The Readiness and Resilience Conference marked a major effort to convene a high-level forum for discussion on key national security issues affecting Canada and the world. The conference was attended by more than 400 registrants and featured presentations by some 80 distinguished experts and practitioners.

The conference executive organizing committee consisted of:

• Serge Blais, Director, uOttawa Centre for Continuing Education/Security and Policy Institute
• Alan Jones, Executive Advisor, uOttawa Centre for Continuing Education
• Tim O’Neil, Director, Oldcastle Security Consulting
• Mike Martin, President, Valley Associates
• John Patterson

The conference was made possible with valuable assistance from:

• Paul Goldenberg, Strategic Advisor
• Marie Dickinson, Event Management
• Paul Grenon, Marketing and Communications
• Jessica Lackie, Materials and Logistics
• Ilya Berlin, International Outreach and Logistics

Given the scale and diversity of the conference discussions, this report will not attempt to capture the details but will endeavor to report out on some of the highlights of the conference presentations and panel discussions. The Security and Policy Institute would be happy to provide a more in-depth after-action report to any client who has need of such a product.

The report editor, Professor Wesley Wark, wishes to thank the dedicated team of rapporteurs whose detailed notes provide the basis for this overview. The rapporteurs numbered nine in total; all are students at the University of Ottawa’s Law Faculty.

The report follows the basic structure of the conference by providing summaries of the morning plenary sessions for the two days and summaries of the many panels that were convened on critical issues.

Remarks by plenary speakers are attributed but the discussions held in the panel sessions were convened under the Chatham House rule and so we do not attribute specific remarks to named individual presenters.
EXECUTIVE SUMMARY

The Security and Policy Institute of Professional Development (SPI) at the University of Ottawa hosted the 2018 conference Readiness and Resilience in the Age of Disruption to provide a high-level forum for business leaders, law enforcement, public and private security practitioners.

The conference focused on disruptive forces in the modern security environment by considering two key phenomena: technology as an enabler of disruption; and the organizational basis for dealing with disruptive threats. Discussion of these phenomena was advanced through both plenary addresses, often focused on the strategic level and through a rich multiplicity of panel discussions which enabled participants to engage with specific issues in more detail.

Technology has long been an enabler of intelligence capabilities for states in the modern era and an enabler of conventional military force. What is new about the 21st century is that while technology continues to enable responsive capacities for intelligence and security, it has also enabled a wide range of new and fast-evolving threats and new threat actors, often at the non-state level. The speed at which technology has enabled threat actors challenges the capacity of technological applications designed to achieve security. This can be witnessed especially in the domain of cyber security, which was a persistent focus for attention throughout the conference. The new technological applications around drones (UAVs) and the systems to operate them (Unmanned Aerial Systems, UAS), like the cyber domain, offer visions of increased threats, but great potential benefits.

How we organize to meet disruptive threats was the second main theme of the conference. Organizing to meet threats can range from considering the health, integrity, capacity and resilience of an entire polity, to the specifics of managing security for a major sporting event or soft target venue. Organizational issues range across the spectrum from developing security capabilities and plans to considering best practices for mitigation and response to threats. In discussing these issues considerable emphasis was given to being able to move from a global to a local focus, and in particular to consider community security needs, vulnerabilities and the best ways to engage with communities that might be targeted or affected. Greater public awareness and education about disruptive threats, especially in regards to cyber security, new technologies coming on line (e.g., drones), and persistence threats such as terrorism, was widely discussed.

No conference can offer guaranteed solutions to problems of the enormity discussed in the 2018 conference. The Ottawa conference contributed to an ongoing discussion about disruptive threats and the best ways to meet them, by offering innovative thinking and creating new networks for cooperation to meet these challenges.
DAY ONE, FEBRUARY 27, 2018

The first day of the conference, February 27, featured a welcome by the President and Vice-Chancellor of the University of Ottawa, Jacques Frémont, as well as several plenary key note addresses during the morning. The afternoon of February 27 was given over to panel discussions on Cyber Crime; Terrorism and Counter-Terrorism, The Threat Posed to Soft Targets; Cyber Defence in an Age of New Technologies; and Drones.

