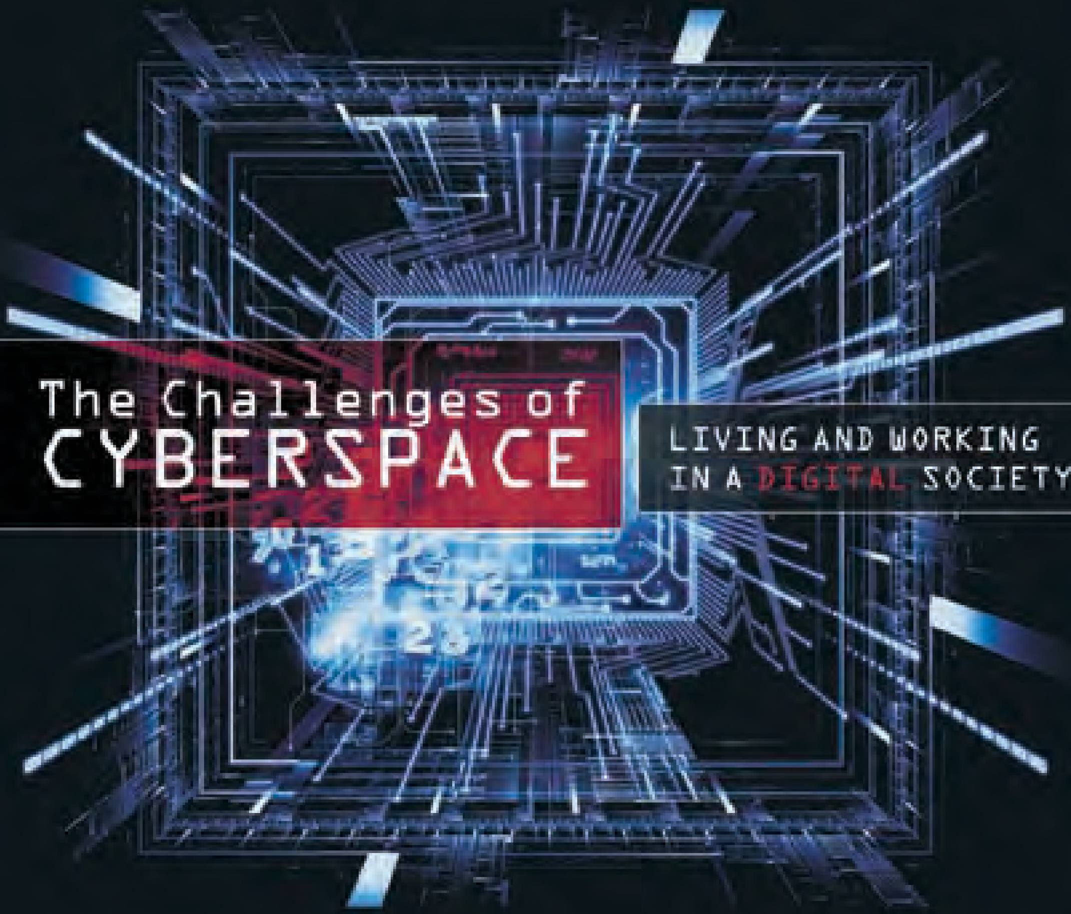

The Challenges of CYBERSPACE

LIVING AND WORKING IN A DIGITAL SOCIETY

2014 Canada-UK Colloquium
Rapporteur's Report

REX B. HUGHES
JIM NORTON

The Challenges of Cyberspace: Living and Working in a Digital Society

Rex B. Hughes and Jim Norton

2014 Canada-UK Colloquium
Rapporteur's Report

The Challenges of Cyberspace: Living and Working in a Digital Society

Rapporteur's Report

Rex B. Hughes and Jim Norton

Canada-UK Colloquium, 24-26 November 2014
Montebello, Québec

School of Policy Studies, Queen's University
Canada-United Kingdom Council

Library and Archives Canada Cataloguing in Publication

Hughes, Rex, author
The challenges of cyberspace : living and working in a digital society
/ Rex B. Hughes and Jim Norton.

(2014 Canada-UK colloquium : rapporteur's report)
Co-published by Canada-United Kingdom Council.
"Canada-UK Colloquium, 24-26 November 2014, Fairmont Le Château
Montebello, Montebello, Québec".
Issued in print and electronic formats.
ISBN 978-1-55339-446-4 (paperback).—ISBN 978-1-55339-499-0 (pdf)

1. Cyberspace—Congresses. 2. Information society—Congresses. 3. Internet—Congresses. 4. Social media—Congresses. 5. Computer crimes—Congresses. I. Norton, Jim, 1952- , author II. Queen's University (Kingston, Ont.). School of Policy Studies, issuing body III. Canada-United Kingdom Council, issuing body IV. Canada-UK Colloquium (2014 : Montebello, Québec) V. Title. VI. Series: Rapporteur's report (Canada-UK colloquium)

HM851.H84 2015 303.48'33 C2015-903774-3
C2015-903775-1

ISSN 2368-7479 (Print)
ISSN 2368-7517 (Online)

The Canada-UK Colloquia

The Canada-UK Colloquia are annual events that aim to promote the advantages of a close and dynamic relationship between Canada and the United Kingdom through the advancement of education in a wider context. These conferences bring together British and Canadian parliamentarians, public officials, academics, business people, journalists and broadcasters, other private sector representatives, graduate students, and others. The organizers focus on issues of immediate relevance and concern to both countries with the aim of exchanging experience and enhancing policy outcomes. One of the main endeavours of the Colloquia is to address these issues through engaging British and Canadian experts in the exchange of knowledge, experience and ideas and the dissemination of their conclusions in a published report. Previous reports can be found at http://www.queensu.ca/canuk/.

The first Colloquium was held at Cumberland Lodge in Windsor Great Park in 1971 to examine the bilateral relationship. A British steering committee, later to become the Canada-United Kingdom Council, was launched in 1986. The School of Policy Studies at Queen's University assumed responsibility for the Canadian side in 1996, succeeding the Institute for Research on Public Policy.

The Colloquia are supported by the Department of Foreign Affairs, Trade and Development in Canada and by the Foreign and Commonwealth Office in the United Kingdom, as well as by private sector sponsors. They are organized by the School of Policy Studies at Queen's University, on the Canadian side, and by the Canada-United Kingdom Council on the British side, from which an executive board, the Council of Management, is elected annually.

About the Authors

Rex B. Hughes is the co-director of the Cyber Innovation Network at the University of Cambridge and a visiting professor at Munk School of Global Affairs, University of Toronto. His research examines the impact of the cyber revolution on financial markets and national security with his analysis and commentary appearing in *International Affairs*, *The Economist*, *Forbes*, *The Financial Times*, *The Times of London*, *The Daily Telegraph*, and *The Asahi Shimbun*. Hughes is a founding member of the Cyber Innovation Network, a joint research initiative of the Cambridge Computer Laboratory and Jesus College, Cambridge. Since 2008, Hughes has advised NATO senior officials on cyber defence policy, including the 2010 NATO Strategic Concept and the 2014 NATO Asia-Pacific Dialogue. From 2005 to 2007, Hughes served as a Cambridge-MIT Institute research associate contributing to disruptive technology roadmaps for British Telecom, Telecom Italia, Nortel, Nokia, and TMobile and for Ofcom's Strategic Review of Telecoms. From 1999 to 2003, Hughes founded and directed the University of Washington Center for Internet Studies, underwritten by the US Department of State, IBM, Lotus, Microsoft, Boeing, Open Society and MacArthur foundations. From 1997 to 1999, Hughes led the development of IBM sponsored iEnvoy, the first secure Internet communications platform for diplomats. From 1999 to 2003, iEnvoy was deployed as an official confidence and security building measure in APEC and ASEAN. Hughes received his PhD in international relations from the University of Cambridge and his BA and MA in international studies from the University of Washington.

Jim Norton, FREng is an external member of the Board of the UK Parliament's Office of Science & Technology (POST) and Chair of the UK Spectrum Policy Forum. He is a Trustee Director of BCS Learning & Development Ltd and Trustee Board Member of BCS, the Chartered Institute for IT. Norton is also a member of the Engineering Policy Committee of the UK Royal Academy of Engineering and Chair of the Academy's Computer Systems Engineering Community of Practice. He is also an adviser to the Irish Commission for Communications Regulation (ComReg) and a member of the Irish Government's Steering Group to oversee the implementation of the Irish National Broadband Plan. He has held senior roles in the private and public sectors and was a founder member Cabinet Office Performance & Innovation Unit (later known as the UK Prime Minister's Strategy Unit). Norton has a long history of involvement in cyber issues, from the 1970s as a founder member of the committee that drafted the original UK standard on modes of use for encryption and the early 1980s as the point of contact between BT and GCHQ on civil cryptography matters including the development of encryption systems for satellite services. In 1999 he was responsible for the report "Encryption and Law Enforcement" commissioned personally by the then Prime Minister. More recently he was a Commissioner in the IPPR Commission on National Security in the 21st Century.

