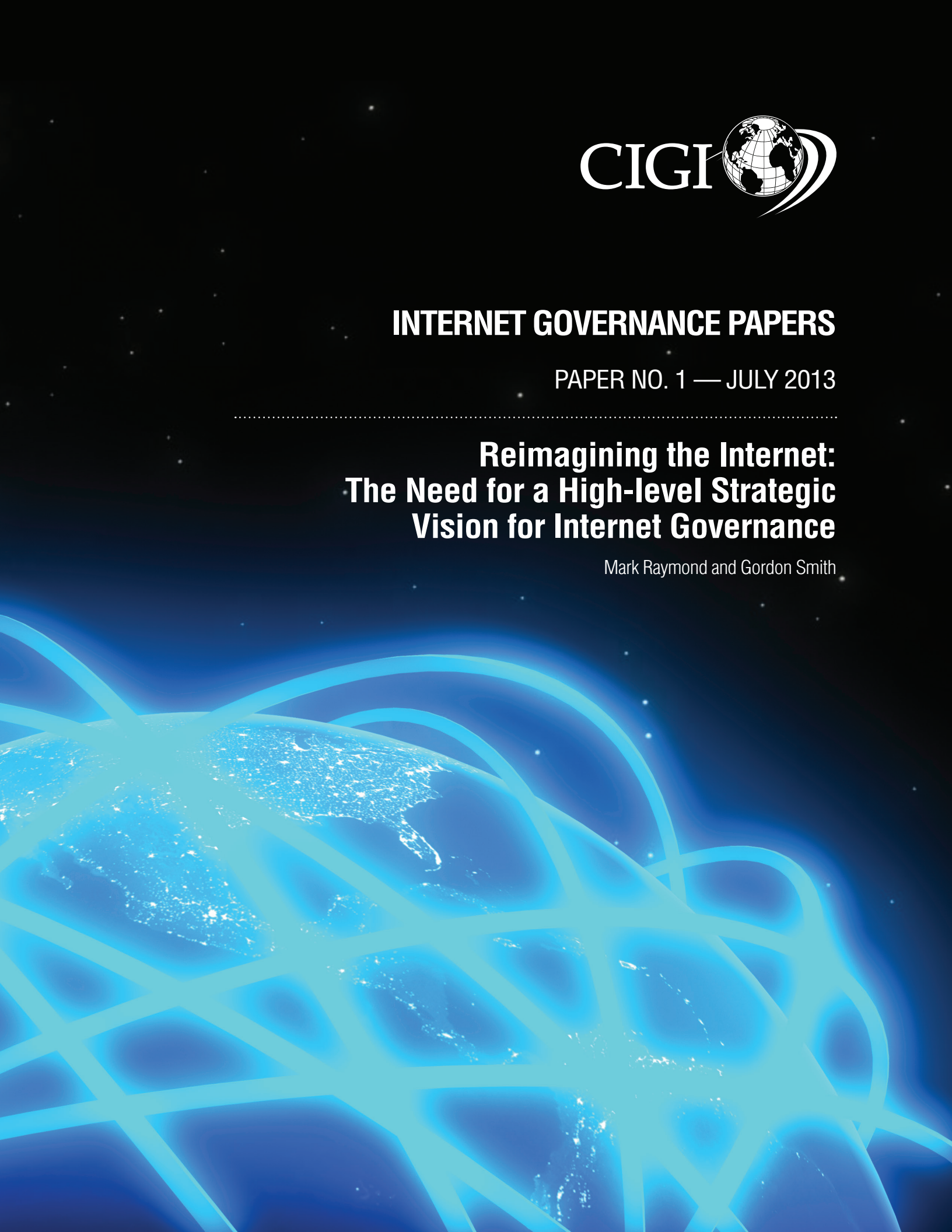

INTERNET GOVERNANCE PAPERS

PAPER NO. 1 — JULY 2013

Reimagining the Internet: The Need for a High-level Strategic Vision for Internet Governance

Mark Raymond and Gordon Smith

INTERNET GOVERNANCE PAPERS
PAPER NO. 1 — JULY 2013

Reimagining the Internet: The Need for a High-level Strategic Vision for Internet Governance

Mark Raymond and Gordon Smith

Cover and page design by Steve Cross.

ACKNOWLEDGEMENT

CIGI gratefully acknowledges the support of the Copyright Collective of Canada.

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

CONTENTS

About the Authors 1

About Organized Chaos: Reimagining the Internet Project 2

Acronyms 2

Executive Summary 3

The Need for a High-level Strategic Vision for Internet Governance, 2015–2020 3

The Legacy System of Internet Governance 7

Global Governance, Rule-making and the Future of the Internet 8

Toward a Comprehensive, Research-based Vision for Internet Governance 15

Works Cited 19

About CIGI 20

ABOUT THE AUTHORS

Mark Raymond

Mark Raymond joined CIGI as a research fellow in August 2012. He has a B.A. in political science and international relations from the University of Western Ontario and an M.A. and Ph.D. in political science from the University of Toronto, and he has taught international relations at the University of Toronto and the University of Waterloo. His research interests include international law and organization, international security and international history, including the history of global governance.

At CIGI, Mark contributes to the Global Security Program. Specifically, he is developing CIGI's work in the area of Internet security and governance.

Gordon Smith

A political science graduate of McGill University (B.A.) and the Massachusetts Institute of Technology (Ph.D.), Gordon Smith became interested in international security and global interdependence while attending university in the United States during the Cuban Missile Crisis in 1962. After graduation, Gordon returned to Canada to work on these issues, and began a long and distinguished career as a public servant with the federal government.

Initially, Gordon worked on Canada's relationship with NATO and the North American Aerospace Defense Command (NORAD) within the Ministry of Defence and Department of External Affairs, but he quickly advanced to more demanding positions in the Privy Council Office. In 1979, Gordon became the deputy under-secretary of state at External Affairs, and in 1985, deputy minister. Shortly thereafter, he was dispatched to Brussels as the permanent representative and ambassador to the Canadian delegation to NATO, and subsequently, was named Canada's ambassador to the European Union.

Returning to Canada in 1994, Gordon was appointed deputy minister of Foreign Affairs, where he fondly remembers establishing a global issues bureau in the ministry to better understand emerging transnational trends affecting Canada. During this time, Gordon began his personal involvement with the G7/G8, as the Sherpa (personal representative) for the prime minister at the G7/G8 summits in Halifax, Lyon and Denver. After retiring from the Government of Canada that same year, Gordon joined the University of Victoria as executive director of the Centre for Global Studies (CFGS), and was appointed chair of the board of governors at the International Development Research Centre. During this period, he also lectured as a visiting professor at the Diplomatic Academy of the University of Westminster in London and Paris.

After collaborating with the think tank for many years on various projects, Gordon joined CIGI in 2010 as a distinguished fellow, and has since been a key contributor to its G20 research activities, events and publications. He looks forward to continuing this work at CIGI, and pursuing another long-time interest: the convergence of technology and global affairs (you can follow Gordon on Twitter @GordonSmithG20).

