A Macdonald-Laurier Institute Publication

MLI

True North in Canadian public policy

Commentary

NOVEMBER 2018

Chinese Cyber Espionage and the National Security Risks Huawei Poses to 5G Networks

Michael Shoebridge

Canada has a decision to make on 5G networks, technologies, and providers. Does international experience have any relevance or parallels? Probably yes, although each nation will have particular circumstances and histories that must be understood. A prominent factor in decision-making in the five nations that make up the Five-Eyes intelligence community is around Chinese telecommunications company Huawei – and to a lesser extent, the other Chinese telecommunications giant, ZTE. This commentary explores some of these issues and potential parallels.[1]

Huawei's end-to-end approach to 5G, providing hardware and software and continuing operational support, is apparently what makes it so attractive as a solution and helps the company undercut competitors' pricing. But it also means that identifying vulnerabilities, providing updates, doing patches, and designing and distributing upgrades of both hardware and software are in Huawei's hands. It combines the Microsoft or even IBM model, which gave us personal computers and the Microsoft operating system, with Bell Telephone's or AT&T's approach to building telecommunications networks.

But we're now living in a world of virtualization and software-defined hardware. The old way of acquiring and operating systems that makes customers dependent on big end-to-end proprietary solutions is not the only way. Similarly, the Internet of things is a world of myriad manufacturers of sensors and devices – control systems, fridges, toasters, TVs, security cameras, machinery, servers, networks, smartphones, and computers – that will connect to 5G and its successors, with no single proprietor having a dominant market share.

So, buying into an end-to-end proprietary 5G solution may be a classic case of catching the last wave – getting the very best copper phone network money can buy.

More narrowly, even if big proprietary telecommunications systems prove viable in the medium- to long-term, Huawei's end-to-end solution, while a commercial advantage, also increases the security risk. The design, hardware, software, identifying vulnerabilities, providing updates, patching, support, and operations all rely on one big Chinese tech company. This is where the Chinese state's high level of cyber espionage for commercial and state purposes is relevant.

"Even if big proprietary telecommunications systems prove viable in the medium- to long-term, Huawei's end-to-end solution, while a commercial advantage, also increases the security risk."

Russia has had a higher profile, but China has been the giant of cyber espionage and is thought to be behind data breaches in the United States, the United Kingdom, and Australian government agencies, including into the Bureau of Meteorology, the Commonwealth Scientific and Industrial Research Organisation (CSIRO), and the Australian Parliament. Beyond government, China has engaged in the cyber-enabled theft of intellectual property, trade secrets, and commercial-in-confidence material from multiple companies internationally – as reporting in the US has clearly demonstrated over the past few years.

Coupled with this demonstrated intent to conduct wide-ranging cyber espionage, China's intelligence law provides the capability to compel Huawei to assist with state intelligence efforts. Article 7 of China's 2017 Intelligence Law obliges organizations and citizens to support, assist, and cooperate with intelligence work.

That China has demonstrated an intent to conduct wide-ranging cyber espionage, combined with the legal obligation for organizations and citizens to assist if required, means that Chinese companies such as Huawei carry additional supply-chain risk compared with companies from countries without a long history of cyber espionage and/or countries without laws that specifically compel cooperation with intelligence agencies.

For those after tangible examples of cyber security trouble in places Huawei systems have operated, the African Union (AU) headquarters experience is relevant.

The AU's grand and sprawling new complex, which opened in 2012, was the focus of intrigue and controversy earlier this year – controversy that sheds light on reported "national security concerns" in Australia and other nations about which companies should be involved in our 5G network and other critical infrastructure projects (Grigg 2018; Cave 2018).

In January 2018, France's *Le Monde* newspaper published an investigation (Tilouine and Kadiri), based on multiple sources, which found that from January 2012 to January 2017 servers based inside the AU's headquarters in Addis Ababa were transferring data between 12 midnight and 2 am – every single night – to unknown servers more than 8000 kilometres away. These servers were hosted in Shanghai. Following the discovery of what media referred to as "data theft," it was also reported that microphones hidden in desks and walls were detected and removed during a sweep for bugs (Maasho 2018).

