Centre for International
Governance Innovation

Policy Brief No. 170 — December 2021

The Canadian Election Template

Stronger Elections at Home, Stronger Canada Abroad

Brian Klaas and Aaron Shull

Key Points

- As a global leader in democratic elections, Canada has an important role to play on the international stage in showing countries how to address growing threats to democratic elections, such as hacking, disinformation campaigns and other types of information warfare.
- By developing an election template, Canada can boost electoral confidence among its own voters while serving as a role model to other countries by exporting best practices for conducting safe and secure elections.
- Favourable global perceptions of Canada's role in foreign relations, plus Canada's strong track record for election administration and security and highly transparent and secure elections, make it an ideal candidate for providing election support to other countries.

Introduction

For the last four years, the world's most powerful champion of democratization has been largely absent from the global stage. The United States is now poised to support a far more pro-democracy agenda, with greater insistence on free and fair elections as part of American foreign policy. Indeed, US President Joe Biden has redoubled efforts by hosting a global summit for democracy, and Canadian Prime Minister Justin Trudeau has committed to partnering with the United States on supporting global democracy.

Nonetheless, the current landscape is bleak. Freedom House's metrics show 15 consecutive years of democratic decline. Unprecedented threats to elections across the world have emerged. Geopolitical adversaries have used hacking, disinformation campaigns and other information warfare attacks to destabilize democracies. Those threats rightly gained prominence after the 2016 US elections. However, while the focus shifted to international threats, domestic actors began to borrow Russian-style tactics, spreading false information and sowing doubt on election integrity. Too often, these campaigns achieve their goals — and democracy suffers.

Despite these urgent, metastasizing threats to election integrity and the global health of democracy, there is

About the Authors

Brian Klaas is an associate professor of global politics at University College London, where he focuses on democracy, authoritarianism, and American politics and foreign policy. He is the co-author of *How to Rig an Election* and author of *The Despot's Apprentice: Donald Trump's Attack on Democracy* and *The Despot's Accomplice: How the West is Aiding and Abetting the Decline of Democracy*. His most recent book, *Corruptible: Who Gets Power and How It Changes Us*, was published in November 2021. Brian is a contributor to *The Washington Post* and is a regular guest on CNN, MSNBC, BBC News, Sky News, NPR News, BBC Radio, Bloomberg and CNBC. He has advised the North Atlantic Treaty Organization, the European Union and several major international non-governmental organizations. Brian received his doctorate in politics from the University of Oxford.

Aaron Shull is CIGI's managing director and general counsel. A member of CIGI's executive team, Aaron provides guidance and advice on matters of strategic and operational importance, while working closely with partners and other institutions to further CIGI's mission. He has expertise in cybersecurity, international law and national security. Prior to joining CIGI, Aaron practised law for a number of organizations, focusing on international, regulatory and environmental law. He has taught courses at the University of Ottawa Faculty of Law and the Norman Paterson School of International Affairs and was previously a staff editor for the *Columbia Journal of Transnational Law*. Aaron received his LL.M. from Columbia Law School, where he graduated as a Harlan Fiske Stone scholar.

no widely accepted "best practices" template for securely holding an election and ensuring transparency around the process to instill confidence among the electorate. This must change.

In this policy brief, the authors outline why Canada is uniquely suited to develop such a model. Templates are not designed to be one-size-fits-all. Rather, they provide a solid foundation that can be adapted to local conditions. That is precisely what is needed to secure modern elections across the globe: a robust set of principles and best practices that can still be tailored to the wide array of challenges and threats that individual countries face.

A new Canadian "clean elections" initiative could be used in domestic elections to further improve Canadian confidence in homegrown democracy. But it could also provide significant foreign policy benefits, giving Canada a major foreign policy "win" by amplifying its soft power at a miniscule cost. Finally, an elections template could advance one of Canada's core national interests: a robust rules-based international order, premised on the rule of law and democratic accountability, with less space for authoritarian regimes to undermine law and order within and among nations.