ABOUT ORGANIZED CHAOS: REIMAGINING THE INTERNET PROJECT

Historically, Internet governance has been accomplished *en passant*. It has emerged largely from the actions of computer scientists and engineers, in interaction with domestic legal and regulatory systems. Beginning at least with the 2003–2005 World Summit on the Information Society process, however, there has been an explicit rule-making agenda at the international level. This strategic agenda is increasingly driven by a coalition of states — including Russia, China and the Arab states — that is organized and has a clear, more state-controlled and monetary vision for the Internet. Advanced industrial democracies and other states committed to existing multi-stakeholder mechanisms have a different view — they regard Internet governance as important, but generally lack coherent strategies for Internet governance — especially at the international level. Given the Internet's constant evolution and its economic, political and social importance as a public good, this situation is clearly untenable.

A coherent strategy is needed to ensure that difficult trade-offs between competing interests, as well as between distinct public values, are managed in a consistent, transparent and accountable manner that accurately reflects public priorities. Guided by these considerations, CIGI researchers believe they can play a constructive role in creating a strategy for states committed to multi-stakeholder models of Internet governance.

In aiming to develop this strategy, the project members will consider what kind of Internet the world wants in 2020, and will lay the analytical groundwork for future Internet governance discussions, most notably the upcoming decennial review of the World Summit on the Information Society. This project was launched in 2012. The Internet Governance Paper series will result in the publication of a book in early 2014.

ACRONYMS

DDoS	Distributed Denial of Service
GAC	Governmental Advisory Committee (ICANN)
G-77	Group of 77 (United Nations)
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISPs	Internet service providers
ITRs	International Telecommunications Regulations
ITU	International Telecommunications Union
OECD	Organisation for Economic Co-operation and Development
OTT	over-the-top
WCIT	World Conference on International Telecommunications
WSIS	World Summit on the Information Society

EXECUTIVE SUMMARY

Internet governance is increasingly the stuff of "high politics." As the Internet has become more important, existing stakeholders have identified new interests; new entrants to the policy space, including a number of emerging market states, are bringing their interests and distinct values to bear. This paper argues that the contemporary politics of Internet governance are best understood as a complex, high-stakes case of rule-making. The key question is how to refine and update Internet governance given a secular increase in state interest, geopolitical rivalry, the existence of legacy institutions and high levels of civil society engagement. This task is complicated by the fact that participants have diverging views on legitimate procedures for making, interpreting and applying rules. Understanding Internet governance as rule-making yields two other insights. First, the Internet is not governed by a single set of rules. Accordingly, the view that the Internet is a commons should be set aside in favour of the image of a series of overlapping voluntary and involuntary groupings governed by multiple sets of rules. Second, openness to employing informal rules and soft law instruments offers advantages in allowing policy makers time to learn about the implications of alternative rules for Internet governance and in allowing procedural flexibility. The paper concludes by articulating the need for a high-level strategic vision for Internet governance. The CIGI Internet Governance Papers series aims to provide world-class research that can underpin the creation of such a vision.

THE NEED FOR A HIGH-LEVEL STRATEGIC VISION FOR INTERNET GOVERNANCE, 2015–2020

The Internet has never been an ungoverned space. Even in its earliest days, it had "rules of the road." In fact, if not for such rules, the Internet would not — could not — exist. Peering agreements, the naming and numbering system, and packet handling protocols are only some of the critical rules that make the Internet possible and regulate its operation. Equally important, however, is the observation that current standards are not the only possible set of such arrangements. As Laura DeNardis (2009) explained in *Protocol Politics*, technical protocols are inextricably political.

The novel nature of the technology, combined with an initial lack of obvious mass social purposes, provided the researchers, engineers and other technologists that comprised the bulk of the original Internet community with a great deal of autonomy in creating and operating its first governance structure.[1] Early Internet governance arrangements were thus primarily the product of a decentralized social network in which authority emerged on the basis of specialized expertise, and problems were typically understood as exclusively technical in nature.[2]

As a result of the social endowments provided by these "parental" influences, current Internet

1 For an overview of this history, see Barry M. Leiner et al. (2012), "A Brief History of the Internet," available at: www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet.

2 Such networks or "epistemic communities" have been previously studied by international relations scholars in other issue areas. See, for example, Peter M. Haas (1992), "Introduction: Epistemic Communities and International Policy Coordination," *International Organization* 46, no. 1: 1–35.

governance arrangements reflect a particular set of values: resilience, openness and interoperability, high potential for anonymity, content neutrality and disregard for national borders in the routing of information between users. These values are at odds, at least in some significant respects, not only with domestic expectations in some states about freedom of expression and the handling of information, but also with central rules and norms of the international system, including classical understandings of state sovereignty.[3]

These tensions were emerging by the time of the initial World Summit on the Information Society (WSIS), which met in Geneva in 2003 for its first phase, with the second phase held in Tunis in 2005. In the intervening years, a number of trends have combined to exacerbate these issues. First, Internet technology penetration rates have increased significantly in all but the most authoritarian and impoverished states.[4] This trend is almost certain to continue; however, even today the changing cultural composition of global Internet users means that new voices (and in some cases different values) are being heard in Internet governance debates and processes. This can be expected to result in a differently governed Internet — although the nature and extent of the change has not yet been determined. Second, the last seven to 10 years have seen considerable maturation of Internet services aimed at mass publics — e-commerce, social networking and cloud computing are obvious examples. Third, multiple critical infrastructure systems are now dependent on the Internet in significant, albeit varying, ways: financial markets and banks, oil and gas production and distribution networks, as well as power grids are vulnerable, as are major transportation and logistics systems. Fourth, there has been significant expansion of what might be termed the Internet's "dark side." This label includes an array of activities performed by a variety of actors for a number of purposes; the common thread is that they are socially undesirable. Cybercrime — including fraud, identity theft, and the creation and operation of illegal botnets — is becoming increasingly widespread and more sophisticated (Glenny, 2011). Multiple reports have shed light on cyber-espionage practices conducted either by states or state agents. There are recent indications that these activities have moved beyond information gathering to include probing for vulnerabilities in both government and private sector networks (Information Warfare Monitor, 2009; Mandiant, 2013). Further, although the evidence is fragmentary, there is reason to suspect that several states have conducted or authorized actual cyber

3 On sovereignty, see Jens Bartelson (1995), *A Genealogy of Sovereignty*, Cambridge: Cambridge University Press; Hedley Bull (1977), *The Anarchical Society*, New York: Columbia University Press; Andreas Osiander (2001), "Sovereignty, International Relations, and the Westphalian Myth," *International Organization* 55, no. 2: 251–287; Daniel Philpott (2001), *Revolutions in Sovereignty: How Ideas Shaped Modern International Relations*, Princeton: Princeton University Press; and Hendrik Spruyt (1996), *The Sovereign State and its Competitors: An Analysis of Systems Change*, Princeton: Princeton University Press.

