Centre for International
Governance Innovation

Policy Brief No. 191 — October 2024

Toward a Model Code for Digital Safety

Michel Girard

Key Points

- Although standards are being published to address privacy, cybersecurity and high-risk artificial intelligence (AI), more needs to be done to address digital harms.
- Stakeholders are playing catch-up with a tsunami of new, unproven digital technologies, and standards are developed after the fact.
- One approach gaining traction is the development of a model code for digital safety.
- This code would define a set of core values that should be embedded in new digital technologies in order to prevent harms from occurring in the first place.
- This would replicate what stakeholders have been doing for close to 100 years to ensure the safety of the built environment.

Introduction

As anticipated five years ago when CIGI published its first paper on standards for big data analytics, industry and governments are turning to standardization to address digital harms (Girard 2019). Standards bodies have published a series of standards to address some of the most pressing privacy and cybersecurity concerns, and risk management standards have been developed to support the European Union's AI legislation (European Commission 2022). Standards covering new digital services, such as digital trust, digital wallets, online electoral voting and use of biometrics for authentication, have either been published or are on their way.[1] And regarding the important issue of conformity assessment, auditing professionals will soon be able to verify and validate compliance with digital governance standards thanks to new certifications.[2]

Although these are positive developments, civil society remains highly vulnerable to digital harms. In a recent declaration, the Group of Seven recognizes that "the governance of digital technologies has not kept pace with its growth" (Group of Seven 2024). Although this

1 See https://dgc-cgn.org/standards/work-program/.

2 See https://pd.cpaontario.ca/ondemand/mastering-digital-assurance-in-the-age-of-ai-certificate/E000478.html.

About the Author

Michel Girard is a senior fellow at CIGI, where he contributes expertise in the area of standards for big data and artificial intelligence (AI). Michel also provides standardization advice to help innovative companies in their efforts to access international markets. He contributes to the Digital Governance Council and to the standardization activities of the Digital Governance Standards Institute.

Michel has 22 years of experience as an executive in the public and not-for-profit sectors. Prior to joining CIGI, Michel was vice president, strategy at the Standards Council of Canada (SCC), where he worked from 2009 to 2018. At the SCC, he led the design and implementation of the Standards and Innovation program, the Climate Ready infrastructure program, the Northern Infrastructure Standards Initiative and the Monitoring Standards in Canadian Regulations project. He managed the negotiation of standardization clauses in trade agreements including the Comprehensive Economic and Trade Agreement and the Canadian Free Trade Agreement. Previously, he was director of the Ottawa office at the Canadian Standards Association, director of international affairs at Environment Canada, corporate secretary at Agriculture Canada and acting director of education and compliance at the Canadian Environmental Assessment Agency. He holds a Ph.D. and a master's degree in history from the University of Ottawa.

declaration "encourages the development and adoption of international technical standards" and affirms the importance of addressing "common governance challenges," there is no consensus to create a body accountable for digital governance (ibid.). With a deluge of new, unproven digital technologies, stakeholders are forced to play catch-up, with standards being developed after the fact. More importantly, well-documented harms associated with digital platforms and social media are not being addressed (Forum on Information & Democracy 2020, 5). Because of a widespread perception that innovation is mismanaged, digital trust is at an all-time low (Edelman Trust Institute 2024).

Governance should drive technological choices, not the other way around: new bottom-up approaches are therefore needed to bridge these gaps. One scenario gaining momentum is bringing together a coalition of stakeholders who share similar values to develop a model code for digital safety (Digital Governance Council [DGC] 2024a). A model code can offer clarity and help create trustworthy data-sharing ecosystems. It can also articulate a set of values to be embedded in digital technologies. This approach can replicate what was accomplished decades ago to make our built environment human-centric, safe and reliable.

This policy brief begins by defining digital governance and describing the digital technology layers that would be covered by this proposed model code. The second section focuses on key features of model codes. It shows that codes, standards and conformity assessment programs can achieve the same outcomes as laws, regulations and enforcement activities. The third section proposes an approach to develop a model code for digital safety in order to address digital harms and restore public trust.

