CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Research Volume Two

Global Commission on Internet Governance

Who Runs the Internet?

The Global Multi-stakeholder Model of Internet Governance

Research Volume Two

Global Commission on Internet Governance

Who Runs the Internet?

The Global Multi-stakeholder Model of Internet Governance

CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Published by the Centre for International Governance Innovation and the Royal Institute of International Affairs

This work was carried out with the aid of a grant from the International Development Research Centre (IDRC), Ottawa, Canada.

The views expressed herein do not necessarily represent those of IDRC or its Board of Governors.

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 conducted and supported independent research on Internet-related dimensions of global public policy, culminating in an official commission report — *One Internet*, published in June 2016 — that articulated concrete policy recommendations for the future of Internet governance. These recommendations 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 focuses 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

PREFACE

When I and my colleagues at the Centre for International Governance Innovation and Chatham House envisioned and launched the Global Commission on Internet Governance (GCIG) in 2014, we were determined to approach the work ahead strictly on the strength of evidence-based research. To make this possible, we commissioned nearly 50 research papers, which are now published online. We believe that this body of work represents the largest set of research materials on Internet governance to be currently available from any one source. We also believe that these materials, while they were essential to the GCIG's discussions over these past months, will also be invaluable to policy development for many years to come.

The GCIG was fortunate to have Professor Laura DeNardis as its director of research, who, along with Eric Jardine and Samantha Bradshaw at CIGI, collaborated on identifying and commissioning authors, arranging for peer review and guiding the papers through the publication process.

Questions about the governance of the Internet will be with us long into the future. The papers now collected in these volumes aim to be forward looking and to have continuing relevance as the issues they examine evolve. Nothing would please me and my fellow Commissioners more than to receive comments and suggestions from other experts in the field whose own research has been stimulated by these volumes.

The chapters you are about to read were written for non-expert netizens as well as for subject experts. To all of you, the message I bring from all of us involved with the GCIG is simple — be engaged. If we fail to engage with these key governance questions, we risk a future for our Internet that is disturbingly distant from the one we want.

Carl Bildt

Chair, GCIG

November 2016

INTRODUCTION

Laura DeNardis

INTRODUCTION

Debates about Internet governance have long embodied a tension between forces advocating for greater government oversight of the Internet and those advocating for a coordinating structure distributed across many actors — ranging from international organizations, governments, the private sector, civil society and new global institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN). What is the appropriate role of governments in running the Internet, on the one hand, versus the administrative coordination of cyberspace distributed across the private sector, traditional governments and civil society, on the other? The government-centric approach can be thought of as multilateral oversight. The distributed governance approach — which captures how Internet governance has evolved historically — is usually called the multi-stakeholder governance model, although explanations of what multi-stakeholder governance actually is and what is at stake are often incomplete. What is this multi-stakeholder model and who are the stakeholders? How should power be distributed across various coordinating entities, and who decides? Is there something unique about this framework of governance or are there analogies in other areas of society?

Governance of the Internet is not a single-issue area. Its governance encompasses a constellation of administrative and technical coordinating tasks necessary to keep the Internet operational and to enact related public policy. The tasks range from technical standard setting and the administration of domain names and numbers to setting policies related to cyber security and privacy. As the Internet has evolved, many of these functions have been carried out by the private sector — such as private telecommunications companies that make contractual decisions to interconnect their networks, and information intermediaries that establish policy via terms of service with end-users — and by the Internet's technical community — which includes the Internet Engineering Task Force (IETF) and its institutional home, the Internet Society; the World Wide Web Consortium; regional Internet registries; and ICANN.

Tensions between multilateral oversight and private-sector-led multi-stakeholder oversight can be seen in many of the global policy controversies around the Internet, ranging from long-standing questions about how to transition US oversight of Internet names and numbers to debates about types of interconnection that arose at the World Conference on International Telecommunications convened in Dubai in 2012. Tensions between governments and the private sector are also evident in debates about encryption that mediate competing values in cyberspace, such as law enforcement and national security versus individual privacy and economic security. This collection of research lays out some of these controversies, seeks to explain the "multi-stakeholder model" of Internet governance and makes recommendations about the types of governance innovations necessary to maintain both Internet freedom and Internet stability in the coming years.

Internet governance can be viewed as a complex ecosystem of tasks carried out by many actors constrained by context-specific policies, markets and norms. In the first chapter in this volume, *The Regime Complex for Managing Global Cyber Activities*, Joseph S. Nye Jr. (2014) applies regime theory to explain this range of actors, institutions, policies and norms collectively constituting Internet governance. The emergence of a unitary cyber regime is improbable because of the different values and norms that exist around issues such as cyber security and because of global disputes over cyber power. Rather, Nye considers the structures underlying cyber governance a *regime complex*, with "a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages" (p. 8).[1] Within this regime complex, governance approaches to issues take various forms. For example, international cooperation is more likely in the area of cybercrime, while governance approaches to online expression vary globally by cultural norms and legal structures. It is unlikely that there will be a single, all-encompassing cyber regime any time soon, and policy fragmentation is likely to persist.

"Multi-stakeholder" is a term used to describe how administration of the Internet takes place in practice, but also often without explaining its actual meaning. What is this institutional form called multi-stakeholder governance and how does it connect to or differentiate from multilateralism? In the second chapter, *Multi-stakeholderism: Anatomy of an Inchoate Global Institution*, Mark Raymond and Laura DeNardis (2016) offer a taxonomy of different types of multi-stakeholder institutional forms, which vary based on the combination of actors and the nature of authority relations among them. The chapter is conceptually based on John Ruggie's pioneering study of multilateralism and seeks to provide an analogous study of multi-stakeholderism, a term not yet well defined. Raymond and DeNardis then apply their taxonomy of different forms of multi-stakeholder governance to five institutional case studies, including ICANN, the IETF and the International Telecommunication Union, as well as institutions involved in the governance of corporate social responsibility and securities regulation. The chapter ultimately concludes that multi-stakeholder arrangements in Internet governance and beyond often fail, in practice, to live up to the rhetoric around multi-stakeholderism.

1 All page numbers refer to pagination in this volume.

There is also rising contention over arrangements of power within the Internet governance ecosystem as cyberspace dependencies increasingly shape national economies and systems of political and social life. Recent global debates over Internet governance have included contention over control of Internet names and numbers, interconnection arrangements, and the increasing co-opting of infrastructure by governments and other forces for political and economic purposes, such as censorship and intellectual property rights enforcement. In the third chapter, *The Emergence of Contention in Global Internet Governance*, Samantha Bradshaw and colleagues (2015) address this phenomenon of rising Internet governance conflicts. Contention, in part, arises from the shift from primarily technical coordination issues to global cooperation problems, in which a rising number of actors with different interests interact in a global arena with complex distributional consequences. The authors suggest a number of explanations for this structural shift: uncertainties born from extrinsic disruptions, such as Edward Snowden's disclosures of National Security Agency surveillance; changes in market conditions; and declining dominance of the United States in the Internet governance regime.

One very specific debate within the Internet governance ecosystem involves the question of how to transition the United States' historic oversight of Internet names and numbers to what is usually described as the global multi-stakeholder community. For more than a decade, Internet governance debates have discussed how to transition US control of the "IANA [Internet Assigned Numbers Authority] functions" at the heart of maintaining a stable and secure Domain Name System. The IANA functions are actually several tasks related to maintaining the globally unique identifiers necessary for the Internet to function, such as the assignment of technical protocol parameters, administration of the Internet's root zone file mapping top-level domains and Internet Protocol addresses, and allocation of Internet numbers. Some central administration has been necessary because of the technical requirement to maintain these resources as globally unique. This administrative oversight has been carried out by the National Telecommunications and Information Administration of the United States Department of Commerce, which also holds the contractual relationship with ICANN. For more than a decade, United States policy has included plans for increasing privatization and internationalization of this oversight. Most recently, the Obama administration announced a timeline for completing this transition.

The fourth and fifth chapters in this volume address various legal and governance aspects of the transition of the IANA functions from the United States to the global multi-stakeholder Internet governance community. Taken together, these chapters explain many of the global legal complexities inherent in administration of a technical infrastructure that crosses borders and jurisdictions. In the fourth chapter, *Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community*, Aaron Shull, Paul Twomey and Christopher S. Yoo (2014) respond directly to the US government's announcement to transition IANA functions with several ideas about how to both ensure the stability of infrastructure and meet the interests of global Internet users. The authors' recommendations centre on ensuring ICANN accountability through improvements to both internal and external evaluation processes and through considering transferring contractual terms into agreements between ICANN and IANA customers. In the fifth chapter, *ICANN: Bridging the Trust Gap*, Emily Taylor (2015) emphasizes how greater accountability in ICANN must be a central feature of an appropriate transition. She discusses the establishment of a diverse membership that oversees board decisions and amendments to bylaws and recommends "numerous horizontal and vertical accountability checks and balances" (p. 92) and greater financial transparency.

One of the challenges of both Internet policy making and scholarship addressing Internet policy is the rapid and relentless pace of technological change. Just over a decade ago, the most popular Internet applications and products (including Twitter and Reddit and smartphones) were not even in existence. Other dynamic features include rapid growth and rising social and economic dependencies that introduce new stakeholders and new institutions into Internet governance arenas. New innovations and new actors create new governance challenges in critical areas including cyber security, privacy and freedom of expression. In this collection's final chapter, *Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem*, Stefaan Verhulst and colleagues (2014) call for more creative Internet governance approaches that are able to keep up with fast-paced technological innovation. Drawing from both the theory and the practice of open governance, the scholars propose "distributed Internet governance" (p. 100). An issue-driven approach, this framework allows for collaboration between various actors and institutions that share their expertise to solve governance issues at the local and global level. Two related tools are at the centre of this framework. First, a "living database" (p. 109) facilitates data and information sharing on tried and new approaches, relevant actors and best practices. Similarly, "knowledge networks" (p. 110) allow experts to share their expertise and organize around issues within their scope of interest.

Taken together, these chapters bring into sharp relief the many global tensions over administrative control of the Internet and the governance innovations necessary to keep the Internet stable and secure in the midst of rapid technological change and rising contention. Internet

governance is not a single task or system but rather a series of many functions necessary to keep the Internet operational and to establish policies about the global flow of information. Many of these functions are appropriately carried out by the private sector, many by traditional governments, and others by the technical community via new global institutions such as ICANN and the IETF. Understanding what is at stake for the economy and society in keeping the shared global Internet operational helps convey the importance of maintaining a balance of powers via a distributed system of oversight in which no one actor has outsized control.

WORKS CITED

Bradshaw, Samantha, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond. 2015. *The Emergence of Contention in Global Internet Governance*. GCIG Paper Series No. 17. Waterloo, ON: CIGI.

Nye, Joseph S., Jr. 2014. *The Regime Complex for Managing Global Cyber Activities*. GCIG Paper Series No. 1. Waterloo, ON: CIGI.

Raymond, Mark and Laura DeNardis. 2016. *Multi-stakeholderism: Anatomy of an Inchoate Global Institution*. GCIG Paper Series No. 41. Waterloo, ON: CIGI.

Shull, Aaron, Paul Twomey and Christopher S. Yoo. 2014. *Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community*. GCIG Paper Series No. 3. Waterloo, ON: CIGI.

Taylor, Emily. 2015. *ICANN: Bridging the Trust Gap*. GCIG Paper Series No. 9. Waterloo, ON: CIGI.

Verhulst, Stefaan G., Beth S. Noveck, Jillian Raines and Antony Declercq. 2014. *Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem*. GCIG Paper Series No. 5. Waterloo, ON: CIGI.

ABOUT THE AUTHOR

Laura DeNardis, CIGI senior fellow, is a scholar of Internet architecture and governance and professor in the School of Communication at American University in Washington, DC. The author of *The Global War for Internet Governance* (Yale University Press, 2014) and several other books, her expertise has been featured in numerous publications. She serves as the director of research for the Global Commission on Internet Governance and is an affiliated fellow of the Yale Law School Information Society Project, where she previously served as executive director. Laura holds an A.B. in engineering science from Dartmouth College, a master's degree in engineering from Cornell University, a Ph.D. in science and technology studies from Virginia Tech, and was awarded a postdoctoral fellowship from Yale Law School.

CHAPTER ONE:
THE REGIME COMPLEX FOR MANAGING GLOBAL CYBER ACTIVITIES

Joseph S. Nye, Jr.

ACRONYMS

CERTs	computer emergency response teams
CSIS	Center for Strategic International Studies
DDoS	distributed denial-of-service
DNS	domain name system
GATT	General Agreement on Tariffs and Trade
GGE	Group of Governmental Experts (UN)
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ISOC	Internet Society
ISP	Internet service provider
ITU	International Telecommunication Union
LOAC	Laws of Armed Conflict
NSA	National Security Agency (US)
W3C	World Wide Web Consortium
WCIT	World Conference on International Telecommunications
WGIG	Working Group on Internet Governance (UN)
WIPO	World Intellectual Property Organization
WTO	World Trade Organization

INTRODUCTION

When we try to understand cyber governance, it is important to remember how new cyberspace is. "Cyberspace is an operational domain framed by use of electronics to…exploit information via interconnected systems and their associated infra structure" (Kuehl 2009). While the US Defense Department sponsored a modest connection of a few computers called ARPANET (Advanced Research Projects Agency Network) in 1969, and the World Wide Web was conceived in 1989, it has only been in the last decade and a half that the number of websites burgeoned, and businesses begin to use this new technology to shift production and procurement in complex global supply chains. In 1992, there were only a million users on the Internet (Starr 2009, 52); today, there are nearly three billion, and the Internet has become a substrate of modern economic, social and political life. And the volatility continues. Analysts are now trying to understand the implications of ubiquitous mobility, the "Internet of everything" and storage of "big data." Over the past 15 years, the advances in technology have far outstripped the ability of institutions of governance to respond, as well as our thinking about governance.

Since the 1970s, political scientists have looked at the international governance processes of various global affairs issues through the perspective of regime theory (Keohane and Nye 1977; Ruggie 1982). This chapter is a mapping exercise of cyber governance using regime theory. Regimes are the "principles, norms, rules and procedures that govern issue areas in international affairs," but these concepts have rarely been applied to the new cyber domain (Krasner 1983). In its early days, thinking about cyber governance was relatively primitive. Ideological libertarians proclaimed that "information wants to be free," portraying the Internet as the end of government controls. In practice, however, governments and geographical jurisdictions have been playing a major role in cyber governance right from the start (see Goldsmith and Wu 2006).

Cyberspace is a unique combination of physical and virtual properties.[1] The physical infrastructure layer largely follows the economic laws of rival resources and increasing marginal costs, and the political laws of sovereign governmental jurisdiction and control. The virtual or informational layers have economic network characteristics of increasing returns to scale, and political practices that make government jurisdictional control difficult.[2] Attacks from the informational realm, where costs are low, can be launched against the physical domain, where resources are scarce and expensive. Conversely, control of the physical layer can have both territorial and extraterritorial effects on the informational layers.

Governments and non-state actors cooperate and compete for power in this complex arena. Cyber power can be defined in terms of a set of resources that relate to the creation, control and communication of electronic and computer-based information — infrastructure, networks, software and human skills. This includes the Internet of networked computers, but also intranets, mesh nets, cellular technologies, cables and space-based communications. Cyber power can be used to produce preferred outcomes within cyberspace, or it can use cyber

1 Martin Libicki (2009, 12) distinguishes three layers of cyberspace: physical, syntactic and semantic. However, with applications added upon applications, the Internet can be conceived in multiple layers. See Blumenthal and Clark (2009, 206ff) for a four-layer model. Nazli Choucri (2012) has also proposed multiple layers.

2 Jonathan Zittrain points out that this may change as unowned apps, such as email, give way to proprietary apps, such as Facebook or Twitter direct messaging (pers. comm.).

instruments to produce preferred outcomes in other domains outside cyberspace. The Internet, which is a network of thousands of independently owned networks, is only part of cyberspace. Cyber attacks can come through several vectors, such as humans and hardware supply chains, as well as malware delivered over the network. Internet governance is the application by governments, the private sector and civil society of principles, norms, rules, procedures and programs that shape the evolution and use of the Internet (Working Group on Internet Governance [WGIG] 2005). Naming and numbering is only a small part of Internet governance, and while Internet governance is at the heart of cyberspace, it is only a subset of cyber governance.

ASPECTS OF CYBER GOVERNANCE

There is considerable insecurity in cyberspace because the barriers to entry are low and offence is cheaper than defence, which is why it is sometimes depicted as analogous to the ungoverned and lawless Wild West. In practice, however, there are many areas of private and public governance. Certain technical standards related to Internet protocols are set (or not) by consensus among engineers involved in the non-governmental Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C) and others. Their informal procedures eschew voting and are sometimes summarized as "rough consensus and running code."

The determination as to which of these standards is broadly applied often depends upon private corporate decisions about their inclusion in commercial products. Private contracts among different tiers of Internet service providers (ISPs) use BGP (border gateway protocols) and undersea cables to connect the many networks that make up the Internet. The Internet Corporation for Assigned Names and Numbers (ICANN) has had the legal status of a non-profit corporation under US law, although its procedures have evolved to include government voices (but not votes). In any event, its mandate is limited to domain names and assignment of top-level numeric addresses, not the full panoply of cyberspace governance. National governments control copyright and intellectual property laws, although they are subject to negotiation and litigation, sometimes within the frameworks of the World Intellectual Property Organization (WIPO) and the World Trade Organization (WTO). Governments also determine national spectrum allocation within an international framework negotiated at the International Telecommunication Union (ITU).

The United Nations Charter, the Laws of Armed Conflict (LOAC) and various regional organizations provide a general overarching framework as national governments try to manage problems of security and espionage. The Council of Europe's Convention on Cybercrime (2014) in Budapest provides a legal framework that has been ratified by 42 states. Incident response teams (computer emergency response teams [CERTs] and CSIRTs [Computer Security Incident Response Teams]) cooperate regionally and globally to share information about disruptions. Bilateral negotiations, track two dialogues, regular forums and independent commissions strive to develop norms and confidence-building measures. Much of the governance efforts occur within national legal frameworks, although the technological volatility of the cyber domain means that laws and regulations are always chasing a moving target.

The cyberspace domain is often described as a public good or a global commons, but these terms are an imperfect fit. A public good is one from which all can benefit and none should be excluded, and while this may describe some of the information protocols of the Internet, it does not describe the physical infrastructure, which is a scarce proprietary resource located within the boundaries of sovereign states and more like a "club good" available to some, but not all. And cyberspace is not a commons like the high seas, because parts of it are under sovereign control. At best, it is an "imperfect commons" or a condominium of joint ownership without well-developed rules (pers. comm. with James A. Lewis; see Center for Strategic International Studies [CSIS] 2008). It has also been termed a club good where a shared resource is subject to various degrees of exclusion according the rules and agreements of different institutions (Raymond 2013).

Cyberspace can also be categorized as what Elinor Ostrom termed a "common pool resource," from which exclusion is difficult and exploitation by one party can subtract value for other parties.[3] Government is not the sole solution to such common pool resource problems. Ostrom showed that community self-organization is possible under certain conditions. However, the conditions that she associated with successful self-governance are weak in many parts of the cyber domain because of the large size of the resource, the large number of users and the poor understanding of how the system will evolve (among others).

In its earliest days, the Internet was like a small village of known users — an authentication layer of code was not necessary and development of norms was simple in a climate of trust. All of that changed with burgeoning growth and commercial use. While the openness and accessibility of cyberspace as a medium of communication provide valuable benefits to all, free-riding behaviour in the form of crime, attacks and threats creates insecurity. The result is a demand for protection that can lead to fragmentation, "walled gardens," private networks and cyber equivalents to the seventeenth century enclosures that were used to solve that era's "tragedy of the commons" (Ostrom 2009, 421; Hurwitz 2009). Internet experts worry about "balkanization" or fragmentation. To some extent

3 See Ostrom et al. (1999, 278), for a challenge to Garrett Hardin's (1968, 1243) formulation of "the tragedy of the commons."

that has already occurred, yet most states do not want fragmentation into a "splinter-net" that would curtail economic benefits.

Providing security is a classic function of government, and some observers believe that growing insecurity will lead to an increased role for governments in cyberspace. Many states desire to extend their sovereignty in cyberspace, seeking the technological means to do so. As Diebert and Rohozinski (2010) put it, "securing cyberspace has definitely entailed a 'return of the state' but not in ways that suggest a return to the traditional Westphalian paradigm of state sovereignty." Moreover, while accounts of cyberwar have been exaggerated, cyber espionage is rampant and more than 30 governments are reputed to have developed offensive capabilities and doctrines for the use of cyber weapons (Rid 2013). US Cyber Command has announced plans to employ 6,000 professionals by 2016 (Garamone 2014). Ever since the Stuxnet virus was used to disrupt Iran's nuclear centrifuge program in 2009 and 2010, the hypothetical use of cyber weapons has become very real to governments (Demchak and Dombrowski 2011, 32).