4 For one estimate, see World Bank, "World Development Indicators," Internet Users (per 100 people), available at http://data.worldbank.org.

attacks.[5] More governments are working to establish and enhance their capabilities to conduct such operations.

As a result of these pressures and tensions, as well as the desire to monetize the Internet to their advantage (or at least the advantage of their corporations), states have increasingly become determined to exert influence and authority over Internet governance. The contractual arrangement between the National Telecommunications and Information Administration (part of the United States Department of Commerce) and the Internet Corporation for Assigned Names and Numbers (ICANN), the California-based non-profit that oversees naming and numbering, has also served to complicate the legitimacy of the current system for Internet governance and to generate demand for a more global alternative.

The desire to extend state control over Internet governance is widely shared, even by advanced industrial economies. The Internet is now simply too important to leave entirely to the technologists. There are, however, significant differences among states with respect to their preferences over the substantive content of such change. The December 2012 World Conference on International Telecommunications (WCIT) held in Dubai, confirmed the existence of complex fault lines in the international community.

A broad coalition led by Russia and China engineered the adoption of updated International Telecommunications Regulations (ITRs) as well as International Telecommunications Union (ITU) resolutions affirming an expanded state role in Internet governance, and empowering the ITU to further debate and discuss Internet issues. This coalition attracted broad participation from the developing world, including key support from Arab states; however, it also included key emerging economies such as South Korea, Indonesia, Turkey, Brazil, Argentina and Mexico. A smaller group of states (including key advanced industrial democracies such as the United States, United Kingdom, Canada, Sweden and New Zealand, joined by a number of other states including India and Kenya) refused to accept either the new ITRs or the accompanying non-binding resolutions (Pfanner, 2012).

There are, undoubtedly, power politics at play in producing these coalitions. Russia and China seek to relocate Internet governance to an institution in which American influence is attenuated, at least in comparison to its current legal and normative dominance of ICANN and its normative influence over the Internet Engineering Task Force (IETF). The United States clearly understands and opposes this

---

5 On Stuxnet, see David Sanger (2012), "Obama Order Sped Up Wave of Cyberattacks Against Iran," *New York Times*, June 1, available at: www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=2&pagewanted=2&seid=auto&smid=tw-nytimespolitics&pagewanted=all. On the Mahdi malware, see Nicole Perlroth (2012),"Cyber Attacks from Iran and Gaza on Israel More Threatening than Anonymous's Efforts," Bits Blog, November 20, http://bits.blogs.nytimes.com/2012/11/20/cyber-attacks-from-iran-and-gaza-on-israel-more-threatening-than-anonymouss-efforts/. On the Flame malware, see Nicole Perlroth (2012),"Researchers Find Clues in Malware," *New York Times*, May 30, available at: www.nytimes.com/2012/05/31/technology/researchers-link-flame-virus-to-stuxnet-and-duqu.html. For information on the Aramco attacks, see Nicole Perlroth (2012), "In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back," *New York Times*, October 23, available at: www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?pagewanted=all. Russia is thought to have employed offensive cyber operations against both Estonia and Georgia. See, respectively, "A Cyber-riot" (2007), *The Economist*, May 10, available at: www.economist.com/node/9163598, and John Markoff (2008), "Before the Gunfire, Cyberattacks," *New York Times*, August 12, available at: www.nytimes.com/2008/08/13/technology/13cyber.html.

attempt by the Russians and the Chinese. In another indication that the two coalitions are not separated purely by principle, the advanced industrial democracies have greatly expanded their technical and legal ability to monitor both the online activity of their own citizens and of foreigners, often over the objections of domestic civil society groups. Attempts to enforce intellectual property laws have also drawn determined opposition (Wortham, 2012). The existence and success of that opposition, however, is a clear indicator that value-based differences among states on Internet governance issues remain highly consequential. It is not purely a cynical matter of national advantage-seeking.

The contemporary politics of Internet governance are also not as simple as the impression that emerged of mutually exclusive camps from the WCIT, for a number of reasons. Eighty-nine states signed the 2012 ITRs, while 55 states announced publicly that they would not. This leaves roughly 50 (admittedly minor) states officially undecided on the matter. Further, even the signatories need to complete the process of ratifying the treaty. Some may yet be persuaded to reconsider. Most important, while the WCIT matters, it is hardly the final word on Internet governance. Indeed, 2013 has already seen modest success at the World Technology Policy Forum in Geneva, as well as positive developments from the United Nations Group of Governmental Experts. The 2013 Internet Governance Forum, 2014 ITU Plenipotentiary and the ongoing decennial review of the WSIS (culminating in 2015) will also provide opportunities for further progress.

Finally, Internet governance is not only a function of state positions. Elements of the global community of Internet users have shown they are prepared to engage in disruptive behaviour in response to unwelcome efforts to change the status quo.[6] Broader civil society groups are also becoming increasingly engaged. A range of corporate interests are pursuing their own agendas, some of which are in direct conflict. Network operators, Internet service companies, equipment manufacturers, intellectual property holders, insurers and others all have significant stakes in Internet governance outcomes. The divisions among corporate actors are geographic as well as sectoral. Legacy telecommunication firms (many of them state-owned and many of these in the developing world) face daunting competition from the migration of voice communication to Internet networks; network operators in some areas of the developing world (such as the Middle East) also act as key intermediaries for the routing of information between advanced industrial economies, and are eager to monetize this transshipment role. This heterogeneous array of interested actors simultaneously complicates the process of reaching agreement and creates opportunities for the assembly of unorthodox coalitions.

Capitalizing on these various opportunities to update and refine global governance of the Internet will require skillful, coordinated diplomacy in a protracted and contentious process of rule-making that has clear implications for human rights, the future course of the global economy and for international security. This paper aims to contribute to this process. It begins with a brief description of the incumbent Internet governance institutions, and then provides an analysis of prospects for rule-making in Internet governance. It concludes by articulating the need for

6 For example, the WCIT spawned Distributed Denial of Service (DDoS) attacks against the ITU website. See Associated Press (2012), "Hackers Said to Hit United Nations Telecoms Talks in Dubai," *Huffington Post*, December 12, available at: www.huffingtonpost.com/2012/12/06/hackers-united-nations-_n_2250364.html.

a high-level strategic vision of Internet governance consistent with democratic values and human rights.

THE LEGACY SYSTEM OF INTERNET GOVERNANCE

Discussion of Internet governance tends to focus disproportionately on ICANN, which plays a central, but limited, role in administering the global system of naming and addressing. There is a range of other key actors that also play indispensable governance roles. Among them are a number of other non-state actors. The IETF develops, approves and promulgates vital technical standards that govern packet handling and exchange, among other issues. The World Wide Web Consortium (known as W3C) plays a similar standard-setting role specifically for the Web. Without uniform standards, the Internet would not be globally interoperable. If standards were not of high quality, the Internet would have diminished functionality.