Digital Governance and Its Domains

Digital governance is the management of harms resulting from the use of digital technologies. It encompasses both objective criteria applied to products and machines and subjective criteria, including values (such as health, safety, security and human rights) and ethics (such as equity and fairness).

To be effective, digital governance should overlay three layers of technologies and applications. The

first layer is the information, communications and technology sector. It encompasses telecommunications, cable, radio and spectrum management. The internet represents the second layer. Interoperability standards led to the creation of a physical network and a transport network. The third layer is associated with an ever-growing array of internet-connected technologies, platforms, applications and software, including AI, involving hundreds of standards development bodies and consortia.

Although digital technologies have resulted in significant positive impacts for the global economy and civil society, they have also introduced new harms. This aspect was examined in 2015 by the UN Commission on Science and Technology for Development (CSTD) through "a comprehensive mapping of international Internet public policy issues, the mechanisms dealing with these issues and potential gaps in those mechanisms." In its research, the CSTD identified 41 broad policy issues that were created because regulators and civil society did not participate meaningfully in the development of digital technology standards. Issues such as privacy, human rights, competition policy and cybersecurity were not properly incorporated, leaving a governance gap for others to solve.[3]

Established standards development bodies have started to fill some of these digital governance gaps. For example, Joint Technical Committe 1's Subcommittee 42, a joint effort from the International Organization for Standardization and International Electrotechnical Commission, focuses on big data and AI.[4] The Institute of Electrical and Electronics Engineers (IEEE) is developing ethical AI standards through its Ethically Aligned Design initiative (IEEE 2022). The Open Community for Ethics in Autonomous and Intelligent Systems is looking at how standards can facilitate innovation while addressing ethics and values.[5] Regional bodies CEN (the European Committee for Standardization) and CENELEC (the European Electrotechnical Committee for Standardization) are coordinating the development of AI standards in support of the EU Artificial Intelligence Act.[6] In the United States, the National Institute of Standards and Technology recently published its voluntary *Artificial Intelligence Risk Management Framework* to incorporate trustworthiness considerations into AI products, services and systems.[7] Canada has also shown leadership. As mentioned above, the Digital Governance Standards Institute is developing a series of standards framing the use of new digital services such as digital trust, digital wallets, online electoral voting and the use of biometrics for authentication. These standards fill important governance gaps and can be expected to be adopted internationally (Digital Governance Standards Institute 2024).

Nevertheless, standards bodies and regulatory authorities are not keeping up with successive waves of new digital products, platforms, devices and services. In addition, long-standing harms associated with digital platforms and social media have not been addressed. There is little standardization work to manage pervasive issues, such as the lack of transparency of platforms, content moderation, managing deepfakes or tagging unreliable information.

International organizations, such as the United Nations and the World Trade Organization, looked at creating a body to manage digital governance (Girard 2020). The United Nations also explored whether existing agencies such as the Internet Governance Forum could be tasked with digital governance. These efforts have not been successful. Three competing regulatory approaches are working against an international consensus. They have been described as the American market-driven model, the Chinese state-driven model and the European rights-driven regulatory model. These distinct and competing regulatory models are battling horizontally for dominance in the global digital economy. Although there is a growing global consensus regarding the need to regulate digital technologies, there is disunity when it comes to defining the specifics of such regulation (Bradford 2023).

3 UNCTAD CSTDOR, 18th Sess, UN Doc E/CN.16/2015/CRP.2 (2015) at 2, 11, online: <https://unctad.org/meetings/en/SessionalDocuments/ecn162015crp2_en.pdf>.

4 See www.iso.org/committee/6794475.html.

5 See https://ethicsstandards.org/.

6 EC, *Draft standardisation request to the European Standardisation Organisations in support of safe and trustworthy artificial intelligence*, [2022], online: <https://ec.europa.eu/docsroom/documents/5237

7 See www.nist.gov/itl/ai-risk-management-framework.

What Are Model Codes?

Model codes are routinely used to set appropriate health, safety and welfare benchmarks and acceptable levels of safety for physical infrastructure. There are model codes covering buildings, fire safety, bridges and roads; systems such as electrical, plumbing and gas; and equipment such as elevators, boilers and pressure vessels. These codes also cover related consumer products.