Efforts to attack or secure a government network also involve the use of cyber weapons by non-state actors. The number of criminal attacks has increased, with estimates of global costs ranging from US$80–400 billion annually (Lewis and Baker 2013, 5). Corporations and private actors, however, can also help to protect the Internet, and this often entails devolution of responsibilities and authority (Deibert and Rohozinski 2010, 30; see Demchak and Dombrowski 2011). For example, banking and financial firms have developed their own elaborate systems of security and punishment through networks of connectedness, such as depriving repeat offenders of their trading rights, and by slowing speeds and raising transaction costs for addresses that are associated with suspect behaviour. Informal consortia, such as the Conficker Working Group, have arisen to deal with particular problems, and hacker groups like Anonymous have acted to punish corporate and government behaviour of which they disapprove.

Governments want to protect the Internet so their societies can continue to benefit from it, but at the same time, they also want to protect their societies from what might come through the Internet. China, for example, has developed a firewall and pressures Chinese companies to self-censor behind it, and the country could reduce its connections to the Internet if it is attacked (Clarke and Knake 2012, 146). Nonetheless, China — and other governments — still seeks the economic benefits of connectivity. The tension between protection of the Internet and protecting society leads to imperfect compromises (see Zittrain 2008). Reaching an agreement on norms to govern security is complicated by the fact that while Western countries speak of "cyber security," authoritarian countries such as Russia and China refer to "information security," which includes censorship of content that would be constitutionally protected in democratic states.

These differences were dramatized at the December 2012 World Conference on International Telecommunications (WCIT) convened by the ITU in Dubai. Although the meeting was ostensibly about updating telephony regulations, the underlying issue was the extent to which the ITU would play a role in the governance of the Internet. Authoritarian countries, and many developing countries, feel that their approach to security and development would benefit from the UN bloc politics that characterize the ITU. Moreover, they dislike the fact that ICANN is a non-profit incorporated in the United States and at least partially accountable to the US Commerce Department. Western governments, on the other hand, fear that the cumbersome features of the ITU would undercut the flexibility of the "multi-stakeholder" process that stresses the role of the private and non-profit sectors as well as governments. While there are different interpretations of multi-stakeholderism, which can be traced back to the Geneva and Tunis meetings of the UN's World Summit on the Information Society in 2003 and 2005 (Maurer 2011), respectively, the vote in Dubai was 89 to 55 (Klimburg 2013, 3) against the "Western" governments (including Japan and India). In the aftermath of the WCIT conference, there were articles about the crisis in Internet governance and worries about a new Cold War (see Klimburg 2013; Mueller 2012). Many of these fears were overstated, however, if one looks at cyber governance through the lens of regime theory.

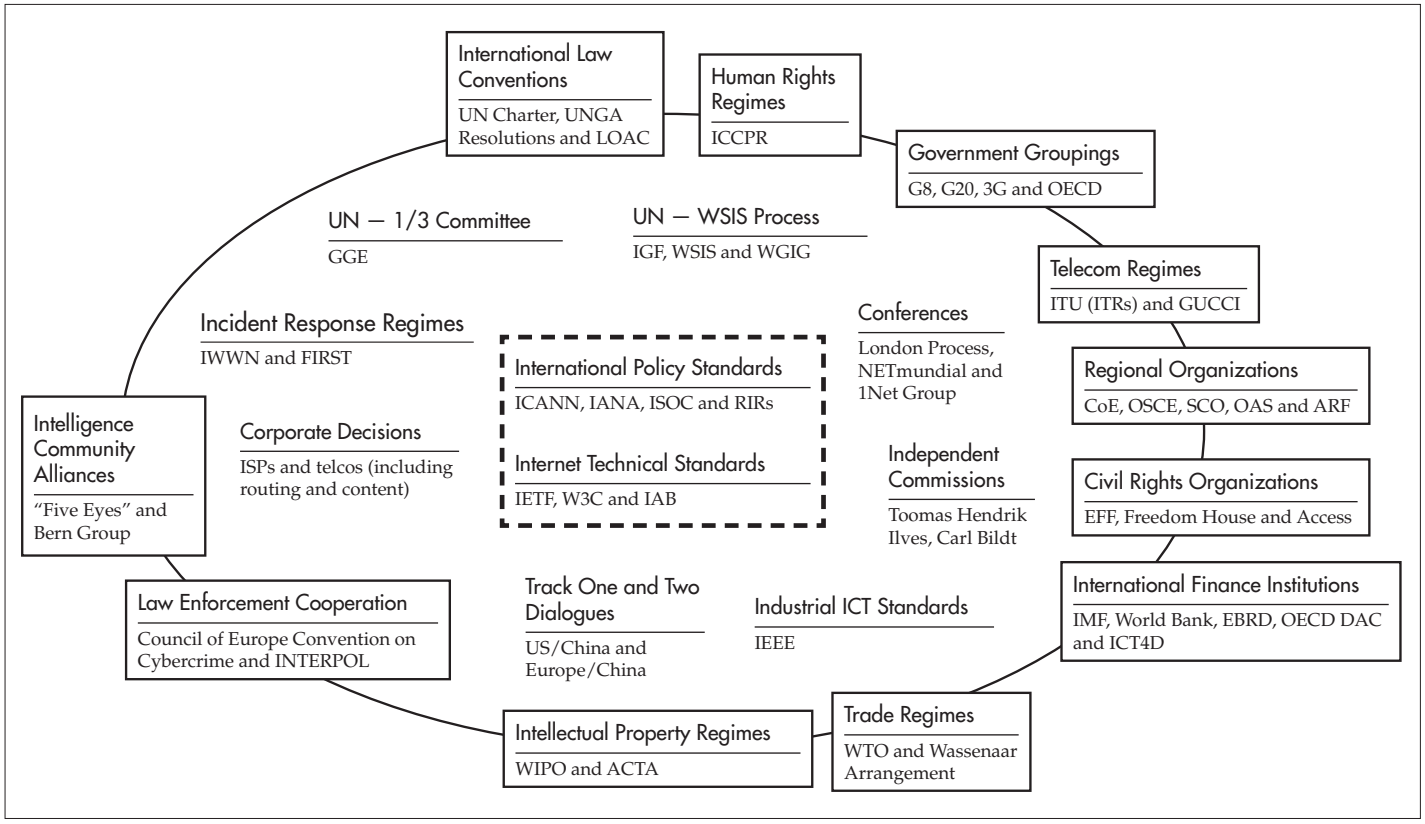
REGIMES AND REGIME COMPLEXES

Regimes are a subset of norms, which are shared expectations about appropriate behaviour. Norms can be descriptive, prescriptive or both. They can also be institutionalized (or not) to varying degrees. A regime has a degree of hierarchical coherence among norms. A regime complex is a loosely coupled set of regimes. On a spectrum of formal institutionalization, a regime complex is intermediate between a single legal instrument at one end and fragmented arrangements at the other. While there is no single regime for the governance of cyberspace, there is a set of loosely coupled norms and institutions that ranks somewhere between an integrated institution that imposes regulation through hierarchical rules, and highly fragmented practices and institutions with no identifiable core and non-existent linkages.

The oval map of cyber governance activities in Figure 1 mixes norms, institutions and procedures, some of which are large in scale, while others are relatively small; some are quite formal and some very informal. The labels are often arbitrary.[4] The oval is not designed to map all governance

4 I am indebted to Alexander Klimburg for help with the labels.

Figure 1: The Regime Complex for Managing Global Cyber Activities



Source: Author.

Acronyms for Figure 1

ACTA	Anti-Counterfeiting Trade Agreement	GUCCI	Global Undersea Communications Cable Infrastructure	ITRs	International Telecommunication Regulations
ARF	Association of Southeast Asian Nations Regional Forum	IAB	Internet Architecture Board	IWWN	International Watch and Warning Network
CoE	Council of Europe	IANA	Internet Assigned Numbers Authority	OAS	Organization of American States
DAC	Development Assistance Committee (OECD)	ICCPR	International Covenant on Civil and Political Rights	OECD	Organisation for Economic Co-operation and Development
EBRD	European Bank for Reconstruction and Development	ICT	information and communications technology	OSCE	Organization for Security and Co-operation in Europe
EFF	Electronic Frontier Foundation	ICT4D	Information and Communication Technologies for Development	RIRs	regional Internet registries
FIRST	Forum for Incident Response and Security Teams	IEEE	Institute of Electrical and Electronics Engineers	SCO	Shanghai Cooperation Organisation
"Five Eyes"	Alliance of Australia, Canada, New Zealand, the United Kingdom and the United States	IETF	Internet Engineering Task Force	telcos	telecommunications company
G8	Group of Eight	IGF	Internet Governance Forum	UNGA	United Nations General Assembly
G20	Group of Twenty	IMF	International Monetary Fund	WSIS	World Summit on the Information Society
GGE	Group of Governmental Experts (UN)	ISOC	Internet Society		

activities in cyberspace (which is a massive undertaking) and, thus, is deliberately incomplete. Like all heuristics, it distorts reality as it simplifies. Nonetheless, it is a useful corrective to the usual UN versus multi-stakeholder dichotomy as an approach to cyber governance, and it locates Internet governance within the larger context of cyber governance. First, it indicates the extent and wide range of actors and activities related to governance that exist in the space. Second, it separates issues related to the technical function of connectivity, such as the domain name system (DNS) and technical standards where a relatively coherent and hierarchical regime exists, from the much broader range of issues that constitute the larger regime complex. Third, it encourages us to think of layers and domains of cyber governance that are much broader than just the issues of DNS and ICANN, which have limited functions and little to do directly with larger issues such as security, human rights or development. As Laura DeNardis (2014, 226) writes, "a question such as 'who should control the Internet, the United Nations or some other organization' makes no sense whatsoever. The appropriate question involves determining what is the most effective form of governance in each specific context."

When we look at the whole range of cyber governance issues, some of the bipolarity in alignments that characterized the WCIT begins to erode. Liberalism is not the only divide. For example, some of the countries that voted against the West were not authoritarian, but were post-colonial or developing countries concerned about issues of sovereignty, which can be swayed by programs to develop their cyber capabilities or to protect the interests of their telecom companies. Also, within the liberal democratic bloc, there are important differences between the United States and Europe over issues of privacy, which have been increased by Edward Snowden's revelations regarding surveillance. Such issues may wind up having strong effects and being resolved within trade agreements like the proposed Trans-Atlantic Trade and Investment Partnership. It oversimplifies the politics of cyber governance to compress all of these dimensions into a bipolar dispute over liberal versus authoritarian approaches to content control.

This mapping of a regime complex also indicates the importance of linkages of cyber to normative and regime structures outside the issue area. The various actors that are located at the edge of the oval have independent structures of power and institutions outside the cyber issue area, but still play a significant role in issues of cyber governance. In other words, much of cyber governance comes from actors and institutions that are not focused purely on cyber. Moreover, these institutions compete and are used in a process of "contested multilateralism," whereby state and non-state actors seek to shape the norms that govern activities within the oval (Morse and Keohane, forthcoming).

Finally, this approach helps to relieve some of the fears of extreme balkanization. Interference with the central regime of domain names and standards could fragment the functioning of the Internet, and it might make sense to consider a special treaty limited to that area (Sofaer, Clark and Diffie 2010). However, trying to develop a treaty for the broad range of cyberspace as a whole could be counterproductive. The loose coupling among issues that now exists permits cooperation among actors in some areas at the same time that they have disagreements in others. For example, China and the United States can use the Internet for economic cooperation even as they differ on human rights and content control. Countries could cooperate on cybercrime, even while they differ on laws of war or espionage.

What regime complexes lack in coherence, they make up in flexibility and adaptability. Particularly in a domain with extremely volatile technological change, these characteristics help both states and non-state actors to adjust to uncertainty. Moreover, they permit the formation of clubs or smaller groupings of like-minded states than can pioneer the development of norms that may be extended to larger groups at a later time. As Keohane and Victor (2011, 7) note of the regime complex for climate change, "adaptability and flexibility are particularly important in a setting...in which the most demanding international commitments are interdependent yet governments vary widely in their interest and ability to implement them."

NORMS AND CYBER SUB-ISSUES

The norms that affect the various sub-issues of regime complexes can be compared along a variety of dimensions such as effectiveness, resilience, autonomy and others (Hasenclever, Mayer and Rittberger 1997). It is more useful to compare cyber issues in terms of four dimensions: depth, breadth, fabric and compliance. Depth refers to the hierarchical coherence of a set of rules or norms. Is there an overarching set of rules, which are compatible and mutually reinforcing (even if they are not adhered to or complied with by all actors)? For example, on the issue of domain names and standards, the norms, rules and procedures have coherence and depth; however, on the issue of espionage, there are few. Breadth refers to the scope of the numbers of state and non-state actors that have accepted a set of norms (whether they fully comply or not). For instance, on the issue of crime, 42 states have ratified the Budapest convention.

"Fabric" refers to the mix of state and non-state actors in an issue area. This is particularly interesting in cyber because the low barriers to entry mean many of the resources and much of the action is controlled by non-state actors. Issues with a high degree of state control have a "tight fabric"; those where non-state actors are pre-eminent have a loosely woven fabric. Security issues such as the laws of war in cyber have a tight fabric of sovereign control, while the DNS has a loose fabric in which non-state actors play

Table 1: Some Issues in the Cyber Regime Complex

	Depth	Breadth	Fabric	Compliance
DNS/standards	High	High	Loose	High
Crime	High	Medium	Mixed	Mixed
War/sabotage	Medium	Low	Tight	Low
Espionage	Low	Low	Mixed	Low
Privacy	Medium	Low	Mixed	Mixed
Content control	Low	Low	Loose	Low
Human rights	Medium	Medium	Loose	Low

Source: Author.

a major role. As suggested above, a loosely woven fabric is not synonymous with shallowness or incoherence. A fourth dimension for comparison is compliance: how widespread is the behavioural adherence to a set of norms? For instance, on the sub-issue of domain names and standards, compliance is high; on issues of privacy it is mixed; and on human rights it is low. Some of the major sub-issues of the cyber regime complex are compared along these dimensions below. (The list is not designed to be complete and other rows for trade, intellectual property or development can easily be added to the table.)

The variation in the characteristics of these sub-issues suggests why cyberspace is likely to remain a regime complex rather than a single, strong regime for some time. As Keohane and Victor (2011, 8) argue in regard to climate change, it is "actually many different cooperation problems, implying different tasks and structures. Three forces — the distribution of interests, the gains from linkages, and the management of uncertainty — help to account for the variation in the institutional outcomes, from integration to fragmentation." This is clearly true of cyberspace as well, though it is important to notice the difference there is one area of the cyber domain where interests and gains from linkages are strong enough that a coherent regime exists.

Partly because of strong common interests in connectivity, and partly because of path dependency and the way the basic standards of the Internet were established in the United States, there is a core regime related to standards and assigned names and numbers including management of the DNS root zone servers. While there has been controversy about the status of ICANN, and the US government has indicated it plans to devolve the IANA function to ICANN in the future, no state has thus far found it would benefit from ceasing to comply. The development of standards is advanced primarily by non-state actors, such as the IETF, the W3C, the IEEE and others, where states and voting have minimal effect. This is the area of cyber where the concept of multi-stakeholderism is most apparent.

Crime might seem to be the next likely sub-issue to be susceptible to regime formation. The issue has a loose fabric in which spammers, criminals and other free riders impose large costs on both states and private actors. The Budapest convention provides a coherent structure with depth, but its breadth has been limited by its origins in Europe. Many post-colonial countries and authoritarian countries such as Russia and China object to obligations that they see as intrusions on their sovereignty as well as the European origin of the norms. Some developing countries also see little to gain by joining, as few of their national companies would benefit, while they fear the potentially high costs of enforcement, should they to become signatories. Moreover, some private companies find it is in their economic interest to hide the extent to which they have been victimized and simply absorb it as a business cost, rather than suffer reputational and regulatory costs. States may also think that the costs are not high enough to merit action — even if cybercrime costs US$400 billion, it is still only 0.05 percent of global GDP. Thus, insurance markets are difficult to develop and compliance is far from satisfactory. This may change in the future if the costs of cybercrime increase, given its sophistication and scope. Despite differences over what information activities constitute a crime in authoritarian and democratic countries, cooperation could be modelled after extradition laws that relate to actions that are "doubly criminal" — that is, illegal in both countries.

War has an overarching normative structure that is derived from the UN Charter and the LOAC. The issue has a tight structure growing out of the nature of war as a sovereign action of states. The third meeting of the UN's GGE, which concluded in July 2013, agreed in principle that such laws applied in the cyber domain. What this means in practice, when there is great technological uncertainty, is more challenging. While a group of NATO legal scholars has produced the Tallinn Manual on International Law Applicable to Cyber Warfare — which attempts to translate general principles regarding proportion, discrimination and collateral damage into the cyber domain — the scope of the acceptance of these principles has been limited by its origins (Schmitt 2013). While there has been no cyberwar in a strict sense, there has been cyber sabotage, such as Stuxnet, and cyber instruments, such as distributed denial-of-service (DDoS) attacks, which were used in the Russian invasion of Georgia. On the other hand, there have been

press accounts that the United States decided not to use cyber adjuncts in Iraq, Libya and elsewhere, because of uncertainties about civilians and collateral damage (Schmitt and Shanker 2011; Markoff and Shanker 2009). Thus, compliance is judged with these norms as mixed.

According to press accounts, there is extensive use of cyber espionage by a wide variety of states and non-state actors. While espionage is an ancient practice that is not against international law, it often violates the domestic laws of sovereign states. Traditionally (for example, in the US-Soviet competition during the Cold War), rough "rules of the road" led to reciprocal expulsions and reductions in diplomatic missions as a means of regulating the friction created by espionage. Thus far, cyber espionage is so easy and relatively safe that no such rules of the road have been developed. The United States has complained about Chinese cyber espionage that steals intellectual property, and raised the issue at the summit between US President Barack Obama and President of the People's Republic of China Xi Jinping in June 2013. However, the US effort to create a norm that differentiates spying for commercial gain from all other spying has been lost in the noise created by the revelations of extensive National Security Agency (NSA) surveillance released by Snowden (Goldsmith 2013). Moreover, normative efforts have been plagued by the loose fabric of the issue. Although the exposure of Chinese spying in 2013 by Mandiant suggested a clear government connection, many other instances are more ambiguous about whether they are by government or non-state actors (Sanger, Barboza and Perlroth 2013).

Privacy is a sub-issue of growing importance given the increases in computing power and storage that are often summarized as the "era of big data." There are widespread concerns about companies, criminals and governments storing and misusing personal data. At the same time, in the age of social media, there are changing generational attitudes in many societies about where to draw the appropriate lines between public and private. Private terms-of-service agreements are often cumbersome and opaque to consumers. Additionally, personal identification information, once on the Internet, can end up in numerous places, rendering futile most efforts to have the initial posting site remove it. At the same time, European efforts to enforce a "right to be forgotten" with legal excisions of history have raised concerns among some civil libertarians. The concept of privacy is poorly defined and understood, and has very different legal structures in Europe and the United States, not to mention authoritarian states (see Brenner 2014). Thus, it is not surprising that while there are conflicting norms, the normative structure for the sub-issue lacks depth, breadth or compliance.

Content control is another sub-issue with conflicting norms with little depth or breadth. For authoritarian states, information that crosses borders by any means and jeopardizes the stability of a regime is a threat. The SCO has, therefore, expressed a concern about information security, and Russia and China have proposed UN resolutions to that effect. In practice, authoritarian countries filter such threatening messages and would like to have a normative structure that would encourage other states to comply. But the United States could not stop a Falun Gang email to China without violating the free speech clauses of the US Constitution. This is why democratic countries refer to cyber security and argue against the control of the content of Internet packets.

At the same time, democratic countries do control some content. Most try to stop child pornography but are divided on issues such as hate speech, and many Internet corporations have been caught between conflicting national legal systems. Moreover, this sub-issue has a loosely woven fabric and various private groups create black and gray lists of what they regard as violators of various norms. In some cases, these vigilantes have been able to borrow the authority of government (Mueller 2010, chapter 9). Copyright is another important area related to content control. For example, the proposed Stop Online Piracy Act in the US Congress would have required Web hosting companies, search engines and ISPs to sever relations with websites and users found in violation of copyright. While such measures have met with strong resistance, it is likely they will remain contentious both in domestic and transnational politics. Thus, there is no depth, breadth or widespread compliance with a normative structure for content control.

