beaulieu transferred to Ottawa where he worked with Legal Applications Support Unit (within the Organized Crime Branch and Covert Operations Branch) and Sensitive and International Investigations.

Since December 2016, S/Sgt. Beaulieu has been with the National Division Cybercrime Investigative Team, responsible for the investigation of cybercrime offences which have an impact on the Government of Canada, critical infrastructure or important Canadian institutions. These are often complex and multifaceted investigations which are international in scope and involve the use of advanced investigative techniques.

SERENE-RISC Poster Competition

During the Workshop, SERENE-RISC will provide graduate students with an opportunity to present recent or research results as well as innovative work-in-progress enquiries.

The aim is to enable graduate students to meet one another and to network and engage with SERENE-RISC researchers as well as government and industry representatives and to receive feedback about their work. A $500 scholarship will be awarded to the best academic poster and a prize of $1000 will be presented to the SERENE-RISC Cyberstat Challenge winning team, as voted by workshop attendees.

The Cyberstat Challenge seeks to popularize cybersecurity and cybercrime statistics through inventive research and informative posters. Students have thoroughly examined the data from Statistics Canada's 2017 Canadian Survey of Cyber Security and Cybercrime and derived useful awareness messages and lessons to better align recent evidence and statistics with best practices for business. Use the single ballot available in your package to vote for your favorite academic and Cyberstat Challenge posters.

Academic Poster Participants

"A Mutation Framework for Evaluating Security Analysis tools in IoT Applications"
Sajeda Parveen & Manar H. Alalfi, Ryerson University

"Analyzing Adversarial Resilience of Deep Learning Models in IoT Network Security"
Kunle Obitoye, Carleton University

"Automated Identification of Over-Privileged SmartThings Apps"
Atheer Abu Zaid, Manar Alalfi & Ali Miri, Ryerson University

"Cyber Electoral Interference in the Five Eyes Countries: Threats and Solutions"
Owen Saunders, Queen's University

"Giving Up Privacy for Fear of Missing Out"
Fiona Westin & Sonia Chiasson, Carleton University

Academic Poster Participants

“On the Real-Time Detection of Covert Channels”
Thomas A.V. Sattolo & Jason Jaskolka, Carleton University

“Privacy Perceptions of At-Home DNA Testing”
Khadija Baig & Sonia Chiasson, Carleton University

“Reinforcement Learning Based Penetration Testing of Microgrid Control Algorithms”
Christopher Neal & José Fernandez, Polytechnique Montréal

“Taint-Things: An Automated Approach for Privacy Leakage Identification in IoT Apps”
Bara Nazzal, Florian Schmeidl & Manar Alalfi, Queen’s University

Cyberstat Challenge Participants

Emmanuel Ayeleso & Parsa Vafaie, PhD in Computer Science, University of Ottawa

Farhan Babar, Vipul Malhotra, M.Sc. in Computer Science, & Mahreen Nasir, PhD in Computer Science, University of Windsor

Loreena Bertoux & Adeline Veyrinas, MA in Criminology, Université de Montréal

Marilyne Bernier & Alexa Charles, MA in Criminology, Université de Montréal

Caroline Dakouré & Camille Felx-Leduc, Master of Computer Science, Université de Montréal

Alex Dos Santos, MS in Governance, Audit and IT Security, Université de Sherbrooke

David Brisebois & Uyên Tang, MA in Criminology, Université de Montréal

Traian Toma, MA in Criminology, Université de Montréal, & Fiona Westin, Master’s in Human-Computer Interaction, Carleton University

SERENE-RISC Partners

BANK OF CANADA
BANQUE DU CANADA

BANQUE
NATIONALE

CAN
SEBP

CGI

Canada
CNRC·NRC

Cilex
CATALYSEUR D'INNOVATION
INNOVATION CATALYST

Cyber Defence Corporation
YOUR SENTINEL INSIDE

eset
ENJOY SAFER TECHNOLOGY™

i am
AUTHENTICATIONS INC.

MAINTIENS LE DROIT
ROYAL CANADIAN MOUNTED POLICE

GoSecure
POWERED BY COUNTERTACK

HEXIGENT
CONSULTING

IN-SEC-M
INNOVATION | SÉCURITÉ | MARCHÉS

nurun
services conseils

ISACA®
Fiabilisez, optimisez et rentabilisez les systèmes d'information
Section de Montréal

ISACA®
Trust in, and value from, information systems
Ottawa Valley Chapter

NCE RCE
Networks of Centres of Excellence of Canada | Réseaux de centres d'excellence du Canada

SÛRETÉ DU QUÉBEC
POLICE
SERVICE INTÉGRITÉ JUSTICE

DRDC | RDDC
technology science technologie

RHEA
GROUP

RISIUQ
Regroupement des Intervenants en Sécurité Informatique des Universités Québécoises

Symantec.