Model codes are composed of two parts. The body of a code outlines values and high-level objectives associated with the installation, use and performance of products, components and systems. It describes what needs to be achieved. Distinct sections of the code focus on specific components. Annexes list the relevant standards and technical specifications that have been reviewed and adopted by the governing body as acceptable to achieve compliance. They showcase how compliance can be achieved. Taken together, model codes in use in Canada reference many thousands of standards and technical specifications. Codes are not static. They are kept evergreen to reflect technological advances or to improve safety outcomes. New editions are issued periodically, generally every five years.

Complement or Substitute to Statutory Instruments

In Canada and in other jurisdictions, a wide range of model codes are referenced in regulations to support policy and legislative objectives. Codes can be adopted by regulators as is or with deviations to reflect the particular circumstances of a given jurisdiction. In many instances in Canada, the governing bodies overseeing the maintenance of codes are composed of members of industry, experts, professionals such as engineers, consumers and regulatory authorities. Regulators can be full participants in the code development and maintenance process. However, model codes do not have to be incorporated in regulations to be impactful. For example, the US-based International Code Council maintains a wide range of voluntary model codes and standards for the built environment. They can be adopted by industry, manufacturers, professional bodies or jurisdictions.[8] As Table 1 illustrates, model codes should be seen as quasi-statutory instruments.

Table 1: Comparing Model Codes and Statutory Instruments

Feature	Model Codes	Statutory Instruments
Values, objectives and requirements (what to achieve)	Outlined in body of the code	Outlined in legislation
Requirements, metrics and testing methods (how to demonstrate compliance)	Outlined in comprehensive annexes of approved standards and technical specifications appended to model codes	Outlined in regulations, approved guidance and approved documents (including standards, technical specifications and model codes)
Compliance mechanisms	Conformity assessment programs encompassing first-party certification/validation code requirements; second- or third-party certification/validation code requirements can be noted in business-to-business and supply chain contracts	Enforcement through inspection; permitting/licensing; audit following complaint
Penalty for non-compliance	Removal of certification, impacts on contractual obligations and operations	Citation, fine or civil/criminal liability

Source: Author.

8 See www.iccsafe.org/products-and-services/codes-standards/.

Table 2: Canadian Model Codes for the Built Environment

Name	Year
Canadian Electrical Code	1927
Boiler, Pressure Vessel, and Pressure Piping Code (CSA B51)	1939
National Building Code	1941
Gas Code (CSA B149)	1958
Elevator Safety Code (CSA B44.1/ASME A17.5)	1960
National Fire Code	1963
National Plumbing Code	1970
National Energy Code for Buildings	1997

Source: Author.

Core Values in Model Codes

Model codes, just like standards, are not neutral or objective. They reflect a set of core values, priorities and objectives shared by those who participated in their development. In order to illustrate this point, one can look at the impacts of model codes for the built environment on the living conditions of Canadians. A series of interlocking model codes were developed in the first half of the twentieth century to address vexing public health and safety challenges, when most dwellings at the time were unsanitary and unsafe (Artibise and Linteau 1984). A plethora of new technologies and systems had the potential to drastically improve the livelihoods of urban dwellers through universal access to potable and hot water, indoor toilets, central heating, electricity and natural gas. In addition, new building materials and systems were available to vastly improve fire safety. However, no common rulebook existed to seamlessly embed these new systems and technologies into people's homes.

Beginning in the 1920s, model codes were published to support a safe and secure built environment. Table 2 presents a cross-section of model codes for illustrative purposes.

The development of these codes was spurred by new professional classes, such as electrical, mechanical and sanitation engineers, land-use planners and public health officials. As a chartered profession, engineering is not focused solely on efficiency and interoperability; since its inception, it has been governed by a charter that "holds paramount the safety, health and welfare of the public" (Engineers Canada 2024). These core values, which were taught to students in engineering faculties during the Progressive Era, guided the development of model codes for the built environment. Box 1 presents core values embedded in the National Building Code of Canada since its first edition was published in 1941.

Over time, as basic harms have been reduced or eliminated, the standards expected of model codes have increased. New values and objectives have .emerged along with new harms that require responses from code developers. One can expect future editions of model codes to reflect new values, such as energy efficiency, sustainability and affordability.