Human rights is a cyber sub-issue that has many of the same problems of conflicting values that plague content control, but there is an overriding legal structure in the form of the Universal Declaration of Human Rights. Moreover, in June 2012, the UN Human Rights Council affirmed that the same rights that people have off-line must also be protected online. Within the declaration, however, there is a potential tension between Article 19 (freedom of opinion and expression) and Article 29 (public order and general welfare). On the other hand, different states interpret the declaration in different ways, and authoritarian states that feel threatened by freedom of speech or assembly make no exceptions for the Internet. The US government has proclaimed an Internet freedom agenda, but has not explained whether this includes a right of privacy for foreigners. This agenda has also been complicated in the wake of the Snowden revelations. In 2011, the Netherlands held a conference that launched a Freedom Online Coalition, which now includes 22 states committed to human rights online, but the disparities in behaviour led to the conclusion that the normative structure in this sub-issue lacks depth, breadth or compliance. Nonetheless, the loose fabric of the issue allows ample opportunity for non-state actors to press for human rights in cyberspace. For instance, the civil society organization Global Network Initiative has been pressing private companies to sign

up to principles that advance transparency and respect human rights (MacKinnon 2012, chapter 14).

THE FUTURE DYNAMICS OF THE CYBER REGIME COMPLEX

Given the youth of the issue and the volatility of the technology, there are many potential paths along which cyber norms may evolve. Regime theorists have developed three quite different causal models that tend to complement each other. Realists argue that regimes are created and sustained by the most powerful state. Such hegemons have the incentive to provide public goods and discipline free riders because they will benefit disproportionately. But, as their power ebbs, the maintenance of regimes becomes more difficult (Gilpin 1987). From this point of view, the declining US control of the Internet suggests future fragmentation.

A second approach, liberal institutionalism, emphasizes the rational self-interest of states seeking the benefits of cooperative solutions to collective action problems. Regimes and their institutions help states achieve benefits by providing information and reducing transactions costs. They cut contracting costs, provide focal points, enhance transparency and credibility, monitor compliance and provide a basis for sanctioning deviant behaviour (Keohane 1984). This approach helps to explain why a regime exists for the DNS where perceived interests in cooperation are high, while a regime does not exist in the sub-issue of espionage where interests diverge significantly.

A constructivist set of theories emphasizes cognitive factors, such as how constituencies, groups and social movements change the perception and organization of their interests over time (Ruggie 1998). It is a cliché that states act in their national interest. The important question is how those interests are perceived and implemented. This is particularly important in the cyber domain, where the technology is new, and states are still struggling to understand and define their interests. In a chronological analogy, state learning of interests in the cyber domain is equivalent to about the year 1960, in what was then a new technology of nuclear weapons and nuclear energy (Nye 2011a). It was not until 1963 that the first arms control treaty was ratified — the atmospheric test ban — and 1968 that the Non-Proliferation Treaty was signed. The situation in cyber is made more complex by the much greater roles of a diverse set of private and non-profit actors responding to rapid social and economic change. Transnational epistemic communities of people and groups that share ideas and outlooks — such as ISOC and the IETF — play important roles (Adler and Haas 1992). Over time, the extent and interests of these cyber epistemic communities has grown. Cognitive theories help to explain the evolution of norms, but also why there is considerable fragmentation in the normative structures of sub-issues like privacy, content control and human rights.

Optimists about the development of norms in the cyber regime complex can point to some recent evidence of progress. For example, the disagreement between the sovereigntist and multi-stakeholder philosophies seemed somewhat less stark at the NETmundial conference in Sao Paolo, Brazil in 2014 than at the WCIT conference in Dubai in 2012. Moreover, while early meetings of the GGE were unable to reach consensus, the latest meeting reached agreement on a number of points, including the principle that international laws of war applied to cyberspace. In addition, the number of states acceding to the Council of Europe's Convention on Cybercrime has gradually increased, and INTERPOL has established a cybercrime centre in Singapore. Forty-one states have agreed to use the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies to stop sales of spyware to authoritarian countries. There has been an increase in international and transnational cooperation among CERTs. Before the recent dispute over Ukraine, the United States and Russia agreed that their hotline arrangements would be extended to cyber events. The United States and China established an official working group on cyber in 2013. Numerous track two groups and various private conferences and commissions continued to work on the development of norms. Industry groups continued to work on standards regarding everything from undersea cable protection to financial services. And non-profit groups pressed companies and governments to protect privacy and human rights.

Conversely, pessimists about normative change in the cyber regime complex point to the overall decline of the trust that is so important in the issue area. Some observers date this loss to what they see as the militarization of cyberspace symbolized by: the DDOS attacks that accompanied the Russian disruption of Estonia in 2007 and invasion of Georgia in 2008; the establishment of the American Cyber Command in 2009; and the discovery of Stuxnet in 2010. Others point to the 2013 Snowden revelations that the NSA not only carried out espionage (which is not new or unique), but allegedly subverted encryption standards and open-source software. Some technologists believe that trust can be rebuilt from the bottom up with new software technologies, as well as procedures for inspection of hardware supply chains. Others argue that low trust will be a persistent condition and it will exacerbate a fragmenting trend toward greater control by sovereign states (see Schneier 2013).

Some analysts reinforce their pessimistic projections by pointing to realist theories about the decline of US hegemony over the Internet. In its early days, the Internet was largely American, but today, China has twice as many users as the United States. Where once only roman characters were used on the internet and HTML tags

were based on abbreviated English words, now there are generic top-level domain names in Chinese, Arabic and Cyrillic scripts, with more alphabets expected to come online shortly (ICANN 2013). And in 2014, the United States announced that it would relax its Department of Commerce's supervision of ICANN and the IANA function. Some experts worried that this would open the way for authoritarian states to try to exert control over the system of root zone servers, and use that to censor the addresses of opponents.

Such fears seem exaggerated both on technical grounds and in their underlying premises. Not only would such censorship be difficult, but, as liberal institutionalist theories point out, there are self-interested grounds for states to avoid such fragmentation of the Internet. In addition, the descriptions in the decline in US power in the cyber regime are overstated. Not only does the United States remain the second-largest user of the Internet, but it is also the home of eight of the 10 largest global information companies (Statista 2013).[5] Moreover, when one looks at the composition of voluntary multi-stakeholder communities such as the IETF, one sees a disproportionate number of Americans participating for path dependent and technical expertise reasons. From an institutionalist or constructivist viewpoint, the loosening of US influence over ICANN could be seen as a strategy for strengthening the institution and reinforcing the American multi-stakeholder philosophy rather than as a sign of defeat (Zittrain 2014).

It is interesting to look at the experience of other regimes when US pre-eminence diminished in an issue area. In trade, for example, the United States was by far the largest trading nation when the General Agreement on Tariffs and Trade (GATT) was created in 1947, and the United States deliberately accepted trade discrimination by Europe and Japan as part of its Cold War strategy. After those countries recovered, they joined the United States in a club of like-minded nations within the GATT (Keohane and Nye 2001). In the 1990s, as other states' shares of global trade increased, the United States supported the expansion of GATT into the WTO, and the club model became obsolete. The United States supported Chinese accession to the WTO and China surpassed it as the world's largest trading nation. While global rounds of trade negotiations became more difficult to accomplish and various free trade agreements proliferated, the rules of the WTO continued to provide a general framework where the norm of most favoured nation status and reciprocity created a structure where particular club deals could be generalized to a larger number of countries. Moreover, new entrants, such as China, found it in their interests to observe even adverse judgments of the WTO dispute settlement process.

Similar to the non-proliferation regime, when the United States had a nuclear monopoly in the 1940s, it proposed the Baruch Plan for UN control, which the Soviet Union rejected in order to pursue it own nuclear weapons. In the 1950s as nuclear technology spread, the United States used the Atoms for Peace program, coupled with inspections by the new International Atomic Energy Agency, to try to separate the peaceful from weapons purposes. During the 1960s, the five nuclear weapon states negotiated the Non-Proliferation Treaty, which promised peaceful assistance to states that accepted a legal status of non-nuclear weapon states. In the 1970s, after India's explosion of a nuclear device and the further spread of technology for the enrichment and reprocessing of fissile materials, the United States and like-minded states created a Nuclear Suppliers Group that agreed "to exercise restraint" in the export of sensitive technologies, as well as an International National Nuclear Fuel Cycle Evaluation, which called into question the optimistic projections about the use of plutonium fuels. While none of these regime adaptations were perfect, and problems persist with North Korea and Iran today, the net effect of the normative structure was to slow the growth in the number of nuclear weapon states from the 25 expected in the 1960s to the nine that exist today (see Nye 1981). In 2003, the United States launched the Proliferation Security Initiative, a loosely structured grouping of countries that shares information and coordinates efforts to stop trafficking in nuclear proliferation-related materials.

In short, projections based on realist theories of hegemony are based on poorly specified indicators of change (see Nye 2011b, chapter 6). Even after monopolies over a new technology erode, it is possible to develop normative frameworks for governance of an issue area.

CONCLUSIONS

Predicting the future of the normative structures that will govern the various issues of cyberspace is difficult because of the newness and volatility of the technology, the rapid changes in economic and political interests, and the social and generational cognitive evolution that is affecting how state and non-state actors understand and define their interests. While the explanations are complementary, it seems likely that liberal institutionalist and cognitive regime theories will provide better tools for understanding those changes than oversimplified theories of hegemonic transition.

One projection does seem clear. It is unlikely that there will be a single overarching regime for cyberspace any time soon. A good deal of fragmentation exists now and is likely to persist. The evolution of the present regime complex, which lies halfway between a single coherent legal structure and complete fragmentation of normative structures, is more likely. Different sub-issues are likely to develop at different rates, with some progressing and

5 Note that Yahoo and Yahoo-Japan have been treated as one entity for the purposes of company rankings.

some regressing in the dimensions of depth, breadth and compliance. Some areas, such as crime, in which states have common interests against third-party free riders, seem ripe for interstate agreement, even if only an agreement to assist in legal and forensic efforts (Tikk 2011). Other issues, such as privacy, may see compromises in the context of trade negotiations, which apparently have no direct connection with the cyber area. And some areas, such as war, may not be susceptible to formal arms control agreements, but may see the evolution of declaratory policy, confidence-building measures and rough rules of the road. Rather than global agreements, like-minded states may act together to avoid destabilizing behaviour, and later try to generalize such behaviour to a broader group of actors through means ranging from formal negotiation to development assistance. Whatever the outcomes, analysts interested in the development of normative structures for the governance of cyberspace should avoid the over-simplified popular dichotomies of a "war" between the ITU and ICANN. Instead, they would do better to view the problems in the full complexity offered by regime theories and the concept of regime complexes.

ACKNOWLEDGEMENTS

I am indebted to Amelia Mitchell for research assistance, and to Laura DeNardis, Fen Hampson, Melissa Hathaway, Roger Hurwitz, James Lewis, Robert O. Keohane, Alexander Klimberg, John Mallery, Tim Maurer, Bruce Schneier and Jonathan Zittrain for comments.

WORKS CITED

Adler, Emmannuel and Peter M. Haas. 1992. "Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program." *International Organization* 46 (1): 367–90.

Blumenthal, Marjory and David D. Clark. 2009. "The Future of the Internet and Cyberpower." In *Cyberpower and National Security,* edited by Franklin D. Kramer, Stuart Starr and Larry K. Wentz. Washington, DC: National Defense University Press.

Brenner, Joel. 2013. "Mr. Wemmick's Condition; or Privacy as a Disposition, Complete with Skeptical Observations Regarding Various Regulatory Enthusiasms." *Lawfare Research Paper Series* 2 (1): 1–43.

Choucri, Nazli. 2012. *Cyberpolitics in International Relations.* Cambridge: MIT Press.

Clarke, Richard A. and Robert K. Knake. 2012. *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Ecco.

Council of Europe Convention on Cybercrime. 2014. "Convention on Cybercrime CETS No.: 185." http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

CSIS. 2008. *Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency.* Washington, DC: CSIS.

Deibert, Ronald J. and Rafal Rohozinski. 2010. "Risking Security: Policies and Paradoxes of Cyberspace Security." *International Political Sociology* 4 (1).

Demchak, Chris C. and Peter Dombrowski. 2011. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* (Spring).

DeNardis, Laura. 2014. *The Global War for Internet Governance.* New Haven: Yale University Press.

Garamone, Jim. 2014. "Hagel Thanks Alexander, Cyber Community for Defense Efforts." American Forces Press Service, March 28. www.defense.gov/news/newsarticle.aspx?id=121928.

Gilpin, Robert. 1987. "The Theory of Hegemonic Stability." *Understanding International Relations:* 477–84.

Goldsmith, Jack. 2013. "Reflections on U.S. Economic Espionage, Post-Snowden." Lawfare, December 10. www.lawfareblog.com/2013/12/reflections-on-u-s-economic-espionage-post-snowden/.

Goldsmith, Jack and Tim Wu. 2006. *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press.

Hardin, Garrett. 1968. "The Tragedy of the Commons." *Science* 162 (3859).

Hasenclever, Andrea, Peter Mayer and Volker Rittberger. 1997. *Theories of International Regimes.* Cambridge: Cambridge University Press.

Hurwitz, Roger. 2009. "The Prospects for Regulating Cyberspace." Unpublished paper. November.

ICANN. 2013. "Internet Domain Name Expansion Now Underway." News release, October 23. www.icann.org/en/news/press/releases/release-23oct13-en.

Keohane, Robert O. 1984. *After Hegemony: Cooperation and Discord in the World Political Economy.* Princeton, NJ: Princeton University Press.

Keohane, Robert O. and Joseph S. Nye. 1977. *Power and Interdependence.* Boston: Little, Brown.

———. 2001. "Between Centralization and Fragmentation: The Club Model of Multilateral Cooperation and Problems of Democratic Legitimacy." John F. Kennedy School of Government, Harvard University Faculty Research Working Paper Series, RWP01-004.

Keohane, Robert O. and David G. Victor. 2011. "The Regime Complex for Climate Change." *Perspectives on Politics* 9.

Klimburg, Alexander. 2013. "The Internet Yalta." Center for a New American Security Commentary. www.cnas.org/sites/default/files/publications-pdf/CNAS_WCIT_commentary%20corrected%20%2803.27.13%29.pdf.

Krasner, Stephen, ed. 1983. *International Regimes.* Ithaca, NY: Cornell University Press.

Kuehl, Daniel T. 2009. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security,* edited by Franklin D. Kramer, Stuart Starr and Larry K. Wentz, 26–28. Washington, DC: National Defense University Press.

Lewis, James A. and Stewart Baker. 2013. *The Economic Impact of Cybercrime and Cyberespionage.* CSIS report. http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

Libicki, Martin. 2009. *Cyberdeterrence and Cyberwar.* Santa Monica: RAND.

MacKinnon, Rebecca. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom.* New York: Basic Books.

Markoff, John and Thom Shanker. 2009. "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk." *The New York Times,* August 1. www.nytimes.com/2009/08/02/us/politics/02cyber.html.

Maurer, Tim. 2011. "Cyber Norm Emergence at the United Nations — An Analysis of the UN's Activities Regarding Cyber-security?" Belfer Center for Science and International Affairs, Harvard Kennedy School Discussion Paper 2011-11.

Morse, Julia and Robert O. Keohane. Forthcoming. "Contested Multilateralism." *The Review of International Organizations.*

Mueller, Milton. 2010. *Networks and States.* Cambridge, MA: MIT Press.

———. 2012. "ITU Phobia: Why WCIT Was Derailed." Internet Governance Project. www.internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/.

Nye, Joseph S. 1981. "Maintaining the Non-Proliferation Regime." *International Organization:* 15–38.

———. 2011a. "Nuclear Lessons for Cyber Security." *Strategic Studies Quarterly:* 18–38.

———. 2011b. *The Future of Power.* New York: PublicAffairs.

Ostrom, Elinor. 2009. "A General Framework for Analyzing Sustainability of Social-Ecological Systems." *Science* 325.

Ostrom, Elinor, Joanna Burger, Christopher Field, Richard Norgaard and David Policansky. 1999. "Revisiting the Commons: Local Lessons, Global Challenges." *Science* 284 (5412).

Raymond, Mark. 2013. "Puncturing the Myth of the Internet as a Commons." *Georgetown Journal of International Affairs Special Issue:* 5–15.

Rid, Thomas. 2013. *Cyber War Will Not Take Place.* New York: Oxford University Press.

Ruggie, John Gerard. 1982. "International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order." *International Organization* 36 (2).

———. 1998. "What Makes the World Hang Together? Neo-utilitarianism and the Social Constructivist Challenge." *International Organization* 42 (4): 855–85.

Sanger, David E., David Barboza and Nicole Perlroth. 2013. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." *The New York Times,* February 18. www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?pagewanted=all.

Schmitt, Eric and Thom Shanker. 2011. "U.S. Debated Cyberwarfare in Attack Plan on Libya." *The New York Times,* October 17. www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html.

Schmitt, Miachael N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press.

Schneier, Bruce. 2013. "The Battle for Power on the Internet." *The Atlantic,* October 24. www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/.

Sofaer, Abraham D., David Clark and Whitfield Diffie. 2010. "Cyber Security and International Agreements." In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, edited by Committee on Deterring Cyberattacks: Informing Strategies and Developing Options and National Research Council.* Washington, DC: National Academies Press.

Starr, Stuart H. 2009. "Toward a Preliminary Theory of Cyberpower." In *Cyberpower and National Security,* edited by Franklin D. Kramer, Stuart Starr and Larry K. Wentz. Washington, DC: National Defense UP.

Statista. 2013. "Market Value of the Largest Internet Companies Worldwide as of May 2013 (In Billion U.S. Dollars)." Statista. www.statista.com/statistics/277483/market-value-of-the-largest-internet-companies-worldwide/.

Tikk, Eneken. 2011. "Ten Rules for Cyber Security." *Survival* 53 (3): 119–32.

WGIG. 2005. *Report of the Working Group on Internet Governance.* Château de Bossey: WGIG. www.wgig.org/docs/WGIGREPORT.pdf.

Zittrain, Jonathan. 2008. *The Future of the Internet and How to Stop It.* New Haven: Yale University Press.

———. 2014. "No Barack Obama Isn't Handing Control of the Internet Over to China." *The New Republic* (224).

ABOUT THE AUTHOR

Joseph S. Nye, Jr. is a university distinguished service professor and former dean of the Kennedy School at Harvard University. He has served as assistant secretary of defense for International Security Affairs, chair of the National Intelligence Council and deputy under the secretary of state for Security Assistance, Science and Technology.

CHAPTER TWO:
MULTI-STAKEHOLDERISM: ANATOMY OF AN INCHOATE GLOBAL INSTITUTION

Mark Raymond and Laura DeNardis

ACRONYMS

DNS	Domain Name System
GAC	Governmental Advisory Committee
GAVI	Global Alliance for Vaccines and Immunization
Global Fund	Global Fund to Fight AIDS, Tuberculosis and Malaria
HTML	Hypertext Markup Language
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation of Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IGOs	intergovernmental organizations
IOSCO	International Organization of Securities Commission
IP	Internet Protocol
IPR	intellectual property rights
IR	international relations
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
NGO	non-governmental organization
NTIA	National Telecommunications and Information Administration
OECD	Organisation for Economic Co-operation and Development
RFC	Request for Comments
RSB	Roundtable on Sustainable Biomaterials
TCP	Transmission Control Protocol
TLD	top-level domain
W3C	World Wide Web Consortium
WGIG	Working Group on Internet Governance
WSIS	World Summit on the Information Society
XML	Extensible Mark-up Language

INTRODUCTION

In 1992, John Gerard Ruggie published a seminal article on the institution of multilateralism in a special issue of the journal *International Organization* (Ruggie 1992). This article and others in the special issue were not the first international relations (IR) work on multilateralism. However, Ruggie's article in particular catalyzed the emergence of a literature studying the phenomenon across a range of issue-areas,[1] and was enormously influential in the development of literatures on global governance and the structure of the international system (Ikenberry 2001; Reus-Smit 1997). In the ensuing decades, multilateral diplomacy has remained both an important object of scholarly inquiry and an enduring international institution.

At the same time, new practices and discourses have emerged in response to the efforts of a range of non-state actors to participate more fully in the enterprise of governing the globe, whether or not in multilateral processes (see Price 1998; Keck and Sikkink 1998; Weissbrodt and Kruger 2003; Glasius 2010). This chapter argues that much of this activity can be understood by thinking in terms of a distinct, emerging and as-yet inchoate institution of multi-stakeholderism or multi-stakeholder governance. Influenced by Ruggie's work on multilateralism, the chapter aims to conduct a parallel analysis of multi-stakeholderism. Existing studies of multi-stakeholderism tend to be issue-specific and concentrated in a small number of technical areas such as Internet governance (see Antonova 2008; Malcolm 2008). Further, the concept remains underdeveloped and susceptible to use in attempts to conceal or advance particular interests or agendas. The framing of multi-stakeholderism in juxtaposition with multilateralism highlights multi-stakeholderism as a broader phenomenon and facilitates comparative study. It also suggests (and speaks to the nature of) potential change in the fundamental institutions of the international system, sheds light on the existence of complex authority relations in that system and connects the global governance literature to the literature on the international system.