The Canadian Election Template

Thankfully, Canada has not yet faced destabilizing attacks on its election infrastructure. Canadian elections have also been largely free of disingenuous allegations of fraud by bad actors. However, that luck will eventually run out. Canada has done important work to plan for such eventualities (with leadership on initiatives such as the Paris Call for Trust and Security in Cyberspace and by developing innovative programming such as the Digital Citizen Initiative at Canadian Heritage). Canada has also been used as a case study in a variety of research publications and reports developed by international non-governmental organizations (NGOs); one of these publications is *Cybersecurity in Elections: Models of Interagency Collaboration* by the International Institute for Democracy and Electoral Assistance. But this knowledge about how to run clean, secure elections has not been harnessed as effectively as possible

because these insights have not been backed by a powerful government on the international stage.

By developing a more sophisticated, rigorous template for securing elections, the Canadian government could provide a two-for-one policy achievement.

While creating greater resilience at home, Canada could also easily export that template abroad by providing guidance and technical assistance to other democratic nations. By providing best practices developed in Canada that draw on the lessons learned from other advanced democracies that have faced more severe threats, the Canadian government can establish itself as a world leader in election security and transparency.

Election monitors have been the gold standard for securing elections since the end of the Cold War. But relying exclusively on them is an outdated approach that must be updated for the twenty-first century. Because election observers try to catch manipulations once they happen, they are the equivalent of the adage of giving someone a fish and feeding them for a day, whereas exporting election security guidance to democracies is like teaching these countries how to fish and feeding them for a lifetime. In the process, Canada can create resilience in allies while also generating soft power that serves Canadian geopolitical interests.

In a global environment of escalating threats to election integrity, the world needs a country to step up and become a global leader at combatting foreign and domestic malign influence attacks. This is not to denigrate or downplay the extremely important work that has been done by international civil society organizations, including their remarkably comprehensive reports that provide clear insights into improving election quality and security. But international NGOs do not have the diplomatic clout of a powerful state actor. To put their insights into place, the geopolitical weight of a government is needed.

For a variety of reasons, the United States cannot be that force; it has severe homegrown challenges that undercut its ability to effectively lecture democracies abroad (most viscerally shown during the attack on the US Capitol on January 6, 2021), and it is often distrusted by some weaker democracies that see America as a biased geopolitical bully. Other countries, such as Britain or France, are often viewed suspiciously in some parts of the developing world for their colonial past. Canada, through decades of responsible international engagement and world-leading election quality, avoids such pitfalls. As a trusted and admired voice on the international stage, Canada's efforts to shore up election integrity and security would be far more welcome in a much larger swath of the globe. This approach provides a unique opportunity that should be seized, both for Canadian self-interest and for the good of global democracy.

Canada's somewhat unique ability to take on this role is based on hard data. In an Ipsos (2020, 4) survey, 81 percent of participants responded that Canada will have a positive influence on foreign affairs over the next decade. The findings demonstrate that the desire for Canada to play a leadership role in the world is enduring and undiminished.

Furthermore, Canada is already a leader in election administration and security. The Office of the Chief Electoral Officer, commonly known as Elections Canada, is a world leader in administering elections. Furthermore, in accordance with the Canada Elections Act, Elections Canada's international affairs office cooperates with election administration organizations throughout the world, providing guidance and sharing insights into evolving threats.

Canada's elections are also highly transparent. Ottawa has openly informed the public about election threats even as other nations are reluctant to do so. The Communications Security Establishment (CSE), Canada's cryptologic agency, first started to share public threat assessments in the summer of 2017 (Government of Canada 2021a). The first threat assessment, updated before the 2019 federal election, provided voters and political campaigns with an overview of the challenges Canada faced.

Canada has also taken concrete steps to secure its elections. Elections Canada[1] improved its information technology (IT) to strengthen critical election infrastructure. In addition, it trained election administration personnel to reduce the vulnerability of human assets in the democratic process (ibid.). Leading up to the 2019 federal

1 See https://elections.ca/content.aspx?section=vot&dir=int&document=index&lang=e.

election, the Canadian government continuously informed voters about its plans to improve overall election security (Government of Canada 2019a.). The plan had four main pillars — topping the list was citizen preparedness (Government of Canada 2020a.). According to the government, "Canada's best defence is an engaged and informed public" (ibid.). To that end, it invested millions of dollars to promote digital literacy.