Table of Contents

Preface xi

Letters from the Prime Ministers xiii

The Challenges of Cyberspace:
Living and Working in a Digital Society 1

Policy Recommendations 28

APPENDIX

Program 36

List of Participants 39

Preface

This Rapporteur's Report summarizes the discussions at the Canada-United Kingdom Colloquium on "The Challenges of Cyberspace: Living and Working in a Digital Society," held in Montebello, Québec, in November 2014.

We would like to take this opportunity to thank the many people who contributed to the success of the 2014 Colloquium. First, the colloquium is only possible because of the on-going assistance of the Department of Foreign Affairs, Trade and Development Canada and the UK Foreign & Commonwealth Office. We would also like to acknowledge the financial support of Thomson Reuters as prime sponsor, Pharos Security and IBM Canada. We are deeply appreciative of their help: we would not have been in Montebello without them.

We would also like to thank Jim Norton in the UK and Mel Cappe in Canada for helping to assemble an exceptional group of presenters and participants. We are also very appreciative of the counsel provided by Anthony Cary as Honorary President of the UK committee and Mel Cappe as chair of the Canadian advisory body. We were again the beneficiary of the exceptional logistical support provided Maureen Bartram of the Centre for International and Defence Policy at Queen's University. The UK team was, as always, ably coordinated by George Edmonds-Brown.

The Briefing Day held for the visiting UK side was ably assisted by John Proctor, Vice-President, Global Cyber Security, CGI Global, and Robert Gordon, Special Advisor on Cyber Security, Public Safety Canada, who presented the UK delegation with overviews of the challenges of cyber, particularly cybersecurity. We would like to thank both Mr Proctor and Mr Gordon for their willingness to share their considerable experience with the Colloquium. We would also like to thank the Canadian Branch of the Commonwealth Parliamentary Association for their hospitality. We owe a special debt of gratitude to Dr Duncan Stewart of the National Research Council, who opened the NRC for our afternoon briefings. We would like to thank both Dr Stewart and members of his team for their briefings on security and disruptive technologies. We are also grateful that Mr Michael Walma, the Internet Foreign Policy Coordinator at the Department of Foreign Affairs, Trade and Development Canada, was able to make time to brief us even though Canada's minister of foreign affairs, Hon. John Baird, was hosting Carl Bildt, Chair of the International Commission on Internet Governance, while the Colloquium was meeting. The coincidence of these two events demonstrates the degree to which governments are seized of the challenges and opportunities of cyberspace.

We would like to express our thanks to H.E. Mr Howard Drake, the United Kingdom High Commissioner to Canada, and his team for their wonderful hospitality at Earnscliffe and their on-going support of the Canada-UK Colloquium.

We would also like to thank the chair of the 2014 Colloquium, the Hon. Bill Graham, former Canadian minister of national defence and minister of foreign affairs and leader of the Liberal Party of Canada. He did a masterful job not only of keeping our proceedings on track, but also of adding to the discussions from his own rich experience.

Finally, we thank Professor Rex Hughes, the Rapporteur for this year's Colloquium, and Professor Jim Norton, for their work in compiling this Report. We hope that the conclusions and recommendations set out in the Report will be useful to policy-makers in both countries.

Kim Richard Nossal
School of Policy Studies
Queen's University

Philip J Peacock
Chairman
Canada-United Kingdom Council

CANADA

PRIME MINISTER · PREMIER MINISTRE

2014 Canada-United Kingdom Colloquium

Three years ago, British Prime Minister David Cameron and I endorsed the Canada-United Kingdom (UK) Joint Declaration with the aim of fostering the deep partnership that our countries share. Since then, Canada and the UK have worked to reinforce our longstanding ties, nurture our solidarity and enhance our cooperation.

One example of this cooperation is the annual Canada-UK Colloquium, which for decades has brought together thinkers from an array of fields to examine issues of mutual concern to our countries. This year's Colloquium, in Montebello, Québec, will focus on "The Challenges of Cyberspace: Living and Working in a Digital Society".

Given the rapid developments in the digital world, and the challenges and benefits they bring, this is a timely theme for the 2014 Colloquium. Our societies can reap the fruits of globalized information sharing and instantaneous communications—in business, education and everyday life—but we must also be on guard and better address the potential threats to the openness, freedom, and security of the Internet. By working together with diverse stakeholders, including academia and civil society, we can build improved systems of responsible governance and policy to safeguard this web of interconnectedness upon which we rely.

It is with great pleasure that I welcome all participants of the 2014 Canada-UK Colloquium, and wish you a successful event.

10 DOWNING STREET
LONDON SW1A 2AA

THE PRIME MINISTER

Britain and Canada are natural partners and Stephen Harper and I have worked closely together over the last few years to get the most out of the relationship between our two countries. The Joint Declaration that we issued three years ago set out our intention to renew and to deepen the bonds that we share.

One of the most effective tools for that purpose is the Canada-UK Council which holds annual policy discussions on subjects chosen with the support of both governments. The purpose is not just to develop networks of expertise, but to come up with policy proposals that we can put into action. Last year's very successful meeting on New Realities for Global Health was a good example.

This year's meeting – which will take place in Quebec – is devoted to the Challenges of Cyberspace: Living and Working in a Digital Society.

In many areas the vast global information and communications system is improving lives, driving productivity and efficiency, accelerating research and creating new opportunities. The democratisation of education, with Massive Open Online Courses, is another example of the potential for good. But the rush to cyberspace can also be something of a leap in the dark. Systems become more powerful as they interconnect. We are grappling, as individuals and as governments, with myriad questions of governance, privacy, security and criminality.

I wish this year's Canada-UK Colloquium every success in finding ways in which our two countries can work even more closely together on these urgent questions.

July 2014

The Challenges of Cyberspace: Living and Working in a Digital Society

Rex B. Hughes and Jim Norton

INTRODUCTION

The pervasiveness of computerization and the equally ubiquitous connectivity of contemporary humankind have created a taken-for-grantedness about what we have come to call cyberspace. In just over twenty years, we have developed a massive dependence on the benefits of what has grown into a vast and complex global information and communications system. A system that allows us to effortlessly withdraw cash anywhere in the world, videochat with loved ones on the other side of the globe, or connect to the office while canoeing a wilderness river, is one side of this communications revolution. The near-perfect capture of a frank phone call by a senior US State Department official in February 2014, the leaking by Edward Snowden of details of global surveillance operations run by the National Security Agency of the United States and its allies, and the widespread use of cyberspace by criminal organizations and ordinary individual criminals is another. And yet there are divergent views on whether to prioritize action on, or to ignore, this darker side of the contemporary communications revolution. We not only produce vast amounts of information, but we routinely, and often unknowingly, allow that information to be accessed by others, sometimes for good and sometimes for malign purposes.

On the positive side of the balance sheet, "data analytics" (often described as "Big Data") is facilitating major strides in improving productivity and efficiency in areas as diverse as "smart" electricity grids, genomic medicine and personal digital assistants. Massive Open Online Courses (MOOCs) offer a fundamental shift in the democratization of education and its outreach to those in emerging economies.

On the negative side, there is the widespread criminal use of cyberspace and a blurring of the boundaries between state and non-state actors in activist attacks and old-style espionage, but with new tools. Similarly abuse of the privacy of personal data, especially in sensitive areas such as medical records, could fundamentally undermine trust.

Governments use cyberspace for a variety of purposes, both defensive—to counter the exploding number of cyberattacks on government agencies—and offensive, such as the Stuxnet worm attack on the Natanz facility in Iran in 2010. The increasing tendency to see cyberspace as a battlespace, and computers as weapons, can be best seen in the declaration in October 2012 by the then US Secretary of Defense, Leon Panetta, that cyberwarfare—conflict between states or non-state actors using attacks on, with, and by computers—is the greatest threat facing the United States. Even though we have not yet developed many of the capabilities that are being bruited, there are nonetheless those who worry about a "cyber Pearl Harbor" that will attack infrastructure targets that were built in the pre-Internet age. Trying to provide cybersecurity against the possibility of cyberwarfare seems to be a constant scramble for government agencies charged with providing their citizens with protection. The creation of a Cyber Command by the United States in 2010 is one such measure.

But it is not just the "weaponization" of cyberspace that has engaged governments and security agencies. In many countries, governments use the Internet and their citizens' seeming addiction to cyberspace connectivity to deepen the control of governing elites. But in all countries, both authoritarian and democratic, governments could use that dependence on cyberspace to weaken the capacity of citizens to challenge the power of the state. Similarly these deeply interconnected and interdependent elements have a tendency to form "accidental systems" whose characteristics are poorly understood and may weaken both technological and social resilience through potential cascades of failure.