Multi-stakeholderism is defined here as two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules. The concept of multi-stakeholderism is further disaggregated into a typology that distinguishes several forms on the basis of the varieties of actors involved and the nature of authority relations between them. This typology reflects the existence of considerable variation among particular instantiations of the generic institutional

1 See, for example, Drezner (2000) on the efficacy of multilateral economic sanctions, and Wilkinson (2000) on multilateralism and international trade regulation.

form. In this sense, it is suggested that the rules and practices structuring the institution remain in flux. It is for this reason that multi-stakeholderism is referred to as an inchoate global institution.

The taxonomy is then applied to a comparative analysis of several examples of institutional arrangements sometimes considered multi-stakeholder. The first three cases address an area of global governance broadly recognized as increasingly contentious, and frequently described as multi-stakeholder — global governance of the Internet. Accordingly, this study makes important secondary contributions to the growing Internet governance literature. In this regard, it is emphasized both that multi-stakeholderism is not unique to Internet governance, and that not all Internet governance tasks and functions are accomplished via multi-stakeholder modalities. The fourth and fifth cases address global governance of securities trading by the International Organization of Securities Commissions (IOSCO) and governance of corporate social responsibility by the United Nations Global Compact. Presentation of the cases is followed by analysis of the variation in actor classes and authority relations, which are in important part the products of different sets of procedural rules that constitute, and therefore at least partially explain, particular instances of multi-stakeholder governance, and that also distinguish multi-stakeholder from non-multi-stakeholder governance (Wendt 1998).

The chapter concludes by offering critiques of how multi-stakeholder models are applied both in theory and practice, and by raising questions for future research about the factors determining whether (and in what form) multi-stakeholderism is practised in a particular issue-area, the dynamics of multi-stakeholderism over time and the appropriate criteria for matching governance modalities to particular governance functions. The chapter also highlights potential gains from increased attention in IR theory to the study of procedural rules, which, it argues, can productively inform scholarship on institutional forms, and on the nature and extent of authority relations in the international system.

FORMS OF MULTI-STAKEHOLDER GOVERNANCE

In the most general terms, multi-stakeholderism entails two or more classes of actors engaged in a common governance enterprise concerning issues they regard as public in nature, and characterized by polyarchic authority relations constituted by procedural rules. Further, there are many possible types of multi-stakeholder governance, produced by variation on at least two dimensions: the types of actors involved; and the nature of authority relations between actors. This section develops the various elements of this definition and explicates a typology of forms of multi-stakeholderism.

In order to qualify as multi-stakeholder governance, at least two classes of actors must be involved. This condition is similar to what Ruggie called the nominal or thin definition of multilateralism proposed by Robert O. Keohane (1990, 731): "the practice of co-ordinating national policies in groups of three or more states, through ad hoc arrangements or by means of institutions." Ruggie argued, persuasively, that such a thin definition of multilateralism "misses the *qualitative* dimension of the phenomenon that makes it distinct" and that "the issue is not the number of parties so much…as it is the kind of relations that are instituted among them" (1992, 566). Nevertheless, starting with the thin definition is appropriate for the purposes of this study because it leaves open the empirical question whether there is, in fact, a single distinctive kind of relation between actors typical of cases commonly described as multi-stakeholder.

Indeed, the available evidence shows that multi-stakeholder governance is (at least at present) a much less coherent institutional form than multilateralism. It is less coherent in the sense that the label multi-stakeholder is routinely applied both by participants and analysts to cases that exhibit significant variance in the nature of relations instituted among the actors. This variation is typically evident in the relevant procedural rules that constitute those relations. One response to this empirical finding would be to declare that multi-stakeholder governance is simply a buzzword rather than an identifiable institutional form. Such a response would amount to prematurely striking the tents. Actors seem eager both to talk about engaging in multi-stakeholderism and to engage in it — whether by speaking about it or in other ways. No doubt actors sometimes deploy the discourse of multi-stakeholderism for political purposes, but their decisions to do so themselves present an interesting puzzle: if the institutional form is ill-defined, why do actors find invoking it useful, and how are they invoking it to suit their purposes? Variation in the forms exhibited by instances of multi-stakeholderism does not provide grounds for abandoning the concept. Rather, it warrants the conclusion that there are several types of multi-stakeholderism. Adopting this stance enables further research on the development of this institutional form, and on the development of institutional forms in the international system more generally.

This study also departs from the literature on multilateralism by defining multi-stakeholder governance as involving two or more classes of actors, rather than three or more (state) parties. Lexically, the prefix "multi" can be used to refer to groups of two or more, or to groups of three or more. Because there is no need to distinguish multi-stakeholder governance from bi-stakeholder governance, since there is not an existing literature on the latter, multi-stakeholderism is defined more broadly here. The primary aim in this regard is to cast the analytical net as widely as possible, so as to

maximize the applicability of its framework to empirical cases. For instance, members of various non-governmental organization (NGO) and civil society communities that routinely engage with firms might well understand these efforts to be examples of multi-stakeholder governance and do not want to foreclose that possibility by fiat. However, defining multi-stakeholder governance to include any case involving two or more classes of actors is a tentative analytic choice that may require revision in light of evidence from further research.

This chapter specifies four classes of actors: states, formal intergovernmental organizations (IGOs), firms and civil society actors. None of these four classes is beyond criticism or without complication.[2] It might be desirable, for instance, to disaggregate the state and include at least some of its component parts in our framework separately. Independent regulatory agencies (such as the American Securities and Exchange Commission) might be identified as an actor class on the basis that they often participate in transgovernmental networks with important roles in global governance (see Slaughter 2004). It might also be important to distinguish between various kinds of firms: for example, publicly traded versus privately held, purely domestic or transnational corporations, or manufacturing firms versus service providers. Similarly, the civil society actor class might also be criticized for including NGOs, social movements, civil society networks and even individuals acting in their private capacities.[3] Kenneth W. Abbott and Duncan Snidal (2009b) opt to use NGOs as a category in their elaboration of the "governance triangle." They also opt against including IGOs as a category of actor, instead characterizing them as "important vehicles through which states manage competition and advance common interests" (ibid.). They justify this choice on the grounds that: IGOs "must ensure their organizational survival" and therefore "may be unwilling to take strong stands against their members, even if doing so is part of their fundamental raison d'être"; and that they "can also develop organizational pathologies that divert them from their missions" (ibid.).[4]

While there may be good reasons to disaggregate the state, firm and civil society actor classes, we have opted not to do so here to avoid further complication in the typology of multi-stakeholder governance forms developed below. Further research could expand these categories in order to assess whether the analytical leverage gained outweighs the loss of parsimony. However, IGOs should be included as a separate actor category and there are four reasons this choice is appropriate. First, there are circumstances under which it is reasonable to expect that agents will possess significant autonomy from principals.[5] Second, even if IGOs are in many cases constrained by the wishes of their member-states, it does not necessarily follow that they should be omitted as a class of actor. After all, some members of each of the other three actor classes can plausibly be understood to face similar constraints. States, and especially democracies, can be understood as agents of their citizens; firms as agents of their owners or shareholders; and NGOs as agents of their members. Third, any concerns such as Abbott and Snidal's about the possibility of organizational pathology is similarly present in states, firms and civil society actors. Fourth, many IGOs have degrees of the "essential capacities" that Abbott and Snidal (2009b, 46) associate with actors engaged in regulatory standard-setting processes: independence, representativeness, expertise and operational capacity. Therefore, IGOs are included as a distinct actor class in this typology; however, we leave open the empirical question of the extent to which IGOs are actual participants in particular instances of multi-stakeholder governance. Based on four classes of actors, and the limiting condition that multi-stakeholder governance must involve at least two of the four classes, there are 11 possible combinations of actor types: a single combination of all four classes, four combinations of three classes and six combinations of two classes.

In order to qualify as multi-stakeholder governance, a case must also involve governance. This raises additional definitional complications. With respect to global governance, Thomas G. Weiss and Rorden Wilkinson (2014, 207) have argued that "imprecision has robbed the term of conceptual rigor." While they do not advance a definition, they identify the need for further research in four areas: historicizing the notion of global governance; identifying and explaining "structures of global authority"; investigating "the myriad ways that power is exercised within such a system"; and improving the discipline's ability to "account for changes in and of the system" by focusing on "the causes, consequences, and drivers of change" (ibid.). James N. Rosenau deliberately advanced a capacious definition, which conceived global governance "to include systems of rule at all levels of human activity — from the family to the international organization — in which the pursuit of goals through the exercise of control has transnational repercussions" (1995, 13-14). He refined this conception slightly in arguing that governance "encompasses the activities of governments, but it also includes the many other channels through which 'commands' flow in the forms of goals framed, directives issued, and policies pursued" (ibid.). The research agenda advanced by Weiss and Wilkinson, and the conception

2 We owe several of the following possibilities to the excellent suggestions of the anonymous reviewers.

3 There is now a voluminous literature on such non-state actors in world politics. One important example is Keck and Sikkink (1998).

4 On the application of principal-agent theory to IR, see Hawkins et al. (2006).

5 For a discussion of such circumstances in the context of international institutions and governance, see Abbott and Snidal (2000).

of governance provided by Rosenau, are both extremely useful in thinking about (global) governance. They are less helpful for deciding what does and does not count as governance. For the purposes of this analysis, we adopt a definition recently developed by David A. Welch in collaboration with students in a graduate seminar; they define governance as "the coordinated, polycentric management of issues purposefully directed toward particular outcomes" (2013, 257). The strengths of this definition for the purposes of examining the phenomenon of multi-stakeholder governance are its agnosticism with respect to precisely how issues are handled and to the identity of the actors handling them, and its recognition that governance is polycentric in nature.

While Welch's crowdsourced definition is useful, two issues require further comment. First, governance (like government) is concerned with managing issues understood by the actors involved to be of shared concern, or part of the public sphere. Thus, we exclude from our conception of multi-stakeholder governance any arrangements concerned primarily with actors' private conduct. However, in so doing, the boundaries of the public sphere are socially constructed rather than natural and fixed. Therefore, the relevant standards for determining whether a particular matter is public or private (and thus legitimately a potential matter of governance or not) are those of the actors rather than of the analyst. Actors contest such boundaries, and the content of their shared agendas; the Internet governance cases examined below demonstrate a great deal of this kind of contention. In noting the public nature of governance, however, it is crucial to remember that this does not entail restriction of participation exclusively to public actors. Private and civil society actors expend a great deal of effort to influence the management of public issues, for a variety of reasons having to do with both their interests and values. Furthermore, relevant procedural rules increasingly accord them the ability, and in some cases even the right, to do so. These procedural innovations are crucial to the emergence of multi-stakeholderism as an institutional form.[6]

Second, the Welch definition treats governance as inherently polycentric — a quality seemingly similar to multi-stakeholderism; however, the two are not identical, as a particular instance of governance may not include multiple actor types. The original articulation of polycentric governance was provided by Vincent Ostrom, Charles M. Tiebout and Robert Warren (1961, 831-32), who wrote that polycentricity "connotes many centers of decision making that are formally independent of one another." They noted further that "whether they actually function independently, or instead constitute an interdependent system of relations, is an empirical question in particular cases" (ibid.; see also Ostrom 2010). Rather than being a rare or special condition, polycentricity thus defined is in fact incredibly common. Most importantly here, it does not require the involvement of multiple classes of actors. Thus, a diplomatic arrangement between states qualifies as polycentric but not multi-stakeholder. So, too, does the creation of an industry association of firms. In contrast, it is difficult to conceive of multi-stakeholder governance that is not polycentric. Such polycentrism can take at least two forms. The first involves an arrangement wherein multiple actor types participate in the operation of a dominant organization responsible for governing a particular issue, or what Tim Büthe and Walter Mattli have called a focal institution (2011, 5, 18–20). The Internet Corporation for Assigned Names and Numbers (ICANN) is such an example with respect to the administration of the Internet's Domain Name System (DNS). The second type of polycentrism consistent with our notion of multi-stakeholderism more closely resembles a regime complex. A regime complex involves multiple issue-specific regimes with overlapping membership and subject matter, as well as "problematic interactions" between the individual regimes (Orsini, Morin and Young 2013, 29). To qualify as a case of multi-stakeholder governance, a regime complex would need to include at least two classes of actors. Joseph S. Nye Jr. (2014) has argued for shifting analytical focus from the narrow Internet governance regime to a broader cyber regime complex that includes all four classes of actors identified here. The coexistence of both kinds of polycentrism within one issue-area illustrates the diversity of particular cases of the general class of multi-stakeholderism, in line with our argument.

These types of polycentrism illustrate the importance of Ruggie's focus on the nature of relations among actors in constituting particular institutional forms. We proceed along the same analytical lines, but reach a different conclusion about the degree of coherence in the generic institutional form of multi-stakeholderism than Ruggie reached with respect to multilateralism. To the extent possible, we identify conceptual boundaries for the kinds of relations among actors consistent with multi-stakeholderism as an institutional form. Governance arrangements can vary according to the nature of the authority relations among actors. This manner of variation is appropriately absent from Ruggie's discussion of multilateralism as an institutional form because the intersubjective understandings and social practices that constitute it limit participation to states and enshrine participation on the basis of formal sovereign equality. These features are inherent to Ruggie's thick definition of multilateralism as "an institutional form which coordinates relations among three or more states on the basis of 'generalized' principles of conduct — that is, principles which specify appropriate conduct for a class of actions, without regard to the particularistic interests of the parties or the strategic exigencies that may exist in any specific occurrence" (1992, 571). Christian Reus-Smit (1999, 9)

6 On the notion of a global public sphere and on emerging shifts in its nature, see Ruggie (2004).

characterizes modern international legal multilateralism in a similar fashion, as comprising "the principle that social rules should be authored by those subject to them" and "the precept that rules should be equally applicable to all subjects, in all like cases." Both the class of actor and the nature of authority relations in this institutional form are fixed, rendering a typology of the kind we construct unnecessary to the analysis of multilateralism.

Instances of multi-stakeholder governance are far less uniform and consistent. This is due in large part to significant variation in the nature of authority relations among actors. There are four ideal-typical possibilities: hierarchy, heterogeneous polyarchy, homogeneous polyarchy and anarchy. Hierarchy entails relations of superordination and subordination, where one is entitled to command and others have a duty to obey. Polyarchy entails situations where authority is distributed among a number of actors (see Dahl 1956; 1972).[7] This kind of distribution can be done in a heterogeneous manner in which distinct actors (or classes of actors) possess different formal powers (such as the division of authority between branches of government). It can also be done in a homogeneous manner, where actors have similar formal powers (such as individual voters in a democracy where each citizen receives an equal vote). As these examples make clear, actual systems of governance may blend elements of these ideal types. The fourth possibility is anarchy, a situation in which no authority relations exist. Of these four, only the two forms of polyarchy are consistent with multi-stakeholderism as an institutional form.

Although anarchy has been at the foundation of IR theory as an academic discipline (see Waltz 1979; Bull 2002), we discard the possibility of anarchic relations between actors (or classes of actors) engaged in a common governance enterprise on the basis of recent scholarship showing the presence of varying kinds and degrees of authority in international history,[8] and on the basis that IR theory has erred in typically attributing authority solely to actors (Hurd 1999; Raymond 2015). Authority is also a potential property of rules. In order for a common governance enterprise to exist, it is necessary that actors mutually accept the authority of a set of rules, however limited, that establishes the scope of the common governance enterprise, the kinds of actors entitled to participate in governance and the terms of that participation — including the way disputes about the application of general rules to particular cases will be handled. Many of these rules are procedural in nature. Even if actors are equally empowered by these rules to participate in the alteration, operation and termination of the governance arrangement in question, it is still accurate to describe the situation as containing authority relations; it is merely a special case where authority is shared equally and symmetrically. Equally shared authority should not be mistaken for the absence of authority. This mistake has unfortunately been all too common in a discipline defined by a binary juxtaposition of hierarchy and anarchy. A weak version of this claim about the ubiquity of authority relations, not hierarchy, in governance arrangements would be constrained to the empirical domain with which this chapter is concerned — the institutional form of multi-stakeholderism — and would suggest only that anarchy drops out of the multi-stakeholder governance typology developed here.

A strong version of this claim about authority relations has wide-ranging implications for IR theory. A full exploration of these implications is beyond the scope of this chapter, but there are a few provisional remarks to be made. First, the category error of treating authority as a binary property attributable only to actors and not also to rules has obscured a great deal of authority in the international system. If authority relations are instead understood in terms of the four categories identified here, it suggests that IR theory has miscoded the international state system as an instance of anarchy. Since international law and diplomacy as fundamental institutions of international society are themselves authoritative rule-sets and since they, at least in their modern variants, also empower state actors to make and alter international rules on a formally equal basis, there is a case for understanding the contemporary state system as a case of homogeneous polyarchy.[9] But this, too, is a simplification. As John M. Hobson and Jason C. Sharman (2005) have pointed out, the main actors in the international system over most of its history have been empires; thus, the system has historically contained elements of hierarchy in that imperial states and their colonies were differentially empowered in the operation, alteration and interpretation of international rules. This is only a single example of a fundamentally important point. A great deal more thinking and research are required to better understand authority relations in the international system. Accordingly, this study proceeds on the basis of the more limited claim that potential instances of anarchy fall outside of the institutional form of multi-stakeholderism.

While authority relations clearly exist in the international system, highly hierarchical social relations are not consistent with multi-stakeholderism as an institutional form (Hobson and Sharman 2005; Hurd 1999; Keene 2007; Keene 2013; Lake 2007; Lake 2009; Sharman 2013). Ideal-typical hierarchy leaves little room for agency on the part

7 For a review of Dahl's scholarship in broader context, see Krouse (1982).

8 See, for example, Sharman (2013); Keene (2007); and Hobson and Sharman (2005).

9 What is coded as "anarchy" in IR theory might also be understood, in similar terms, as what Ostrom, Tiebout and Warren (1961) define as polycentricity — namely, "many centers of decision making that are formally independent of one another." Since they wrote about governance of metropolitan areas, it is clear they did not understand these actors as operating in a context entirely devoid of authority relations.

of the subordinate actor in core governance tasks including rule making, interpretation and application. In such cases, the subordinate actor is a clear rule-taker. Accordingly, highly subordinate actors are not meaningful participants in governance; rather, they are the governed. For this reason, hierarchy is omitted from the kinds of relations among actors consistent with multi-stakeholderism.

However, it does not follow from the exclusion of ideal-typical hierarchy that authority is irrelevant to multi-stakeholderism. The four kinds of authority relations identified here are ideal-types; therefore, the framework departs from the IR literature on anarchy and hierarchy in treating authority relations as variegated rather than binary. David A. Lake (2007, 56) has suggested treating hierarchy as a continuous variable. While this treatment is an advance over traditional binary understandings of the relationship between anarchy and hierarchy, we prefer to think in terms of distinct types of authority relations. This move is crucial to our introduction of homogeneous and heterogeneous polyarchy, and to understanding multi-stakeholderism as an institutional form. Variation among different kinds of authority relations is not purely a matter of there being more or less of exactly the same kind of thing. Rather, individual instances of authority relations "are defined by shared rules and understandings that constitute them" (Raymond 2015). It follows that there can be substantial within-category variation among instances of both heterogeneous and even homogeneous polyarchy. That is, two different governance arrangements might be roughly equally heterogeneous in the way they distribute authority among participating actors, and yet exhibit important institutional differences.[10] If authority is thought of as only, or even primarily, varying in quantity rather than kind, this variation is rendered invisible. We believe this more granular understanding of authority relations serves as a correction both to the literature on anarchy and also to the emerging literature on hierarchy. However, more importantly here, this understanding highlights the connection between variation in procedural rules and variation in types of authority relations.

Combining the 11 possible combinations of actor types with the two categories of authority relations consistent with multi-stakeholderism yields 22 possible forms of multi-stakeholder governance (indicated by the check marks in Table 1).[11] This typology serves three purposes. First, it is a mechanism for identifying and classifying key features of actual cases. Second, it will also be useful in identifying (and ideally explaining) clusters and gaps in the distribution of actual governance institutions and processes; we do not expect that the actual universe of cases will be equally distributed among these possible forms. Third, with further research on the effectiveness of various governance modalities for specific kinds of issue-areas and governance functions, the typology presented here could assist in improving governance effectiveness by more appropriately matching governance functions with particular governance processes, mechanisms and institutions.[12] With this typology in mind, the following sections examine several cases of multi-stakeholder governance that vary based on the types of actors involved and the nature of authority relations between actors.