The second item on the agenda was enhanced cooperation between different government agencies to improve organizational readiness (Government of Canada 2019b). Elections Canada, for example, works with the Canadian Security Intelligence Service and CSE to "identify threats, emerging tactics and systems vulnerabilities" (ibid.). This whole-of-government approach, which also includes various other federal departments, makes it easier to "prepare and respond to threats of foreign interference" (ibid.). In the same spirit, the government agencies at the frontline of combatting foreign interference, such as Global Affairs Canada and the Royal Canadian Mounted Police, have formed a task force to facilitate a more effective common response (Government of Canada 2021b).

As part of this process, the Government of Canada also put in place the Critical Election Incident Public Protocol (Government of Canada 2021c). The protocol itself has a very limited mandate. A public announcement would be made during the writ period if there was an incident, or incidents, that threatened Canada's ability to have a free and fair election. During the writ period, Parliament is dissolved and the caretaker convention kicks in, which essentially means that the existing government must exercise restraint because in Canadian parliamentary democracy, the legitimacy of the government flows from its ability to maintain confidence in the House of Commons and with Parliament dissolved, there is no House of Commons that can maintain that confidence.

Given that it would be impossible to simultaneously exercise restraint and to inform all Canadians that the bedrock of democracy had been compromised, the determination surrounding notification falls to senior civil servants, who are apolitical, including the clerk of the Privy Council, the national security and intelligence advisor to the prime minister, the deputy minister of justice and deputy attorney general, the deputy minister of public safety and the deputy minister of foreign affairs. In this way, the decision surrounding interference, whether the threshold to notify the public has been met, and what options are available to address the interference are divorced from the political process completely.

Moving beyond transparency and internal organization, Canada enlisted the help of social media companies through a mix of voluntary and mandatory measures. The firms, including Facebook and Twitter, agreed to a common declaration that guides their behaviour during elections (Government of Canada 2020b). In addition, Parliament passed legislation that requires "major online platforms to maintain a registry of partisan and election advertising published during the pre-election and election periods" (ibid.). This makes it much easier for voters to identify who is trying to influence them.

While these are favourable steps forward, it should be noted that these solutions do not address the deep systemic problems grinding away at democracy; that is, the convergence of surveillance capitalism, big data, and the lack of algorithmic transparency that is used to micro-target voters and sometimes misinform them. These factors largely impact the ways in which individuals consume political news and information, which ultimately exacerbates the challenges surrounding fake news, computational propaganda and voter suppression. It seems these companies will do the minimum required to avoid public controversies and keep stock prices stable and, regrettably, in the meantime, consumers continue to pay the price. There need to be limitations placed on the diffusion of ad targeting, specifically, the inability to target based on political affiliation and audience reach to better control the flood of disinformation and any attempts to suppress voters in marginalized groups.

Canada has developed these innovations on its own, albeit drawing from threat assessments elsewhere. But there are two important gaps that, if filled, would benefit Canadian national interest. First, Canada still has not done enough to create sophisticated resilience against destabilizing election threats that are yet to come. Second, many other countries simply do not have the capacity to develop such a comprehensive strategy from scratch. They need help and support to create more robust election processes, and Canada can bolster its international engagement to show them how.

Better Defences at Home

Canada is much better at mitigating the impacts of foreign attacks than it is at preventing them from being launched. Canada should therefore put more emphasis on deterrence. There are several possible strategies that would be effective. The government should publicize specific consequences that will be triggered if a geopolitical adversary attempts to undermine Canadian elections. Germany provides an instructive example for this, as does France.[2] Before the last federal elections in Germany in 2017, high-ranking German officials let it be known that Russian interference would not be tolerated (Zeit Online 2017). German Chancellor Angela Merkel was so concerned about Russian hacking that she raised it with Russian President Vladimir Putin directly during a face-to-face meeting (Brattberg and Maurer 2018). President Biden did the same in his summit with Putin shortly after the Group of Seven (G7) Summit in June 2021. Furthermore, since all Western democracies face similar threats, a united front — in which allies agree to impose joint costs on a malign actor — could amplify the deterrence effect. Recent advances in international cooperation through the G7's Rapid Response Mechanism are promising — but too limited (Hanlon and Rosenberger 2019). Canada would be well placed to organize such an initiative, and the current US administration would likely be far more receptive to it than the previous one.