Mr. Jacques Frémont, the University of Ottawa President, welcomed participants to the conference and extolled its value as a place to foster an important dialogue on national security issues, to share best practices and to offer insights. He was emphatic in reminding the audience that issues of security and of human rights are intertwined. Without security, as he said, there can be no human rights. President Frémont said that he believed the University of Ottawa and the university community in general had an important role to play in fostering what he called “security literacy,” among students, policy makers, industry stakeholders, and the general public. The Universities need to play a role in understanding the security challenges we face as a society both today and in the future.

Ray Boisvert, the provincial security adviser to the province of Ontario, and a former senior CSIS official, provided an opening tour d’horizon on the conference themes of the age of disruption, of resilience and of readiness. The threat environment we face is one marked by a rapid pace of change and a lack of certainty over the principles and institutional actors that are designed to meet the security challenges we face. He argued that terrorism remains an important threat but that the public discussion and understanding needs to be considerably broadened to embrace other threats from state actors such as a rising China and an aggressive Russia as well as the disruptive influences of economic change, technological change, and changes to the informational universe in which we live.

Mr. Boisvert emphasized the need to ensure we have the best possible situational awareness of the threat environment so that we can best manage its consequences.

The CSIS Director, David Vigneault, gave a key note address to the audience on the topic of the “Security Challenges for the 21st Century.” Appointed to his post in the summer of 2017, this was Mr. Vigneault’s first opportunity to deliver a public presentation.

The CSIS Director began by telling the audience that he has long believed that Canada needs a more mature public discussion about national security and intelligence, and believed the conference could make a contribution to that end. He stressed that as the security environment has changed, so has CSIS. One of those changes has been to require CSIS to have a more global footprint, as evidenced by its operations in Afghanistan after 9/11. Alongside that global presence CSIS has had to engage in a shift from its historic focus on counter-intelligence to one more centred on counter-terrorism, even while the nature of the terrorism threat itself rapidly evolved.

Director Vigneault described the moment in history that we now live in as “unique and ominous.” CSIS has to confront the threat of returned foreign fighters, even if overseas terror conflict zones have not yet produced a sizeable number of returnees to Canada. Counter-terrorism is aimed at prevention but prevention has grown more challenging as the nature of terrorist attacks has changed and as the time lines around radicalization to violence have speeded up under the influence of social media messaging. One of the tools available to CSIS is a significant research capacity to try to make sense of the threat landscape and aid in prevention. Director Vigneault stated that “the analytical or research side of our business has become more important than ever.”
The CSIS Director also stressed that while terrorism is the most immediate threat to the public safety of Canadians, there are a host of other threats that the Service must be alert to. These include espionage, and especially economic espionage, the cyber threat, foreign influence activities designed to interfere in our democratic institutions, and international insecurity. In dealing with international issues CSIS can use its Section 16 powers in the CSIS act to collect foreign intelligence in Canada.

David Vigneault concluded by making two points. One was that he was determined to ensure that CSIS pursued “mission excellence.” The other was that he recognized that the achievement of mission excellence depended on sustaining public trust. “If we don’t have public confidence, then we cannot fulfill our mandate.”

John Brennan, the former CIA Director under President Obama and, before his retirement, a long-serving career CIA officer with special expertise in the Middle East, delivered a lunchtime key note address that touched on some of the themes mentioned by Director Vigneault. Mr. Brennan gave the audience his vision of four core challenges for security. These challenges include globalization and the management of its unequal effects; governance problems, themselves sparked by globalization, linking an inept, incompetent and corrupt handling of globalization to the rise of authoritarian regimes attempting to lord power over disaffected populations; the changing dynamics of international relations including the current US retreat from a global leadership role; and the omnipresent problem of cyber security. He urged all stakeholders to “keep ringing the bell” on cyber security issues.

In the Q and A session that followed his remarks, Director Brennan gave a perhaps surprising answer to a question about existential threats. The threat he pointed to was deep political partisanship in the US which was crippling the US’s ability to provide leadership and engage effective national security. He did offer an optimistic note about the future, suggesting that the US was a very resilient society, with strong institutions, that would be able to move forward eventually. He also used an intriguing metaphor about recognizing threats, arguing that you needed to keep your eye on both the “wolves” nearest the door and those “down the street and in the neighbourhood.” North Korea was offered as an example of a wolf down the street whose threat was not seen clearly until late in the day. But he was also concerned about cyber security not been fully understood, particularly in the context of technological developments that might thwart the ability to deliver security.