The Chinese government refuted *Le Monde*'s reporting. According to Chinese state media outlet CGTN (formerly CCTV), China's foreign ministry spokesperson called the *Le Monde* investigation "utterly groundless and ridiculous" (Bhaya 2018). China's ambassador to the AU said it was "ridiculous and preposterous." The BBC (2018) also quoted the ambassador as saying that the investigation "is not good for the image of the newspaper itself."

Other media outlets, including the *Financial Times* (Aglionby 2018), confirmed the data theft in reports published after the *Le Monde* investigation. It's also been reported by think tanks and private consultancies from around the world (Fidler 2018; Awokoya 2018).

One AU official told the *Financial Times* that there were "many issues with the building that are still being resolved with the Chinese. It's not just cybersecurity" (Aglionby 2018).

The *Le Monde* report also said that since the discovery of the data theft, "the AU has acquired its own servers and declined China's offer to configure them." Other media reports confirmed that servers and equipment were replaced and that following the incident "other enhanced security features have also been installed" (Aglionby 2018).

What seems to have been entirely missed in the media coverage at the time was the name of the company that served as the key ICT provider inside the AU's headquarters.

"By the time the building hosted its first AU Summit on January 29, 2012, Huawei's ICT solution – which included computing, storage sharing, WiFi, and unified resource allocation services through cloud data centres – was in play."

It was Huawei.

The AU Commission signed a contract with Huawei on 4 January 2012 (Yuhong 2012). By the time the building hosted its first AU Summit on January 29, 2012, Huawei's ICT solution – which included computing, storage sharing, WiFi, and unified resource allocation services through cloud data centres – was in play. As explained on Huawei's website:

> As a top organization coordinating pan-African political, economic, and military issues, the African Union Commission (AUC) needed a robust information system to support a large number of conferences and the larger amounts of data that they entail. As most of this information is of a confidential nature, legacy PCs were proving too vulnerable to hackers, phishing, viruses, and other forms of compromise. (Yuhong 2012)

Huawei provided a range of services to the AU. It provided cloud computing to the AU headquarters and signed a memorandum of understanding with the AU on ICT infrastructure development and cooperation (Huawei 2015; African Union 2015a). It also trained batches and batches of the AU Commission's technical ICT experts (Xinhua 2017; African Union 2015b).

The main service that Huawei provided to the AU was a "desktop cloud solution." Huawei (2013) described the service provision as follows:

> The AU needed a robust solution to streamline their conference operations and protect their data from a variety of security threats. They chose Huawei's FusionCloud Desktop Solution, which offers computing, storage sharing, and resource allocation through cloud data centers.

According to Huawei's (2013) website, part of this solution included providing equipment and resources to the AU's data centre:

> The [Huawei] solution deployed all computing and storage resources in the AU's central data center where it seamlessly connects to the original IT system. Then, Huawei installed Wi-Fi hotspots and provided the industry's first Thin Clients (TC) customized with Wi-Fi access . . . Traditional PC-based architecture exposes data to serious security risks. With Operating Systems (OS) and applications installed on individual machines, data is vulnerable to viruses and plain text transmissions are easier to steal. The FusionCloud solution moves the OS and applications to centralized servers in the AU's data center to minimize information leakage while TC security measures such as authentication and encryption further secure data.

Huawei's desktop cloud solution was central to the AU's cybersecurity and data-protection efforts (Velazquez 2015). Huawei (2013) listed "better security" as one of its key benefits. Huawei described the provision of this better security as follows:

> Centralized storage in the data center protects data from attack and prevents data leakage from PCs. The system further protects with terminal authentication and encrypted transmission.

But despite the installation and use of Huawei's ICT services, reputable media outlets reported that the AU's confidential data wasn't protected (Aglionby 2018; Tilouine and Kadiri 2018; Laing 2018; Financial Times 2018).