Aside from raising political costs, Canada could also consider a more forceful approach to election interference. The US military, for example, pre-emptively attacked the infamous Russian Internet Research Agency (IRA) during the 2018 midterm elections: "In the weeks leading up to the elections, the U.S. Cyber Command (CYBERCOM) reportedly targeted individual IRA operatives and Russian intelligence officers with direct messages warning them that they had been identified and that their activity was being tracked. On the day of the midterms, CYBERCOM also reportedly launched cyber-attacks against the IRA to cut off the organization's Internet access and prevent it from spreading disinformation" (ibid.). Pre-emptive attacks such as this cannot stop foreign interference campaigns entirely, but they would demonstrate that Canada takes attacks on its democratic process seriously (ibid.).

It is therefore worth considering a new North Atlantic Treaty Organization (NATO) article 5-style collective security principle to deter cyberattacks on elections. Foreign adversaries should be aware that any cyberattacks or information warfare targeting an allied country's elections (perhaps starting with the Five Eyes security alliance before expanding to NATO) will lead to a massive cyber response. Too often, foreign adversaries launch cyberattacks or information warfare campaigns knowing full well that the retaliation is likely to be muted, possibly involving the expulsion of diplomats or the closure of a consulate. That is a disproportionately weak response to an offensive campaign aimed at swaying the composition of a Western government. If Canada spearheads an initiative to create a collective security principle that extends the umbrella of mutual protection to cybersecurity around elections, it will create an important update that is sorely needed to keep pace with catastrophic risk in the twenty-first century. With the new legal authorities granted to CSE under Bill C-59 (an act regarding national security matters) for both offensive and defensive cyber operations, Canada could lead the effort in principle and help to execute in practice.

Furthermore, every possible effort should be made to cooperate with NATO allies to ensure rapid attribution of cyberattacks that target democratic institutions. Unlike conventional threats, cyber-based destabilization campaigns often involve a degree of uncertainty as to who launched them. Alongside greater legal authorities and offensive capabilities, Canada should prioritize a more robust "early warning" system that helps ensure quick attribution.

Additionally, political parties collect vast troves of personal information in an effort to map voter constituencies, tailor political messaging and shape electoral outcomes through data-driven profiling. Public concern and frustration with the state of data protection for Canadians when it comes to political parties have been mounting, as this issue has only attracted more attention in recent years, particularly in the aftermath of the 2016 Facebook/Cambridge Analytica scandal. Currently, there is no federal privacy legislation that covers the activity of political parties with respect to voter data. The Personal Information Protection and Electronic Documents Act only applies to the

2 For more information on France, see David Levine (2020).

commercial collection of personal data; the Privacy Act excludes political parties in the definition of "government institutions"; and the Canada Elections Act does not oversee data collection, analysis, use or storage. Nonetheless, "there is no compelling public policy rationale for why political parties should be exempt from robust privacy rules, as nearly every other significant public or private sector organization in Canadian society is subject to them" (Judge and Pal 2019). Despite the recent enactment of the Elections Modernization Act being a step in the right direction, requiring parties to meet mandatory minimum standards by publishing their privacy policies on their websites, the act leaves much to be desired. One of the principal flaws is there is no objective procedure for measuring the adequacy of each party's privacy policy since it does not stipulate what the policies should contain. In addition, there is also no proper enforcement or external oversight in place.

If we want to protect the integrity of our democratic processes, Canada needs to develop legal mechanisms that address issues to do with data privacy and political campaigning. Among other data protection norms, parties should be required to obtain informed consent from individuals for the collection, use and disclosure of their personal information and be transparent by explaining in plain language what personal information is collected, how it is used, whether it is shared with others and how it will be disposed of thereafter. In addition, parties should be obligated to keep voters' data secure and notify affected individuals of a security breach that poses significant harm. Lax data protection is neither the rule in Canada nor the norm internationally. Applying basic data-protection laws to political parties is a simple starting point for policy makers concerned with safeguarding democracy in the digital age.