In addition, private network operators (including commercial Internet service providers [ISPs] and companies that provide "over-the-top" [OTT] online services , such as Google or Instagram) also perform governance roles. For example, interconnection between network operators is privately governed, often on the basis of informal, unwritten agreements that provide for the exchange of traffic on the basis of reciprocity rather than payment. This practice is referred to as "settlement-free peering." To facilitate stable, low-cost exchange of traffic, industry has also played a key role (alongside the Internet Society, known as ISOC, and the ITU) in encouraging the creation and maintenance of Internet exchange points. OTT service providers perform content filtering by virtue of their roles as information intermediaries. Terms of service adopted by large market players shape what a user will see online, whether in search results (for example, Google, Yahoo or Bing), in streaming video (YouTube) or shared photos (Facebook, Instagram or Flickr, among others). Both ISPs and OTT providers are, increasingly, called on to engage with law enforcement and security services to provide information about the activities of their users. Finally, governments play an often indirect role in governing the Internet, largely through law enforcement activity, competition policy and judicial review of individual lawsuits.

The critical point is that Internet governance is complex and highly decentralized, as illustrated by the examples above. Efforts to cut through this complexity typically begin and end with the assertion that the Internet is governed in a "multi-stakeholder" (rather than a multilateral) fashion. A great deal of care should be taken when using this terminology, for three reasons.

First, it is certainly true that non-state actors, both for-profit and not-for-profit, play critical roles in Internet governance; however, this is not unique to this issue area. Private actors play major governance roles with respect to the global financial system, the International Committee of the Red Cross plays an important role in managing the legal regime governing conduct in armed conflict, and NGOs help individual states and international organizations provide crucial goods and services to large populations in the developing world. Each of these issues (finance, laws of war and development) could thus be described, to varying degrees, as examples of multi-stakeholder governance.

Second, these examples illustrate that the involvement of multiple kinds of stakeholders is not sufficient to ensure good governance. The aftermath of the 2008 financial crisis demonstrated the perils of industry self-regulation or regulatory capture; similarly, the highly uneven record of international development efforts shows that a combination of state and non-state actors is not necessarily able to deliver goods and services efficiently or effectively.

"Multi-stakeholderism" must not be seen as a panacea. It also must not become an ideological commitment or article of faith.

Third, the "multi-stakeholder" descriptor is indeterminate — even within the Internet governance issue area, there are various kinds of multi-stakeholder governance. ICANN and the IETF can usefully be treated as limiting cases for the purpose of illustration. ICANN has a relatively formal governance structure headed by a board and a chief executive officer; board seats are allocated to particular stakeholder groups. The management is also counselled by a number of advisory committees. Among these, the Governmental Advisory Committee (GAC) is accorded special rights and powers by virtue of the fact that it represents states. When the GAC issues formal advice to the board, the board is obligated either to accept this advice or to justify its decision to the GAC and enter a reconciliation process. In contrast, the IETF is much less formalized and more consensus-based. The IETF does not have a formal membership structure, has a modest secretariat and its decisions on particular standards are made in the "Request for Comments" process that emphasizes technical soundness and expert consensus. Finally, people participate in IETF processes in their capacity as individuals rather than as representatives of organizations. Multi-stakeholder bodies thus vary in the kinds of stakeholders included and in the authority relations between those stakeholders. This variation means that understanding how a particular domain of Internet governance operates is impossible without additional information.

GLOBAL GOVERNANCE, RULE-MAKING AND THE FUTURE OF THE INTERNET

The conceptual starting point of this paper, and of CIGI's Internet Governance project as a whole, is that global governance consists of attempts to make, alter, interpret and apply social rules. In the modern international system, this is accomplished by drawing on established (but sometimes unwritten) procedural rules drawn from international law and diplomacy (Raymond, 2011).

Our entire social world is made possible by sets of written and unwritten rules that direct our behaviour, shape our identities and define basic categories that determine the horizons of the possible. For example, the rules of chess define the objective or purpose of the game, establish conditions for victory and simultaneously empower and constrain the player to move pieces in various ways. These rules shape players' behaviour in ways they may not fully realize. It would be strange to imagine a chess player physically threatening or attacking an opponent. Even the thought of doing so simply would not occur to most players and, if suggested, would likely be summarily dismissed.

Like chess, rule-making in diplomacy and global governance is a social game governed by rules. This rule-making game has extremely high stakes. The power and durability of rules ensure that the creation, alteration and interpretation of rules are some of the most intensely political human activities. The power to write the rules amounts to ruling over others.[7]

---

7 On rules in social life and specifically in international relations, see Nicholas Greenwood Onuf (1989), *World of Our Making: Rules and Rule in Social Theory and International Relations*, Columbia: University of South Carolina Press, and Friedrich V. Kratochwil (1991), *Rules, Norms, and Decisions: On the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs*, Cambridge: Cambridge University Press. On the connection between rule-making and power, see also Michael Barnett and Raymond Duvall (2005),"Power in International Politics," *International Organization* 59, no. 1: 39–75. Finally, on rules about rule-making, see H.L.A. Hart (1994), *The Concept of Law*, Oxford: Clarendon Press.

Internet governance has been complicated by the collision of at least five different sets of procedural rules. The first, employed most consistently by the Organisation for Economic Co-operation and Development (OECD) states, is drawn from international law and diplomacy. These rules have increasingly been codified, in large part due to the work of the International Law Commission, which played a significant role in the development of the Vienna Convention on Diplomatic Relations and the Vienna Convention on the Law of Treaties, among other instruments. The International Court of Justice has also played a key role in establishing procedures for determining, interpreting and applying both treaty law and customary international law. The result is a set of generally well-understood (if admittedly not always followed) procedural rules. These rules require good faith conduct, encourage what has been called "thick multilateralism" and specifically empower states as the actors competent to make, change, interpret and apply rules, either directly or by delegating these tasks to international organizations and other agents.[8]

A second set of rules is embraced most prominently by Russia and China, the core members of the Shanghai Cooperation Organization. Russian and Chinese conduct suggests a preference for procedural rules that accord the state significant latitude (both with respect to domestic actors and to international monitoring, whether by other states or by international organizations) and that privilege great powers over secondary states. In many respects, this view of procedures for rule-making resembles nineteenth-century practice.

Third, some basic similarities on procedural rules can be identified among the members of the Group of 77 (G-77).[9] While this group of states is culturally heterodox, they can generally be said to prioritize the principle of sovereign equality and to be highly concerned about issues of equity. These commitments reflect the colonial experiences of the vast majority of G-77 members.