There are several possible explanations why the AU's confidential data wasn't protected and safeguarded appropriately from security threats. Let's say that Huawei was in no way complicit in the alleged data theft. With this option placed to the side, what else is left on the table? There's the possibility of a (very lengthy) insider threat, for example. There's also cybersecurity incompetence. Or perhaps the company never discovered the alleged five-year data theft? But none of this is reassuring.

"There are several possible explanations why the AU's confidential data wasn't protected and safeguarded appropriately from security threats."

Is it possible to mitigate the risk involved in Huawei technology combined with Chinese state activity and legal powers?

Scott Jones, the head of the Canadian Centre for Cyber Security has stated that "We have a very advanced relationship with our telecommunications providers, something that is different from most other countries to be honest from what I have seen." Perhaps this combined with "layers" of defence in depth will be sufficient (Fife and Chase 2018a; Freeze 2018)?

The British experience seems to say no and looks like it offers parallels and lessons for Canada – it certainly offered lessons to Australia as our government considered the difficult issues that led to the two big Chinese telcos, Huawei and ZTE, being excluded from supply into Australia's 5G network.

In 2011 the UK government set up the Huawei Cyber Security Evaluation Centre (HCSEC) to deal with the perceived risks of Huawei's involvement in UK critical infrastructure by evaluating the security of Huawei products used in the UK telecommunications market.

On the face of it, the UK approach to mitigate this supply-chain risk with HCSEC – assessing products to reassure ourselves that they are operating as expected – seems entirely reasonable. Can't we assess products to make sure they won't be used to spy on us?

The four HCSEC oversight board annual reports (2015, 2016, 2017 and 2018) show that it is very difficult indeed.

On the bright side, the reports have consistently stated that "HCSEC continues to provide unique, world-class cyber security expertise and technical assurance of sufficient scope and quality as to be appropriate for the current stage in the assurance framework around Huawei in the UK" (2017, 4).

HCSEC is also developing new tools and techniques to better understand security assurance in telecommunications, has found vulnerabilities that Huawei has subsequently remediated, and is improving Huawei's basic engineering and security processes and code quality. These efforts have resulted in a more secure Huawei product.

> "Worse yet, the trend across the four oversight board reports suggests that as HCSEC has improved in capability, confidence that the security evaluation process will sufficiently mitigate risks has declined – the more HCSEC learned, the less confident they were."

Despite all this, the latest oversight board reports have noted that HCSEC cannot confirm that what it has been testing matches what Huawei is using in the UK: the source code HCSEC has been given (that is, the computer instructions for Huawei's equipment) doesn't correspond with what has been deployed in the UK. So, much of the security testing that HCSEC has been doing may be irrelevant to the security of products used in the UK. At this point, the oversight board "can offer only limited assurance" (2018, 16).

This year's report indicates that some security-critical third-party software used in Huawei equipment is "not subject to sufficient control" (2018, 16). This is viewed as possibly a significant risk to UK telecommunications infrastructure mostly because of inconsistent product support lifetimes.

In its carefully bureaucratically worded report, the UK's National Cyber Security Centre has advised that "it is less confident that the NCSC and HCSEC can provide long term technical assurance of sufficient scope and quality around Huawei in the UK" (HCSEC 2018, 18), adding that there are further medium-term risks associated with shifts in technology like virtualization and edge computing architectures like 5G. That's as close to alarm bells and flashing lights as such a report can get.

Worse yet, the trend across the four oversight board reports suggests that as HCSEC has improved in capability, confidence that the security evaluation process will sufficiently mitigate risks has declined – the more HCSEC learned, the less confident they were.