A COMPARATIVE STUDY OF MULTI-STAKEHOLDER GOVERNANCE AS A CLASS OF PHENOMENA

As a small but representative selection of cases of multi-stakeholder governance, this section examines the administration of Internet names and numbers by ICANN, standard setting by the Internet Engineering Task Force (IETF), international telecommunications regulation by the United Nations International Telecommunication Union (ITU), aspects of global financial governance by IOSCO and emerging governance of corporate social responsibility by the United Nations Global Compact.

A significant motivation for conceptually examining multi-stakeholderism emanates from prevailing global controversies over how the Internet is controlled, and uncritical and unexplained assertions that the Internet is, or should be, governed in a multi-stakeholder arrangement. As such, we were compelled in our own cases to include ICANN — the institution around which the majority of global deliberation on Internet governance revolves — and the ITU — an organization historically proposed as an alternative for taking over key functions of Internet governance, including some narrow tasks performed by the US government. In contrast to the turbulent global negotiations over the roles of ICANN and the ITU, the IETF has had a relatively uncontroversial, long and well-regarded history in Internet governance and is

10 One such example is the contrast between ancient Greek city-states and the contemporary international system given in Reus-Smit (1997). While he described these cases as different anarchies, if we are right about the authoritative nature of rules and institutions in constituting actors, these cases can be reconceived as (non-multi-stakeholder) homogeneous polyarchies.

11 Because only a single actor class is involved in multilateralism, it obviously does not appear in our typology. However, for purposes of comparing the institutional form of multilateralism with the institutional form of multi-stakeholderism, it is useful to note that the authority relations between state actors participating in multilateralism correspond closely to the category of homogeneous polyarchy in the table.

12 Expectations for such improvements should remain modest, however, given path dependency and the general inefficiency of institutional change. For arguments along these lines, see March and Olsen (1998) and Wendt (2001).

thus included for comparison. The fourth and fifth cases are included to complement the Internet governance issue-area and were selected because they are themselves described as multi-stakeholder. The inclusion of cases outside of Internet governance serves as a check on the prevailing discourses suggesting that multi-stakeholderism is unique to this issue-area — but it is not. Collectively, the cases exhibit variation in terms of the combination of actor classes, the issues involved and the forms of multi-stakeholderism employed. The final section of the chapter alludes to several other potential cases not examined in detail here. These and other cases offer opportunities for further research extending the framework developed herein.

Table 1: Types of Multi-stakeholder Governance

Stakeholder Types	Nature of Authority Relations			
	Hierarchy	Polyarchy		Anarchy
		Heterogeneous	Homogeneous	
States, IGOs, Firms, NGOs		✓	✓	
States, IGOs, Firms		✓	✓	
IGOs, Firms, NGOs		✓	✓	
States, IGOs, NGOs		✓	✓	
States, Firms, NGOs		✓	✓	
States, IGOs		✓	✓	
States, Firms		✓	✓	
States, NGOs		✓	✓	
IGOs, Firms		✓	✓	
IGOs, NGOs		✓	✓	
Firms, NGOs		✓	✓	

Source: Authors.

DISAGGREGATING MULTI-STAKEHOLDER INTERNET GOVERNANCE

An examination of cases of multi-stakeholder governance reasonably begins with governance of the Internet, both because it is an area so often considered as multi-stakeholder and also because of the rising importance of Internet coordination and oversight to economic, political and social life. Questions about the Internet's security and stability have emerged as a crucial international political concern on par with more long-standing global problems such as environmental protection, human rights, and basic infrastructural systems of finance, telecommunications, water and energy. These shared global issues transcend national borders and sovereignty. No state acting alone can address these issues *in toto*; yet local actions within national borders can have significant network externalities that reach across the globe.[13]

While Internet governance includes important instances of multi-stakeholder governance, and while preserving that model is a primary goal for the broader Internet community as well as for many governments, it is important to note that Internet governance is not a monolithic enterprise. Rather, it involves layers of distinct coordinating and administrative tasks that cumulatively keep the Internet operational. Many of these functions are accomplished in non-multi-stakeholder ways. Before turning to particular cases of Internet governance, therefore, there must be a more nuanced and disaggregated understanding of the broader landscape.

For the majority of its history, the Internet has been governed in a piecemeal fashion by a variety of standard-setting and other technical bodies, and by private companies performing key roles as network operators and information intermediaries. It is thus an excellent example of the power of epistemic communities to shape governance.[14] This legacy has generated two predominant characteristics of Internet governance arrangements. First, with a few notable exceptions, states have been either generally uninvolved or involved only as participants

13 While these issues are comparable in scale and significance, the Internet is not itself a commons. Given its non-rivalrous and excludable nature, it is more accurately thought of as a set of nested club goods. See Raymond (2013b).

14 On epistemic communities, see Haas (1992).

without superordinate decision-making authority.[15] Second, decision making for Internet governance has typically been driven by technical and market considerations. In terms of institutionalist IR scholarship, coordination problems have been more common than cooperation problems.[16] These features, and especially the general lack of an authoritative role for states, have led both scholars and practitioners to conclude that the Internet is an example of multi-stakeholder governance (see Cerf, Ryan and Senges 2014).

The computing devices and content to which end-users are exposed constitute only the surface of a massive underlying infrastructure of networks, services and institutions that keep the Internet operational. Most of this material and virtual architecture is comprised of private information intermediaries such as network operators, exchange points, search engines, hosting services, e-commerce platforms and social media providers. Despite the privatized and somewhat autonomous nature of these network components, global coordination is necessary to keep the overall Internet operational. Global technical standardization ensures interoperability; cyber-security governance maintains stability and authentication; and centralized coordination ensures that each Internet name and number is globally unique. These and other tasks necessary to keep the Internet operational, as well as the substantive public policy issues that arise around these functions, are collectively referred to as "global Internet governance."

Internet governance has sometimes been viewed by policy makers and scholars as a monolithic system. Hence, policy deliberations and scholarship examining multi-stakeholderism have analogously sought a uniform definition of what counts as participatory and diverse governance. Various definitions also reflect historically specific power struggles and stakeholder interests. The definition of Internet governance emerging from the aftermath of the 2003 World Summit on the Information Society (WSIS) in Geneva, Switzerland serves as an example of such homogeneity and politicization. Kofi Annan, former Secretary-General of the United Nations, established a Working Group on Internet Governance (WGIG) as a response to open issues over control of the Internet left unresolved at the WSIS.[17] The WGIG — which included 40 participants from government, the private sector and civil society — was charged with developing a definition of Internet governance: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet" (WGIG 2005).

The context from which this arose was politically charged and historically specific. There was mounting political concern over the unique and enduring role of the US Department of Commerce in contracting with ICANN to perform the global administration of Internet names and numbers. The states represented in the WSIS/WGIG process were primarily concerned with what they perceived as unilateral American control of the Internet. The ITU, the United Nations' specialized agency for information and communication technologies, was also increasingly stressing its intergovernmental legitimacy as a rationale for attempting to take a greater role in both the administration of names and numbers and the governance of Internet standards, to counter the prevailing administrative role of ICANN and the predominance of private-industry contributions in various standard-setting entities, including the IETF. Within this context, the WGIG definition conveyed some strong normative positions. The definition assigned an Internet governance role to "Governments," commensurate with global interest in greater multilateral administration and potentially a unique role for intergovernmental entities such as the United Nations in Internet oversight.

The composition of the WGIG did not represent key constituencies with a stake in the outcome of the definition or those with responsibility for Internet governance in practice. The UN group did not significantly include the input of large Internet users (for example, corporations relying on the Internet for financial and business transactions and basic operations); private sector companies involved in provisioning Internet products or providing infrastructure; or any representatives from the leading standard-setting and administrative entities operationally responsible for the security and stability of the Internet. The United States chose not to participate in the working group. Of the 40 members, the majority of participants were high-level governmental officials involved in national technology policy. Many of these officials represented countries — Saudi Arabia, Pakistan, Cuba, China, Egypt, Tunisia, Russia and Iran — with notoriously repressive Internet policies (WGIG 2005).

Thus, the formulation of an international definition of multi-stakeholderism was arguably not a multi-stakeholder effort. Also sometimes lost is that the convocation of the United Nations' Internet Governance Forum (IGF) — first held in Athens, Greece, in 2006 — was a compromise emanating from an impasse over UN and governmental calls for a diminishment of US coordination of certain Internet administrative functions and American resistance to these recommendations. The IGF was formed to create an international space for multi-stakeholder

15 This feature encapsulates part of what has been referred to as networked governance. See Mueller, Schmidt and Kuerbis (2013).

16 On the different implications of these styles of games, see Martin and Simmons (1998) and also Krasner (1991).

17 For background about the WSIS process, see Stauffacher and Kleinwächter (2005).

dialogue about Internet policy. These multi-stakeholder gatherings have been distinct from the actual *practice* of Internet governance; rather, they are *deliberations* about Internet policy. International gatherings, as "talk shops," potentially have agenda-setting and framing functions but, at least thus far, realistically have limited influence over policy making in practice (Dutton, Palfrey and Peltu 2007).

This distinction between Internet governance *discourse* and *praxis* highlights a prevailing feature of scholarship on multi-stakeholderism. Many examinations interrogate the question of who can contribute to discussions about Internet governance, particularly in the WSIS/WGIG/IGF context, rather than who can contribute to the actual *practice* of Internet governance (see Malcolm 2008; Epstein 2013). Although this question about multi-stakeholder dialogue is valuable *sui generis*, it does not directly address the question of how Internet coordination does or should occur in practice.

Within the actual practice of Internet governance, the phrase multi-stakeholderism is too often employed uniformly and uncritically. It is a misnomer to speak of *the* multi-stakeholder model for Internet governance. A question such as "Who should control the Internet: the United States, the United Nations or some other entity?" is incongruous because it inherently assumes that Internet governance is a singular system, and also completely discounts the highly privatized nature of Internet administration. There is no unitary system that oversees and coordinates the Internet. Some tasks are carried out by private industry operating as part of markets, some tasks are overseen by relatively new institutions such as ICANN, and some administrative jurisdiction resides with sovereign states or multilateral governmental coordination.

Explanations of the various tasks of Internet governance and associated taxonomies abound (see DeNardis 2014; Mathiason 2008; Mueller 2010; Bygrave and Bing 2009; Brousseau, Marzouki and Méadel 2012). One way to understand the Internet governance ecosystem is to divide its main functions into six areas: control of critical Internet resources; setting Internet standards; access and interconnection coordination; cyber-security governance; the policy role of information intermediaries; and architecture-based intellectual property rights (IPR) enforcement.

Critical Internet resources are the globally unique virtual identifiers — including domain names, Internet Protocol (IP) addresses and Autonomous System Numbers — necessary for the day-to-day operation of the Internet, as well as the DNS, a distributed set of servers that translates domain names into associated IP addresses for routing information to its destination. Internet standards are the common rules, or protocols, that computing devices follow to ensure global interoperability (for example, Transmission Control Protocol [TCP]/IP and Voice over Internet Protocol). Access and interconnection coordination addresses how various networks conjoin to collectively form the global Internet and the regulation of access, such as net neutrality rules. Cyber-security governance encompasses the challenge of securing the essential shared infrastructures of Internet governance, including routing, authentication systems and the DNS, as well as responding to Internet security problems such as worms and Distributed Denial of Service attacks. The policy role of private information intermediaries (such as Google and Facebook) includes functions such as the formulation of subscriber privacy rules or responding to government censorship and lawful intercept requests. Architecture-based IPR enforcement addresses the turn to infrastructure for copyright enforcement as well as IPR embedded within Internet governance infrastructure, such as the adjudication of domain name trademark disputes.

Table 2 disaggregates Internet governance into these six functional areas and then further into 43 specific tasks of administrative responsibility. The table also lists the primary, although often not exclusive, institutional actor historically responsible for executing each task. For example, under the functional area of Internet standardization, one critical task is the establishment of standards for the web, such as Hypertext Markup Language (HTML) and Extensible Mark-up Language (XML), primarily carried out institutionally by the World Wide Web Consortium (W3C).

The table captures several features of how Internet governance actually works. Most obviously, Internet governance is not a singular enterprise; the coordination and administration of the Internet involves many layers of distinct tasks. Equally evident, the Internet does not just autonomously "work" but remains operational via considerable, and sometimes costly, administrative coordination. This reality sits uneasily with some parts of the Internet community that embrace what can be thought of as "cyber libertarianism"; this view is encapsulated in the conviction that "legal concepts of property, expression, identity, movement, and context do not apply [online]… they are all based on matter, and there is no matter here" (Barlow 1996). There is, of course, matter: buildings, power supplies, switches, fiber optic equipment, routers and undersea cables. Many scholarly approaches from law, economics and communication inherently focus on content, applications or usage, and do not reach into many of the material and virtual technological functions of Internet governance.

A disaggregated Internet governance taxonomy also helps illustrate a connection between functional technological governance areas and direct public policy formulation. For example, IPR enforcement approaches designed to block access to users who have repeatedly downloaded copyrighted material have accompanying implications

Table 2: Disaggregated Internet Governance Taxonomy

Functional Area	Tasks	Primary Institutional Actor
Control of critical Internet resources	Central oversight of names and numbers	ICANN, Internet Assigned Numbers Authority (IANA), US Department of Commerce
	Technical design of IP addresses	IETF
	New top-level domain (TLD) approval	ICANN
	Domain name assignment	Internet registrars
	Authorization of root zone file changes	US Department of Commerce/National Telecommunications and Information Administration (NTIA)
	IP address distribution (allocation/assignment)	IANA, regional Internet registries, local Internet registries, national Internet registries, Internet Service Providers (ISPs)
	Management of root zone file	IANA
	Autonomous system number distribution	IANA, regional Internet registries
	Operating Internet root servers	VeriSign, Cogent and others
	Resolving DNS queries (billions per day)	Registry operators (VeriSign and others)
Setting Internet standards	Protocol number assignment	IANA
	Designing core Internet standards	IETF
	Designing core Web standards	W3C
	Establishing other communication standards	ITU, Institute of Electrical and Electronics Engineers, MPEG, JPEG, International Organization for Standardization (ISO) and others
Access and interconnection coordination	Facilitating network interconnection	Internet exchange point operators
	Peering and transit agreements to interconnect	Private network operators, content networks and content delivery networks
	Setting standards for interconnection (such as Border Gateway Patrol)	IETF
	Network management (quality of service)	Private network operators
	Setting end-user access and usage policies	Private network operators
	Regulating access (such as net neutrality)	National governments/agencies
Cyber-security governance	Securing network infrastructure	ISPs, network operators and private end-user networks
	Designing encryption standards	Standard-setting organizations
	Cyber-security regulation/enforcement	National statutes/multilateral agreements
	Correcting software security vulnerabilities	Software companies
	Software patch management	Private end-users
	Securing routing, addressing and DNS	Network operators, IETF and registries
	Responding to security problems	Computer emergency response teams and computer security incident response teams
	Trust intermediaries authenticating websites	Certificate authorities

(continued on next page)

Table 2 *(continued)*

Functional Area	Tasks	Primary Institutional Actor
Information intermediation	Commercial transaction facilitation	E-commerce sites and financial intermediaries
	Mediating government content removal requests (discretionary censorship)	Search engines, social media companies and content aggregation sites
	App mediation (guidelines and enforcement)	Smartphone providers (such as Apple)
	Establishing privacy policies (via end-user agreements and contracts)	Social media, advertising intermediaries, email providers and network operators
	Responding to cyberbullying and defamation	Content intermediaries
	Regulating privacy, reputation and speech	Statutory and constitutional law
	Mediating government requests for personal data	Content intermediaries and network operators
Architecture-based IPR enforcement	Domain name trademark dispute resolution	ICANN's Uniform Domain-Name Dispute-Resolution Policy, registrars and accredited dispute resolution providers
	Removal of copyright infringing content	Content intermediaries
	Algorithmic enforcement (such as search rankings)	Search engine companies
	Blocking access to infringing users	Network operators and ISPs
	DNS IPR enforcement	Registries/registrars
	Regulating online IPR enforcement	National statutes and international treaties
	Standards-based patent policies	Standard-setting organizations
	Enacting trade secrecy in content intermediation	Search engines and reputation engines

Source: Authors.

for freedom of expression, access and due process (Dutton et al. 2011). Similarly, private industry mediation of government content removal requests, and the decision to comply with or reject these requests, establishes conditions of what counts as free expression in the digital public sphere (Balkin 2008). These connections between technical coordination and public policy and the reality of highly privatized governance raise questions about adequate conditions of accountability, transparency and oversight for non-governmental actors to make and carry out such public policy.

Even such an extensive taxonomy misses part of how Internet governance works. Contextual factors such as technological constraints, economic conditions and social and cultural forces all shape the nature of this governance. For example, civic (as well as corporate) engagement influenced the failure of the Stop Online Piracy Act and PROTECT IP Act in the US Congress in 2012.

Even with these limitations, there are rational reasons to disaggregate Internet governance as practised into specific functions. These functions are performed by different types of actors. They also involve a variety of distinct governance activities such as contracting, deliberating, legislating, standard setting, regulating, adjudicating and enforcing.

This disaggregation also demonstrates that existing Internet governance arrangements vary in the classes of actors involved, and not all clearly meet the first criterion of multi-stakeholder governance provided above. Several specific functions of Internet governance are not multi-stakeholder at all because they involve a single actor or single class of actor. Many Internet governance functions have traditionally been governed solely by firms. An example involves the private contractual arrangements among private network operators to conjoin their networks at bilateral interconnection points or shared Internet exchange points. Private Internet registries, such as VeriSign, oversee the operation of generic TLDs. Network operators carry out network management tasks and respond to security problems on their private networks. Media companies set privacy policies to which users must agree before using these services. These are clear instances of how some Internet governance in practice does not currently meet our first, minimal criterion for multi-stakeholder governance (or how policy makers and the media describe Internet governance). This

privatization of oversight is a dominant feature of how Internet governance has evolved in practice.

Some functions are also relegated to the state, such as multilateral treaties about IPR enforcement. One contentious example is the authorization of changes to the Internet's root zone file[18] by an agency of the US Department of Commerce, the NTIA, although the United States announced in 2014 that it would transition this unique oversight to a global multi-stakeholder entity. International tension about how this transition would occur, as well as the privatized and contextually shaped nature of Internet governance and long-standing tensions between territorial state jurisdiction and non-territorial technological modes of communication, help explain the recent public attention to what counts as "multi-stakeholder governance" in each layer of Internet governance.

The key point here is that, contrary to popular narratives, much of Internet governance is not multi-stakeholder. However, the issue-area does include important cases of the institutional form. We examine three potential cases and find significant variation, including two very different forms of multi-stakeholderism and a third case (the ITU) that is ultimately classified as primarily hierarchical in terms of the relations among classes of actors.

ICANN

Considerable Internet governance scholarship focuses on the governance functions over critical Internet resources enacted by ICANN and the form of multi-stakeholderism that has arisen in ICANN (see Antonova 2008; Mueller 2002). ICANN is a private, non-profit corporation (incorporated in California) that formed in 1998 under contract with the US government to administer the Internet's names (for example, cnn.com) and numbers (the globally unique binary addresses assigned to computing devices, similar to postal addresses, but virtual rather than physical). ICANN and its assigned numbers authority, IANA, carry out a number of distinct functions including: allocation of blocks of Internet numbers to regional Internet registries for further distribution; oversight of the Internet's root server system operations; the establishment of policies for introducing new TLDs to the root system; oversight of domain name assignment, albeit delegated to Internet registrars; assignment of unique protocol parameters; and management of the root zone file.

The technical design decision requiring globally unique names and numbers to use the Internet created an accompanying need to ensure that each name and number is globally unique. The combination of this requirement for centralized control, the fact that there is a finite pool of these resources and the criticality of these resources for the ability to use the Internet has over time shaped a certain form of multi-stakeholderism. In the Internet's early history, a single individual, Jon Postel, administered names and numbers. In the context of Internet growth and globalization, this coordination institutionally evolved and eventually came under the auspices of ICANN.[19]

While ICANN and its subsidiary organization IANA carry out highly technical administrative functions, these functions have significant global public policy implications.[20] For example, the expansion of TLDs (such as .xxx, .wine, .amazon, .gay) raises public interest issues related to IPR, free speech and stakeholder interest disputes between territorial states and global corporations. Because of the significant number of stakeholders with an interest in critical Internet resources, the coordinating functions ICANN performs are viewed as inherently multi-stakeholder.