These alternate interpretations of legitimate procedural rules nevertheless bear a clear family resemblance in that they accord a central place to states. In contrast, there are two sets of procedural rules that do not do so. The rejection of a role, or at least a privileged role, for states in Internet governance is, in some respects, part and parcel of a democratizing trend in international relations; this pattern has been repeated across a number of issue areas, including trade, the environment, human rights, global economic governance and even international security (Keck and Sikkink, 1998; O'Brien et al., 2000; Khagram, Riker and Sikkink, 2002; Price, 1998; Glasius, 2006). One early expression of these ideas can be found in John Perry Barlow's 1996 articulation of "A Declaration of the Independence of Cyberspace."[10]

Corporate procedural rules are hierarchical in nature, entail executive decision making that is subject to investor oversight and are rooted in contract law. These rules shape the understanding and approach

8 On "thick multilateralism," see John Gerard Ruggie (1992), "Multilateralism: The Anatomy of an Institution," *International Organization* 46, no. 3: 561–598. For further discussion, see Christian Reus-Smit (1999), *The Moral Purpose of the State: Culture, Social Identity, and Institutional Rationality in International Relations*, Princeton: Princeton University Press.

9 The G-77 is a working coalition of developing states in the United Nations. It now includes 132 active members; for a current list, see: www.g77.org/doc/members.html.

10 To read the full text of "A Declaration of the Independence of Cyberspace," see: https://projects.eff.org/~barlow/Declaration-Final.html.

of key players such as network operators, equipment manufacturers, software companies and companies that provide online services (for example, Google and Facebook).

Finally, there is a distinct view on legitimate procedures for rule-making in the technology community. This view emphasizes distributed, peer-produced rule-making on the basis of rough consensus. Influence and authority are typically derived from expertise rather than organizational roles, and claim to represent a community or financial interest. These views have sparked determined opposition to state involvement in Internet governance on the part of "hacktivist" groups, and have led them to minimize substantive differences between the positions of states (Coleman, forthcoming 2013). Whether such a system would be workable at the global level or broadly accepted as legitimate by mass publics is beside the point, which is that these expectations (however unrealistic they may be in the short term) are driving the reactions and behaviour of these actors, as well as (in more muted form) the views of legacy institutions of Internet governance such as ICANN and the IETF.

The existence of these distinct views on how to legitimately make and interpret rules for Internet governance has had, and will continue to have, significant effects on actual outcomes. A full accounting of these is beyond the scope of this paper, but a few significant examples can be briefly enumerated. First, while it is unlikely that the relationship between ICANN and the US government is the source of Russian and Chinese desires for alternate Internet governance bodies, the relationship causes significant political unease in a range of states because it raises concerns over state sovereignty. Specifically, the concern is that the United States is able to unilaterally make decisions that affect the entire global community of Internet users, including other states. At a minimum, this is a powerful rhetorical weapon. Second, existing procedural rules provided a basis to exclude hacktivists and many other segments of civil society from WCIT negotiations. Third, this decision sparked DDoS attacks on the ITU website during the conference, and has arguably made further such disruptions more likely in the future. Fourth, whether as the result of a daring attempt to manipulate procedural rules or a lack of social competence in utilizing them, negotiations on the updated ITRs collapsed over a controversial procedural move, in which what was purported to be an informal poll was treated *ex post facto* as an official and authoritative vote on an important question, in contravention of the ITU's established tradition of consensus decisions (Pfanner, 2012). This incident led, finally, to the rejection of the ITRs and the accompanying resolutions by a significant minority of states, including the bulk of the advanced industrial democracies.

Under established international procedural rules, this outcome could potentially significantly complicate international telecommunications, as it creates a situation where there will be two treaties concurrently in force on the same subject matter. Such situations are explicitly contemplated by Article 30 of the Vienna Convention on the Law of Treaties.[11] The general approach is to determine applicable rules of law according to the treaty in force between the specific states involved in a particular instance of conduct governed under the treaties. This general approach yields four possible cases: where both states are parties only to the 1988 ITRs, those terms apply; where one state is party only to the 1988 ITRs and the other is party to both the 1988 and

11 The Vienna Convention on the Law of Treaties is available at: http://untreaty.un.org/ilc/texts/instruments/english/conventions/1_1_1969.pdf.

2012 ITRs, the 1988 ITRs apply; where both states are parties to the 2012 ITRs, those terms apply; and where one state is party only to the 1988 ITRs and the other state is party only to the 2012 ITRs, there is no treaty in force between those two states and, thus, no legally binding rules.

The fourth case is the most immediately problematic of the four, although the larger problem in the long term is the overall degree of complexity introduced into the governance of international telecommunications, the potential for increased transaction costs and the eventual possibility of significant divergence between the two treaty regimes over time. Given the similarity between the two treaties, as well as the long history of routine cooperation on international telecommunications and the resulting business relationships and accumulated social practice, there are reasons to believe that this complexity may be manageable, if suboptimal. This assessment may not apply, however, in the event that the parties to the new ITRs engage in subsequent negotiations, building on the accompanying resolutions to erect a parallel institution for Internet governance. In the event such a parallel institution duplicates the function of the Internet Assigned Numbers Authority or the IETF, the potential exists for serious harm to global interoperability. Further, since routing is currently done without regard for international borders, the existence of parallel Internet governance regimes that may evolve with very different privacy protections poses challenging questions about the sustainability and desirability of legacy routing practices.

The key question is how to update and refine systems for Internet governance in light of the general increase in interest on the part of states, geopolitical rivalry, the existence of legacy institutions and intense commitment to the status quo by a wide array of civil society actors. Disagreement on legitimate procedural rules also greatly complicates what is already a daunting task. This suggests the need to focus consciously on a procedural *modus vivendi* in order to prevent negotiations and discussions from foundering on procedural grounds.

Viewing Internet governance as a matter of making, interpreting and applying rules yields two other important insights. First, the Internet is not governed by a single set of rules. Accordingly, the misleading assertion that the Internet is a commons should be abandoned in favour of the more nuanced view that it is comprised of a series of overlapping voluntary and involuntary groupings governed by a heterodox variety of written and unwritten rules.[12] This move has the advantage of more effectively delineating issues where global coordination is required and those where varying degrees of subsidiarity are possible, and even desirable. It also clearly highlights the importance of the rules that govern different social groups. Second, it is important not to conflate rules and law; rather, there are good reasons to take a broad view of the available means for accomplishing Internet governance. It is vital to avoid the mistake of fixating on multilateral treaties and formal international organizations. The current political context and the nature of the issues indicate that soft law instruments are likely to be more plausible and more effective.

The assertion that the Internet is a commons is made, paradoxically, both by civil society activists

12 These groupings can be thought of as nested clubs, in the sense of "club goods" (as opposed to common goods).

and by major Western militaries.[13] Relying on the mistaken understanding of the Internet as a commons encourages overly expansive approaches to Internet governance, which apply rules with insufficient regard for differences between issues and that neglect the importance of fostering the club governance arrangements that can ensure the continued smooth development of the Internet's multitude of clubs.

Economists define a commons as a good that is rivalrous and non-excludable.[14] A good is rivalrous if it cannot be used simultaneously by multiple people or if its use by one person reduces the quantity and/or quality of the good available for others. A good is non-excludable if people cannot be prevented from using it (whether on the basis of payment or some other similar principle). Neither of these criteria are applicable to the Internet.