Whilst the technologies underpinning cyberspace have seen some forty years of continuous exponential growth in performance per unit price, humans still think in linear terms; they do not adapt well to exponential change. This points to a key area where more work is required. The growing impact on individual citizens and organizations of these developments is poorly understood. Good security is a holistic balance of personnel security, physical security and electronic/cybersecurity. In many organizations excessive trust in the (nonetheless important) technological approaches to cybersecurity has led to neglect of the other areas with potentially disastrous results. There is also a poor understanding across general populations of the basics of "cyber hygiene." Even the fundamental tools of business lag behind. The failure to be able to properly value "intangible assets" (such as customer and design information) on corporate balance sheets means that we are using 19th century tools to manage 21st century companies. As a consequence we fail to apply many tried and tested corporate disciplines and accounting processes to these new challenges.

Finally, the increased use of social media continues to transform politics in countries around the world, posing challenges to long-established political institutions. Does social media have the political impact that is so often attributed to it?

These were the overarching questions that animated the Colloquium participants.

THE COLLOQUIUM SESSIONS

The Challenges of Cyberspace

The Colloquium began with an exploration by the Rt Hon Baroness Neville-Jones of the challenges of cyberspace, and an assessment of the issues posed by the emergence of cyberspace as a largely autonomous sphere. What issues remain the most important for governments—and for citizens? Questions discussed on the positive side of the balance sheet included:

- The continuing exceptional and positive impact on many aspects of society from education to healthcare and scientific research to international trade.
- The huge impact of 24/7 western banking on China.

- Massive further opportunities facilitated by “Data Analytics” (so-called “Big Data”) techniques.

Questions discussed on the negative side included whether:

- Cyber technologies fundamentally favour attack over defence.
- Cyber disruption was now an inevitable precursor to conventional conflict, with the inherent difficulties of unambiguous attribution.
- The nature of national economies had been fundamentally changed with tighter coupling, reduced redundancy and greater implicit dependence on the reliability of infrastructure.
- The new tools disproportionately empower rogue individuals and protest groups.
- Erosion of trust was undermining a vital element of democracy? It was asserted that many people now feel more insecure than during the Cold War.
- White collar occupations were now threatened with as yet no obvious new opportunities for mass employment.

It became clear that many issues were finely balanced. Each benefit seemed to come with a countervailing negative. Strong global growth driven by e-commerce, but with a similarly globalized “black economy.” Greater opportunities, but with greater risks. Burgeoning opportunities for direct, participative democracy, but with what impact on representative democracy? Immense opportunities for states to gather information on their citizens, yet Governments weakened by the spread of new mass communication channels such as social media. Many personal benefits, but at the cost of personal privacy?

Recommendations from these discussions included:

- The vital need for shared and enhanced situational awareness, developing further trusted forums for information sharing, breaking down public, private and academic silos.
- The importance of developing a second “Geneva Convention.” The principles of international law still remained relevant, but how might these best be applied in cyberspace?

- The potential to disrupt criminal activity as well as seeking conventional prosecution.
- The critical importance of STEM (Science, Technology, Engineering and Mathematics) education and digital literacy as an essential precursor.
- The opportunity to embed issues of cybersecurity into normal risk management. It is imperative that this is recognized as a key "risk" issue for the whole board and not simply an IT problem. Good security requires a balanced approach to physical, personnel and cybersecurity.
- The need to find ways to incentivize good cyber hygiene and behaviour, rather than relying excessively on regulation.

The Politics of Cyberspace

The second session addressed the contemporary politics of cyberspace. It was jointly led by Mr Paul Meyer, a former Canadian Ambassador and Permanent Representative to the United Nations, and the Rt Hon James Arbuthnot MP, a former Chair of the UK House of Commons Defence Select Committee.

The origin of the term cyberspace was discussed. It was noted that it was coined by American-Canadian science fiction writer William Gibson, first in his short story "Burning Chrome" and more extensively in his 1984 novel *Neuromancer.* His definition—"A consensual hallucination experienced daily by billions of legitimate operators, in every nation…"—seemed particularly ironic.

The various initiatives on Internet governance were also explored. While the International Telecommunications Union might lay claim, the case was not so straightforward. Despite the process of the World Summits on the Information Society (WSIS) held in 2003 and 2005 and the ten subsequent annual Internet Governance Forums, all held under ITU auspices, the consensus was that the Internet is not and should not be state run, rather it is an international public space.

The two most important current political issues were recognized as state surveillance, for the domestic agenda, and inter-state conduct for the international agenda. On the first topic, the participants discussed how to balance a necessary degree of state surveillance against individuals' rights to privacy. It was recognized that transparency and the rule of law were essential. An Australian example of cooperative public dialogue stretching over two years and with more than 300 public submissions was commended. On the second topic, it was agreed that a global consensus on norms of state behaviour was essential. Both the US, through President Obama's 2011 International Strategy for Cyberspace, and the UK, through former Foreign Secretary William Hague's multilateral, multi-stakeholder conferences, had launched initiatives but momentum had faded away. Not always helpfully, China and Russia were filling the void at the UN.

Discussion moved on to an increasing pan-European disenchantment with politicians in general. Reasons were debated including: economic challenges; inflated expectations of lifestyle; a rose tinted desire to return to some past Shangri-La; pervasive 24-hour rolling news; increased communications through social media; and contempt for politicians' inability to deliver "instant solutions." Harking back to the first session, concerns were raised that instant single-issue campaigns on social media and increasing use of referenda were eroding representative democracy.

The session concluded with a discussion on the vulnerability and inter-dependency of modern infrastructure. A cascade of energy and communications infrastructure failures leading back quite literally to a "dark age" was mooted. The vulnerability of key (very hard to replace) electricity grid transformers to a lone sniper was used as an example. Vulnerability of infrastructure to both physical and cyberattack was seen as an ultimate asymmetric threat.

Recommendations from this session included:

- Maintaining the Internet as an international, multi-stakeholder, open, public space.
- Ensuring that well resourced and independent oversight was in place to give confidence to the public regarding the use of state surveillance techniques.

- Establishing some clear and focussed deliverables for the ongoing discussions on norms for state behaviour.
- Creating markets in resilience and making cybersecurity a matter of competitive differentiation.

The Business of Cyberspace

The third session focused on the business of cyberspace. It was jointly led by Mr Pat Horgan of IBM Canada and Mr Mark Connelly of Thomson Reuters. The session focussed on the new advances being fuelled by the combination of Internet connectivity and access to large stores of information in near real time. What will be the potential impact and consequences of these changes? What are the downsides from increased criminal activity?

Areas explored included:

- The growing shortage of data scientists with the hybrid mix of skills (mathematics, statistics, computer science, engineering) and sector specific knowledge to extract the real value from data analytics. Figures from McKinsey[1] suggested demand for such staff was growing at 20 percent per annum and that by 2018 the US economy would need 180,000 more data scientists than were currently available.
- The need for greater collaboration between industry, academe and government. IBM Canada was working with seven key Canadian universities proving access to High Performance Computing (HPC) and an Analytics Cloud Computing system. The Southern Ontario Smart Computing Innovation Platform (SOSCIP) was heralded as a great example of such collaboration with some fifty projects and a roadmap through to 2018.
- Making data analytics tools available to small and medium enterprises (SMEs) and not simply the province of large corporations. Applications of IBM's "Watson" technology were felt to be relevant to that challenge.

[1] McKinsey & Company "Seizing the potential of 'big data,'" October 2011.

- While the benefits are huge, the “Dark Net” remains a serious and growing problem. The cost of an average US security breach had grown from $7 million in 2013 to $8.5 million in 2014. Detections of mobile malware had grown more than 600 percent between March 2013 and March 2014. Deep penetration of systems had been found that had remained undetected for some eighteen months. Typically only some twenty targeted phishing attacks were required to achieve full penetration of a system or network. Colloquium members were advised to visit the “Black Hat” conventions to understand the depth of challenge faced.
- The challenge of the vulnerability of legacy systems both in commerce and infrastructure where these represented soft targets for hackers.

Recommendations from this session included:

- The importance of deploying tools and methodologies for much higher quality in software development, including where appropriate formal mathematical methods, and providing “Kite Marks” of assured quality.
- Adding investors to the collaboration triad of industry, academe and government.
- Exploring new business models, as data analytics facilitates an evolution from selling products to selling service or availability.
- Recognizing that there was still a great deal more economic and social value to be extracted even from the existing e-business and social network toolsets.