In terms of actors, the organization has a CEO and a board, each of which have particular authorities within the organization. Board members are selected by various stakeholder organizations (such as the Address Supporting Organization representing regional Internet registries) and an independent nominating committee made up of representatives from several supporting organizations and advisory committees.[21]

ICANN has three supporting organizations and four advisory committees.[22] While each of these entities is empowered by ICANN's procedural rules to do certain things, their formal roles differ. The GAC is especially noteworthy; it is unique among ICANN's component units in that when it issues formal advice to the ICANN Board, the board is required either to adopt the GAC's advice or to formally justify its refusal to do so in writing to the GAC. This provides the GAC (and thus its member governments) with a degree of authority over ICANN operations. GAC membership is open to national governments, but IGOs and treaty organizations often participate under observer status (such as the Organisation for Economic Co-operation and Development [OECD], the Council of Europe, the World Intellectual Property Organization, the ITU and others).

18 The root zone file (or root zone database) is the definitive list of IP addresses for servers for TLDs, including country code TLDs.

19 For an extensive description of ICANN functions and associated history, see Mueller (2002).

20 See DeNardis (2014, chapter 2) for a comprehensive list of the policy implications of Internet names and numbers.

21 See ICANN By-laws Article VII, Section 2, available at www.icann.org/resources/pages/bylaws-2012-02-25-en#VII-1.

22 The supporting organizations are the Generic Names Supporting Organization, the Address Supporting Organization and the Country Code Names Supporting Organization. The advisory committees are the Governmental Advisory Committee (GAC), the Security and Stability Advisory Committee, the Root Server System Advisory Committee and the At-Large Advisory Committee.

There has been international tension over the historic relationship between the US Department of Commerce, specifically the NTIA, and the control of a narrow but important set of Internet governance functions, including oversight of the Internet's root zone file that definitively tracks the list of names and IP addresses of all the authoritative servers for TLDs (such as .com, .edu., .uk). ICANN via IANA continues to administer the Internet's root on the basis of an agreement with the US government. The symbolic and practical implications of this American oversight have created pressure for greater internationalization of this narrow function and have more generally created tension in Internet governance debates.

In 2014, the Department of Commerce announced its intention to transition its historic oversight of Internet names and numbers, and specifically the IANA functions, to a "global multi-stakeholder community" (NTIA 2014). This announced transition, as well as a number of Internet governance controversies such as 2013 disclosures about the expansiveness of US National Security Agency surveillance, drew a great deal of public and media attention to the question of who controls the Internet and, by extension, considerable scrutiny over the structure and evolution of multi-stakeholder governance in ICANN.

ICANN is a clear example of Internet governance involving multiple types of stakeholders, including participants from corporations, civil society and governments. Further, ICANN can be classified as a heterogeneous polyarchy. Authority over distinct functions is distributed among various actors, with formal powers varying by actor. Even this relatively clear example of multi-stakeholder governance has been subject to criticisms ranging from insufficient civil society participation; insufficient government authority; too much government oversight; too much American authority; questions about legitimacy; and long-standing and ongoing concerns about its contractual relationship with the US government.

THE IETF AND INTERNET STANDARD SETTING

The IETF also has considerable coordinating influence over the Internet. It has developed many core Internet technical standards — such as the TCP/IP protocols — that serve as the rules enabling computing devices to exchange information over the Internet. Without these common specifications, devices made by one manufacturer would not be interoperable with other manufacturers' devices.

The IETF is one of many institutions that collectively create the blueprints enabling the Internet to have common addressing, compression standards, encryption standards, security standards, error detection and correction, formatting and other key engineering features. Another standards organization, the W3C, has established most core standards specific to the web (such as HTML and XML). While these organizations perform highly technical functions, they also enact public policy in a variety of ways. For example, the strength and features of encryption standards mediate between conflicting values of law enforcement and privacy. Web accessibility standards determine the extent of online accessibility for the disabled. Economically, common standards provide a level playing field for competition and have contributed greatly to the network effects and growth of the Internet.[23]

The IETF is in many ways more open, but less formally multi-stakeholder than ICANN. The organization does not have an official or defined membership. Anyone is permitted to participate in standards development, either via online mailing lists or in person at one of several yearly gatherings. Those participating do so in their individual capacities rather than on behalf of institutions but, in practice, are usually associated with an employer, especially large technology companies that inherently develop, implement and depend upon Internet standards in their products (IETF 2004). Others work for governments or, less frequently, for civil society institutions such as universities and NGOs. Despite the institutional norm of participants acting in their personal capacity, it is included here as a type of multi-stakeholder governance because many of the IETF's participants do in fact have other institutional affiliations with governments, NGOs and, of course, with corporations. Whereas IETF members participate in their individual capacities despite often having institutional affiliations, membership in the W3C is typically held by organizations, including companies, NGOs and units of governments, such as the Australian Government Information Management Office; each member has one advisory committee representative.

While this type of participatory openness is inclusive, meaningful participation requires specialized technical knowledge, the ability to speak English, funds to travel to international gatherings, and cultural competence in the stylistic and procedural norms of the organization. To this extent, even a completely participatory multi-stakeholder organization can have barriers related to knowledge, language, money and culture.

The IETF is also unusually open and transparent regarding its deliberative process, informational documents and standards. The entire history of its meeting proceedings is available online, as are most mailing list archives. The IETF has published the actual standards and supporting materials in an archive known as the Request for Comments (RFC) series.[24]

The IETF and the W3C can most accurately be classified as homogeneous polyarchies. The IETF has no formal

23 On the policy implications of standards, see Palfrey and Gasser (2012).

24 All of the Internet RFCs are freely accessible on the IETF website, available at www.ietf.org.

voting but makes decisions based on what has been called "rough consensus and running code" (a term derived from Clark 1992). Both the IETF and the W3C adopt proposed standards according to public commentary processes that are open to participation. Although particular individuals may wield greater or lesser influence in practice (typically according to technical expertise and/or reputation), this influence does not stem from procedural rules vesting authority in a particular office-holder.

THE ITU AND INTERNATIONAL TELECOMMUNICATIONS REGULATION

The ITU is a specialized UN agency with global coordinating responsibility for information and communication technology areas such as radio spectrum allocation, coordination of satellite orbital positions, telecommunications standards, and the promotion of information and communication infrastructure advancements in the developing world. Originally called the International Telegraph Union, the organization was founded in 1865 to arrange for global telegraph standards.

Because Internet data travels over a range of communication media, regulations set out by the ITU can influence most network operators. For example, it plays a facilitating role in the development of mobile communications networks that are increasingly important to Internet connectivity, especially in the developing world where wireless penetration is surpassing fixed broadband. The ITU also administers the International Telecommunications Regulation, a treaty comprising binding rules of international law.

As described earlier, there is also a long history of tensions between the US government's unique coordinating oversight of the Internet's names and numbers (that is, its contract with ICANN and oversight of root zone file changes) and international calls for moving this oversight function, as well as other areas of Internet governance, to the ITU. The impasse has become a historic legitimacy contest (see Bukovansky 2002). Many governments have requested a diminishment of the US Commerce Department's authority over the root, both symbolic and actual, and American interests have pushed back against the prospect of replacing this coordinating function with ITU oversight. For example, a 2012 US House of Representatives hearing addressed concerns about a possible takeover of multi-stakeholder Internet governance by the United Nations ITU.[25] The expressed position of the US government is to preserve the fundamental multi-stakeholder model of governance. The United Nations, the ITU and dominant multinational Internet companies have all espoused similar valorizations of multi-stakeholderism. These discourses around multi-stakeholderism reflect long-standing international tensions about administrative control of the Internet and they all fail to define what is acceptable multi-stakeholder governance for any particular function.

The ITU most centrally involves the representatives of governments (member states) but also includes international organizations, firms, NGOs and academic institutions that can pay an annual membership fee to become "sector members" and associates. Sector members, qua sector members, are not entitled to participate in altering either the Constitution and Convention of the ITU, or the treaties it oversees pertaining to radio communication or international telecommunications. These capacities are reserved to the ITU's 193 member states. Individual states may, and many routinely do, consult their sector members — even including them in treaty negotiation delegations — but such consultations are at the discretion of the state, which is equally free to consult interested parties that are not sector members. Sector members are able to participate more fully in the day-to-day standards-related work of the ITU. They receive access to the statistics and studies produced by the ITU in its information-gathering capacity, and they participate in its ongoing study groups. However, in a range of cases, study group recommendations must ultimately be approved by member states.

While we recognize that aspects of the ITU standard-setting process may approximate heterogeneous polyarchy, we nevertheless categorize the ITU as primarily hierarchical and thus not a case of multi-stakeholderism.[26] It reserves important rule-making functions solely to one class of stakeholder. Further, while ITU sector membership is open to international organizations, firms and academic institutions, it is not open to individuals. This differentiates it from many, though not all, other instances of multi-stakeholderism.

IOSCO

IOSCO establishes and promotes adherence to global standards for securities. It claims to regulate 95 percent of the securities markets around the world with the core objectives of protecting investors; maintaining fair, efficient and transparent markets; and decreasing systemic risks in global securities markets (IOSCO 2010, 3). IOSCO is primarily an example of heterogeneous polyarchy, but it is also a somewhat ambiguous case that includes elements of homogeneous polyarchy.

IOSCO's 198 members include three actor classes: states, IGOs and collections of firms. The organization recognizes three classes of membership: ordinary, associate and affiliate members. The largest group, ordinary members, includes national securities commissions such as the Securities and Exchange Commission in the United States and the Financial Services Agency in Japan. Associate

25 See *International Proposals to Regulate the Internet* (2012).

26 This characterization is consistent with Büthe and Mattli (2011, 34). They classify the ITU as a non-market public institution.

members are government agencies (other than principal securities regulators) or IGOs, such as the World Bank and International Monetary Fund, that have a relevant oversight function. Affiliate members include "self-regulatory organizations, stock exchanges, financial market infrastructures, investor protection funds and compensation funds, and other bodies with an appropriate interest in securities regulation."[27] These classes of membership instantiate heterogeneous polyarchy by differentially empowering actors to attend meetings, provide oral and written contributions to deliberations and to vote. In keeping with the expectations of IR theory, state actors are generally privileged in these matters; however, IOSCO's practice of awarding membership to specific securities regulation agencies complicates the typical treatment of the state as a unitary actor. This provides some basis to think that it might be analytically productive to disaggregate the state as a class of actor in multi-stakeholder governance, along the lines suggested by analysts who emphasize intergovernmental networks.

IOSCO is also notable in that self-regulatory organizations can become full voting members if they are the primary securities regulator for a particular jurisdiction. The potential inclusion of private, self-regulatory associations as voting members makes IOSCO a rare instance of multi-stakeholderism that contemplates formal procedural equality between state and private actors.[28] In such cases, the private actor would have a procedurally superordinate position to state agencies and IGOs in the associate member category as well as to other private actors in the affiliate member category. This complicates our treatment of polyarchy, in that authority relations do not break down neatly according to class of actor; a private ordinary member would have a formally equal position to some state agencies, a superordinate position with respect to others and would also have a superordinate position with respect to other private actors. This illustrates the growing complexity of authority relations in contemporary global governance and suggests that the typology presented here may eventually need to be extended in light of human creativity. Nevertheless, it remains generally reflective of current patterns of authority relations and represents an advance over previous binary treatments of authority in IR theory.

THE UNITED NATIONS GLOBAL COMPACT

The United Nations Global Compact is an initiative promoting corporate citizenship and socially responsible business practices in areas such as the promotion of human rights, environmental protection and the elimination of corruption. Launched by former UN Secretary-General Kofi Annan in 2000, it is a voluntary partnership between the United Nations and the private sector, with the involvement of hundreds of NGOs as equal partners. The core of the Global Compact is a set of principles drawn from international instruments including the Universal Declaration of Human Rights, the Fundamental Principles and Rights at Work and the Rio Declaration on Environment and Development. Participating firms are asked to "advocate the [Global Compact] in mission statements, annual reports, and similar public venues" to "raise the level of attention paid to, and the responsibility for, these concerns within firms" (Ruggie 2001, 371-72). They are also asked to contribute reports documenting their efforts to translate the core Global Compact principles into concrete action, as part of learning networks. Finally, they are asked to join UN "partnership projects to benefit developing countries" (ibid.).

An important caveat is that the principles of corporate citizenship adopted by the Global Compact do not have any binding authority, regulatory teeth or enforcement mechanism. Instead, it relies on market mechanisms, more direct forms of public pressure by civil society groups and on the force of legitimate international norms to generate pressure for compliance. But, like the example of voluntary technical standards above, it can be loosely categorized as an example of "governance" to the extent that it can contribute to norm setting and can influence and constrain private action in a number of public interest areas. Ruggie (2014, 10-11) has argued that the Global Compact is an interorganizational network, and that it constitutes an example of "new governance" wherein international organizations take what Abbott and Snidal have called a facilitative orchestration role (2009a, 558–75). Accordingly, it is also consistent with the working definition of governance we adopted above: "the coordinated, polycentric management of issues purposefully directed toward particular outcomes" (Welch 2013, 257).

The Global Compact involves IGOs, states, firms and NGOs. While it primarily entails firms committing to principles of corporate social responsibility, it also entails important roles for states, international organizations and civil society. States established the Global Compact via a UN General Assembly Resolution and provided voluntary funding, as well as diplomatic support (Ruggie 2004, 514). Firms' commitments are supplemented by the work of more than 100 local networks that conduct "learning exchanges, information sharing, working groups" and "partnerships and dialogues that tackle issues specific to local contexts" (UN Global Compact Office 2012, 6). The United Nations reports that these networks include "continued engagement by a diverse group of stakeholders, including academic institutions, business enterprises, NGOs and government entities" (ibid.). The Global Compact Board is "a multi-stakeholder

27 See IOSCO fact sheet at www.iosco.org/about/pdf/IOSCO-Fact-Sheet.pdf.

28 For information on IOSCO membership rules, see www.iosco.org/about/index.cfm?section=membership. On private international law-making in IOSCO, see Bradley (2005).

advisory body that meets annually…to provide ongoing strategic and policy advice for the initiative as a whole and make recommendations to the Global Compact Office, participants and other stakeholders."[29] It "is comprised of four constituency groups — business, civil society, labour and the United Nations — with differentiated roles and responsibilities apart from their overall advisory function."[30] Thus, the Global Compact has explicitly adopted the language of multi-stakeholder governance, and it has instantiated the concept in a heterogeneously polyarchic way, with differentiation of roles and responsibilities. While expressions of authority relations recede as a result of the relatively egalitarian distribution of authority among participants in the Global Compact, again it is important to recognize that the equal distribution of authority is not the same as its absence. The principles underlying the Global Compact and the more specific rules that outline conduct expected from participants are authoritative to the degree that participants accept them as legitimate. These rules differentially empower and constrain various actors; for example, constraining firms to meet their commitments, and constraining the United Nations, states and civil society groups from branding compliant firms as bad actors, while empowering them to criticize participating actors found to violate their commitments, as well as actors that refuse to participate.

VARIATION IN MULTI-STAKEHOLDER FORMS: AUTHORITY RELATIONS AND PROCEDURAL RULES

Claims about multi-stakeholder governance clearly permeate several areas of global concern such as environmental protection, human rights, Internet governance and finance. For scholars and practitioners of Internet governance, the issue-area in which this concept is most fully and consistently articulated, this examination is valuable in that it calls into question the article of faith that the Internet is governed in a unique, multi-stakeholder manner increasingly threatened by the encroachment of sovereign states. Multi-stakeholder governance is identifiable in other issue-areas such as financial governance and corporate social responsibility. Equally, some important Internet governance functions are performed in ways that are clearly not instances of multi-stakeholderism, such as the policy-making role of information intermediaries in establishing practices for dealing with public interest areas, such as cyberbullying, or establishing policies that directly determine the extent of user privacy online. Perhaps the most striking conclusion of our work for the study and practice of Internet governance is to call into question the extent to which Internet governance actually lives up to the talk about multi-stakeholderism. Across a number of crucial governance functions, the reality is perhaps closer to industry self-regulation than to genuine multi-stakeholder governance.

Of the five selected cases of institutions and initiatives that do involve multi-stakeholder coordination, there is variation in both types of actors and the authority relations among these actors. Table 3 summarizes this variation by classifying each case example into the schema of 22 forms of multi-stakeholder governance indicated in Table 1's taxonomy.

ICANN and the IETF both involve multiple types of stakeholders and both adopt authority relations distributed across these actors. In the case of ICANN, these authority relations are heterogeneous in the sense that formal powers vary by actor. Participation rights and decision-making powers in the IETF (and W3C) are more homogenously distributed among participants. The ITU, in contrast, is primarily hierarchical. Even though many classes of actors can weigh in as sector members, only member states are permitted to vote on international telecommunication regulations or on the organization's constitutive instrument, and member states must also approve some recommendations emerging from multi-stakeholder study groups. In the area of financial regulation, IOSCO is primarily an example of heterogeneous polyarchy (albeit with elements of homogenous polyarchy) with influence distributed among states, IGOs and firms in their capacity as participants in industry self-regulatory collectives. The UN Global Compact differentiates roles heterogeneously among all four actor classes — states, IGOs, firms and NGOs — but does so in the least hierarchical fashion among the three cases of heterogeneous polyarchy examined.

The five cases examined provide a small window into the variation in types of multi-stakeholder governance, but they do not exhaust the list of cases. In order to facilitate future scholarly work along these lines, we briefly survey additional instances of multi-stakeholderism that have been speculatively positioned in Table 3 using parentheses. We also discuss gaps in the empirical illustration of the typology. Finally, we turn to the implications of the findings of our cases.

First, while we have treated two specific Internet governance cases as individual instances of multi-stakeholderism, another possibility would be to treat the entirety of what practitioners routinely call "the Internet governance ecosystem" as a single, macro-level case of multi-stakeholderism. We opted not to take this approach, in order to point out meaningful variation in the way multi-stakeholderism is instantiated within this issue-area, and also to point out that much of Internet governance (including one of our cases) is decidedly not multi-stakeholder. We prefer Nye's approach drawing

29 See www.unglobalcompact.org/AboutTheGC/stages_of_development.html.

30 Ibid.

Table 3: Classification of Cases

Stakeholder Types	Nature of Authority Relations			
	Hierarchy	Polyarchy		Anarchy
		Heterogeneous	Homogeneous	
States, IGOs, Firms, NGOs	ITU	ICANN, Global Compact, (Global Fund to Fight AIDS, Tuberculosis and Malaria [Global Fund]), (Global Alliance for Vaccines and Immunization [GAVI])	(Roundtable on Sustainable Biomaterials [RSB])	
States, IGOs, Firms		IOSCO		
IGOs, Firms, NGOs				
States, IGOs, NGOs				
States, Firms, NGOs			IETF, W3C	
States, IGOs				
States, Firms			(International Accounting Standards Board), (ISO), (International Electrotechnical Commission)	
States, NGOs				
IGOs, Firms				
IGOs, NGOs				
Firms, NGOs				

Source: Authors.

on the regime complex literature, but feel it important to point out this alternate perspective.

Büthe and Mattli (2011) characterize the ISO, the International Electrotechnical Commission and the International Accounting Standards Board as private, non-market standard-setting bodies. However, this characterization overlooks the degree to which these bodies include a variety of types of actors. For example, the ISO is an international network comprising national standards bodies. Some of these bodies are government agencies or arms-length quasi-governmental entities, while others are non-profit entities, often with close ties to manufacturing firms. While the ISO and the International Electrotechnical Commission are instances of multi-stakeholderism, Büthe and Mattli's characterization of their activities as "centrally coordinated global networks comprising hundreds of technical committees," as well as their finding that these organizations are fundamentally political, is accurate (ibid., 5). Given the restriction of membership in these bodies to national standards bodies and the formally horizontal procedures for standard setting within them, we tentatively classify these three organizations as cases of homogeneous polyarchy including states and firms. Furthermore, Büthe and Mattli's focus on the politics of global rule making is compatible with the approach taken here.

Kenneth W. Abbott and David Gartner (2012, 4) find that "recent global health institutions have embraced a multi-stakeholder model in which [NGOs], the private sector, private foundations, and other constituencies within civil society — including populations directly affected by health threats — participate directly in governance structures, deliberation, and decision-making." They identify the Global Fund and GAVI as prominent examples. Both are broadly multi-stakeholder, including all four of the classes of actors we identify. Both also have complex governance structures that distribute roles and responsibilities differentially (see GAVI Alliance 2015; Global Fund 2014). Accordingly, we suggest they are best seen as instances of heterogeneous polyarchy.

Finally, the RSB is an instance of relatively homogeneous polyarchy including states, IGOs, firms and civil society

actors.[31] Members of the RSB are divided by actor class into seven "chambers": three comprised of firms; three comprised of various kinds of civil society organizations; and one combining government, IGOs and academics. Each chamber has equal weight in constituting the RSB's main governing body, the Assembly of Delegates. The assembly votes on modifications to the organization's core standards and appoints the RSB Board to run daily operations (RSB 2015). While voting shares are not equally allotted to different actor classes, the RSB does not distinguish classes of membership or endow different actor classes with distinctive powers and responsibilities.