In Australia, Mike Burgess, head of the Australian Signals Directorate (ASD) – Australia's equivalent to Canada's Communications Security Establishment (CSE) – gave a landmark public speech last month where he addressed the recent government decision to exclude 'high-risk vendors' from Australia's 5G networks – notably China's two tech telco giants ZTE and Huawei. Burgess (2018) laid out ASD's advice on 5G in crystal-clear language:

> Our starting point was that, if 5G technology delivers on its promise, the next generation of telecommunications networks will be at the top of every country's list of critical national infrastructure. (And presumably every nation's intelligence agencies' target lists as a result.)
>
> 5G is not just fast data, it is also high density connection of devices – human to human, human to machine and machine to machine – and finally it is much lower signal latency or speed of response.
>
> 5G technology will underpin the communications that Australians rely on every day, from our health systems and the potential applications of remote surgery, to self-driving cars and through to the operation of our power and water supply.
>
> The stakes could not be higher. This is about more than protecting the confidentiality of our information – it is also about the integrity and availability of the data and systems on which we depend.
>
> Historically, we have protected the sensitive information and functions at the core of our telecommunications networks by confining our high-risk vendors to the edge of our networks.
>
> But the distinction between core and edge collapses in 5G networks. That means that a potential threat anywhere in the network will be a threat to the whole network.
>
> In consultation with operators and vendors, we worked hard this year to see if there were ways to protect our 5G networks if high-risk vendor equipment was present anywhere in these networks.
>
> At the end of this process, my advice was to exclude high-risk vendors from the entirety of evolving 5G networks.

Canada's Communications Security Establishment will be aware of Australia's ASD work and advice and of the UK's Huawei work. CSE has, in fact, been quietly running its own Security Review Program, at what is known as the "White Lab" (Fife and Chase 2018b). So, it's likely they'll have run into the same difficulties the UK has; whether that leads Canada to exclude both ZTE and Huawei from Canada's 5G networks is yet to be seen.

That decision is a critical one for the future of Canadian cyber security and the integrity and availability of data to Canadian government agencies, businesses, and people. It's not about politics, it's about making the right long-term decision.

About the Author

Michael Shoebridge joined the Australian Strategic Policy Institute in February 2018 as the Director of the Defence & Strategy program. Michael has worked in policy, intelligence and project delivery in Defence.

He headed the Defence, Intelligence and Research Coordination Division in the Prime Minister's department. Michael also started a new Defence Capability Assessment Branch in the Department of Finance, which provided the Finance department's assessment of all major Defence capability investment proposals to inform Cabinet decision making.

Michael led the Defence team that wrote the 2013 Defence White Paper when he was head of Defence's Strategic Policy Division. He has worked as the Deputy Director of Australia's Defence Intelligence Organisation (one of two assessment agencies in Australia's intelligence community and partner to the US DIA) and as one of the four deputies in the Australian Signals Directorate (partner to the US NSA).

He was the senior Defence civilian in the Australian Embassy in Washington during the time of the Iraq surge and the return of the Australian SAS to Afghanistan. He has worked in two Commonwealth Ministers' offices.

His role before joining ASPI was as the head of Defence's Contestability function, providing critical but constructive analysis of the projects and programs in the Government's $200 billion integrated investment program for Defence, which is the investment element of the 2016 Defence White Paper.

References

African Union. 2015a. "AUC Signs MoU with Huawei for Partnership on ICT." Press release, February 3. Available at https://au.int/en/newsevents/29758/auc-signs-mou-huawei-partnership-ict.

———. 2015b. "20 African ICT Experts To Take Part in a Training Offered by Huawei in China." Press release, December 3. Available at https://au.int/en/pressreleases/20151203-3.

Aglionby, John. 2018. "African Union Accuses China of Hacking Headquarters." *Financial Times*, January 29. Available at https://www.ft.com/content/c26a9214-04f2-11e8-9650-9c0ad2d7c5b5.

Awokoya, Ayo. 2018. "African Union Rocked by China Spying Allegations." *Geopolitical Monitor*, February 18. Available at https://www.geopoliticalmonitor.com/african-union-rocked-by-china-spying-allegations/.

BBC. 2018. "China Dismisses 'Absurd' African Union HQ Spying Claim." *BBC News*, January 29. Available at https://www.bbc.com/news/world-africa-42861276.