The additions suggested above would help with deterring election attacks from abroad, but what about those that come from within? In order to create more confidence in elections, Canada should mandate that ballot processing and tabulation be recorded on video, ideally with a live-streaming link for each count. The 2020 US elections showed how easy it is for dangerous misinformation to spread when citizens believe that "something" is happening behind the scenes. The best way to pre-emptively debunk such destabilizing conspiracy theories is to let people see the process for themselves. The cost would be negligible — webcam and streaming technology is now very cheap and easily scalable — but it would pay significant dividends in how much Canadians trust their election process.

Finally, Canada should create a comprehensive annual review of its election security protocols. The threats evolve rapidly, and without a systematic process of updating defences, an attack will eventually succeed. Given that threats to democracy are a meta threat (as they affect every other aspect of government), attacks on democracy should be treated as a national security issue as much as one related to transparency and good governance.

Using Election Training to Generate Soft Power Abroad

The threats that Canada faces are not unique to Canada. And while challenges to election security and election integrity have changed dramatically in the last several years, election monitoring strategies have stayed largely static since the end of the Cold War. This is obviously not ideal, as it means that countries across the globe are playing electoral defence with a twentieth-century playbook against twenty-first-century adversaries. But that unfortunate failing provides a significant opportunity for Canada to emerge as the de facto international leader on protecting election integrity. Doing so would amplify Canadian soft power by generating significant goodwill at low cost.

Strange as it seems, there is no comprehensive, widely used "best practices" guide to protecting elections. Using Canada's expertise in the field to develop a template for developing countries to follow could, at virtually no cost, empower reform-minded countries to secure their democratic processes. For example, many of these countries face pressure from companies to buy digital voting machine technology but would benefit more from advice from a country that has (wisely) stuck to paper ballots in federal elections. And a simple template — adapted to local challenges — could also create effective pressure to democratize in less reform-minded countries. If reform-minded countries pledged to follow the best practices, it

would create pressure on the holdouts to explain why they were deliberately leaving their elections vulnerable to attacks both foreign and domestic.

Once the template is established, Canada could train and deploy, at minimal cost, two teams of experts to help strategic allies (and developing countries in need) hold successful elections. One team would consist of election administration experts and IT professionals. Remarkably, most election observation missions do *not* include anyone with IT expertise, which leaves an enormous vulnerability unexamined. A second team would be deployed to help ensure transparency throughout the run-up to election day. It could provide guidance on live-streaming vote tabulation while also donating the software infrastructure to create real-time updates as the results are being collated. Furthermore, at extraordinarily low cost, Canada could design a "citizen monitor" app for ordinary voters to use during the election. Most actual election monitors are given a tablet in which they answer yes or no to a variety of easily observable questions and take photos of precincts to detect any manipulations or intimidation. With a small investment, Canada could allow that monitoring to be crowdsourced, offering a much more comprehensive deterrent to those who seek to manipulate elections.

Furthermore, Canada should strongly consider pioneering an election certification scheme, which validates whether elections have met minimum international standards for election security. The logic would be equivalent to the LEED (Leadership in Energy and Environmental Design) certification scheme for green building standards, whereby architects and builders try to bolster their public profile by meeting various levels of recognized standards. By creating a uniform code of silver, gold and platinum levels of election security, countries could have a standardized international benchmark that they seek to achieve in order to bolster the legitimacy of elections. This certification would be based on elastic principles and would therefore fit easily with any form of democratic election, regardless of specific forms of rules or procedures. In the process, Canada could spark a race to the top, where citizens demand that their elected officials protect their elections by meeting these clear international standards.

It is worth noting that electoral assistance is usually provided indirectly through international organizations or NGOs, but there are several benefits to helping governments directly. Government-to-government assistance is an opportunity for Canada to wield soft power and further a critically important agenda. It can showcase Canadian capabilities to other countries while making Canada a major player in staving off attacks on democracy from geopolitical adversaries or homegrown extremists. Canada also has much more credibility on the topic because it is not constrained by accusations of imperialism (such as the United States) or colonialism (such as many European countries). That makes it easier for developing countries to request Ottawa's help, which would facilitate existing global outreach efforts for Elections Canada.