Cyber Risks and Cybersecurity

The fourth session sought to balance the enthusiasm from the business of cyberspace with the extensive challenges of cyber risk and cybersecurity. It was jointly led by Mr Robert Gordon, Special Adviser on Cybersecurity for Public Safety Canada, and Mr James Quinault CBE, Director of the Office of Cyber Security and Information Assurance at the UK Cabinet Office.

Both governments have sought to maximize cybersecurity: how to protect public and private actors in Canada and the UK from cyber-attacks? How to ensure cross-border cooperation on cybersecurity against both state-sponsored and criminal hackers?

Areas explored included:

- The value of the US National Institute of Standards and Technology (NIST) framework and associated cybersecurity best practice documents.
- The economic risks from theft of Intellectual Property (IP) "on an industrial scale," destructive attacks and more general cybercrime. These needed to be balanced against the economic benefits of the open, creative, and economically beneficial Internet public space discussed in session two.
- The challenge of providing protection in "real time." It was felt that this was still some way from achievement.
- The important roles of governments in providing: support to securing critical national infrastructure (CNI); driving up public awareness and basic "cyber hygiene" skills; investing in research and skills development; and building strong international partnerships.
- The value of timely information sharing mechanisms and a strong national Computer Emergency Response Team (CERT).
- The need to address causes and not just symptoms. This ranges from political initiatives on failed or failing States through to incentives for enhanced software and system quality.

Recommendations from this session included:

- The importance of bringing market forces to bear on the cybersecurity challenges. The biggest companies now have some board appreciation but much more is required. Security should be seen as a competitive differentiator. More opportunities should be explored in the insurance industry.
- A broader approach to policing, including the disruption of criminal networks, the use of asset recovery and greater international cooperation.

Breakout Groups

Four breakout groups examined specific issues associated with cyberspace and reported back in a fifth session to the plenary.

Cyber and Privacy

This group was led by Major General John Adams, CMM, CD, former Chief of the Communications Security Establishment Canada, and Professor Peter Sommer, a UK digital forensics specialist. It discussed the challenges to states posed by the widening use of cyberspace, looking at the threats to personal privacy that are implicit in the rise of what some have called the "Surveillance State." Areas explored included:

- The fact that security and privacy are not necessarily opposing concepts and the public hold a range of strong, but often conflicting, views.
- Intelligence agencies face the challenge of a large number of "false positives" thrown up in their use of search tools.
- The importance of clear audit trails, which can be reviewed to confirm the necessity and proportionality of actions.
- The vital need to re-build trust following the Snowden and similar revelations.

Recommendations from this group presented in plenary session included:

- The importance of appropriately resourced and skilled Parliamentary and commissioner oversight, recognizing that this will inevitably be drawn into classified arenas.
- The need for intelligence agencies to engage in open, transparent public dialogue, but without compromising methods, tradecraft and sources.
- For Canada to build on the UK experience of the Intelligence & Security Committee formed from Privy Councillors. Canada might consider forming such a Committee of Parliamentarians cleared at a minimum of "Top Secret" and provided with appropriately skilled and resourced support staff.

Cyber and Social Media

This group was led by Mr Rob Rosenfeld of the U15 Group of Canadian Research Universities and Prof Bill Dutton, Quello Professor of Media and Information Policy at Michigan State University, a former Director of the Oxford Internet Institute. It examined how the increasing use of social media was affecting public policy and politics in countries around the world, how the use of social media influenced political debates in Canada and the United Kingdom, and what impact social media had had on existing political institutions. Areas explored included that:

- Social media reflected a special case of a much larger Internet challenge and was young (less than ten years old). It was felt that norms and practices were still evolving.
- Facebook in itself had a massive penetration—over half of all Canadians were said to use Facebook at least once each month.
- Social media had evolved in two phases. The first four to six years had been regarded as an unalloyed blessing, for example its role in the "Arab Spring." The last few years had been characterized by moral panic. Social media were blamed for: isolation, echo chambers, misinformation, sexting, cyberbullying and similar ills.
- Governments were coming under increasing pressure to "do something"!

Recommendations from this group presented in plenary session included the need for:

- Evidence-based decision-making, including the impact of existing legislation, before leaping to hurried action.
- Investment in digital citizenship, for example how to engage appropriately. The education sector was seen as key, with the UK Cyber Champions program cited as helpful. There was a need to build an appropriate curriculum, focusing on implications, responsibilities and norms of usage.
- Political engagement with social media. Petitions, campaigns, electronic bombardment are all one-way only, potentially undermining representative democracy. Might it be possible to

develop norms that would discredit such initiatives until there had been third-party fact checking and an opportunity for those holding contrary views to set out their case? There was a need for *balanced* petitions.

Information Flows and High Frequency Trading

This group was led by Mr Brennan Carley, Global Head of Platforms at Thomson Reuters, and Prof Kim Nossal, Director of the School of Policy Studies at Queen's University. The group looked at information flows and associated high-frequency trading (HFT), recognizing that HFT was simply the latest manifestation of market arbitrage. Areas explored included:

- The effect that the emergence of HFT has had on the stability and integrity of equity markets, including its impact on liquidity.
- The extent to which HFT has driven massive innovation in low-latency telecommunications.
- The degree to which HFT has increased competition, driven down costs and reduced commissions/spreads.
- The pros and cons of seeking to regulate high-frequency trading.

Recommendations from this group presented in plenary session included the need for:

- Greater transparency in the operation of HFT.
- Greater exploration of the benefits (or otherwise) of payment for order flow.

Threats of the Fragmentation of the Internet and/or Cloud Computing

The final group was led by Prof Marina Gavrilova of the Department of Computer Science at the University of Calgary and Ms Sally Costerton, Senior Adviser at ICANN. It discussed the potential fragmentation of the Internet, and the concerns about the Internet being partitioned up through national and regional interventions, looking at the difficulties of protecting the integrity of cloud computing against extraterritorial legal action. Areas explored included:

- The nine major challenges to cloud computing: data breach; data loss; service traffic hijacking; insecure application program interfaces (APIs); denial of service; malicious insiders; direct attack; inadequate risk analysis; and shared technology. These had much in common with normal IT security challenges.
- The five key threats: tension between political control and fragmentation; trust in technological solutions (and the US/UK Governments post-Snowden); jurisdiction on data ownership and/or possession, following the Microsoft Irish servers case; fragmentation and the right to require revocation; and the economic implications of fragmentation.

The group concluded that solutions should be based around:

- The free flow of data across international borders;
- An inclusive world authority responsible for Internet and communications standards;
- The NetMundial Principles on: human rights and shared values; multi-stakeholder, open, transparent, accountable, inclusive and collaborative Internet governance; and open standards.

Recommendations from this group presented in plenary session included:

- The need to ask the Canadian and UK governments to endorse the NetMundial Principles.
- The identification and prioritization of a subset of these principles for early implementation, drawing on a multi-stakeholder community.

The Challenges of Cyberspace: Policy and Governance Implications

The concluding sixth session of the Colloquium was led by Prof Benoît Dupont, Director of the Canadian SERENE-RISC CyberSecurity Network, and Prof Martyn Thomas, former Vice President of the UK Royal Academy of Engineering. It focused on how Britain and Canada might respond to the contemporary political challenges posed by the exponential expansion of cyberspace. What might be the best future governance models? What are some of the steps that the British and Canadian governments, working together, can take to advance shared values around the world? Areas explored included:

- Whether "old" solutions might profitably be applied to certain of these "new" problems?
- The schizophrenic tension between the necessary national security mindset (protection of Critical National Infrastructure (CNI), developing cyber weapons) and the liberal security mindset (privacy protection, consumer protection, policing).
- Raising broad cybersecurity awareness in ways that empower and provide paths to effective action rather paralytic fear.
- How to improve enforcement? In Canada there are 30 million people and 65,000 police but only 300 of these police specialize in cybercrime.
- How to move a focus that has necessarily been on providing universal Internet access to one that includes the necessary elements of cybersecurity?
- The growing democratization facilitated by the Internet should be welcomed, but cyberspace must not become (or remain) the unpoliced "wild west" of contemporary society. It is highly desirable that norms of acceptable behaviour be established and enforced.
- Cyberspace has permeable international borders so international cooperation is essential for effective policing. Bilateral and multilateral agreements have been, and must continue to be, negotiated with states whose behaviour and actions raise other concerns.
- Evidence-based policy-making can benefit enormously from well targeted data analytics. Full use should be made of these benefits while taking cognizance of the risks and necessary mitigating actions in areas such as personal privacy, digital divides in terms of access to online services, and the fact that different demographics have very different digital footprints

(meaning that great care must be taken in extrapolating from digital data).

