CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 10 — MARCH 2015

A Primer on Globally Harmonizing Internet Jurisdiction and Regulations

Michael Chertoff and Paul Rosenzweig

A PRIMER ON GLOBALLY HARMONIZING INTERNET JURISDICTION AND REGULATIONS

Michael Chertoff and Paul Rosenzweig

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and Chatham House.

Authors' Note

The views expressed in this paper are solely those of the authors and not attributable to The Chertoff Group or any other individual or organization.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHORS

Michael Chertoff is executive chairman and co-founder of The Chertoff Group, a premier global advisory firm focused exclusively on the security and risk management sector. In this role, he provides high-level strategic counsel to corporate and government leaders on a broad range of security issues, from risk identification and prevention to preparedness, response and recovery. During 2004 to 2009, he served as secretary of the US Department of Homeland Security, where he led the federal government's efforts to protect the United States from a wide range of security threats. Earlier in his career, Michael served as a federal judge on the US Court of Appeals for the Third Circuit and head of the US Department of Justice's Criminal Division where he investigated and prosecuted cases of political corruption, organized crime, corporate fraud and terrorism — including the investigation of the September 11 terrorist attacks.

Paul Rosenzweig is a senior adviser to The Chertoff Group. He previously served as the deputy assistant secretary for policy and as acting assistant secretary for international affairs at the US Department of Homeland Security. During this time, Paul developed policy, strategic plans and global approaches to homeland security, ranging from immigration and border security to avian flu and international rules for data protection. He currently provides legal and strategic advice on cyber security, national security and privacy concerns to individuals, companies and governments.

EXECUTIVE SUMMARY

We stand on the cusp of a defining moment for the Internet. Existing trends, left unaddressed, might very well lead to the legal fracturing of the World Wide Web. This brief paper offers some thoughts on how this challenge should be resolved, concluding that multilateral agreement on a choice-of-law framework is essential to the continuing growth of the network.[1]

THE PROBLEM DEFINED

The Internet is a globe-spanning domain. As of late 2014, more than 2.7 billion citizens of the world are connected to the network. Estimates vary, but somewhere around 500 billion different devices are also connected — and those numbers will only grow exponentially in the coming years.

The result is an increasingly common phenomenon: disputes and transactions that cross national boundaries. To be sure, the phenomenon is not new. There have been transnational commercial transactions (and transnational criminal activity) since the time that borders between nations were first created. But the growth of a system of near-instantaneous global communication and interaction has democratized the phenomenon of cross-border commerce in a transformative way that challenges and disrupts settled conventions.

The effect is most noticeable when we consider the intersection between private commercial activities and sovereign nations. Nations, quite naturally, seek to affect behaviour through laws and regulations that apply to individuals and corporations within their jurisdiction. But the growth in cross-border commerce is rendering traditional choice-of-law rules problematic at best. If one adds in the distributed structure of the network, inherent in the growing use of cloud architecture, the application of diverse legal systems to a unitary network becomes especially difficult.

For example, if a Swede stores his data with an American company that has a data centre in Canada, which country's law controls access to the data? What if (as is often the case given cloud architecture) his data is stored in more than one data centre located in more than one jurisdiction? When that same Swede provides personal information to a Chinese company, which then reuses the data for its own commercial purposes, where does he go to complain? And how is any actor to respond to inconsistent rules — where, say, one country requires disclosure of data in a context that another country prohibits?

These jurisdictional problems are, if anything, confounded by the overtly political nature of many contemporary data disputes. They arise against a backdrop of authoritarian nations that want to control the content of the network and public concern about the extent to which nations undertake espionage in the cyber domain. These confounding factors are not strictly germane to the question of choice of law. Espionage is always illegal in the country in which it occurs, and content regulation is often more about political control than legal rules. But it would ignore reality to fail to acknowledge the contemporary political dynamic.