Paul Goldenberg and John Farmer, in their morning plenary presentations, shared a common theme around the need to have a local focus and understanding in dealing with global threats. This is found to be particularly true in dealing with all types of politically and religiously motivated terrorism, which can tear communities, and even wider societies, apart should they instill a culture of fear. Democratic institutions themselves are under stress. Mr. Goldenberg concluded his remarks by stating that “2018 is all about how we engage our communities.”

Professor Farmer, who served as a senior counsel with the groundbreaking 9/11 Commission in the United States, and who wrote a book about his experiences on the Commission, framed some of his remarks around the theme of connecting global events and local practices in security. This connectivity has been the subject of study at the Rutgers University Centre on Community Violence and Resilience. He believes there is an important role for academia in helping governments identify new risks and bridge cognitive dissonance in dealing with a complex and fast changing threat environment. Professor Farmer stressed the need for liberal democracies to “look in the mirror” and defend basic values, otherwise, he said, we can be “subverted digitally and ideologically.” But Professor Farmer also emphasized the need to understand and engage with communities that might be under threat. Best practices for community engagement are urgently required.

The final morning plenary involved a presentation by Colonel (US, retd.) Greg Gardner. Colonel Gardner provided a detailed and valuable look at the evolution of US cyber security strategy, from the 2014 Commission on Cyber Security to President Trump’s May 2017 Executive Order, “Strengthening Cyber Security of Federal Networks and critical infrastructure.” In reviewing developments in US cyber policy he argued for a balanced approach and an understanding that tradeoffs were inevitable. It will be important to reconcile security with innovation, to prevent either from suffering inordinately. The keys are resilience, economic prosperity and connectedness, into which the cyber security piece must be made to fit.
DAY ONE, PANEL SUMMARY

Cyber Crime, Moderated by Justin Fogarty, Chairman of Regent Law

The panel featured a range of speakers from the private sector and law enforcement. Key points of discussion included the challenge of keeping up with technological change and understanding the impact of globalization. Social media was addressed as an enabler of cyber crime. Leadership and governance in organisations are important to ensure strong incidence management. The potential impacts of AI in offense and defence with regard to cyber crime was raised. Several of the panelists agreed that the role of the individual in dealing with cyber crime was important and that there were requirements for better public education, better citizen engagement and better government policy.

The Canadian Government’s Budget 2018 document has unveiled plans for increased spending to combat cyber crime and new organisational nodes to enhance cyber security and public-private partnerships.

Terrorism and Counter-Terrorism, moderated by Assistant Commissioner James Malizia, RCMP

The panel was very international in composition, featuring speakers from Belgium, the UK, Turkey, and the US. Several of the speakers were law enforcement officials with long experience.

One panelist addressed the importance of understanding the terrorist ecosystem, both in its internal dynamics within communities and in outside influences. Another with experience of counter-terrorist policing in a large urban environment talked about the significance of resources and innovative ways to develop deterrents. Police forces must have a good strategic response plan to maximize interventions and responses to terrorist incidents. Many of the panelists agreed on the fact that counter-terrorism depends on affected communities who must be supported and protected.

The role of data analytics in counter-terrorism was discussed, with one presenter arguing that the future of counter-terrorism was ‘left of bang’, involving better data mining and predictive analysis that could feed intelligence-led preventive policing.

The New Soft Targets: The Threat in Perspective, moderated by Paul Goldenberg

The panel consisted of senior practitioners, many with law enforcement experience.

Soft targets were discussed as universally challenging, requiring good strategic planning but also the ability to innovate tactically and quickly in response to the unforeseen. The threat is evolving but so are tools to deal with it, including drone mitigation. Soft target protection is costly and requires public buy-in. The public also has an important role to play as information providers—“see something, say something.” There are tradeoffs between security and public access and use of spaces that might present themselves as soft targets. One presenter highlighted the problem of the insider threat in regard to infrastructure protection. Individual security clearance procedures are important.
Cyber Defence in an Era with Artificial Intelligence, Quantum Computing and Beyond, moderated by Dr. Michelle Mosca

The panel discussed the technological changes that will be wrought by the advent of quantum computing and AI.

While quantum computing may have huge impacts, what is unusual in the cyber domain is the lead time available to develop security responses. The migration of data to a quantum safe environment will be one of the primary challenges.