Bhaya, Abhishek G. 2018. "China, African Leaders Slam French Report on AU Headquarters Hacking as 'Ridiculous', 'Nonsense'." *CGTN*, January 31. Available at https://news.cgtn.com/news/346b6a4e30677a6333566d54/share_p.html.

Burgess, Mike. 2018. Speech to ASPI National Security Dinner, Canberra, October 9. Available at https://asd.gov.au/speeches/20181029-aspi-national-security-dinner.htm.

Cave, Danielle. 2018. "National Security: The public debate and the end of 'just trust us'." *The Strategist*, July 10. Available at https://www.aspistrategist.org.au/national-security-the-public-debate-and-the-end-of-just-trust-us/.

Cave, Danielle et al. 2018. "Huawei and Australia's 5G Network." Australian Strategic Policy Institute. October 10. Available at https://www.aspi.org.au/report/huawei-and-australias-5g-network.

China. 2017. *National Intelligence Law of the P. R. C.* Translation by users on chinalawtranslate.com. Available at https://www.chinalawtranslate.com/%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E5%9B%BD%E5%AE%B6%E6%83%85%E6%8A%A5%E6%B3%95/?lang=en.

Fidler, Mailyn. 2018. "African Union Bugged by China: Cyber espionage as evidence of strategic shifts." Council on Foreign Relations (blog post), March 7. Available at https://www.cfr.org/blog/african-union-bugged-china-cyber-espionage-evidence-strategic-shifts.

Fife, Robert, and Steven Chase. 2018a. "No Need to Ban Huawei in Light of Canada's Robust Cybersecurity Safeguards, Top Official Says." *Globe and Mail*, September 23. Available at https://www.theglobeandmail.com/politics/article-no-need-to-ban-huawei-in-light-of-canadas-robust-cybersecurity/.

———. 2018b. "Ottawa Probes Huawei Equipment for Security Threats." *Globe and Mail*, September 7. Available at https://www.theglobeandmail.com/politics/article-cse-says-canada-tests-chinas-huawei-equipment-for-security/.

Financial Times. 2018. "Chinese Bugs Expose Africa's Weak Defences." *Financial Times*, January 30. Available at https://www.ft.com/content/c9f8367a-05b1-11e8-9650-9c0ad2d7c5b5.

Freeze, Colin. 2018. "Ottawa's Top Cybersecurity Official: Canada has 'layers' to protect against Huawei threat." *Globe and Mail*, October 2. Available at https://www.theglobeandmail.com/canada/article-ottawas-top-cybersecurity-official-canada-has-layers-to-protect/.

Grigg, Angus. 2018. "Can We Trust the Spies on China's Huawei?" *Financial Review*, June 15. Available at https://www.afr.com/business/telecommunications/can-we-trust-the-spies-on-chinas-huawei-20180615-h11fe7.

Huawei. 2013. "Desktop Cloud Draws Praise in Africa." *Huawei.com*, July 25. Available at https://e.huawei.com/au/case-studies/global/older/hw_201214.

———. 2015. "African Union and Huawei Sign MoU on Partnership." Press release, January 29. Available at https://www.zawya.com/story/African_Union_and_Huawei_Sign_MoU_on_Partnership-ZAWYA20150130041842/.

Huawei Cyber Security Evaluation Centre Oversight Board [HCSEC]. 2015. *1st Annual Report*. Huawei Cyber Security Evaluation Centre Oversight Board. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/416878/HCSEC_Report.pdf.

———. 2016. *Annual Report.* Huawei Cyber Security Evaluation Centre Oversight Board. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/525761/huawei_cyber_security_evaluation_centre_oversight_board_2nd_annual_report_2016.pdf.

———. 2017. *Annual Report.* Huawei Cyber Security Evaluation Centre Oversight Board. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/626110/20170413_HCSEC_Oversight_Board_Report_2017_-_FINAL.pdf.