What we see today, in response to this conundrum, is an increasing effort by sovereign nations to unilaterally assert jurisdiction and control over matters they think are within their sphere of influence. These efforts fit under the general rubric of data localization requirements — the idea that data about, say, Germans must be stored in Germany and subject to German law. Even worse, such efforts are often ineffectual; although a nation such as Germany can demand localization, other nations are not obliged to honour that determination, and many nations (for example, the United Kingdom's Data Retention and Investigatory Powers Act) apply their laws extraterritorially.

A BRIEF NOTE ON JURISDICTION

At the heart of this problem lies the fundamental idea of jurisdiction: the question of which nation and which nation's laws may control the disposition of a matter. It reflects both a narrow power — that of a court to adjudicate a case and issue an order — and a broader concept of defining the territorial and lawful bounds within which a court, agency or government may properly exercise its power and authority.

Jurisdictional rules, of course, vary widely around the globe. There are often disputes about the legitimacy, in some broader sense, of a sovereign's assertion of jurisdictional authority.[2] Jurisdiction, in either sense of the word, is principally tied to the location of a person (including juridical persons, such as corporations) or things, as well as the subject matter authority to deal with an issue or dispute. Most nations have both courts of general jurisdiction that may hear any matter and courts that are limited to specific areas of subject matter expertise.

And so, when one characterizes the problem as one of jurisdiction, one is really speaking of power. Under what

1 We acknowledge at the outset of this paper that such a framework may be difficult (some might say impossible) to achieve. We do not necessarily disagree. As outlined here, however, it is clear that the current situation, in the absence of such a framework, is untenable in the long run and destructive of economic prosperity. It may, indeed, be incapable of international resolution, but at a minimum, it is worth recognizing the necessity for action.

2 For example, in the United States (the jurisdiction with which the authors are most familiar), foreigners may be obliged to answer complaints in American courts only if they have a certain irreducible minimum of contacts with the jurisdiction such that they could reasonably anticipate the possibility of being called to account in that place. See *International Shoe Co. v. Washington*, 326 U.S. 310 (1945).

circumstances may the authority in one nation demand a response to its own legitimate inquiries? Given the complexity of the network and the increasing globalization of data transfers, problems of jurisdiction are multiplying rapidly.

TOWARD A SOLUTION

The current situation is untenable. Data localization and sovereign unilateralism will come with significant costs — both economic and social ones (Hill 2014). Global companies will be subject to competing and inconsistent legal demands, with the inevitable result that consumers will suffer diminished access to the network overall. Among other things, decisions about the location of servers and hardware will be driven by legal gamesmanship rather than technological or infrastructure considerations. The current free-for-all of competing nations needs to be replaced with an agreed-upon international system for a choice-of-law rule. What is needed is to harmonize existing rules within an agreed-upon framework of law.

What would such a framework look like? To answer this, it is useful to have a paradigmatic case in mind. Consider the case of an American company holding data about a European data subject at a data centre in Europe. When the US government seeks access to that data for law enforcement purposes, should the access be controlled by American or European law?[3] What if they conflict?

One approach would carry the data localization movement to its logical conclusion and hold that the law of the country where the data resides controls access to it and rules relating to its processing. This parallels the usual case with physical evidence. Under such a system, for example, our paradigm case would be resolved by applying European law. This choice-of-law rule would have the virtue, at least, of clarity. Everyone concerned would know which jurisdiction's law would control.

But, in many ways, this clarity is illusory. In contemporary cloud structures, data is often stored in more than one location, either in disaggregated form or with copies resident in more than one data centre. It may also transit through multiple physical locations. A data localization choice-of-law rule would force corporations to alter the most economical structures of their data systems in order to secure legal certainty — an unnecessary cost. Alternatively, the data holders might choose not to take these costly steps, thereby creating the very legal uncertainty the rule is intended to avoid.