The application of AI for cyber security will proceed in waves, with the present wave being defined as machine learning. An emerging third wave may involve “explainable” AI. The core challenge is that AI cannot be modeled on how humans interact with cyber systems, but AI can have useful security effects with regard to control systems for critical infrastructure and cyber physical domains (hardware).

Panelists agreed that complexity was a real challenge. One panelist raised the question of whether quantum and associated technological developments would require a Manhattan project-style effort. Security by design should be promoted but communication and public education is key to ensuring action and investment. The Universities have a role to play as partners.

Drones, The New Threat Platform, moderated by David Domoney

The panel was the first of two days of discussion around drone usage. The Day one panel featured a keynote address by Major General James Foss, USAF, and panel discussion by individuals involved in drone development and use.

Drone use is spreading, and the panel discussion indicated that private sector and commercial use of drones was an area where states are playing catch-up. Commercial drones are easily adaptable to carry weapons payloads. They are “dream” platforms for espionage. Counter-drone techniques are challenging particularly in civilian airspace. Denied air space and radio frequency detection and intervention are the best available methods for countering drone threats.

One panelist suggested that the “clueless, the careless and the criminal” are the ones who will cause the real dangers with drone usage and challenge mitigation. Another stressed the need for proper data storage and use for drone deployment.

Another panelist talked about the development of analytical tools for intelligence decision making, using the example of solving the security protection to be applied to a mid sized oil refinery in a remote location.

Standards are necessary to advance safe technological use not just for UAVs themselves but for the network required to operate them, UAS (unmanned aircraft systems), and ensure public education and acceptance.
DAY TWO, FEBRUARY 28, 2018

The morning of February 28 was devoted to plenary addresses by the Honourable Andrew Leslie, Parliamentary Secretary to the Minister of Foreign Affairs, Angela Mondou, the President of Canada Company, and Brigadier-General Assaf Orion, Senior Research Fellow at the Institute for National Security Studies, Israel.

There were also morning sessions devoted to the subject of threats to places of worship; and to the media. New Canadian government programs for research and development were described.

The second day of the conference also featured panels on Executive Security; State Cyber Ops and Cyber Security; Radicalization and the Foreign Fighter Phenomenon; Crowd Management; and a continued conversation on Drones and the Quantum Threat.

Morning Keynote by The Honourable Andrew Leslie, Parliamentary secretary to the Minister of Foreign Affairs

Mr. Leslie described a global order in flux, facing challenges to our notions of a rules-based order. New ways of thinking and allocating security resources are required.

Mr. Leslie referred to the government’s recent Defence Policy Review and noted that climate change security impacts are of increasing importance, while raising questions about future access to power sources and strategic resources.

Problem solving will have to take place in a “digital first” environment and there is a growing realization that cyber issues have not had the prominence they should. The Government of Canada has responded with new investments in cyber security outlined in Budget 2018 and will be releasing its new national cyber security strategy. The government recognizes that we have to increase the collective security of our cyber systems.

Keynote by Angela Mondou, President, Canada Company, “Filling the Gap: Cybersecurity Readiness and the Talent Dilemma.”

Ms. Mondou’s presentation addressed what she described as a looming cyber security talent crisis. There are different elements to the crisis but an important one is the question of time. There are no long lead times available to fill the talent gap. She estimated that Canada will need 216,000 positions filled as early as 2021. The figure is exponentially larger globally.

Diversity is a massive challenge with regard to cyber security professionals. Less than 10% of this cadre are women. New methods are needed to train and recruit, amounting to the creation of a talent-industry ecosystem.

Ms. Mondou called for a national conversation on the talent crisis in the cyber security field; for a whole of government approach to the problem; and for multi-dimensional private sector engagement to build a future “pipeline of talent.”
Keynote Presentation by Brigadier-General Assaf Orion (Israel Defence Forces, Res.), Senior Research Fellow, Institute for National Security Studies, Israel

General Orion described counter-terrorism as being partly about state security paradigms, using available tools and building resilience to protect the state while not over-doing it and driving the state into anti-democratic practices. Counter-terrorism is also, importantly, about knowing the enemy, a lesson derived from Sun Tzu’s classic, The Art of War.

The virtual domain is increasingly the most important in understanding the enemy. Here the challenges are not just around information, but understanding belief systems and perceptions.

He argued that special attention needed to be given to what he called “recruitment pyramids.” Terrorist groups need to be deprived of popular support and their narrative and belief systems challenged, but such challenges cannot be mounted from outside. Conditions and leadership are critical factors in the art of knowing terrorist groups.