———. 2018. *Annual Report.* Huawei Cyber Security Evaluation Centre Oversight Board. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf.

Laing, Aislinn. 2018. "China 'Planted Bugs' While Building African Union HQ." *Times*, February 1. Available at https://www.thetimes.co.uk/article/china-planted-bugs-while-building-african-union-hq-wqgw5ff7q.

Maasho, Aaron. 2018. "China Denies Report It Hacked African Union Headquarters." *Reuters*, January 29. Available at https://www.reuters.com/article/us-africanunion-summit-china/china-denies-report-it-hacked-african-union-headquarters-idUSKBN1FI2I5.

Tilouine, Joan, and Ghalia Kadiri. 2018. "A Addis-Abeba, le siège de l'Union africaine espionné par Pékin." *Le Monde*, January 26. Available at https://www.lemonde.fr/afrique/article/2018/01/26/a-addis-abeba-le-siege-de-l-union-africaine-espionne-par-les-chinois_5247521_3212.html.

Velazquez, Fernando. 2015. "Re-imagining Your Enterprise End-User Computing – The END of desktop anarchy." Slideshow. Available at http://cdn2.hubspot.net/hubfs/756638/Descargas/Fernando_Velazquez.pdf?t=1460755143345.

Xinhua. 2017. "AU Experts Undergo Training in China under Huawei-sponsored Program." *New China*, May 26. Available at http://www.xinhuanet.com/english/2017-05/26/c_136318335.htm.

Yuhong, Chen. 2012. "Desktop Cloud Draws Praise in Africa." *huawei.com*, August 7. Available at https://www.huawei.com/en/about-huawei/publications/winwin-magazine/13/HW_147045.

Endnote

1 This piece draws heavily on work already published on these topics by a number of ASPI colleagues – notably Danielle Cave and Tom Uren. The ASPI report, Huawei and Australia's 5G network, contains their work and that of other colleagues. See Danielle Cave et al., 2018, "Huawei and Australia's 5G Network."

MLI

True North in Canadian public policy

Critically Acclaimed, Award-Winning Institute

The Macdonald-Laurier Institute fills a gap in Canada's democratic infrastructure by focusing our work on the full range of issues that fall under Ottawa's jurisdiction.

- One of the top five think tanks in Canada and No. 1 in Ottawa according to the University of Pennsylvania.
- Cited by five present and former Canadian Prime Ministers, as well as by David Cameron, the British Prime Minister.
- First book, *The Canadian Century: Moving out of America's Shadow*, won the Sir Antony Fisher International Memorial Award in 2011.
- *Hill Times* says Brian Lee Crowley is one of the 100 most influential people in Ottawa.
- The *Wall Street Journal*, the *Economist*, the *Globe and Mail*, the *National Post* and many other leading national and international publications have quoted the Institute's work.

"The study by Brian Lee Crowley and Ken Coates is a 'home run'. The analysis by Douglas Bland will make many uncomfortable but it is a wake up call that must be read."

FORMER CANADIAN PRIME MINISTER PAUL MARTIN ON MLI'S PROJECT ON ABORIGINAL PEOPLE AND THE NATURAL RESOURCE ECONOMY.

Ideas Change the World

Independent and non-partisan, the Macdonald-Laurier Institute is increasingly recognized as the thought leader on national issues in Canada, prodding governments, opinion leaders and the general public to accept nothing but the very best public policy solutions for the challenges Canada faces.

CTV

cpac FOR THE RECORD

corus ENTERTAINMENT

CBC news

FP Foreign Policy

tvo

The Economist

WALL STREET JOURNAL

THE HILL TIMES

THE GLOBE AND MAIL
CANADA'S NATIONAL NEWSPAPER • FOUNDED 1844

NATIONAL POST

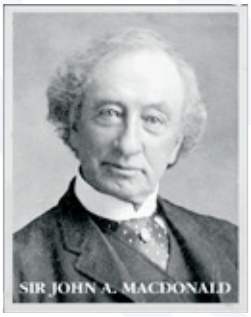
About the Macdonald-Laurier Institute

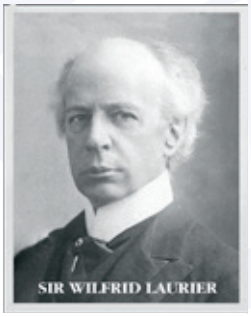
What Do We Do?