Perhaps more importantly, a data localization choice-of-law rule would create perverse incentives. Technologically, the most economically efficient place to store data is a product of a number of factors such as climate, infrastructure and proximity to users. With a localization choice-of-law rule we can anticipate at least two inefficient responses. First, some jurisdictions, either out of legitimate concern for their citizens or an authoritarian interest in control, will see this legal rule as a licence to mandate inefficient local storage requirements. Second, conversely, we might see other jurisdictions in a "race to the bottom" as they attempt to create data-access rules that are favourable to the data holders as a way of attracting business interests. Still others might develop rules that make them data-access "black holes," where malicious actors can find a safe haven from legitimate scrutiny. None of these results is optimal, leading us to recommend against such a formulation of the choice-of-law rules.

Instead, we propose four alternate formulations that will also provide clarity in defining the jurisdiction that controls while being systematically less susceptible to economic gamesmanship and rent seeking than a data-location rule. We propose a choice-of-law rule based on either: the citizenship of the data creator; the citizenship of the data subject; one based on the location where the harm being investigated has taken place; or one based on the citizenship of the data holder or custodian.

A rule based on the citizenship of the data creator would tie jurisdiction over data to a familiar concept of personal jurisdiction — that is, the idea that one aspect of jurisdiction is the ability to exercise control over the person who created an item and, therefore, typically has ownership or control of the object or thing that is the subject of litigation. The overlap is not exact; sometimes the creator may not be the owner, in which case the interests of the creator may need to be distinguished, as they tend to be more personally direct than those of the owner.

In either instance, in most cases, citizenship brings with it universal personal jurisdiction — that is, the theoretical ability (often unexercised by a sovereign) to impose rules of conduct on a citizen wherever he may be in the world. The data creator or data owner citizenship rule would extend that paradigm in familiar ways such that those in control of data, wherever located, would be subject to the demands of their sovereign.

That rule may, however, be problematic, inasmuch as in the globalized economy the data creator or owner is often not the subject of the data. In other words, the data creator may be different than the individual whom the data concerns. For example, a photographer may be a data creator of a third party who is the data subject. In that case, the creator has an ownership interest, but it may be the latter who has the more compelling privacy interest.

3 This paradigmatic case is modelled on a current dispute. See *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, M9-150/13 MJ 2814 (S.D.N.Y. July 31, 2014) directing Microsoft to disclose email maintained in Ireland. Other examples abound, including the move in Europe to require global compliance with EU privacy laws and the proposal in the United States to give court-approved search warrants global effect.

Furthermore, an individual or corporate data owner with citizenship in one nation may store its data with a holder who has citizenship of another. Hence, the alternative of relying on the citizenship of the data holder would give primacy not to whose law the owner is subject to, but rather to the law of the entity holding the data — a result that will typically, but not always, apply the law of the physical server location where the data resides. This alternative would enhance geographic aspects of the network over legal ownership perspectives. In addition, it may be valuable to recognize that holders who disclaim ownership will likely be treated in a manner different from those holders who also take an ownership interest in the data that they hold.

A rule that focuses on the citizenship of the data subject would serve to elevate personal jurisdiction as it relates to the individual or corporation to whom the data most directly relates and who often, although not always, is the creator of the data in question. This alternative would serve to enhance personal control of data, at the expense of degrading the comparative value of a sovereign's control of the data owners or data holders subject to its jurisdiction.

Finally, jurisdictional rule that determines the result based on the locus of the harm would reflect a sea change in current trends, away from jurisdictional assertions based on status. It would, instead, substitute a predominant effects-like test of jurisdictional primacy that would be more flexible and indefinite, with uncertain application. It would, however, be more certain in addressing legal harms caused by the conduct that is the underlying subject of inquiry.

To be sure, all of these rules will have grey areas at the margins. Some data subjects may be dual citizens. Some data holders may have corporate headquarters in more than one nation. And some events may give rise to harm in more than one location. But none of these are circumstances that are as readily capable of manipulation as data location; indeed, in many instances they will be extrinsic to the data and the product of other circumstances.