The Internet is technically rivalrous in the sense that the computer networks on which it depends (its "physical layer") accommodate a finite amount of traffic. At peak usage times, especially in congested sections of the network, users may receive a degraded experience — that is, bandwidth-intensive use by a large number of users may mean that many receive lower-quality service.[15]

In practice, however, such problems have relatively easy solutions: more physical infrastructure (fibre optic cable, switches and routers) can be constructed, easing congestion; more efficient protocols for routing and directing traffic can perform a similar function, directing traffic through portions of the network with excess capacity; and usage-based billing can incentivize users to moderate their consumption of bandwidth. These three solutions are already part of Internet governance, and while there are potential drawbacks or limitations associated with each, there is little reason to expect that combinations of such policies cannot continue to meet demand for bandwidth, given appropriate investment strategies.

The case for regarding the Internet as non-excludable is even weaker than the case for believing that it is rivalrous. Multiple kinds of exclusion are already occurring, many of them at the Internet's physical layer.

First, many states already employ their domestic law to block various kinds of content, including child pornography, hate speech, intellectual property violations and political dissent. This kind of exclusion is typically accomplished by requiring ISPs to prevent the resolution of certain domain names and their associated Internet Protocol addresses. In the extreme, it entails states ordering the physical shutdown of Internet service. The governments of Egypt and Myanmar have both employed this tactic,

13 For a military assertion, see Maj. Gen. Mark Barrett et al. (2011), "Assured Access to the Global Commons," Supreme Allied Command Transformation, Norfolk: NATO, available at: www.act.nato.int/mainpages/globalcommons. A commons mentality is evident in the statements and actions of Anonymous, at least after 2008. See Coleman (forthcoming 2013).

14 Two critical works on the concept of the common goods and the problems associated with their management are Garrett Hardin (1968), "The Tragedy of the Commons," *Science* 162, no. 3859: 1243–1248, and Elinor Ostrom (1990), *Governing the Commons: The Evolution of Institutions for Collective Action*, Cambridge: Cambridge University Press.

15 The recent DDoS attack on Spamhaus targeted Internet Exchange Points and resulted in significant service degradation for a large number of users. See John Markoff and Nicole Perlroth (2013), "Attacks Used the Internet Against Itself to Clog Traffic," *New York Times*, March 27, available at: www.nytimes.com/2013/03/28/technology/attacks-on-spamhaus-used-internet-against-itself.html?hpw&abra=test&_r=0.

albeit for limited periods of time (Williams, 2011; Wang, 2007).

Second, some recently proposed pieces of legislation (for example, the Stop Online Piracy Act, or SOPA, in the US Congress, and Bill C-32 in the Canadian Parliament) have sought to strengthen copyright protections, including requiring Web hosting companies, search engines and ISPs to sever relations with websites and users found to violate copyright. While such measures have met strong resistance, it is likely they will remain on the agenda at the insistence of copyright-owning firms.

Third, DDoS attacks accomplish short-term exclusion by bombarding a targeted website with requests for information, overwhelming server capacity and preventing servicing of legitimate requests. These attacks are inexpensive and sometimes difficult to attribute to particular agents, making them an attractive option for hackers and for cybercriminals. They are also blunt instruments, which can have significant unintended consequences such as denying access to additional, unintended targets. Finally, they allow virtually anyone with minimal technical expertise and computer hardware to engage in excluding others from the Internet.

Fourth, it is possible to exclude people from the Internet by destroying physical infrastructure (fibre or wireless) critical to their connectivity. Such attacks are imaginable both in the context of terrorism and in the context of a major military conflict. While the decentralized nature of the Internet means that terrorist attacks would be unlikely to cause widespread long-term disruption, major military conflict could pose a significant risk to the Internet.

If the Internet is, in fact, non-rivalrous and excludable, it more closely resembles what economists call a club good. Club goods include access to satellite television or the status that comes with a country club membership. Experience tells us that some clubs are more exclusive than others, and that different clubs have varying rules, norms and bylaws. The Internet is easily mistaken for a commons because it has historically been an extremely open club, with incredibly sparse rules for its members.

In some ways, barriers to joining the club continue to fall rapidly: Internet access is more affordable for more people than it has ever been. However, in other important respects, the Internet club looks not only less like a commons than it once did, but also less like a single club.

Rules increasingly circumscribe user behaviour online and pockets of the Internet are now more likely to allow access only to members — with highly variable requirements for membership, ranging from unverified assertions that a user is above a certain age or resides in a particular place (often employed to restrict access to various kinds of entertainment content), to contractual arrangements on a fee-for-service basis (such as pay walls on major newspaper websites), to requirements that the user be a member of a particular offline organization such as a corporation or government.

Accordingly, the Internet is best understood as a set of nested clubs. At the most basic level, all Internet users are members of the club of people with Internet connections. However, they are also members of smaller clubs composed of people who access the Internet via a particular ISP, and people who access the Internet from a particular country. It is impossible for an Internet user to avoid membership in any of these three kinds of clubs. Beyond this minimal baseline, users will typically also be members of other clubs based on their personal identities and interests.

This view of the Internet facilitates a more nuanced discussion of online rights and responsibilities, one

that recognizes that different areas of the Internet may correspond closely with the open-access norms associated with commons regimes while others may not, and that while trade-offs between distinct public values such as liberty, property rights and security may not be entirely avoidable, applying different rules to particular portions of the Internet can help ensure that restrictions on online rights are minimized and do not cause unintended collateral damage to freedom.

Understanding the Internet as a set of nested clubs calls attention to the need to think explicitly about the rules for the three most basic types of clubs: the club of all Internet users; the clubs comprised of each individual ISP and its clients; and the clubs of national users. Maintaining the global reach and interoperability of the Internet, and thus maximizing its value to humanity, requires ensuring that access to these clubs remains open to all, and that restrictions on member behaviour do not exceed the minimum requirements of public safety.

The vibrancy of any club over time depends on its ability to respond effectively and legitimately to its members' desires. This highlights the need to augment fora that enable discussion and potential revision of shared understandings about online rights and duties at each level of the nested clubs that comprise the Internet. Doing so will be especially difficult, but is particularly important at the most fundamental level — the club of all Internet users.

Beyond conceiving of the Internet as a series of nested clubs, thinking clearly about Internet governance requires attention to the legal forms employed. Legalization has been noted as a distinctive characteristic of modern international relations and global governance.[16] A great deal of legalization has taken the specific forms of multilateral treaties and the creation of formal, chartered international organizations; however, it is critical to avoid conflation of these particular mechanisms with the concept of legalization in general.[17] For at least two main reasons it is likely that less formalized legal mechanisms will be more helpful and successful in this issue area for the foreseeable future.