Recommendations from this session included:

- The notion that sensitive personal data can be anonymized should be retired for good. It is impossible to predict the effectiveness of future methods for data re-identification. Linked to this, a clear policy is needed for compensation of those individuals who have suffered demonstrable harm because their private data, entrusted to government, has been exposed.
- The urgent need to accelerate the establishment of professional engineering norms for digital systems and software development. The alternative is to have a society reliant on technologies that cannot be trusted and could be disrupted at any time by hostile states, criminals, pressure groups, vandals or natural disasters.
- That strict liability should be imposed on producers and importers of IT systems, following the examples in the safety domain. At present, the benefits of new systems accrue primarily to the developers and owners, yet the risks are borne mainly by end users and third parties. This market distortion needs to be corrected.
- That, in order to reduce vulnerabilities, an international program be established to replace the most important software components in key infrastructure with hardened versions.
- For critical systems, such as national CNIs, a "license to practice" be explored for professional software engineers.

What follows draws together the threads from two days of discussion in Montebello.

CANADA AND BRITAIN IN CYBERSPACE

The UK and Canada are two leading members of the Commonwealth connected across the Atlantic Ocean via a shared political, economic, and cultural history. Thanks to a plethora of information technology innovations made possible via the Internet, personal computer, and mobile revolutions, these shared connections are increasingly coordinated and sustained through the digital medium of cyberspace.

Today a cyberspace of more than two billion Internet users and 4.5 billion mobile phone users forms the basis of what Canadian-British-educated communications scholar Marshall McLuhan aptly called the "The Global Village."[2]

In order to understand the long term significance of the cyber revolution, the 2014 Colloquium started from the following three questions:

- Where do Britain and Canada fit in the emergent global cyber order?
- What trends, practices, and innovations are most salient to the cyber future of Canada and of the UK?
- What actions can both nations take to make cyberspace a more secure and prosperous space?

In looking at this phenomenon and considering its implications for Canada and the UK, the Colloquium conducted a balanced discussion of the *opportunities* and *risks* confronting British-Canadian cyberspace.

CYBER OPPORTUNITIES

Disruptive Information Technology

Given that the heart of cyberspace is powered by innovative information technology, the Colloquium recognized the need for both countries to stay abreast of disruptive information technology developments globally, and generate more of their own indigenous information technology where strategic competitive advantage can be secured. While both countries are blessed with global digital innovation hubs such as Vancouver and Toronto in Canada and Cambridge and London in the UK, there was a general recognition that both nations could do more to develop home grown indigenous information technology. In keeping with this theme,

[2] Marshall McLuhan began his work as a communications scholar professor at Cambridge and subsequently at the University of Toronto as a professor of communications.

the following three areas of IT sector development and innovation were viewed as critical to silicon successes in both Canada and the UK.

- ***The Cloud*** is a ubiquitous virtual application space that allows the provision of advanced IT services at low cost. Cloud services are already a critical part of IT infrastructure in banking, manufacturing, defence, energy, education, and health care. At present the US tech giants such as Google, IBM, Amazon AWS, and Microsoft Azure, dominate the rapidly growing cloud service market. Given the increasing demand for Cloud services in both countries, there is ample opportunity for more home grown Cloud products and services to develop. In the UK, firms such as ElasticHosts, Firehost, and Exponential, have developed successful niche products outside of the US cloud. Canada's low cost energy market makes it an attractive location for global cloud service providers, especially outside Toronto, Montreal, and Vancouver. There are already a healthy number of British and Canadian firms addressing the expanding Cloud market.[3]
- ***Big Data*** is a highly networked process of storing and accessing massive quantities of digital information. Given the proliferation of digital information in both large scale and small scale institutions, there is a greater need among business managers to unlock economic value from these massive datasets. This value demand will only grow as more commercial and private data is generated and stored in the Cloud. At present Canadian and UK companies are at the forefront of using big data. Cambridge based data analytics firm Autonomy (now owned by HP) is a world leader in this area. In the healthcare field, Big Data affords medical practitioners new insights into complex fields such as cancer screening for genetic diseases. Big Data can also be used to analyze societal trends such as consumer spending and

[3] For a listing of Canadian IT firms with ties to Silicon Valley, see http://www.thec100.org/.

Cambridge Silicon Fen listings are available at http://www.cambridgenetwork.co.uk/.

infectious diseases. The UK has shown its commitment to Big Data science with its £42 million investment in the five university Alan Turing Centre for Data Science. In time Canada may consider a similar university consortium.

- ***Internet of Things*** (**IoT**) is a global platform for bringing pervasive networked computing to everyday objects such as appliances, utilities, and wearables. Given the desire to network nearly everything, such a platform is viewed as critical to the Internet futures of both nations. Internet connected light switches and wristwatches are part of the IoT as are autonomous vehicles and industrial robots. As more system on chip and sensor technologies are adapted to everyday systems, the IoT will grow exponentially. Cambridge UK based chip designer ARM is expected to profit immensely from the IoT revolution as are Canadian telecom firms such as Telus and Bell. Telus issued forecasts show that at least 30% of Canadian business plans to deploy IoT technology in the next 24 months.[4] When combined with cloud and mobile revolutions, IoT is seen as an unstoppable force for ubiquitous connectivity and more intelligent information infrastructure. The soon-to-be-complete 24 terabit Japan-Alaska-UK Arctic Fiber is in the process of bringing the IoT revolution to Canada's Last Frontier.[5]

Banking and Finance

The Colloquium also examined the role that the cyber revolution is playing during the post-financial crisis disruption to the financial services sector. Given the prominence of both London and Toronto as leading global financial service hubs, the cyber finance revolution is viewed by the Colloquium as a major target of opportunity for both

[4] See, for example, http://www.thestar.com/business/tech_news/2014/07/15/internet_of_things_technology_poised_to_take_off_in_canada.html.

[5] http://spectrum.ieee.org/telecom/internet/arctic-fibre-project-to-link-japan-and-uk.

nations. The following trends were recognized by the Colloquium as having strategic importance.

- ***Crypto Currencies*** are secure digital monetary units that allow for the exchange of goods and services without the co-ordination of a central bank. Bitcoin, the most popular crypto currency is already in widespread use in both Canada and the UK. There was a consensus among Colloquium members that experimental crypto currencies such as Bitcoin were here to stay thanks to their global popularity and need for more globally transportable currencies. Trends show a growing number of British and Canadian firms accepting Bitcoins and other cryptocurrencies as alternative payment forms.[6] In the coming years, such payment forms are expected to increase. Thus, authorities in both countries would be wise to make sure regulation gives ample space for crypto currency experimentation and growth. If crypto currencies become widely adopted alternatives to the Canadian dollar and the pound sterling, Canadian and UK central banks may need to factor them into future monetary policy.[7]
- ***Mobile Payment*** is an emergent category of banking that make it possible for mobile users to transact with merchants via an Internet connected mobile device. Banks such as TD and HSBC are investing heavily in mobile payment technology as more mobile users activate their devices for electronic commerce and banking. Canada and the UK are also seeing a rush of new entrants to the emergent mobile payment sector such as that of Toronto based Wi-Py and from the UK that of Mi Pay, Zapp, and Pingit. The mobile payment sector also benefits from reciprocal growth in the crypto currency market. There was

[6] The world's first Bitcoin ATM was installed in Vancouver, BC: Robert McMillan, "Take a tour of robocoin, the world's first Bitcoin ATM," *Wired,* 29 October 2013.

[7] See, for example, http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf.

a consensus among Colloquium participants that light-touch regulation may be necessary to keeping both countries at the forefront of these markets. Light touch regulation will also play an important role in attracting sector level foreign direct investment where needed.

- ***Peer-to-Peer Lending (P2PL)*** is an innovative method of monetary lending that allows individuals and companies to bypass traditional banking institutions through the use of social media. Its origins can be traced to UK P2PL pioneer Zopa. The world's leading P2PL firm Lending Club transacted a staggering US$4 billion P2P loans in 2014 with double digit growth expected in 2015 and beyond. According to Colloquium experts, this phenomenon is driven by several macro level trends such as the negative interest rate banking system, demography, and the rush of entrepreneurship in many key sectors. While the UK is a pioneer in this sector, Canada is held back by restrictive banking laws that restrict P2PL to only accredited investors. Until fundamental legal changes are made to Canadian lending laws and regulation, Canada will continue to miss out on this lucrative fast growth sector. P2PL can also play an important role in the foreign policy of both countries in efforts to expand banking to the unbanked in developing countries.[8]

Education and Healthcare

Given the growing pressures on both countries' education and health systems to deliver more services at lower costs, benevolent cyber disruptions are seen as critical to the future of education and health delivery. Thus, the Colloquium recognized the following three trends as critical to Canada and the UK's education and healthcare cyber future.

1. ***Massive Open Online Courses (MOOCs)*** are a highly disruptive technology currently being deployed in the higher education sector. Since 2012, private sector MOOC firms such as

[8] See http://www.gatesfoundation.org/What-We-Do/Global-Development/Financial-Services-for-the-Poor.