There are sound arguments for and against each of these possible rules:

- A rule based on citizenship of the data subject would ground Internet jurisdiction in a familiar legal construct. It would focus on the individual, whose privacy rights and activities are likely to be most directly implicated by any jurisdictional rule. It would also reinforce the idea that citizenship and sovereignty are closely linked. It might, however, be the most difficult rule to implement technologically, since data often does not have a flag for citizenship of origin or ownership and retrospectively adding such a marker might prove challenging, if not impossible.

- A rule based on citizenship of the data holder would have the virtue of ease of application — a single rule would apply to all data held by the data holder. It would also, however, have the unfortunate effect of creating transnational incentives of the same sort as a data localization rule, with the added consequence of fostering economic nationalism. And data holders who are also data owners may have greater obligations than those who are not owners. Finally, since localization rules are not self-executing, their adoption may increase confrontation at the cost of cooperation and will ultimately have harmful effects on innovation and economic development.

- Much the same would be true of a rule tied to the citizenship of the data creator or owner. Such a rule would incentivize unilateralism at the expense of cooperation. Moreover, where the data owner and data subject are different, focusing on the former for jurisdictional purposes might have the unintended effect of undervaluing privacy values.

- A rule based on the location of harm seems the least capable, generally, of manipulation and most directly linked to cognizable sovereign interests. It suffers, however, from the ability of sovereigns to define and manipulate the definition of harm, and would only be implementable for certain universally agreed upon harmful acts, such as murder.

None of these rules is perfect. Each is capable of manipulation and each will require some transnational cooperation to implement. When the matter involves an inquiry outside the jurisdiction of the nation seeking the data, requests for assistance under each of these rules will have to be processed through cumbersome and possibly unavailing mutual legal assistance treaty (MLAT) channels. This means that some jurisdictions will continue to serve as safe havens for malicious actors no matter what choice-of-law rule is chosen.

Accordingly, concurrent with a revision to the choice-of-law rules, we would be wise to develop a more streamlined MLAT structure. If countries could rely upon the prompt response to data requests, they would be less inclined to act unilaterally in the assertion of jurisdiction. Better MLAT responsiveness (combined with reciprocity obligations) would minimize the temptation to create safe harbours through data localization. It would also lessen the adverse effects of a new rule on law enforcement that would result from adopting one of our possible jurisdictional approaches. MLAT reform would assure law enforcement that, in the end, despite jurisdictional rules that would limit its ability to act unilaterally, it could still avail itself of a reformed MLAT procees for an effective response to criminality.

The virtue, however, of these suggested rules lies in their ability to create clarity and ease of use among willing participants. We could, for example, imagine a transnational agreement on data availability tied to the protection of life and property, perhaps with some degree of judicial oversight, which could be implemented throughout the West. That limited goal itself would be a major achievement in creating security, clarity and consistency on the network.

WORKS CITED

Hill, Jonah Force. 2014. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policy Makers and Industry Leaders." *Lawfare Research Paper Series* 2 (3). www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf.

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

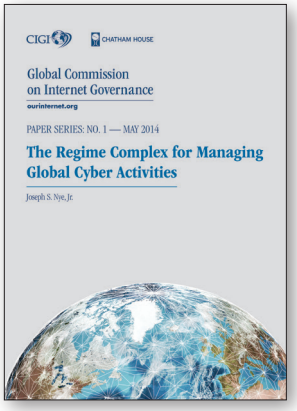
Global Commission on Internet Governance

The Global Commission on Internet Governance (GCIG) was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem. Launched by two independent global think tanks, the Centre for International Governance Innovation and Chatham House, the GCIG will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

Finding Common Ground

A Briefing Book Prepared for the Global Commission on Internet Governance

This briefing book contextualizes the current debate on the many challenges involved in Internet governance. These include: managing systemic risk — norms of state conduct, cybercrime and surveillance, as well as infrastructure protection and risk management; interconnection and economic development; and ensuring rights online — such as technological neutrality for human rights, privacy, the right to be forgotten and the right to Internet access.