First, Internet governance is a novel and highly complex issue from the perspective of the diplomats and government officials who will be tasked with negotiating and implementing international rules. While existing institutions tasked with Internet governance have a greater degree of familiarity with the technical issues involved, these organizations lack expertise in the technical aspects of international law, public policy and regulation. Kenneth Abbott and Duncan Snidal (2000) have argued persuasively that in complex, novel situations, so-called "soft law" instruments (for example, voluntary codes of conduct and best practices) are often a superior choice relative to traditional "hard law" instruments such as treaties. Their rationale is that soft law offers decision makers opportunities to learn about the social effects of particular sets of rules over time — and to amend them accordingly, typically with lower negotiation costs than entailed by the renegotiation of hard law (ibid.). This pattern is especially likely to hold with respect to the governance of cyber security. Just as attempts to craft rules for the global governance of nuclear weapons required an extended period of mutual (if often highly conflictual) learning, attempts to govern cyber-security and even to govern the Internet more generally are likely to develop via various forms of soft law and norm development prior to the creation

16 See Kenneth W. Abbott et al. (2000), "The Concept of Legalization," *International Organization* 54, no. 3: 410–419.

17 This point has been recognized both by rationalist scholars and by scholars of international law drawing on constructivist theories of international relations. For the rationalist view, see Abbott and Snidal (2000). For the constructivist view, see Brunnée and Toope (2010).

of any multilateral treaties or formal international organizations. Put simply, states need time to learn about the technology and to arrive at conclusions about the kinds of governance arrangements they prefer. The recent conclusion by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security that international law applies in cyberspace is a welcome development, but this must be understood as a starting point rather than a conclusion (US Department of State, 2013). Agreeing on specific interpretations for applying general international legal rules to particular cases will require a great deal of work.

Second, informal soft law instruments are also attractive, given the current political context for Internet governance, which is characterized by geopolitical rivalry and by disagreement over legitimate procedural rules. The distributional consequences of different Internet governance arrangements are not yet well understood, and states are increasingly sensitized to the potential for relative losses associated with being on the losing end of newly established institutions. This argument is related to the prior argument about the impact of uncertainty on the desirability of hard versus soft law instruments. Soft law instruments are also more attractive in this context because they are typically subject to less precise procedural rules. Whereas the procedures for creating a legally binding treaty are highly specific, the procedures and forms for creating informal codes of conduct are less demanding and require less prior agreement. They also allow more flexibility and innovation, thus increasing the scope for agreement between parties that do not agree completely on procedural rules.

These observations dovetail with the perspective on international law offered by Jutta Brunnée and Stephen Toope (2010: 5), who argue that an exclusive focus on treaties and hard law is insufficient, because it neglects what they call "the hard work of international law" — or the ongoing social process of enacting legal rules (whether hard or soft) by interpreting and applying them in concrete cases. On this view, law always entails soft law processes and processes of adjudication that are vital to the operation of even the most well-developed hard law regime. International soft law, like domestic statutory law, will never yield perfect compliance. Spoilers may remain, but this is likely to be the case even under the most well-developed treaty regime and, thus, is not an argument against the advantages of soft law instruments for rule-making, interpretation and application in an uncertain environment characterized by political contention.

Refining and updating Internet governance entails a process of rule-making for a series of nested clubs in a difficult and uncertain context that privileges procedural flexibility and a willingness to employ soft law instruments.

TOWARD A COMPREHENSIVE, RESEARCH-BASED VISION FOR INTERNET GOVERNANCE

The goal of this rule-making process should be a vibrant, responsibly governed Internet that safeguards privacy and other essential rights. The difficulty, of course, is managing the trade-offs between the distinct values and interests of a variety of public and private actors in an effective and legitimate manner. To date, both state and civil society actors have generally lacked coherent, comprehensive strategic visions of the kind of Internet they want and how to get there.

The major exception to this lack of strategic vision, unfortunately, has been the coalition of states (led by Russia and China) seeking the greatest degree of state control over the Internet. These states have sought to

trade cynically on the global legitimacy of the UN system in order to consecrate the worst excesses of state conduct against domestic populations. They have done so while simultaneously developing and deploying significant offensive cyber capabilities.

The advanced industrial democracies and other states committed to the maintenance of Internet governance structures that balance security, rights and economic dynamism have begun to devote additional attention to these issues; however, these efforts have lacked coordination both at the national level (between agencies with a primary interest or responsibility in one particular policy area) and at the international level. The lack of a well-organized coalition advancing what might be termed a liberal democratic vision for Internet governance has left a vacuum that is increasingly being filled by the more authoritarian coalition led by Russia and China. Given the expectations of good faith attempts at compromise in many established international organizations, the likelihood is that this coalition will attain a portion of its agenda. This risk is amplified if other states lack a positive vision and are routinely in the position of simply blocking the coalition's proposals. In such a situation, wavering and currently undecided states might be persuaded or induced to support proposals that undermine basic rights, alter the monetization of the Internet in ways that coincide with Russian and Chinese interests, and further establish a permissive environment for cyber espionage and cyber attacks.

Similarly, while hacktivists and other highly motivated segments of the global community of Internet users have been adept at "naming and shaming" in cases where governments and companies engage in questionable behaviour,[18] the diversity of this community and its strong normative bias in favour of decentralized social organization complicate efforts to articulate a coherent, positive vision for Internet governance that extends beyond denunciation of attempts to alter the status quo. Further, many members of this community understand themselves to primarily be "activists." Such an identity can encourage mono-value thinking antithetical to a governance mindset, which attempts to balance and partially satisfy multiple perspectives and values in cases of tension or conflict.

The diversity of basic social institutions among democracies suggests there is little chance that there is a unique legitimate liberal democratic system of Internet governance. Indeed, given that modern global governance often leans heavily on the principle of subsidiarity, crucial components of Internet governance are likely to continue to reside at the national level and, therefore, handled differently by different political communities. Having a coherent, legitimate strategic vision for Internet governance does not mean an all-encompassing multilateral treaty or even an informal global agreement on every issue. Rather, the key is to identify critical issues where truly global norms, rules and standards are required. On other issues, especially including rights, it will be necessary to identify broad parameters that bound legitimate difference in state practices.

---

18 The Chilling Effects website is one example of such a campaign; see www.chillingeffects.org. There are also indications of emerging alliances between hacktivists and civil society groups engaged in protest over other issues. See Boris Manenti (2013), "Hacktivism United: NGOs, Hackers Team Up to Take Down Common Enemies," *Worldcrunch*, February 5, available at: www.worldcrunch.com/tech-science/hacktivism-united-ngos-hackers-team-up-to-take-down-common-enemies/anonymous-hacking-activists-greenpeace-internet/c4s10811/#.UTjNNTD_l8F. Such campaigns appear to follow many of the patterns identified in Keck and Sikkink (2002).

Among the principles critical to a liberal democratic view of Internet governance are: guarantees of due process, freedom of expression and other basic freedoms; mixed public and private ownership of property, with a government regulatory and oversight role to protect public interests and to correct market failures; compliance with international law, especially including restriction on hostile acts to instances of self-defence and collectively authorized response to threats; and the creation, alteration and interpretation of rules in good faith and in accordance with transparent, mutually accepted rules of procedure.