Box 1: Core Values Embedded in the Building Code

Human dignity: Access to potable water, hot water, toilets, heating, ventilation, privacy

Safety:

- Fire: Occupants can leave a building safely in case of a fire (fire detectors, combustible materials, width of hallways)
- Structural: Limiting the probability of a person in or adjacent to the building that will be exposed to an unacceptable risk of injury due to structural failure (e.g., load bearing of a building, damage to building materials, instability of a building, etc.)
- Use: Avoiding accidents/incidents when using the building (e.g., size and height of windows, electrical components, plumbing, water temperature, railings, stairs, etc.)

Health: Reducing the risks of exposing a person to an unacceptable risk of illness (e.g., inadequate indoor air quality, humidity, temperature, clean water, noise protection, etc.)

Interoperability: Systems, equipment and appliances (one set of voltage, amp., hertz)

Resilience: Structural integrity based on one in 100 years climate events.

Reasonable cost: Balance between safety and costs of building/operating a house

Source: Author.

Model Code for Digital Safety

In the absence of an international agency, new approaches are needed to address digital harms. One scenario gaining momentum is bringing together a coalition of stakeholders sharing similar values in order to develop a voluntary model code for digital safety. In 2024, the DGC began to explore the feasibility of developing such a code. The DGC is a Canadian member-based organization representing public, private and not-for-profit sector organizations. The model code envisaged by its members would aim to preserve health, safety, privacy and security in the digital realm, safeguarding individuals and organizations from potential risks and harms.

The development and maintenance of the model code could be led by a task force supported by a secretariat. The task force would be composed of representatives from civil society, professionals and members of organizations with an interest in addressing digital harms and improving digital governance across sectors, ecosystems and value chains. Federal, provincial and territorial government officials would also be at the table, likely those representing organizations that deliver government services to the public as well as those accountable for innovation and trade policy.

The task force could oversee the development of the model code and set in place processes to develop a series of modules, each focusing on a specific domain. For example, a working group would oversee the development of a lexicon of terms and definitions. Additional working groups would be created to develop and maintain individual modules. Annexes featuring approved standards, technical specifications and compliance programs would be appended to each module. Given the wide number of domains to be covered, one would expect that hundreds of standards and technical specifications will be required. Working groups would review existing standards and determine whether they are

suitable for adoption to the code, with or without deviations. In other cases, when no specific standard exists, the task force could make a standardization request to a suitable standards development body.

Regarding compliance issues, the task force would need to support the creation of new classes of professionals to manage specific components of data value chains. They include data collection and grading (data engineers); data access and sharing (data comptrollers); data analytics (data scientists); and digital comptrollership functions, as well as auditing and validation against digital governance standards. Professional codes of conduct will be required to frame the accountabilities of these new professional classes; these would be referenced in a model code.

Although the task force would primarily respond to the needs, values and interests of Canadian stakeholders, it will have to ensure that the code supports and enables international trade. As such, one can envisage that modules of a future model code for digital safety could be reviewed, adopted and used by like-minded organizations and jurisdictions around the world.