One important cluster of cases not addressed here cuts across a wide variety of issue-areas: those involving states and IGOs. These are among the most familiar cases to students of IR, and can be reasonably expected to number among the most common types in practice, but they are not typically thought of as cases of multi-stakeholder governance. Recent scholarship has studied these relationships in terms of principal-agent theory (see Hawkins et al. 2006).[32] However, insofar as these agents exhibit de facto independence from their principals, it may be more productive to approach some such cases as instances of multi-stakeholder governance. Doing so places additional emphasis on the agency of at least some IGOs, and might permit more complete understanding of those that are highly autonomous in at least some areas of their work. Candidates for such treatment would include the European Union, as well as dispute resolution procedures in the World Trade Organization. At a minimum, there are parallels between multi-stakeholder governance and highly delegated principal-agent relationships that should be explored in greater depth; it may be that these relationships are best thought of in terms of a spectrum.

Shifting from examination of state-IGO relations in terms of principals delegating to agents, to an understanding of these relations in terms of multi-stakeholder governance also seems promising in light of the increasing role of civil society actors. Major IGOs increasingly face demands from civil society groups of various kinds, including NGOs and indigenous peoples' movements, as well as from firms. These non-state actors cannot formally delegate to IGOs by virtue of the structure of their constitutive instruments, but they increasingly factor into the decisions IGOs make about how to implement programs and fulfill their missions. This influence is difficult to explain as a function of the power resources possessed by these non-state actors, especially relative to those possessed by states. A better explanation might be that IGO secretariats increasingly accept as appropriate the notion that such non-state actors' concerns should be taken into account. Put another way, the secretariats increasingly accept that these non-state actors are entitled to participate as stakeholders in governance, albeit not typically in precisely the same ways as other classes of actors. Developing conceptual tools that more easily accommodate such emerging patterns may prove useful.

The range of cases involving states and firms is also not well covered by the empirical illustrations of this study. These include various kinds of regulatory mechanisms where private firms, and associations of firms, play governance roles with varying degrees of oversight from and interaction with state agencies (see Haufler 2001), as well as the standard-setting cases covered by Büthe and Mattli (2001). While such privatization of governance has occurred in a range of industry sectors, it has perhaps been most consequential in the global financial system, where it arguably compromised the effectiveness and legitimacy of the system and involved a high degree of regulatory capture (see Underhill and Zhang 2008; Baker 2010; Helleiner, Pagliari and Zimmerman 2010).

Taken together, the cases suggest that even using a limited set of examples, there is clearly variation among different instances of multi-stakeholder governance. Much of this variation is produced by the procedural rules constituting particular governance institutions, mechanisms and processes. These rules govern eligibility for various kinds of membership and the distribution of various decision-making capacities among members (including voting rules). They also establish standards for evaluating and responding to proposals, interpretations and arguments presented by other actors (Raymond 2011). They therefore simultaneously empower and constrain actors, to the point of determining whether and how they are entitled to participate in a particular governance process.

Thus, the nature of authority relations between actors in a given social context is a product of these procedural rules. Classifying a particular governance institution or organization as hierarchic or (homogeneously or heterogeneously) polyarchic is a matter of inductively identifying procedural rules. Further, two institutions or organizations that fall into the same broad classificatory category may also employ slightly different procedural rules that share family resemblances; and the same institution or organization may undergo change in its procedural rules over time, which may or may not require that it be reclassified in the schema proposed above. Finally, this means that if an attempt were made to make an institution more or less multi-stakeholder in nature, or if an attempt were made to change the form of multi-stakeholderism employed in a particular organization, the procedural rules would need to be changed. These changes must be such that different classes or combinations of classes of actors

31 We thank an anonymous reviewer for alerting us to the existence of the RSB.

32 This conception of the relationship between states and international organizations is similar to the notion of delegation elaborated in Abbott et al. (2000).

would be relatively enabled and constrained in exercising control over the institution or organization in question.

An understanding of the connections between procedural rules, authority relations and variations in forms of multi-stakeholder governance is important at least in part because in the absence of mutually agreed-upon procedural rules for rule making, interpretation and application, the creation of new governance mechanisms is unlikely. Discussions and negotiations are likely to founder on procedural grounds. Disagreement over procedural rules complicates not only the creation of new governance mechanisms, but also the operation of existing ones. This is because the social reproduction of these rules, institutions and processes occurs through the continued application of general rules to particular cases, which in turn depends on mutually accepted procedures for rule making, interpretation and application. Legitimate procedural rule-sets are therefore crucial to the continued operation of the extensive system of global governance that characterizes contemporary world politics. The increasing demands for increased participation (and new forms of participation) being articulated by emerging powers and by non-state actors are inconsistent both with each other and with pre-existing international rule-making procedures. Accordingly, the potential for increased friction is considerable and likely to grow.[33]

Such disagreements on legitimate procedures for rule making are evident in the Internet governance issue-area; at least five partially overlapping sets of procedural rules are identifiable. The first might usefully be called an OECD view, since it is held primarily by its member states. It consists of commitment to the rule of law (domestically and internationally), even to the point of considering a conditional view of sovereignty, along with acceptance of multilateral cooperation among states and the relatively routine consultation of stakeholders. This consultation of stakeholders has begun, primarily over the past 20 years, to take the form of increased reliance on industry self-regulation not only in the Internet field, but also in financial governance of various kinds and other areas involving technical standard setting. Within the information governance area broadly conceived, this procedural approach to rule making is evident in the 1988 International Telecommunications Regulation treaty and in the World Intellectual Property Organization.

The second set of procedural rules can be summarized as the Shanghai Cooperation Organisation view. It emphasizes great power privilege in the operation of the international system and entails a strong, rather than conditional, interpretation of sovereignty. It is based on hierarchical state-society relations and limited or nonexistent stakeholder consultation. This view is held primarily by China and Russia, but bears some similarities to the procedural views of the remaining BRICS countries (Brazil, India and South Africa). Because this approach to rule making is held by states that have lacked dominant influence both over the Internet and over world politics since the Internet's commercialization, institutionalized examples of such procedures are difficult to identify within the Internet governance issue-area. These views, however, inform the opposition of these states to legacy mechanisms of Internet governance given their connections to the United States; they also inform suspicion of, and opposition to, the multi-stakeholder model.

The third set of procedural rules is held by the primarily postcolonial members of the Group of 77. While this is the most diverse of the five sets of procedural rules, some commonalities can be identified. First, like the Shanghai Cooperation Organisation view, the Group of 77 view of procedural legitimacy emphasizes a robust conception of sovereignty. This insistence on sovereignty stems in part from the challenges faced by weak states emerging from colonization (Jackson 1990). In addition, these states struggle to varying extents with issues of expertise and capacity; these inequalities have contributed to preferences that privilege existing multilateral institutions (those with which states have extensive experience) over innovative forms of international and multi-stakeholder cooperation. The preference among many developing world states for a broader ITU role in Internet governance is an example of this preference for existing multilateral institutions with voting rules based on sovereign equality.

The first three sets of procedural rules are endemic to international relations, but the fourth and fifth are not. The epistemic community of technologists has a distinct view of how to legitimately make and interpret rules, which is perhaps best exemplified by the IETF's RFC process, in which "the basic ground rules were that anyone could say anything and that nothing was official" (see Reynolds and Postel 1987). The IETF (2004) mission statement continues to reflect this ethos, with its affirmation of the organization's commitment to "rough consensus and running code." Although individual bodies have their own processes, the Internet technical community tends to adopt horizontal, distributed and voluntary rule-making procedures reflective of its members' values.

Fifth, and finally, corporate stakeholders that have driven the development of the commercial Internet also have distinct views on rule making and interpretation. These views are rooted in voting by corporate boards subject to shareholder accountability, hierarchical chains of accountability within the firm and external relationships based on private contracts. Although some technology companies make conscious efforts to embody the spirit of the technical community, norms of corporate governance also affect their behaviour; this is especially true of companies that pursue public stock offerings. ICANN's

33 For a similar argument in the context of contemporary international law, see Raymond (2013a).

contractual model of delegating to regional Internet registries and to generic TLD registries is one example of Internet governance done on the basis of corporate procedural rules; interconnection between network operators is another.

The increasing importance of the Internet to everyday life has begun to generate new entrants into the governance process. Corporate actors were the first non-technical players, but the current trend is increased interest on the part of both industrial and non-industrial states. The Internet's growing integration with a range of public and private activities is also creating new interests and making additional social values salient for existing governance participants. Resolving the attendant conflicts and trade-offs is complicated by the diversity of views on appropriate procedures for making, interpreting and applying rules. Without a procedural *modus vivendi*, it is unlikely that distributional questions will be effectively addressed.[34]

CONCLUSION

This chapter attempts to provide a more nuanced study of multi-stakeholder governance as a class of phenomena across multiple issue-areas, albeit with particular attention to Internet governance issues. Multi-stakeholderism is not a single approach to governance, and multi-stakeholder forms of multi-stakeholder governance are not unique to, or even always applicable to, how the Internet is run.

Multi-stakeholderism is sometimes viewed as a value in itself rather than a possible set of approaches for meeting more salient public interest objectives such as human rights, Internet security and performance, or financial stability. The more appropriate approach to responsible and efficacious governance requires determining what types of administration are optimal in any *particular* functional and political context. For example, in the area of Internet governance, some policy-making tasks may appropriately be relegated to the private sector, some to the purview of traditional sovereign state governance or international treaty negotiations, and some more appropriately as multi-stakeholder. Determining which mode of governance is appropriate for various global administrative functions may require conceptual and theoretical tools that have not yet been developed. The study of multi-stakeholderism as an institutional form presented here provides a foundation on which they can be built.

The practical value of this approach is evident in the case of Internet governance. Our argument highlights a set of more prescriptive questions that are impossible without nuanced conceptions of Internet governance and of multi-stakeholderism such as the ones presented here. One such question is whether there is a need for more multi-stakeholderism in particular functional areas of Internet governance, or whether there are more effective and appropriate means of instantiating democratic values in areas of policy likely to engage important public values and interests. Another question made possible by a more sophisticated conceptual framework is whether particular governance functions are matched with appropriate forms of multi-stakeholder governance — or, more fundamentally, whether particular functions are better accomplished through means other than multi-stakeholderism. Finally, to what extent is the concept of multi-stakeholderism deployed as a proxy for broader political struggles, or as an impediment to the types of coordination necessary to promote conditions of responsible governance? For example, governments can advocate for top-down and formalized multi-stakeholderism to gain additional power in areas in which they have traditionally not had jurisdiction. Alternatively, companies and other actors with vested interests in current governance arrangements can deploy multi-stakeholderism in a manner either meant to exclude new entrants (whether public or private) with incommensurate interests and values, or to preserve incumbent market advantage.

Definitively answering such questions requires a great deal of further research on the connections between issue characteristics and the properties of rule-sets and organizations, on the one hand, and the effectiveness and legitimacy of governance on the other hand. It is especially important to adopt a broad comparative strategy that looks for insights from other related areas. Given the global nature of the Internet, literature in IR and global governance offers promising sources. However, scholars in these fields remain in the early stages both of understanding issues of institutional performance and design,[35] and of studying forms of governance where the state is (at least under some conditions) merely one actor among many.

In addition, the comparative study of multi-stakeholder governance as a class of phenomena offers substantial benefits to scholars of IR and global governance. First, it provides additional cases in which to study the role of private actors in governance. Second, it offers the potential to extend understanding of what kinds of institutions perform most effectively and enjoy greater legitimacy in dealing with novel, complex, technical and transnational issues of increasing political salience. It does so by extending the types of institutions studied in the literatures on institutional effectiveness and design. Third, it furnishes additional evidence of the presence and

34 IR theory has, with a small number of exceptions, taken insufficient notice of the empirical importance of justice considerations (whether procedural or distributive) in explaining outcomes. On these questions, see Welch (1993) and Albin (2001).

35 For one notable effort, see Koremenos, Lipson and Snidal (2001). See also the other articles in this special issue of *International Organization*, including the critical piece by Wendt (2001).

complexity of authority relations in international politics. It demonstrates the existence of authority relations in world politics in which the state is either absent or embroiled in heterogeneously polyarchic relations with non-state actors of various kinds. At a more general level, the comparative study of multi-stakeholder governance demonstrates the inadequacy of conceiving authority as binary and of understanding authority as a property solely of actors and not also of rules.

Finally, the argument presented here is relevant both to scholars of Internet governance and IR because it demonstrates the importance of procedural rules. Specifically, it clearly connects them to the study both of institutional forms and of authority in world politics. Such rules are critical to producing variation in institutional and organizational forms, both among and within the types elaborated here, as well as between multi-stakeholder and non-multi-stakeholder forms of governance. As such, procedural rules are also of vital practical importance; institutions and organizations that depend on illegitimate procedures are unlikely to enjoy broad acceptance and thus effectiveness. Further, the fact that major actors in Internet governance endorse diverse views of procedural legitimacy helps explain the rising tension in this issue-area and also suggests that actors should attempt to forge a procedural *modus vivendi* prior to attempting to resolve substantive issues.

ACKNOWLEDGEMENTS

This study was first published in *International Theory* in November 2015 and is reprinted with permission of Cambridge University Press. The authors thank the Centre for International Governance Innovation for its support of their research. They also thank Samantha Bradshaw for her research assistance. An earlier version was presented at the 8th Annual GigaNet Symposium, Bali, Indonesia, October 21, 2013; the authors thank the participants for their helpful comments. Finally, the authors thank the anonymous reviewers and *International Theory*'s editorial team for their invaluable suggestions. Any remaining errors are, of course, their own.

WORKS CITED

Abbott, Kenneth W. and David Gartner. 2012. "Reimagining Participation in International Institutions." *Journal of International Law and International Relations* 8: 1–35.

Abbott, Kenneth W. and Duncan Snidal. 2000. "Hard and Soft Law in International Governance." *International Organization* 54 (3): 421–56.

———. 2009a. "Strengthening International Regulation Through Transnational New Governance: Overcoming the Orchestration Deficit." *Vanderbilt Journal of Transnational Law* 42: 501–78.

———. 2009b. "The Governance Triangle: Regulatory Standards Institutions and the Shadow of the State." In *The Politics of Global Regulation*, edited by Walter Mattli and Ngaire Woods. Princeton, NJ: Princeton University Press.

Abbott, Kenneth W., Robert O. Keohane, Andrew Moravcsik, Anne-Marie Slaughter and Duncan Snidal. 2000. "The Concept of Legalization." *International Organization* 54 (3): 401–19.

Albin, Cecilia. 2001. *Justice and Fairness in International Negotiation*. Cambridge, MA: Cambridge University Press.

Antonova, Slavka. 2008. *Powerscape of Internet Governance — How was Global Multistakeholderism Invented in ICANN?* Saarbrücken, Germany: VDM Verlag.

Baker, Andrew. 2010. "Restraining Regulatory Capture? Anglo-America, Crisis Politics and Trajectories of Change in Global Financial Governance." *International Affairs* 86 (3): 647–63.

Balkin, Jack M. 2008. "The Future of Free Expression in a Digital Age." *Pepperdine Law Review* 36. http://ssrn.com/abstract=1335055.

Barlow, John Perry. 1996. "A Declaration of the Independence of Cyberspace." Davos, Switzerland, February 8. https://projects.eff.org/~barlow/Declaration-Final.html.

Bradley, Caroline. 2005. "Private International Law-Making for the Financial Markets." *Fordham International Law Journal* 29 (1): 127–80.

Brousseau, Eric, Meryem Marzouki and Cécile Méadel, eds. 2012. *Governance, Regulation, and Powers on the Internet*. Cambridge, MA: Cambridge University Press.

Bukovansky, Mlada. 2002. *Legitimacy and Power Politics: The American and French Revolutions in International Political Culture*. Princeton, NJ: Princeton University Press.

Bull, Hedley. 2002. *The Anarchical Society: A Study of Order in World Politics*, 3rd ed. New York, NY: Columbia University Press.

Büthe, Tim and Walter Mattli. 2011. *The New Global Rulers: The Privatization of Regulation in the World Economy*. Princeton, NJ: Princeton University Press.

Bygrave, Lee A. and Jon Bing, eds. 2009. *Internet Governance: Infrastructure and Institutions*. Oxford, UK: Oxford University Press.

Cerf, Vint, Patrick Ryan and Max Senges. 2014. "Internet Governance is Our Shared Responsibility." *I/S: A Journal of Law and Policy* 10 (1): 1–41.

Clark, David. 1992. "A Cloudy Crystal Ball, Visions of the Future." In *Proceedings of the Twenty-Fourth Internet Engineering Task Force, Massachusetts Institute of Technology, NEARnet, Cambridge, July 13–17, 1992.* IETF, 539–44. www.ietf.org/proceedings/24.pdf.

Dahl, Robert A. 1956. *A Preface to Democratic Theory*. Chicago, IL: University of Chicago Press.

———. 1972. *Polyarchy: Participation and Opposition*. New Haven, CT: Yale University Press.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Drezner, Daniel W. 2000. "Bargaining, Enforcement, and Multilateral Sanctions: When is Cooperation Counterproductive?" *International Organization* 54 (1): 73–102.

Dutton, William H., Anna Dopatka, Michael Hills, Ginette Law and Victoria Nash. 2011. "Freedom of Connection-Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet." Paris: UNESCO. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1654464.

Dutton, William H., John Palfrey and Malcolm Peltu. 2007. "Deciphering the Codes of Internet Governance: Understanding the Hard Issues at Stake." Oxford Internet Institute and e-Horizons Institute Forum Discussion Paper No. 8.

Epstein, Dmitry. 2013. "The Making of Institutions of Information Governance: The Case of the Internet Governance Forum." *Journal of Information Technology* 28: 137–49.

GAVI Alliance. 2015. "Governing GAVI." www.gavi.org/about/governance.

Glasius, Marlies. 2010. *Expertise in the cause of justice: Global civil society influence on the statute for an international criminal court*. Oxford, UK: Oxford University Press.

Global Fund. 2014. *Governance Handbook*. www.theglobalfund.org/en/board.

Haas, Peter M. 1992. "Introduction: Epistemic Communities and International Policy Coordination." *International Organization* 46 (1): 1–35.

Haufler, Virginia. 2001. *A Public Role for the Private Sector: Industry Self-Regulation in a Global Economy.* Washington, DC: Carnegie Endowment for International Peace.

Hawkins, Darren G., David A. Lake, Daniel L. Nielson and Michael J. Tierney, eds. 2006. *Delegation and Agency in International Organizations*. Cambridge, MA: Cambridge University Press.

Helleiner, Eric, Stefano Pagliari and Hubert Zimmermann, eds. 2010. *Global Finance in Crisis: The Politics of International Regulatory Change*. New York, NY: Routledge.

Hobson, John M. and Jason C. Sharman. 2005. "The Enduring Place of Hierarchy in World Politics: Tracing the Social Logics of Hierarchy and Political Change." *European Journal of International Relations* 11 (1): 63–98.

Hurd, Ian. 1999. "Legitimacy and Authority in International Politics." *International Organization* 53 (2): 379–408.

IETF 2004. "A Mission Statement for the IETF." RFC3935. www.ietf.org/rfc/rfc3935.txt.

Ikenberry, G. John. 2001. *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars*. Princeton, NJ: Princeton University Press.

International Proposals to Regulate the Internet: Hearing Before the Committee on Energy and Commerce, House of Representatives. 2012. 112th Congress. Washington, DC: United States Government Printing Office.

IOSCO. 2010. "Objectives and Principles of Securities Regulations." www.iosco.org/library/pubdocs/pdf/IOSCOPD323.pdf.

Jackson, Robert H. 1990. *Quasi-States: Sovereignty, International Relations and the Third World*. Cambridge, MA: Cambridge University Press.

Keck, Margaret E. and Kathryn Sikkink. 1998. *Activists Beyond Borders*. Ithaca, NY: Cornell University Press.

Keene, Edward. 2007. "A Case Study of the Construction of International Hierarchy: British Treaty-Making against the Slave Trade in the Early Nineteenth Century." *International Organization* 61 (2): 311–39.

———. 2013. "International Hierarchy and the Origins of the Modern Practice of Intervention." *Review of International Studies* 39 (5): 1077–90.

Keohane, Robert O. 1990. "Multilateralism: An Agenda for Research." *International Journal* 45 (4): 731–64.

Koremenos, Barbara, Charles Lipson and Duncan Snidal. 2001. "The Rational Design of International Institutions." *International Organization* 55 (4): 761–99.

Krasner, Stephen D. 1991. "Global Communications and National Power: Life on the Pareto Frontier." *World Politics* 43 (3): 336–66.