Coursera and Udacity have caught fire in both Canada and the UK. In both countries millions of adults and children participate in paid or free MOOCs. While MOOCs were initially perceived as a negative disruption for institutions of higher-learning and some forms of private education, a general consensus has emerged that now see them as a vital tool for delivering educational products and services to a hungry public while acting as a constraint on runaway education costs. Some politicians also see MOOCs as playing an important role in displaced worker re-training. MOOCs were also viewed by the Colloquium as a promising export opportunity for both schools and private sector education service providers to meet high demand in developing countries. A challenge for both countries will be to bridge the gap between conventional institutions of learning and fast and nimble MOOC providers, ensuring sustainable business models.

2. ***Personalization*** is a growing trend in the education and health sectors made possible by the digital delivery of advanced information services. As more education and health data enter the digital realm, new software services make advanced customization possible, thus moving away from the traditional mass production-industrialization model. For UK and Canadian health and education providers, harnessing this trend is considered important for keeping costs down while boosting overall service and product quality. Online courses can be adapted to meet specific individual learning needs and deficits. Similarly individual tailored treatments should mean better quality of care for patients. Wearables and next generation mobile devices will deepen personalization options. Given proper investment and regulatory guidance, Canadian and the UK health and education users should see improved access to online education and health services.

3. ***Artificial Intelligence (AI)*** uses advanced computer science to bring human like intelligence to computing. It is an exciting trend that promises to bring greater interactivity and responsive software to health and education. One of the sponsors of the Colloquium, IBM Canada, showed how its powerful Watson system is being used across Canada to conquer some of the

biggest grand challenges in healthcare, including youth cancer and infectious diseases. Another sponsor of the Colloquium, Thomson Reuters, uses artificial intelligence to spot market trends within nanoseconds. Since high-performance computing analytics require new research methodologies, many of the grand challenges will require close cooperation between the health and education sectors. In Canada, IBM is already partnering with a number of leading universities, including the University of Toronto, the University of British Columbia, and the University of Manitoba. Similar UK partnerships with IBM and other service providers exist with the University of Oxford, the University of Cambridge, and King's College London. A sustained lead in AI technology could propel IT services in both countries into new emerging markets.

CYBER RISKS

While cyberspace is full of amazing economic opportunities it is not without serious risks. Colloquium discussions about cyber risks in Canada and the UK largely fell into the following three categories.

Business Continuity

As business becomes more cyber dependent and data driven, the risk of serious business disruption grows. As recent cyber disruptions have shown, business can suffer serious economic damage. The following three trends are viewed by the Colloquium as critical to maintaining business continuity in cyberspace.

- ***Data Breaches*** of some consequence have impacted a majority of Colloquium members. IDC estimates Internet data breaches on a worldwide basis cost US$364 billion.[9] In both Canada and the UK, in the private sector financial and retail sector data breach damage was especially acute as were health and social

[9] https://blog.bit9.com/2014/03/19/data-breaches-to-cost-364-billion-worldwide-in-2014-study-finds/.

services in the public sector. In both countries national agencies have experienced some of the most expensive and embarrassing breaches. Given that nearly all firms and agencies present in Montebello had experienced some type of data breach incident in the last five years, the need for better public-private threat reduction was real. While the advent of new technologies and services were seen as important measures in preventing future firm level data breaches, there was a general consensus among Colloquium members that reporting requirements were out of step with actual enterprise computing practices and that more study was needed.

- ***Critical Infrastructure (CI)*** protection from cyberattack is a growing concern on both sides of the Atlantic. Canada's overstretched North American energy network is especially vulnerable to disruption. Large scale infrastructure upgrades taking place in both countries, such as smart grids and next generation broadband networks, create a new level of risk to business and citizen users. Colloquium members encouraged both countries to share information on the societal risks posed by new critical infrastructure projects as well as systemic vulnerabilities uncovered in legacy systems and networks. Organizations such as the Canadian Office of Critical Infrastructure Protection and Emergency and the UK Centre for the Protection of National Infrastructure were generally viewed as competent managers, while new public-private partnerships and information sharing agreements may be needed to coordinate CI aspects of new platforms such as the Internet of Things. National regulatory agencies (NRAs) also need to do more to stay abreast of the effects of disruptive technologies on critical infrastructure. CI standard harmonization across borders is also an important step for reducing costs and creating new efficiencies for commercial providers such as British Gas and Ontario Power.

- ***Insurance*** is viewed by the Colloquium as a vital instrument for mitigating cyber risk among both public and private entities. While cyber insurance is still a nascent market in Canada and the UK, demand for such products is expected to grow as cyberattacks become existential business threats. Given their unique position in the global insurance and re-insurance marketplace, London and Toronto stand to benefit from the growth of the cyber risk insurance and re-insurance industry. However, according to Colloquium experts, two major problems are preventing the full development of the cyber insurance market. The first is a lack of history and risk models to create proper levels of risk and asset pricing. The second problem is the role of government in identifying cyber risk outside of normal risk models. In these areas regulators can again play a key role by bringing the necessary parties together. At no time should a data breach put a major corporation at risk of business failure. However, without cyber insurance, many businesses face the prospect of cyber induced catastrophic business failure. Over time cyber insurance could also reduce risk for consumers and vulnerable small businesses.[10]

National Security

The growing use of cyberspace for tactical and strategic advantages is one of the most challenging areas of twenty-first century national security. For both countries, three main challenges were identified. When coupled with changing demography, rising powers, and globalization, the challenges listed below are among some of the greatest in terms of existential threats to national security.

- ***Digital Espionage*** threatens nearly all British and Canadian firms thanks to stealth and skill demonstrated by a range of perpetrators of covert digital attacks. Signal intercept capabilities that were once the exclusive domain of an elite group of nation states are now commonplace in the cyber domain. Most large scale Canadian and UK firms have become targets for a growing legion of state and non-state cyberspies. Everything from

[10] For example, Lloyd’s of London lent considerable to support to the UK Government’s initiatives to make London a global centre for cybersecurity insurance: see http://www.lloyds.com/news-and-insight/news-and-features/lloyds-news/2015/03/government-cyber-initiatives.

commodities reports to aircraft blueprints are fair game for the current generation of cyberspies. The lasting economic damage from the loss of flagship Canadian telecom company Nortel shows what can happen when state sponsored cyberattackers are able to exfiltrate advanced military grade intellectual property with ease. Given the penetration of cyberspace into Canadian and British online business infrastructure, the risk of a similar debilitating event is high. New investments and recruitment by the Communications Security Establishment (CSE) in Canada and GCHQ in the UK are critical to thwarting digital espionage, especially from strategic competitors in the Far East and Eurasia.

- ***Transnational Crime*** is now widespread in cyberspace and puts at risk nearly every British and Canadian Internet user. A new generation of Internet-savvy criminals has emerged globally creating a range of new problems for law enforcement and the judicial system. The resources of both the Royal Canadian Mounted Police (RCMP) and the National Crime Agency (NCA) in the UK[11] are already stretched thin, and much more will be needed to successfully combat the exponential proliferation of cybercrime. Innovations in the IT sector will also be needed to deter future cybercrime. Increased international partnerships can also play a key role.[12] The banking sector is especially vulnerable as more legacy system weaknesses become known to cyberattackers. Better coordination with foreign partners and transnational crime fighting organizations such as Interpol and Europol are needed. There was a general consensus among Colloquium members that new legislation as well as modifications to existing legislation would be needed to bring about a sustained reduction in cybercrime. In some cases traditional

[11] The National Crime Agency replaced the Serious Organised Crime Agency (SOCA) in October 2013.

[12] Canada and the UK are strong supporters and founding members of the new IGCI in Singapore

http://www.futuregov.asia/articles/6436-interpol-launches-singapore-research-complex.

law enforcement and judicial law enforcement boundaries may need to be re-thought.

- ***Autonomous Warfare*** is one of the most revolutionary and lethal domains of cyberwarfare. The demand for autonomous warfare is only expected to grow as the political-military interface seeks more lethal precision strike capability in ungoverned spaces. The use of drone warfare in the Afghanistan conflict and in Iraq has proven the utility of the technology. It has however opened a Pandora's Box given the lack of any international treaty framework or rules based system. The precedent set may yet come back to haunt the western democracies. While use of drone warfare has largely operated in the air domain, a new class of land, space, and sea drones is emerging. The use and availability of such technologies by strategic competitors will pose serious issues of Anti-Access/Area Denial (A2/AD) for Canada-UK surface and underwater fleets as well as commercial and civilian aircraft as the People's Republic of China and the Russian Federation deploy more network-enabled fleets. Greater training and preparation of a new generation of cyberwarriors will be needed to control these systems and defeat them when meeting cyber battlefield aggressors. The rise of autonomous warfare likely represents the greatest revolution in military affairs since the advent of nuclear weapons. In time autonomous warfare will require substantial changes to the international Laws of Armed Conflict (LoAC).