The Regime Complex for Managing Global Cyber Activities
GCIG Paper Series No. 1
Joseph S. Nye, Jr.

Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate
GCIG Paper Series No. 2
Tim Maurer and Robert Morgus

Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community
GCIG Paper Series No. 3
Aaron Shull, Paul Twomey and Christopher S. Yoo

Legal Interoperability as a Tool for Combatting Fragmentation
GCIG Paper Series No. 4
Rolf H. Weber

Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem
GCIG Paper Series No. 5
Stefaan G. Verhulst, Beth S. Noveck, Jillian Raines and Antony Declercq

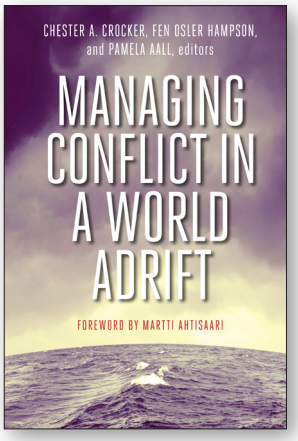
The Impact of the Dark Web on Internet Governance and Cyber Security
GCIG Paper Series No. 6
Tobby Simon and Michael Chertoff

On the Nature of the Internet
GCIG Paper Series No. 7
Leslie Daigle

Understanding Digital Intelligence and the Norms That Might Govern It
GCIG Paper Series No. 8
David Omand

ICANN: Bridging the Trust Gap
GCIG Paper Series No. 9
Emily Taylor

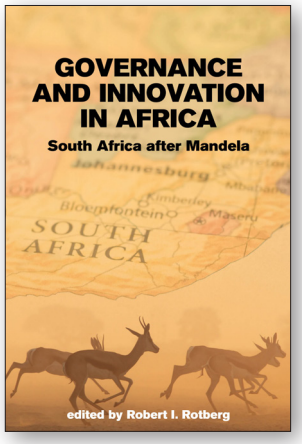
CIGI PRESS



Managing Conflict in a World Adrift
CDN$50 (Available Now)

Edited by Chester A. Crocker, Fen Osler Hampson and Pamela Aall

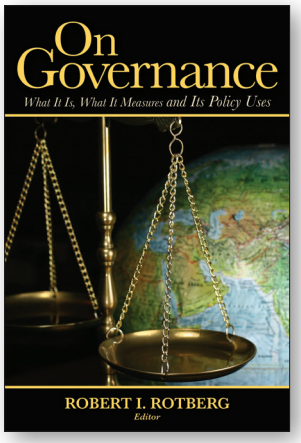
In *Managing Conflict in a World Adrift*, over 40 of the world's leading international affairs analysts examine the relationship between political, social and economic change, and the outbreak and spread of conflict.



Governance and Innovation in Africa
CDN$25 (Available Now)

Edited by Robert I. Rotberg

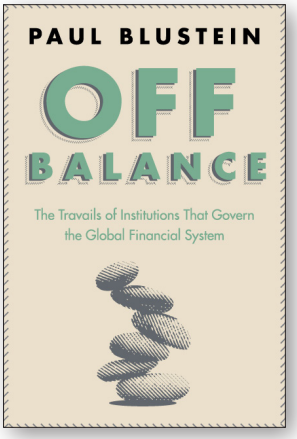
Courageous, intelligent, bold and principled political leadership is required if South Africa is going to build upon Mandela's legacy, according to the expert authors in *Governance and Innovation in Africa*.