Of course, these initiatives would also benefit Canada. Other countries are set to learn from Canadian election teams, but those teams will also take new ideas back home. Those ideas can then be used to fortify domestic elections. Elections Canada has a mandate to learn from others, and this approach would be a more effective way of doing so.

Furthermore, it is definitely in Canada's interest to help other countries stay one step ahead of malign actors. The electoral assistance programs in place and election monitoring organizations that already operate provide an important service toward that goal. But these measures are not sufficient, and Canada can help fill the void while bolstering international stability in a highly unstable era.

The proposed election template and training initiative provide a unique opportunity for Canada to expand its soft power at minimal cost. The defence of liberal democracy is one of the greatest challenges of our time, and Canada can lead the way.

Conclusion

New threats and a lack of international leadership have created a vacuum around election security that Canada can fill. Foreign adversaries and domestic extremists are attacking elections in democracies around the world. So far, no country has been willing to push back as a leader on this issue. It is time for the Canadian government to rise to that challenge, twinning efforts to solidify its own election integrity with teaching others to follow suit.

Works Cited

Brattberg, Erik and Tim Maurer. 2018. "Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks." Carnegie Endowment for International Peace, May 23. https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

Government of Canada. 2019a. "Government of Canada unveils plan to safeguard Canada's 2019 election." Press release, January 30. www.canada.ca/en/democratic-institutions/news/2019/01/government-of-canada-unveils-plan-to-safeguard-canadas-election.html/.

———. 2019b. "Improving organizational readiness." www.canada.ca/en/democratic-institutions/news/2019/01/improving-organizational-readiness.html.

———. 2020a. "Enhancing citizen preparedness." www.canada.ca/en/democratic-institutions/news/2019/01/enhancing-citizen-preparedness.html.

———. 2020b. "Expecting social media platforms to act." www.canada.ca/en/democratic-institutions/news/2019/01/encouraging-social-media-platforms-to-act.html.

———. 2021a. "Protecting democracy." www.canada.ca/en/democratic-institutions/services/protecting-democracy.html.

———. 2021b. "Security and Intelligence Threats to Elections (SITE) Task Force." www.canada.ca/en/democratic-institutions/services/protecting-democracy/security-task-force.html.

———. 2021c. "Cabinet Directive on the Critical Election Incident Public Protocol." www.canada.ca/en/democratic-institutions/services/protecting-democracy/critical-election-incident-public-protocol/cabinet.html.

Hanlon, Bradley and Laura Rosenberger. 2019. "Countering Information Operations Demands A Common Democratic Strategy." Alliance for Securing Democracy, October 14. https://securingdemocracy.gmfus.org/countering-information-operations-demands-a-common-democratic-strategy/.

Ipsos. 2020. "World Affairs." November. www.ipsos.com/sites/default/files/ct/news/documents/2020-12/world-affairs-ipsos-study.pdf.

Judge, Elizabeth F. and Michael Pal. 2019. "Election Cyber Security Challenges for Canada." In *Governing Cyberspace during a Crisis in Trust,* 16–20. Waterloo, ON: CIGI. www.cigionline.org/publications/governing-cyberspace-during-crisis-trust/.

Levine, David. 2020. "Cyberattacks, Foreign Interference, and Digital Infrastructure: Conducting Secure Elections Amid a Pandemic." Alliance for Securing Democracy, October 8. https://securingdemocracy.gmfus.org/conducting-secure-elections-amid-a-pandemic/.

Zeit Online. 2017. "Cyberattack on the Bundestag: Merkel and the Fancy Bear." May. www.zeit.de/digital/2017-05/cyberattack-bundestag-angela-merkel-fancy-bear-hacker-russia/seite-6.

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

Managing Director and General Counsel Aaron Shull
Program Manager Aya Al Kabarity
Publications Editor Susan Bubak
Graphic Designer Sami Chouhdary

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

Printed in Canada on Forest Stewardship Council® certified paper containing 100% post-consumer fibre.

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