Dr. Dennis Moreau, Senior Security Architect, Technology Security Office, VMWare, gave a brief, technical presentation over the lunch period which focused on the problem of the multiplicity and proliferation of cyber security tools used by single organisations to confront cyber threats, the ease with which malware can penetrate organizational systems, and the need for new thinking to combat the cyber threat.

Eric Fournier introduced the conference registrants to the IDEaS program (Innovation for Defence Excellence and Security) introduced in Canada’s Defence Policy Review document, Strong, Secured, Engaged, published in June 2017. IDEaS is exclusively focused on resolving defence and security challenges through support and interaction with innovators in the private sector and academia seeking to develop new products and concepts.

Christopher Scharapenko provided an overview of the BCIP (Build in Canada Innovation Program). BCIP operates through a continuous intake model, allowing Canadian innovators to submit bids regarding first sales and testing of products when ready.
DAY TWO, PANEL SUMMARY

Threats in Places of Worship

Panelists described places of worship as a new soft target. Such attacks are increasing. In response authorities must use sophisticated engagement and outreach approaches to threatened communities and places of worship. Existing programs for outreach can be further leveraged to this end. Security standards for places of worship need to be considered.

Media Discussion Panel

The media environment, like the threat environment, is fast changing, driven by technological change and by fundamental shifts in the business model. Media companies must now invest in cyber security practices themselves to protect data and safeguard the integrity of their reporting. A trust deficit has developed which is linked to the decline of the place of quality journalism.

Yet the value of the media for national security may ultimately be enlarged. Ensuring the validity of open source information “becomes a strategic foundation for national security.” The public must be educated about digital consumption.

Drones, The New Threat Platform, moderated by David Domoney

One of the unique features of the Readiness and Resilience conference was the sustained attention paid to the drone threat. The discussion on drones continued in a day long panel on February 28, which deepened the discussion from the first day. Many of the presenters are involved with the technological development of drone counter-measures.

Presenters discussed the many kinds of threats posed by drones, the different kinds of nefarious actors that may use drones (terrorists, some hobbyists, criminals), and the variety of mitigation efforts that have been developed or are in the development stage. The point was made that drones may pose a particular threat to the security of critical infrastructure, but that their data itself poses cyber security risks. In general understanding the threat to the home environment (home game) is less well developed than understanding the threat in an overseas environment (away game). RF based techniques may offer the best currently available defence and mitigation against drones according to some. Radar based detection systems for drones may be the future.

At the same time, drones bring considerable advantages, including overhead inspections, geo-mapping, medical and other deliveries, assistance to the agriculture sector, perimeter security, and search and rescue.

Deep Dive on the Quantum Threat, moderated by Dr. Michele Mosca

This panel also continued the debate around quantum computing and its security implications from Day one.

The key message in this panel was that the advent of quantum computing will increase uncertainty about encryption safeguarding of data and communications. Organisations will need a plan. Components of such a plan should include identifying the organization’s reliance on encryption; tracking developments in quantum to avoid unnecessary surprises; considering IT purchases and technology upgrades in light of quantum developments and known threats. The ultimate objective will be to move an organization’s information technology to a “quantum-safe state.”

Executive Security in the Age of Disruption, moderated by Benoit Parent

This panel engaged in an effort to broaden understanding of what constitutes executive security, arguing that it is not just about the security of high-level principals but of the entire eco-system of an organization. It has to be recognized that some executives require education in security and risks. For executives travelling abroad the calculus changes and becomes more complex. Not only do risks need to be accurately identified but contingency planning becomes more complex. Kidnapping and ransom planning are important. Table top security exercises with key officials in attendance can help in planning and help in educating the executive level. Imagination is a core requirement. Executive security is not just about guns, gates and guards.
State Cyber Ops and Cyber Security, moderated by Mark Weatherford

Panel presenters gave a portrait of the variety of major cyber attacks known to have been perpetrated, which can be broken down by categories such as cyber crime (conducted against a Bangladeshi bank); deterrence espionage (the hack of the system operated by the Office of Personnel Management in the US); sabotage (the famous Stuxnet assault on Iranian nuclear centrifuge arrays); terrorism (citing the North Korean attack on Sony); information warfare (Russian election meddling) and economic aggression.