When you change how people think, you change what they want and how they act. That is why thought leadership is essential in every field. At MLI, we strip away the complexity that makes policy issues unintelligible and present them in a way that leads to action, to better quality policy decisions, to more effective government, and to a more focused pursuit of the national interest of all Canadians. MLI is the only non-partisan, independent national public policy think tank based in Ottawa that focuses on the full range of issues that fall under the jurisdiction of the federal government.

What Is in a Name?

The Macdonald-Laurier Institute exists not merely to burnish the splendid legacy of two towering figures in Canadian history – Sir John A. Macdonald and Sir Wilfrid Laurier – but to renew that legacy. A Tory and a Grit, an English speaker and a French speaker – these two men represent the very best of Canada's fine political tradition. As prime minister, each championed the values that led to Canada assuming her place as one of the world's leading democracies. We will continue to vigorously uphold these values, the cornerstones of our nation.


SIR JOHN A. MACDONALD


SIR WILFRID LAURIER

Working for a Better Canada

Good policy doesn't just happen; it requires good ideas, hard work, and being in the right place at the right time. In other words, it requires MLI. We pride ourselves on independence, and accept no funding from the government for our research. If you value our work and if you believe in the possibility of a better Canada, consider making a tax-deductible donation. The Macdonald-Laurier Institute is a registered charity.

Our Issues

The Institute undertakes an impressive program of thought leadership on public policy. Some of the issues we have tackled recently include:

- Aboriginal people and the management of our natural resources;
- Making Canada's justice system more fair and efficient;
- Defending Canada's innovators and creators;
- Controlling government debt at all levels;
- Advancing Canada's interests abroad;
- Ottawa's regulation of foreign investment; and
- How to fix Canadian health care.

True North in
Canadian public policy

CONTACT US: Macdonald-Laurier Institute
323 Chapel Street, Suite #300
Ottawa, Ontario, Canada
K1N 7Z2

TELEPHONE: (613) 482-8327

WEBSITE: www.MacdonaldLaurier.ca

CONNECT WITH US:

@MLInstitute

www.facebook.com/
MacdonaldLaurierInstitute

www.youtube.com/
MLInstitute

What people are saying about the Macdonald-Laurier Institute

In five short years, the institute has established itself as a steady source of high-quality research and thoughtful policy analysis here in our nation's capital. Inspired by Canada's deep-rooted intellectual tradition of ordered liberty – as exemplified by Macdonald and Laurier – the institute is making unique contributions to federal public policy and discourse. Please accept my best wishes for a memorable anniversary celebration and continued success.

THE RIGHT HONOURABLE STEPHEN HARPER

The Macdonald-Laurier Institute is an important source of fact and opinion for so many, including me. Everything they tackle is accomplished in great depth and furthers the public policy debate in Canada. Happy Anniversary, this is but the beginning.

THE RIGHT HONOURABLE PAUL MARTIN

In its mere five years of existence, the Macdonald-Laurier Institute, under the erudite Brian Lee Crowley's vibrant leadership, has, through its various publications and public events, forged a reputation for brilliance and originality in areas of vital concern to Canadians: from all aspects of the economy to health care reform, aboriginal affairs, justice, and national security.

BARBARA KAY, NATIONAL POST COLUMNIST

Intelligent and informed debate contributes to a stronger, healthier and more competitive Canadian society. In five short years the Macdonald-Laurier Institute has emerged as a significant and respected voice in the shaping of public policy. On a wide range of issues important to our country's future, Brian Lee Crowley and his team are making a difference.

JOHN MANLEY, CEO COUNCIL