Digital Public Infrastructure Modules

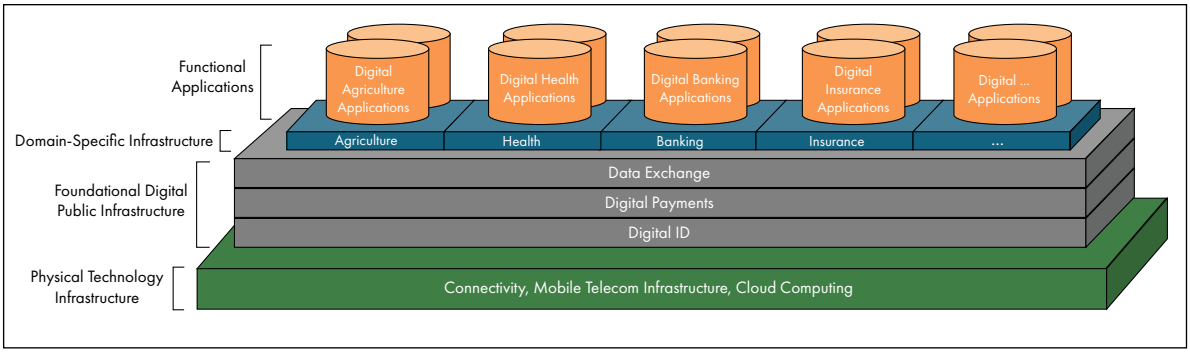
DGC members are currently investigating whether there is sufficient support to design a first series of modules focusing on digital public infrastructure (DPI). An international consensus recently emerged on that front. In 2023, Group of Twenty (G20) countries stressed the importance of prioritizing secure, inclusive and accountable approaches to DPI in driving resilience and innovation (G20 2023a.). The G20 New Delhi Leaders' Declaration recognized a voluntary Framework for Systems of Digital Public Infrastructure (G20 2023b). DPIs are created and used by both the public and private sectors. They can serve as shared infrastructure for building applications and products and for sharing data. One could envisage modules setting requirements for sectors such as agriculture, health, government and financial services, as well as functions such as emergency response and supply chain management.

An important task for stakeholders developing these first modules will be the selection and ranking of core values and objectives that will drive the creation of the DPI architecture. In addition to interoperability and meeting privacy and cybersecurity regulations, DPIs should be human-centric: that is, they should be designed to respond to the needs and rights of users/clients/patients first. By creating human-centric DPIs, related objectives such as data portability, equity and trustworthiness can be addressed.

Looking Forward

Stakeholders engaged in the development of a model code for digital safety are not starting with a blank page. In addition to the valuable work undertaken under the G20 banner to create the

Figure 1: Conceptual Model for DPI



Source: Republished with permission from DGC (2024b).

DPI architecture, detailed guidance is available on managing digital transformation. In its voluntary digital governance code aimed at organizations, Japan's Ministry of Economy, Trade and Industry (2020) recommends setting up digital strategies that are aligned with overall business objectives, agile governance rules, and robust data management systems and controls, as well as human-centric AI.

As a next step, a future task force may want to target the technologies and platforms that inflict the greatest harms on civil society. In its report titled *Working Group on Infodemics: Policy Framework*, the Forum on Information & Democracy made more than 200 recommendations to address the harms generated by digital platforms and social media. A module on digital platforms would likely cover issues such as requirements for transparency of platforms, as well as for content moderation and quality and safety in platform design. A module on social media would likely cover the responsibilities and obligations of network users and account holders and guidance for the identification and the creation of reliable sources of information, as well as guidelines for inhibiting the spread of potentially unreliable content, such as managing deepfakes and addressing scamming (Forum on Information & Democracy 2020).

The potential harms associated with generative AI could also be addressed through a specific module. Although some jurisdictions are taking steps to regulate high-risk AI, there is considerable uncertainty as to how to reduce harms associated with its misuse. A recent UN resolution promoting the safe and trustworthy development of AI was adopted without opposition in March 2024.[9] However, no mechanism has been set in place to manage its enforcement (Zakrzewski 2024).

Embedding core values and ethics in digital technologies, platforms, applications and services represents a new and exciting frontier for standardization. Many digital technologies, such as digital platforms, social media and generative AI, are not static. They are dynamic as they constantly learn, adapt and change. Organizations using these technologies will need ongoing monitoring and verification in order to maintain validation for digital governance standards. This is different from the certification of tangible products. For example, a typical water heater will be tested by an accredited certification body against specific standards at the prototype stage and will be certified during production runs; the same cannot be achieved with generative AI or bots.

The standardization system is evolving in response to these new demands. Compliance with digital governance standards will likely rest on the expertise of new classes of chartered professionals. Software engineers could oversee the development and testing of new technologies and platforms. Chartered accountants are well positioned to play a variety of digital comptrollership, monitoring, auditing and validation roles. Perhaps new chartered professions will be created in order to monitor data collection, access and analytics functions. A model code for digital safety would create demand for these new services.