The Public Square

Given the direct participation at the Colloquium by several high-level British and Canadian public officials, past and present, the Colloquium took a special interest in how cyberspace is changing the face of state-society relations in the public square. The following three areas were seen as crucial to the success and health of cyber democracy.

- ***Privacy*** is a fundamental right for all citizens in liberal democracies and should continue to be so in cyberspace. However, the technical architecture of cyberspace, as well as global user base diversity, makes implementing traditional privacy policies and norms difficult. For Canada and the UK leaders, getting the privacy-security balance right is fundamental to the sustained growth and confidence in cyberspace. In certain instances, unlimited anonymity can cause difficult social frictions, especially when used to bully or threaten children. The transmission of health records and other sensitive data across the global cloud is also a serious global governance issue for states. The Colloquium recognized that law enforcement and the state security operations will continue to play the central role in maintaining cyber order where attackers seek to do harm. However, given the permissive boundary that social networking technologies afford and the nascent social norms that currently govern cyberspace many new challenges will continue to arise.

- ***Free Expression*** is another cherished value fundamental to the health of state-society relations in the public square. While the public principles and norms of free speech are fairly established in the traditional media spheres, they are only just beginning to be shaped in cyberspace. The Colloquium discussed how the social media revolution is reshaping traditional speech boundaries and speculated where future state-society friction points may lie. While there have been some attempts to regulate speech in some popular social media such as Facebook and YouTube, the private nature of ownership and traditional interpretations of copyright laws make this a difficult problem. The Leveson Inquiry in the UK is seen as an important step forward for re-considering free speech issues in the Internet Age. Future national security legislation dealing with terrorism will likely need to pay greater attention to the expression vs. security balance.
- ***Light Touch*** approach to regulation is a longstanding value that binds both countries. Despite the challenges evident from the global financial crisis starting in 2008, this approach continues to play a fundamental role in shaping the economic rules of the liberal democratic order. For other democratic members of the Commonwealth, light touch regulation is key to maintaining the openness and freedom that the Internet has been associated

with in the democratic West. The light touch approach to governance and regulation is also viewed by the Colloquium as a key principle to resisting authoritarian states that seek to impose more controls and restrictions on the Internet. Canada and UK engagements in the London Cyberspace Conference process have stressed the need for light touch regulation as have engagements in other international fora such as the International Telecommunications Union (ITU) and the Commonwealth Telecommunications Organisation. For the sake of the open Internet, this posture should continue. The Canada-UK position on light touch regulation is important domestically in order that foreign policy in this area can remain credible.

POLICY RECOMMENDATIONS

Based on the discussions at Montebello, the members of the 2014 Canada-UK Colloquium propose the following policy recommendations. These recommendations seek to strengthen the competitive position of Canada and the United Kingdom in cyberspace, while at the same time contributing to global cyber prosperity and stability.

1. Multi-stakeholder Governance was discussed extensively in Sessions 1 and 2, plus Breakout Group 4. It is seen as critical to the future health and economic growth of cyberspace. This is especially true in global governance institutions such as ICANN (Internet Corporation for Assigned Names and Numbers). However, there is much doubt about its future if the multi-stakeholder model can become hijacked by authoritarian states and/or pressure groups.

The Canada-UK Colloquium recommends that both Governments:

- *Ensure that the Internet is maintained as an international, multi-stakeholder, open, public space.*
- *Use the London Cyberspace Conference process to refine the multi-stakeholder model in order to make it more operationally sustainable and resistant to anti-democratic forces.*
- *Endorse the NetMundial Principles and prioritize a subset of these principles for early international implementation.*

- *Work towards a second "Geneva Convention" on the application of international law to cyberspace.*
- *Seek urgently to negotiate an international treaty framework governing autonomous warfare, including the deployment of drones in offensive operations.*

2. Privacy was a focus of Session 6 and Breakout Group 1. It is a fundamental democratic right that is under attack in cyberspace. All cyberspace users have a right to privacy in accordance with local, national, and supranational laws.

The Canada-UK Colloquium recommends that:

- *Citizens and corporations utilize access technologies and platforms that allow for enhanced privacy protections in cyberspace.*
- *The notion that sensitive personal data can be anonymized should be retired for good.*
- *Governments recognize the need to introduce compensation schemes for those individuals who have suffered demonstrable harm because their private data, entrusted to government, has been exposed.*

3. Trusted Hubs and the themes of risk and competitive advantage flowed through all the Colloquium sessions and are fundamental to national economic growth in cyberspace. Toronto and London have the potential to become major hubs for cyber innovation.

The Canada-UK Colloquium recommends that:

- *Both London and Toronto undertake public policy actions and strategic investments to make both cities world class trusted cyber hubs.*
- *Both countries take action to embed issues of cybersecurity into normal board-level risk management and encourage genuine Board ownership of these issues.*
- *Companies should be encouraged to recognize resilience and enhanced cybersecurity as important sources of competitive advantage.*

4. Education and Skills were addressed in particular in Session 6. They are fundamental to creation and maintenance of advanced cyber economies that require a robust education and skill base. Cyber innovations have often outpaced professional standards and credentials.

The Canada-UK Colloquium recommends that:

- *Government and private sector bodies in both countries increase investments in cyber education and training individuals at all levels.*
- *Governments and professional bodies work closely together to address the growing "digital divide" between those who have full access to the Internet and those whose access is limited through poverty, lack of awareness or sensory impairment.*
- *Governments and professional bodies accelerate the establishment of professional engineering norms for digital systems and software development.*
- *Both governments investigate the feasibility of a "licence to practice" for software engineers working on critical systems, such as national Critical National Infrastructure.*

5. Innovation is fundamental to the advancement and growth of cyberspace. However, Canada and the UK have a way to go in order to close the cyber innovation gap with other advanced knowledge economies. However, as addressed in Session 5, specific opportunities have been identified.

The Canada-UK Colloquium recommends that both countries:

- *Recognize the importance of deploying tools and methodologies for much higher quality in software development, including where appropriate formal mathematical methods, and providing "Kite Marks" of assured quality, adding investors to the collaboration triad of industry, academe and government.*
- *Explore whether market incentives to improve software quality could be created, for example through the introduction of strict liability on producers and importers of IT systems, following the examples in the safety domain. Action in this area should be a priority for future Canada-UK co-operation.*
- *Promote an international programme to reduce vulnerabilities by replacing the most important software components in key infrastructure with hardened versions.*

- *Explore and incentivize new business models, as data analytics facilitates an evolution from selling products to selling service or availability.*
- *Devise policies and economic incentives that encourage cyber innovations across all relevant economic sectors and especially those outlined in this report.*

6. Transnational Crime was addressed in Sessions 1 and 4. Crime in cyberspace costs the global economy US$445 billion per annum, according to US cybersecurity company McAfee. If left unchecked transnational cybercrime threatens the long term prosperity of cyberspace.

The Canada-UK Colloquium recommends that:

- *A larger share of national and local law enforcement budgets be devoted to combating cybercrime.*
- *A broader approach be taken to policing, including the disruption of criminal networks, the use of asset recovery and greater international cooperation.*
- *Further trusted forums for information sharing and enhancing situational awareness be developed, breaking down public, private and academic silos.*
- *Britain and Canada work together to make the Commonwealth Telecommunications Organisation a central organization for the pursuit of cybersecurity, in the first instance by establishing a cybercrime task force for better coordination in fighting cybercrime across the Commonwealth.*

7. Economic Espionage was discussed in Session 2. It is a threat to every major Canadian and UK firm connected to the Internet. In the UK alone McAfee estimates that it costs British firms US$27 billion per annum when added with cybercrime.

The Canada-UK Colloquium recommends that:

- *The Communications Security Establishment Canada (CSEC) and GCHQ in the UK devote substantially more resources to identifying and preventing cyberespionage.*
- *Clear and focussed deliverables be established for the ongoing discussions on norms for state behaviour.*
- *Economic sanctions be used where possible to thwart repeat offender states.*

8. Civil Liberties were discussed in Session 1 and were the focus of Breakout Group 1. There was a lively debate between those who believe that civil liberties should be protected at all levels of society in order for cyberspace to function optimally and those who believe, subject to safeguards, that some level of intrusion/surveillance is necessary is the interests of national security.