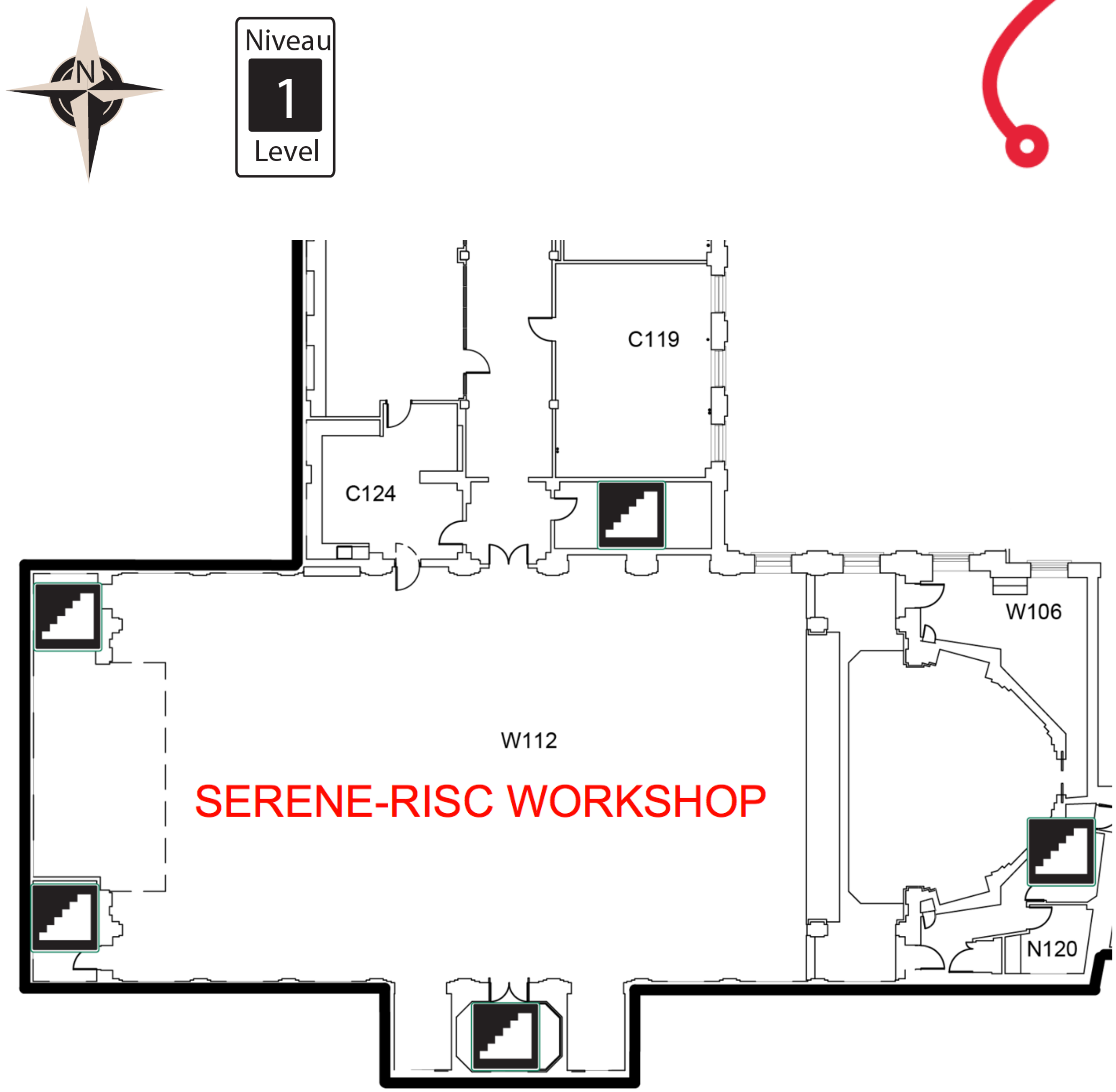
Public Safety Canada
Sécurité publique Canada

Someone
social media education every day

Université de Montréal

Workshop Floor Plan

Room W112 – Tabaret Hall



Men's washrooms

Women's washrooms

Washrooms can be found on Level 1 on the North wing (near Room L141) and on the South wing on Level 2, in Section C, just above Room W112.

… and on the web at: SERENE-RISC.CA KONNECT.SERENE-RISC.CA