Democratic societies cannot afford to repeat the same mistakes that were made 30 years ago, when digital technologies were introduced without appropriate checks and balances to ensure that they were safe and secure. Core values and ethical considerations need to be baked-in digital technologies. A model code for digital safety represents a way forward in establishing a governance framework and addressing digital harms from the ground up.

9 *Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development*, GA Res 78/265, UNGAOR, 78th Sess, UN Doc A/78/L.49 (2024), online: <https://digitallibrary.un.org/record/4040897?v=pdf&ln=en>.

Works Cited

Artibise, Alan F. J. and Paul-André Linteau. 1984. *The Evolution of Urban Canada: An Analysis of Approaches and Interpretations*. The Institute of Urban Studies Report No. 4, University of Winnipeg. https://winnspace.uwinnipeg.ca/bitstream/handle/10680/581/The%20Evolution%20of%20Urban%20Canada_webversion.pdf.

Bradford, Anu. 2023. *Digital Empires: The Global Battle to Regulate Technology*. Oxford, UK: Oxford University Press.

DGC. 2024a. *Implementing Model Digital Governance*. February 5. Ottawa, ON: DGC.

———. 2024b. *Enhancing Prosperity in the Digital Era: Advancing Digital Cooperation and Infrastructure*. April 3. Ottawa, ON: DGC.

Edelman Trust Institute. 2024. *2024 Edelman Trust Barometer Global Report*. www.edelman.com/sites/g/files/aatuss191/files/2024-02/2024%20Edelman%20Trust%20Barometer%20Global%20Report_FINAL.pdf.

Engineers Canada. 2024. *Guideline on the code of ethics*. July. Ottawa, ON: Engineers Canada. https://engineerscanada.ca/guidelines-and-papers/public-guideline-on-the-code-of-ethics#-the-code-of-ethics.

Forum on Information & Democracy. 2020. *Working Group on Infodemics: Policy Framework*. November. https://informationdemocracy.org/wp-content/uploads/2020/11/ForumID_Report-on-infodemics_101120.pdf.

Girard, Michel. 2019. *Big Data Analytics Need Standards to Thrive: What Standards Are and Why They Matter*. CIGI Paper No. 209. Waterloo, ON: CIGI. www.cigionline.org/publications/big-data-analytics-need-standards-thrive-what-standards-are-and-why-they-matter/.

———. 2020. *Standards for Digital Cooperation*. CIGI Paper No. 237. Waterloo, ON: CIGI. www.cigionline.org/publications/standards-digital-cooperation/.

G20. 2023a. *G20 New Delhi Leaders' Declaration*. September 9. www.international.gc.ca/world-monde/international_relations-relations_internationales/g20/2023-09-9-g20-new-delhi.aspx?lang=eng.

———. 2023b. *Annexure 1: G20 Framework for Systems of Digital Public Infrastructure*. September 9. https://g7g20-documents.org/fileadmin/G7G20_documents/2023/G20/India/Sherpa-Track/Digital%20Economy%20Ministers/2%20Ministers%27%20Annex/G20_Digital%20Economy%20Ministers%20Meeting_Annex1_19082023.pdf.

Group of Seven. 2023. *G7 Hiroshima Leaders' Communiqué*. May 20. www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2023-05-20-hiroshima-leaders-communique-dirigeants.aspx?lang=eng.

IEEE. 2022. "IEEE Standard for Transparency of Autonomous Systems." In *IEEE Std 7001-2021*, 1–54. March. https://ieeexplore.ieee.org/document/9726144.

Ministry of Economy, Trade and Industry. 2020. *Digital Governance Code*. Ministry of Economy, Trade and Industry of Japan. November 9. www.meti.go.jp/shingikai/mono_info_service/dgs5/pdf/20201109_e01.pdf.

Zakrzewski, Cat. 2024. "United Nations adopts U.S.-led resolution to safely develop AI." *The Washington Post*, March 21. www.washingtonpost.com/technology/2024/03/21/united-nations-adopts-ai-safety-resolution/.

.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

President, CIGI Paul Sampson
Director, Program Management Dianna English
Program Manager Jenny Thiel
Publications Editor Christine Robertson
Graphic Designer Sami Chouhdary

For publications enquiries, please contact publications@cigionline.org.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org