There are tensions within and between these principles. For example, certain kinds of speech are often deemed incompatible with other basic freedoms. Restrictions on both privacy and due process are sometimes deemed acceptable in the name of ensuring public safety. The appropriate scope of state regulatory involvement in areas of private investment is also politically controversial. With respect to hostile acts, the last decade witnessed a notable and as-yet-unresolved debate on the legitimate scope for preventive (as opposed to pre-emptive) self-help action.

As a result, a complete strategic vision for Internet governance must go beyond first principles to explicitly contemplate these and other key trade-offs. It must provide guidance in differentiating critical areas for global rule-making from other areas that, while important, are best handled at regional, bilateral, national and even sub-national levels. On these latter issues, a strategic vision should, where possible and appropriate, go at least some distance toward discussing the bounds of legitimate difference in state conduct while recognizing that answers to these questions must, ultimately, be crafted by states themselves in consultation with civil society and other relevant actors.

A strategic vision must also be research-based. While a great deal of attention has been paid to specific Internet issues in a number of academic disciplines, there has been a relative neglect of core governance issues. Accordingly, CIGI has commissioned a set of papers from leading experts that address both a range of pressing governance challenges and also the international political implications of a handful of the most likely Internet governance scenarios in the 2015–2020 timeframe. The papers, of which this is the first in a series, are divided into two clusters.

The first cluster identifies the pressing near-term governance challenges on a number of fronts. These will include technical standards and the governance of interconnection, cyber security issues, including state efforts at monitoring and surveillance, civil society hacktivism by groups such as Anonymous and the future of intellectual property in a digital age.

The second cluster of papers examines various plausible outcomes for Internet governance in the remainder of the current decade and attempts to assay their implications for global governance and the international system as a whole. These papers are, of necessity, somewhat speculative; however, social science has developed scenario-based methods for forecasting the proximate future within reasonable tolerances.[19]

In order to impart a degree of structure and comparability to the scenario papers, authors were asked to consider and engage with four ideal-typical scenarios. The first entails incremental change to the current model for Internet governance built largely around ICANN and the IETF. The second involves the creation of largely self-contained yet functional "blocs"; for example, an Internet comprised largely

19 See, for example, Steven Bernstein et al. (2000), "God Gave Physics the Easy Problems: Adapting Social Science to an Unpredictable World," *European Journal of International Relations* 6, no. 1: 43–76.

of users from OECD-member states, and another of users primarily drawn from Russia, China and the Arab world. Each bloc would have distinct governance structures and global interoperability could be expected to be both technologically limited and subject to substantial political control. Third, authors were asked to consider an outcome in which failure to agree on a global Internet governance regime for key issues leads to major breakdowns in interoperability and in the basic functioning of the Internet. While this kind of generalized governance failure is relatively unlikely, there is reason to think carefully about low-probability, high-significance outcomes. This is especially true in complex and novel issue areas, where the implications of new rules and other actions are not well understood in advance. The final scenario is one in which hacktivists (such as Anonymous), cyber criminals, terrorists and other groups successfully destabilize large portions of the Internet as an expression of protest.

These scenarios are intended as analytical aids rather than straitjackets. Reality is not expected to wholly match any of them; rather, it will blend elements of multiple scenarios, including some not enumerated here. However, it is also true that the four scenarios are not equally probable. So long as there is some realistic prospect of identifying and selecting policy that is more likely to lead to better outcomes, such efforts to understand the costs and benefits of alternate outcomes remains worthwhile.

Together, these two clusters of papers provide: a clear sense of the critical problems facing efforts to update and refine Internet governance; the appropriate modalities for doing so; and the costs and benefits associated with the most plausible outcomes. They therefore provide the foundation for developing the research-based, high-level strategic vision required to successfully navigate a complex, shifting and uncertain governance environment.

WORKS CITED

Abbott, Kenneth W. and Duncan Snidal (2000). "Hard and Soft Law in International Governance." *International Organization* 54, no. 3: 421–456.

Brunnée, Jutta and Stephen J. Toope (2010). *Legitimacy and Legality in International Law: An Interactional Account*. Cambridge: Cambridge University Press.

Coleman, Gabriella (forthcoming 2013). "Anonymous in Context." CIGI Internet Governance Paper Series No. 3.

DeNardis, Laura (2009). *Protocol Politics: The Globalization of Internet Governance.* Cambridge: MIT Press.

Glasius, Marlies (2006). *The International Criminal Court: A Global Civil Society Achievement*. New York: Routledge.

Glenny, Misha (2011). *Dark Market: How Hackers Became the New Mafia*. Toronto: Anansi.

Information Warfare Monitor (2009). "Tracking GhostNet: Investigating a Cyber Espionage Network." Available at: www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network.

Keck, Margaret E. and Kathryn Sikkink (1998). *Activists Beyond Borders: Advocacy Networks in International Politics*. Ithaca: Cornell University Press.

Khagram, Sanjeev, James V. Riker and Kathryn Sikkink (2002). *Restructuring World Politics: Transnational Social Movements, Networks, and Norms*. Minneapolis: University of Minnesota Press.

Mandiant (2013). "APT1: Exposing One of China's Cyber Espionage Units." Available at: http://intelreport.mandiant.com/.

O'Brien, Robert et al. (2000). *Contesting Global Governance: Multilateral Economic Institutions and Global Social Movements*. Cambridge: Cambridge University Press.

Pfanner, Eric (2012). "U.S. Rejects Telecommunications Treaty." *New York Times*, December 13. Available at: www.nytimes.com/2012/12/14/technology/14iht-treaty14.html.

Price, Richard (1998). "Reversing the Gun Sights: Transnational Civil Society Targets Land Mines." *International Organization* 52, no. 3: 613–644.

Raymond, Mark (2011). "Social Change in World Politics: Secondary Rules and Institutional Politics." Ph.D. dissertation. University of Toronto, Canada.

US Department of State (2013). "Statement on Consensus Achieved by the UN Group of Governmental Experts on Cyber Issues," press release, June 7. Available at: www.state.gov/r/pa/prs/ps/2013/06/210418.htm.

Wang, Stephanie (2007). "Pulling the Plug: A Technical Review of the Internet Shutdown in Burma." *OpenNet Initiative Bulletin*. Available at: https://opennet.net/sites/opennet.net/files/ONI_Bulletin_Burma_2007.pdf.

Williams, Christopher (2011). "How Egypt Shut Down the Internet." *The Telegraph*, January 28. Available at: www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html.

Wortham, Jenna (2012). "Public Outcry Over Antipiracy Bills Began as Grass-Roots Grumbling." *New York Times*, January 19. Available at: www.nytimes.com/2012/01/20/technology/public-outcry-over-antipiracy-bills-began-as-grass-roots-grumbling.html?pagewanted=all.

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 four themes: the global economy; global security; the environment and energy; and global development.

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.

CIGI MASTHEAD

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