One of the ways that cyber is being developed as a weapon is in regard to the conduct of economic warfare; examples have been seen in Estonia in 2007 and in the Ukraine in 2016.

Key vulnerabilities are less to do with technology and more with people, and their misuse of cyber security protocols. More proactive safeguarding is needed. There are lots of changes that can be advocated to boost cyber security. One has to be the ability to react and leverage consequences for an adversary. Many countries are creating a central agency responsible for cyber security.

The audience was provided with a comprehensive picture of the Canadian sigint and cyber security agency, the Communications Security Establishment. Legislation currently before Parliament (Bill C-59) would create a stand-alone legislative statute for CSE and expand its mandate to include active and defensive cyber operations, designed to give CSE the policy option to engage in proactive and preemptive cyber operations.

Panelists agreed on the need to be in a state of readiness for cyber attacks; that readiness and knowledge of the threat environment needs to extend to the public at large. CSE is now in a transformative moment where more attention is being paid to reasonable transparency and the need for appropriate public education.

Radicalisation and the Foreign Fighter Phenomenon, moderated by Dr. Paul Taillon

Panelists discussed the on-going threat posed by the Islamic state and the problem of terrorist travellers and returning foreign fighters. One solution that needs work is the development of cooperative intelligence and sector networks across countries and regions. Working with affected and vulnerable communities remains vital.

We continue to explore the fundamental problem of what brings people to embrace terrorism. One panelist emphasized the importance of ideological attraction and binding. There was general agreement in reiterating the expert view that no single profile of how radicalization to terrorism can occur exists, just over-simplified ideas, particularly around poverty and low social and educational status, mental health issues, petty crime backgrounds, immigrant status. One panelist argued that among the great diversity of pathways to terrorism, a couple of commonalities stand out in the available evidence. One is the burgeoning sense of community victimisation; the other is the role of family members and peers. The internet plays a large role in recruitment to terrorism.

Dealing with returned foreign fighters will be a major law enforcement and intelligence challenge, not least because the returnees are not one size fits all. They will have to be carefully filtered to determine the risks they pose and the best ways to deal with them.


This panel featured presenters who have executive responsibility for the security of major sporting events. Major sporting events are classic soft targets and frequently the subject of threat warnings. Responsibility associated with protecting such events is huge. Threats range from low probability-high impact events (various forms of targeted attacks) to things that are simply high probability, such as theft, alcoholism, crowd control breakdowns.

As one presenter noted, the responsibility takes two forms—to try to prevent any incidents; and to react quickly and well to them if incidents do occur that threaten the safety of individuals present. Prevention is about good intelligence, good detection systems and good deterrence. Having great staff is important. Reaction is about sophisticated planning and deep cooperation across first responder communities.
The conference organisers wish to extend a special thanks to the corporate sponsors of the Readiness and Resilience Conference:

Cummins Eastern Canada LP  
CyberNB  
Accenture Inc.  
Thinklogical, a Belden Brand  
Robotics-Centre  
Allen-Vanguard  
SAS Canada  
Leonardo  
Capital Hill  
NetApp  
VMware  
Lenovo Canada

We also extend thanks to the companies that joined the conference to display and discuss their products in the Technology Expo:

Dasco Storage Solutions  
LRAD Corporation  
Valley Associates  
Senstar  
Visiontec Systems  
Calian Emergency Management  
Lind Equipment Ltd.  
QinetiQ Canada  
Levitt Safety  
Cummins Eastern Canada LP  
Twenty20 Insight  
Dynasafe US  
Esterline  
Sailpoint Technologies  
PlanB Solutions  
Cyber NB  
Thinklogical, a Belden Brand  
Robotics-Centre  
Allen-Vanguard  
AVSS-Aerial Vehicle Safety Solutions Inc  
SAS Canada  
Accenture  
Vidisco  
VMware  
NetApp  
Leonardo  
Department of National Defence/Canadian Armed Forces  
Reticle

Finally, we want to express our most sincere thanks to all the Keynote speakers, Plenary Speakers, Panel Moderators and Panelists. The development and delivery of this conference could not have been completed without their valuable contributions.

The conference organizers will provide all registrants to the 2017 conference with advance news of plans for a 2018 conference and we welcome suggestions for topics of interest.

Please send conference suggestions and feedback to: Serge Blais, Director, Centre for Continuing Education, University of Ottawa (sblais@uottawa.ca)