On Governance
CDN$25 (Just Published)

Edited by Robert I. Rotberg

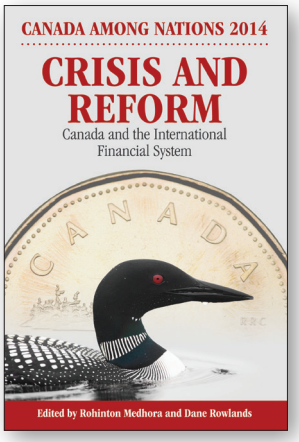
On Governance unpacks the complex global dimensions of governance, and proposes a new theory premised on the belief that strengthened, innovative national and global governance enables positive outcomes for people everywhere.



Off Balance
CDN$25 (Available Now)

Paul Blustein

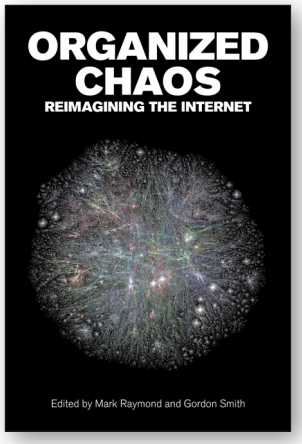
In *Off Balance*, award-winning journalist and author Paul Blustein weaves a compelling narrative that details the failings of international economic institutions in the global financial crisis that erupted in 2008.



Crisis and Reform
CDN$32 (Available Now)

Edited by Rohinton Medhora and Dane Rowlands

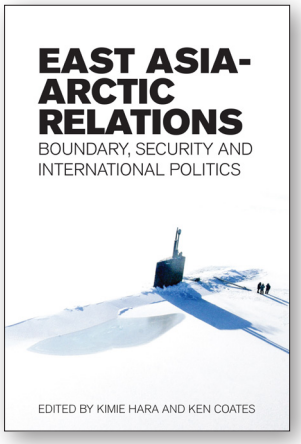
The 28th volume in the influential Canada Among Nations book series, *Crisis and Reform* examines the global financial crisis through Canada's historical and current role in the international financial system.



Organized Chaos
CDN$25 (Available Now)

Edited by Mark Raymond and Gordon Smith

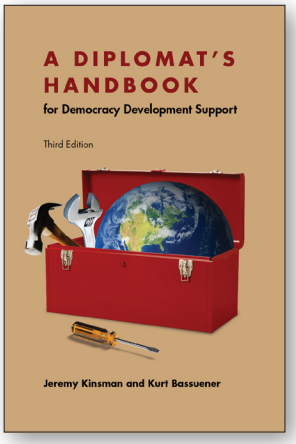
In *Organized Chaos*, leading experts address a range of pressing challenges, including cyber security issues and civil society hacktivism by groups such as Anonymous, and consider the international political implications of some of the most likely Internet governance scenarios in the 2015–2020 time frame.



East Asia-Arctic Relations
CDN$25 (Available Now)

Edited by Kimie Hara and Ken Coates

The culmination of an international collaborative project, *East-Asia Arctic Relations* is a focused and detailed conversation about the historic, contemporary and future dimensions of East Asian countries' relationships with and interests in the Arctic.



A Diplomat's Handbook
CDN$28 (Available Now)

Jeremy Kinsman and Kurt Bassuener

A *Diplomat's Handbook for Democracy Development Support* presents a wide variety of specific experiences of diplomats on the ground, identifying creative, human and material resources. This book focuses on the policy-making experience in capitals, as democratic states try to align national interests and democratic values.

CIGI

Centre for International Governance Innovation
Single copy orders: cigionline.org/bookstore
Available in paperback and ebook form.

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Vivian Moser
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Graphic Designer	Melodie Wakefield
Graphic Designer	Sara Moore

EXECUTIVE

President	Rohinton Medhora
Vice President of Programs	David Dewitt
Vice President of Public Affairs	Fred Kuntz
Vice President of Finance	Mark Menard

COMMUNICATIONS

Communications Manager	Tammy Bender	tbender@cigionline.org (1 519 885 2444 x 7356)

67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org