The Canada-UK Colloquium recommends:

- *That any changes to the legislation governing the national surveillance of cyberspace contain demonstrable protections for basic civil liberties.*
- *The importance of appropriately resourced and skilled Parliamentary and Commissioner oversight, recognizing that this will inevitably be drawn into classified arenas.*
- *The need for intelligence agencies to engage in open, transparent public dialogue, but without compromising methods, tradecraft and sources.*
- *That Canada build on the UK experience of a Parliamentary Intelligence & Security Committee formed from Privy Councillors. Canada might consider forming such a Committee of Parliamentarians cleared at a minimum of "Top Secret" and provided with appropriately skilled and resourced support staff.*

9. Social Media and Censorship lay at the heart of discussions in Breakout Group 2. Censorship is antithetical to the open end-to-end architecture of the Internet yet a growing number of states are using new technologies to impose strict censorship controls.

The Canada-UK Colloquium recommends that:

- *The relevant national agencies develop and deploy helpful technologies for Internet users in authoritarian states.*
- *Evidence-based decision-making, taking into account the impact of existing legislation, be undertaken before leaping to hurried action on the perceived challenges of social media.*
- *Research be undertaken on means to balance political engagement around social media mitigating the one-way nature of existing petitions, campaigns and electronic bombardment.*

We hope that both the public and private stakeholders in Canada and the United Kingdom, as well as the broader global cyber village, will cooperate in giving public and private support for the implementation of these policy recommendations and the general ideas we have outlined in this report.

APPENDIX

PROGRAM

The 2014 CANADA-UK COLLOQUIUM

The Challenges of Cyberspace:
Living and Working in a Digital Society

MONDAY, 24 NOVEMBER

20h00
Reception hosted by Mr Tom Barry, Deputy High Commissioner of the United Kingdom to Canada

TUESDAY, 25 NOVEMBER

08h45
Colloquium chair's opening remarks
Hon Bill Graham, former Canadian Minister of Foreign Affairs, Minister of National Defence, and Leader of the Opposition.

08h45
Session 1. The Challenges of Cyberspace
Rt Hon Baroness Neville-Jones DCMG

09h30
Session 2. The Politics of Cyberspace
Canada: Mr Paul Meyer, Simon Fraser University
UK: Rt Hon James Arbuthnot MP

10h45
Coffee/Tea

11h00
Session 3. The Business of Cyberspace
Canada: Mr Pat Horgan, IBM Canada Ltd.
UK: Mr Mark Connelly, Thomson Reuters

12h15
Lunch

13h30
Session 4: Cyber Risks and Cybersecurity
Canada: Mr Robert Gordon, Public Safety Canada
UK: Mr James Quinault CBE, Cabinet Office

14h45
Coffee/Tea

15h15
Session 5: Breakout Groups

Group 1: Cyber and Privacy
Canada Co-chair: Mr John Adams, Queen's University
UK Co-chair: Prof Peter Sommer

Group 2: Cyber and Social Media
Canada Co-chair: Mr Rob Rosenfeld, U-15 Group
UK Co-chair: Prof Bill Dutton, Michigan State University

Group 3: Information Flows and High Frequency Trading
Canada Co-chair: Prof Kim Richard Nossal, Queen's University
UK Co-chair: Mr Brennan Carley, Thomson Reuters

Group 4: Threats of the Fragmentation of the
Internet and/or Cloud Computing
Canada Co-chair: Prof Marina Gavrilova, University of Calgary
UK Co-chair: Ms Sally Costerton, ICANN

18h15
Reception

19h15
Dinner
Keynote: Mr Steve Rubley, Thomson Reuters

WEDNESDAY, 26 NOVEMBER

08h45
Comments from Parliamentary Secretary David Anderson

09h00
Session 6: Reports from Breakout Groups

10h30
Coffee/Tea

10h45
Session 7: The Challenges of Cyberspace: Policy & Governance Implications
Canada: Prof Benoît Dupont, Smart CyberSecurity Network
UK: Prof Martyn Thomas, Oxford University

12h15
Lunch

13h30
Concluding Discussion

14h30
Closing remarks by Colloquium chair

17h30
Organizers' meeting for the 2015 Colloquium

LIST OF PARTICIPANTS

COLLOQUIUM CHAIR

Hon Bill Graham, PC, QC, CM
Former Canadian Minister of Foreign Affairs, Minister of National Defence, and Leader of the Opposition.

RAPPORTEUR

Professor Rex B. Hughes
University of Cambridge/University of Toronto

CANADIAN PARTICIPANTS

Mr John Adams
Adjunct Professor, School of Policy Studies, Queen's University

Mr David Anderson
Parliamentary Secretary to the Minister of Foreign Affairs, Foreign Affairs, Trade and Development Canada

Mr Tom Balint
Deputy Director, EU-EFTA Relations, Foreign Affairs, Trade and Development Canada

Mr Paul Bowes
Market Development Canada, Thomson Reuters

Dr Mel Cappe
Professor, University of Toronto

Professor Benoît Dupont
Scientific Director, Smart CyberSecurity Network

Mr Colin Freeze
Reporter, The Globe and Mail

Dr Marina Gavrilova
Professor, University of Calgary

Mr Robert Gordon
Special Advisory on Cyber Security, Public Safety Canada

Mr Patrick Horgan
VP Manufacturing, Development & Operations, IBM Canada Ltd.

Dr Joel Martin
Director of Research, Information and Communications Technology, National Research Council Canada

Mr Paul Meyer
Fellow in International Security, Simon Fraser University; Senior Fellow, The Simons Foundation

Professor Kim Richard Nossal
Queen's University – Canadian Coordinator

Mr John Proctor, CD, CISM
Vice-President, Global Cyber Security, CGI Global

Mr Douglas Scott Proudfoot
Minister–Counsellor, Canadian High Commission, London

Mr Konrad Roberts
Senior Desk Officer for Ireland and the United Kingdom, Foreign Affairs, Trade and Development Canada

Mr Rob Rosenfeld
Director of Advocacy, U15 Group of Canadian Research Universities

Dr Duncan Stewart
General Manager, Security and Disruptive Technologies, National Research Council Canada

Mr James Taylor
Senior Coordinator, Academic Outreach Program, Canadian Security Intelligence Service

BRITISH PARTICIPANTS

Rt Hon James Arbuthnot MP
former Chair House of Commons Defence Select Committee

Mr James Ball
Special Projects Editor, The Guardian.

Mr Tom Barry
Deputy High Commissioner, British High Commission, Ottawa

Mr Brennan Carley
Head of Platform & Analytics, Finance & Risk, Thomson Reuters

Mr Anthony Cary CMG
Honorary President, Canada-UK Council

Mr Nick Collier
Global Head of Government and Regulatory Affairs, Thomson Reuters

Mr Mark Connelly
Chief Information Security Officer, Thomson Reuters

Ms Sally Costerton
Head of Stakeholder Engagement, ICANN

Dr Tom Crick
Associate Professor in Computing Science, Cardiff University

Professor Bill Dutton
Quello Professor of Media and Information Policy, Michigan State University

Mr George Edmonds-Brown
Executive Secretary, Canada-UK Council

Mr Douglas Ferguson
CEO Pharos Security Ltd

Ms Jodie Ginsberg
Chief Executive, Index of Censorship

Mr Benedict Hamilton
Managing Director, Investigations & Disputes, Kroll Associates UK Ltd

Mr Nicolas Maclean CMG
CUKC Council Member and Chief Executive, MWM (Strategy)

Mr Brendan McManus
British High Commission, Ottawa

Professor Keith Martin
Director Information Security Group, Royal Holloway, University of London

Mr David McNaught
Deputy Head, North America Department, Foreign and Commonwealth Office

Rt Hon Baroness Neville-Jones DCMG
former Minister of State for Security and Counter Terrorism and former Chairman of the Joint Intelligence Committee

Professor Jim Norton FREng
External member, Board of the UK Parliament's Office of Science & Technology, Chair of the UK Spectrum Policy Forum, and Adviser, 2014 Colloquium

Ms Louisa-Jayne O'Neill
Vice Chairman of the Information Assurance Advisory Council

Mr Philip Peacock
Chair of the Canada-UK Council

Ms Elizabeth Phillips
University of Oxford Cybersecurity CDT

Mr James Powell
Chief Technology Officer, Thomson Reuters

Mr James Quinault CBE
Director, Office of Cyber Security and Information Assurance, Cabinet Office

Professor Peter Sommer
Digital Forensics specialist and expert witness

Professor Martyn Thomas CBE, FREng
Visiting Professor of Software Engineering, Oxford University

Ms Pip Thornton
Royal Holloway, University of London

GUEST PARTICIPANT

Ms Megan Richards
Principal Adviser, DG Connect, European Commission

CONFERENCE ORGANIZATION

Ms. Maureen Bartram
Administrator, Centre for International and Defence Policy, Queen's University

THOMSON REUTERS

Foreign Affairs, Trade and Development Canada
Affaires étrangères, Commerce et Développement Canada

Foreign & Commonwealth Office

IBM

pharos

Queens University | Policy Studies

Centre for International and Defence Policy
Queen's University

Canada-UK Council

2014 Canada-UK Colloquium