Krouse, Richard W. 1982. "Polyarchy and Participation: The Changing Democratic Theory of Robert Dahl." *Polity* 14 (3): 441–63.

Lake, David A. 2007. "Escape from the State of Nature: Authority and Hierarchy in World Politics." *International Security* 32 (1): 47–79.

———. 2009. "Regional Hierarchy: Authority and Local International Order." *Review of International Studies* 35 (S1): 35–58.

Malcolm, Jeremy. 2008. *Multi-Stakeholder Governance and the Internet Governance Forum*. Wembley, Australia: Terminus Press.

March, James G. and Johan P. Olsen. 1998. "The Institutional Dynamics of International Political Orders." *International Organization* 52 (4): 943–69.

Martin, Lisa L. and Beth A. Simmons. 1998. "Theories and Empirical Studies of International Institutions." *International Organization* 52 (4): 729–57.

Mathiason, John. 2008. *Internet Governance: The New Frontier of Global Institutions*. New York, NY: Routledge.

Mueller, Milton L. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

———. 2010. *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: MIT Press.

Mueller, Milton L., Andreas Schmidt and Brenden Kuerbis. 2013. "Internet Security and Networked Governance in International Relations." *International Studies Review* 15 (1): 86–104.

NTIA. 2014. "NTIA Announces Intent to Transition Key Internet Domain Name Functions." Press release, March 14. www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

Nye, Joseph S., Jr. 2014. *The Regime Complex for Managing Global Cyber Activities*. GCIG Paper Series Paper No. 1. Waterloo, ON: CIGI. www.cigionline.org/publications/regime-complex-managing-global-cyber-activities.

Orsini, Amandine, Jean-Frédéric Morin and Oran Young. 2013. "Regime Complexes: A Buzz, a Boom, or a Boost for Global Governance?" *Global Governance* 19 (1): 27–39.

Ostrom, Elinor. 2010. "Beyond Markets and States: Polycentric Governance of Complex Economic Systems." *The American Economic Review* 100 (3): 641–72.

Ostrom, Vincent, Charles M. Tiebout and Robert Warren. 1961. "The Organization of Government in Metropolitan Areas: A Theoretical Inquiry." *American Political Science Review* 55 (4): 831–42.

Palfrey, John and Urs Gasser. 2012. *Interop: The Promise and Perils of Highly Interconnected Systems*. New York, NY: Basic Books.

Price, Richard. 1998. "Reversing the Gun Sights: Transnational Civil Society Targets Land Mines." *International Organization* 52 (3): 613–44.

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

———. 2013a. "Renovating the Procedural Architecture of International Law." *Canadian Foreign Policy Journal* 19 (3): 268–87.

———. 2013b. "Puncturing the Myth of the Internet as a Commons." *Georgetown Journal of International Affairs* (December): 5–16.

———. 2015. "Locating Authority in the International System: Authoritative Rules and Post-Anarchy International Relations Theory." Paper presented at the International Studies Association Annual Conference, New Orleans, LA, February 21. web.isanet.org/Web/Conferences/New%20Orleans%202015/Archive/2a4f40c4-2b9b-4e24-acc6-2ee07be7bacd.pdf.

Reus-Smit, Christian. 1997. "The Constitutional Structure of International Society and the Nature of Fundamental Institutions." *International Organization* 52 (4): 555–89.

———. 1999. *The Moral Purpose of the State: Culture, Social Identity and Institutional Rationality in International Relations*. Princeton, NJ: Princeton University Press.

Reynolds, J. and J. Postel. 1987. "The Request for Comments Reference Guide." RFC1000. www.ietf.org/rfc/rfc1000.txt.

Rosenau, James N. 1995. "Governance in the Twenty-First Century." *Global Governance* 1 (1): 13–43.

RSB. 2015. "RSB Governance." http://rsb.org/about/governance/.

Ruggie, John Gerard. 1992. "Multilateralism: The Anatomy of an Institution." *International Organization* 46 (3): 561–98.

———. 2001. "global_governance.net: The Global Compact as Learning Network." *Global Governance* 7 (4): 371–78.

———. 2004. "Reconstituting the Global Public Domain — Issues, Actors, Practices." *European Journal of International Relations* 10 (4): 499–531.

———. 2014. "Global Governance and 'New Governance Theory': Lessons from Business and Human Rights." *Global Governance* 20 (1): 5–17.

Sharman, Jason C. 2013. "International Hierarchies and Contemporary Imperial Governance: A Tale of Three Kingdoms." *European Journal of International Relations* 19 (2): 189–207.

Slaughter, Anne-Marie. 2004. *A New World Order*. Princeton, NJ: Princeton University Press.

Stauffacher, Daniel and Wolfgang Kleinwächter. 2005. *The World Summit on the Information Society*. New York, NY: United Nations Information and Communication Technologies Task Force.

Underhill, Geoffrey R. D. and Xiaoke Zhang. 2008. "Setting the Rules: Private Power, Political Underpinnings, and Legitimacy in Global Monetary and Financial Governance." *International Affairs* 84 (3): 535–54.

UN Global Compact Office. 2012. *Global Compact Local Network Report 2012*. New York, NY: United Nations. http://unglobalcompact.org/docs/publications/LN_Report_2012.pdf.

Waltz, Kenneth N. 1979. *Theory of International Politics*. Boston, MA: McGraw-Hill.

Weiss, Thomas G. and Rorden Wilkinson. 2014. "Rethinking Global Governance: Complexity, Authority, Power, Change." *International Studies Quarterly* 58 (1): 207–15.

Weissbrodt, David and Maria Kruger. 2003. "Norms on the responsibilities of transnational corporations and other business enterprises with regard to human rights." *American Journal of International Law* 97 (4): 901–22.

Welch, David A. 1993. *Justice and the Genesis of War*. Cambridge, MA: Cambridge University Press.

———. 2013. "What is 'Governance,' Anyway?" *Canadian Foreign Policy Journal* 19 (3): 253–58.

Wendt, Alexander. 1998. "On Constitution and Causation in International Relations." *Review of International Studies* 24 (5): 101–18.

———. 2001. "Driving with the Rearview Mirror." *International Organization* 55 (4): 1019–49.

WGIG. 2005. *Report of the Working Group on Internet Governance*. Chateau de Bossey. June. www.wgig.org/docs/WGIGREPORT.pdf.

Wilkinson, Rorden. 2000. *Multilateralism and the World Trade Organization*. London, UK: Routledge.

ABOUT THE AUTHORS

Mark Raymond is the Wick Cary Assistant Professor of International Security at the University of Oklahoma, and a Fellow with the Center for Democracy and Technology. His work appears in *International Theory*, the *Georgetown Journal of International Affairs* and the *Canadian Foreign Policy Journal*. He is also the co-editor of *Organized Chaos: Reimagining the Internet* (CIGI, 2014). He has testified before the United Nations Commission on Science and Technology for Development, and participated in the Internet Governance Forum. His current research projects examine the politics of global rule making, as well as Internet governance. He received his Ph.D. from the University of Toronto.

Laura DeNardis, CIGI senior fellow, is a scholar of Internet architecture and governance and professor in the School of Communication at American University in Washington, DC. The author of *The Global War for Internet Governance* (Yale University Press, 2014) and several other books, her expertise has been featured in numerous publications. She serves as the director of research for the Global Commission on Internet Governance and is an affiliated fellow of the Yale Law School Information Society Project, where she previously served as executive director. Laura holds an A.B. in engineering science from Dartmouth College, a master's degree in engineering from Cornell University, a Ph.D. in science and technology studies from Virginia Tech, and was awarded a post-doctoral fellowship from Yale Law School.

CHAPTER THREE:
THE EMERGENCE OF CONTENTION IN GLOBAL INTERNET GOVERNANCE

Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond

ACRONYMS

ccTLD	country code top-level domain
DNS	Domain Name System
DOC	Department of Commerce
GAC	Governmental Advisory Committee
gTLD	generic top-level domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	information and communication technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IPv4	Internet Protocol version 4
IR	international relations
ISOC	Internet Society
ITU	International Telecommunication Union
NSA	National Security Agency
NTIA	National Telecommunication and Information Administration
SCO	Shanghai Cooperation Organisation
TLD	top-level domain
UNGA	United Nations General Assembly
WCIT	World Conference on International Telecommunications

INTRODUCTION

Contention in global Internet governance systems is evident in a series of recent controversies. They have made visible the connection between Internet governance and a number of public interest concerns, such as infrastructure availability, security and individual civil liberties (such as freedom of expression and privacy). Such controversies include the state-induced Egyptian Internet outage, increasingly frequent and sophisticated cyber attacks — such as the recent episode involving Sony — an online boycott over the Stop Online Piracy Act in the United States, global tension over the arcane United Nations international treaty conference known as the International Telecommunication Regulations and disclosures about the National Security Agency's (NSA's) expansive surveillance programs.

Combined, these controversies have precipitated three related public and policy-maker perceptions of Internet governance: first, it made visible the complex distributed ecosystem of Internet governance; second, it politically challenged perceptions that the coordination of the Internet is "just a technical administration issue"; and third, it engendered a public loss of trust in the systems, companies, governments and institutions that coordinate the Internet. The administrative tasks keeping the Internet operational, while never without tension and controversy, now reflect both real and perceived conflicts of interest among stakeholders and a heightened geopolitical concern about the cooperation necessary to resolve these conflicts.

This chapter is organized around three questions. First, what does the emerging contention in Internet governance look like? The chapter illustrates emerging contention in the Internet governance ecosystem in five ways: the escalation of conflict over the root zone file; state actors pushing for alternative arrangements in interconnection governance; technical infrastructure tensions; co-opting of Internet governance infrastructures to achieve political and economic objectives; and discourses of (de)legitimation and attempts at institutional design.

The second section of the chapter draws on international relations (IR) literature to answer the question why has contention in the Internet governance regime increased? It argues that contention is the product of two simultaneous shifts in the fundamental problem structure underlying Internet governance. The first is that Internet governance now presents problems of cooperation, in which parties have an incentive to cheat at each other's expense, in addition to more familiar problems of coordination. The second is that these coordination problems are becoming more complex and severe. They increasingly involve greater numbers of players, as many more actors have interests in how the Internet is governed and thus become new entrants to the process, thereby increasing the complexity of creating and maintaining stable arrangements. Coordination problems are also more severe in that the magnitude of players' interests in the outcome are greater. As there are more joint gains from cooperation to distribute among players, the stakes involved in deciding how to distribute such gains naturally increase.

In noting these shifts in problem structure and connecting them to increased contention in Internet governance, the chapter makes two contributions to the IR literature. First, to the authors' knowledge, the rapid rise in contention in a formerly technical area of governance is unique. Where the literature has addressed shifts in problem structure, it has typically sought to explain either a reduction in the severity of cooperation problems or their transformation into more benign problems of coordination. Therefore, an explanation for a degenerative shift to a situation involving both high-stakes coordination and problems of cooperation is significant to the literature and, beyond

that, has practical and urgent implications. There is a risk that Internet governance is a canary in the coal mine and that shifts in problem structure may occur in other issue areas. Determining the extent of this risk requires an understanding of what conditions are associated with these degenerative shifts in problem structure.

Second, this chapter makes a contribution to the growing body of literature on the concept of regime complexes in general, and the cyber regime complex, in particular. Building on earlier work on regime complexes, Joseph S. Nye, Jr. (2014) argues that Internet governance should be understood as embedded in a broader set of rules, institutions and processes that govern related issue areas including trade, development, security, law enforcement and intellectual property, among others. This argument has two implications: Internet governance now often includes actors whose primary responsibilities only tangentially include Internet issues; and actors are often tempted to accomplish objectives relating to patterns of Internet use by means of technical Internet architecture. The cyber regime complex, however, is still in the process of formation. Indeed, it is precisely this process of regime complex formation that is likely contributing to the rapid rise of contention over Internet governance. At the same time, regime complex formation is being driven by shifts in the underlying nature of the cooperation and coordination problems faced by actors. Processes of regime complex formation are not yet well understood. This chapter therefore contributes to the regime complex literature by studying an important case of regime complex formation involving a wide variety of actor types, generating better understanding both of the generic nature of these processes and the conditions under which they become contentious.

The final section of the chapter asks why there has been a shift in the underlying problem structure of the Internet governance regime. The presence of extrinsic uncertainty, changing market conditions, declining US dominance in the Internet governance system, and social processes of institutional change and regime complex formation all drive shifts in the underlying problem structure in Internet governance. These five explanations are not mutually exclusive; they interact and overlap in a number of ways and are each necessary to properly understand the roots of contention.

RISING CONTENTION IN INTERNET GOVERNANCE

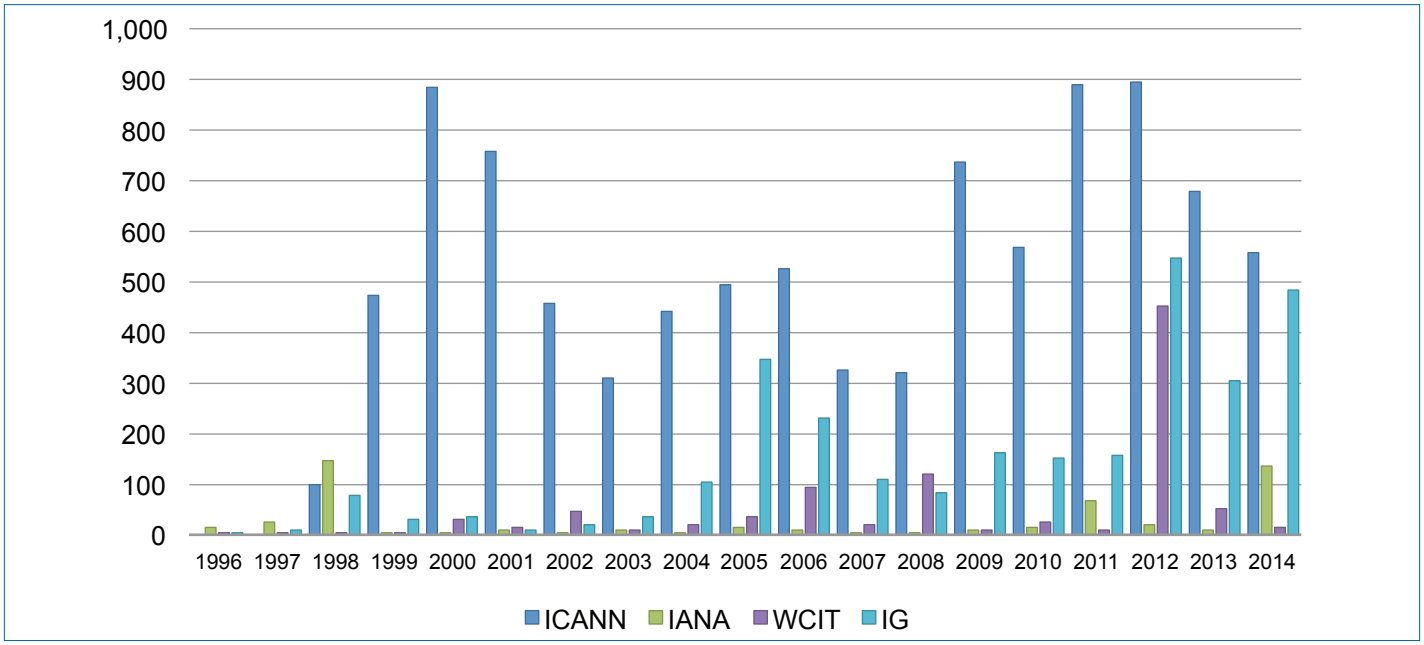
Contention over Internet governance predates Edward Snowden's disclosures about the expansive surveillance practices of the NSA (see Figure 1). Current disputes reflect the high-profile controversies mentioned above, as well as an inherent asymmetry between the rapid growth of Internet adoption in emerging markets and legacy Internet governance mechanisms developed in the West. At the same time, there is an increasing turn to infrastructure and governance systems for uses exogenous to the core operational functions of this infrastructure. There is a shift from governance *of* Internet infrastructure to governance *by* Internet infrastructure, such as the use of the Domain Name System (DNS) for intellectual property rights enforcement. This section points to five illustrations of rising contention in Internet governance.

ESCALATION OF CONFLICTS OVER THE ROOT ZONE FILE

The US government's contractual relationship with the Internet Corporation for Assigned Names and Numbers (ICANN) and the question of who controls critical Internet resources, oversees the DNS, and authorizes changes to the root zone file have long been contested topics in global Internet governance debates. These issues predate global concerns over nation-state surveillance, and contention in these areas is about more than issues of surveillance or even security. Various corporate and consumer interests, as well as civil liberties and community rights, are at stake. Nevertheless, concern about expansive NSA Internet surveillance practices has created a loss of trust in the stewardship and unique relationship of the US government in other areas related to the Internet, and has heightened the already entrenched global interest in continuing to internationalize ICANN and control of critical Internet resources.

Numerous studies address the history of ICANN and long-standing conflicts over control of the governance functions carried out under the auspices of this institution (Mueller 2002; Matthiason 2008; Bygrave and Bing 2009; Brousseau, Marzouki and Méadel 2012). In 1998, a memorandum of understanding between ICANN and the US Department of Commerce (DOC) initiated a process that transitioned technical DNS coordination and management functions to ICANN, while retaining accountability to the US government. The contractual agreement between the DOC and ICANN, among other things, authorizes the Internet Assigned Numbers Authority (IANA) to perform a number of critical Internet governance functions including DNS root zone management, administration of Internet numbers and management of protocol parameters (Security and Stability Advisory Committee 2014). One long-standing point of contention is the DOC's authority — through the National Telecommunication and Information Administration (NTIA) — to approve changes to the root zone file, which are then entered into the master root server by the US company VeriSign and distributed and replicated on the Internet's root servers. Since the inception of ICANN, the US government's position has been to gradually internationalize and privatize ICANN and, ultimately, relinquish ties to the organization. However, US authority continues to be a primary concern for various governments and stakeholders.

Figure 1: Comparative Media Coverage over Time of Internet Governance Topic



Source: Authors.

Global concern over this relationship dates to the World Summit on the Information Society (in 2003 in Geneva and 2005 in Tunis). The very formation of the Internet Governance Forum (IGF) was a compromise designed to continue the dialogue about the transition. ICANN structures, processes, composition, accountability and scope have been core topics of the IGF since its inception. In the meantime, the NTIA has continued to award the IANA contract to ICANN, most recently in July 2012.

In the wake of mass surveillance revelations, this already extant tension escalated and new voices questioned the exclusive US-IANA contract and its control over the root zone file (Corwin 2013). For example, the surveillance revelations spurred the Brazilian-hosted global gathering, NETmundial — the Global Multistakeholder Meeting on the Future of Internet Governance. The gathering did not address surveillance as much as it addressed the future of multi-stakeholder governance around ICANN and, if anything, the gathering was a win for multi-stakeholder, rather than multilateral, governance. In March 2014, just prior to NETmundial, the NTIA announced that the United States would transition oversight to the multi-stakeholder community by 2015. However, no consensus proposal for replacing the current model exists as of this writing and contention continues.

Despite a degree of agreement on the desirability of multi-stakeholder governance involving private industry, technical experts, civil society and governments, there has also been increasing politicization and calls for greater government intervention. A 2014 French Senate report on Internet governance called for the formation of a "World Internet Corporation for Assigned Names and Numbers," rather than ICANN, to oversee IANA functions and also called for the formation of a new Global Internet Council under an international treaty to ensure compliance with NETmundial principles (French Senate 2014). In the United States, there is mounting partisan debate and contention over the transition of ICANN oversight to a "global multi-stakeholder community."

Contention has always surrounded the US government's close relationship with ICANN and its ability to award the IANA functions contract and authority for changes to the root zone file. Yet the level of contention increased as the visibility of ICANN and other Internet governance functions came into stark relief with the explosion in the economic importance of the Internet as a global communications facility and with Edward Snowden's disclosures of NSA surveillance.

INTERCONNECTION GOVERNANCE

Evidence of rising contention also materialized during the 2012 World Conference on International Telecommunications (WCIT) in Dubai. The meeting was designed to review and update the International Telecommunication Regulations, a global set of rules governing the exchange of telecommunication traffic across national borders. Administered by the International Telecommunication Union (ITU), the telecom interconnection rules were previously updated in 1988 prior to Internet commercialization and the development of the Web.

Since the commercialization of the Internet in the 1990s, there have been calls for greater government regulation

of Internet interconnection. Much of this has stemmed from concerns about creating fair payment structures for exchanging information among network operators, sometimes viewed as net neutrality-type concerns about first mover advantage and exploitative extractions of high rents for carrying traffic. Yet Internet interconnection has been one of the most privatized areas of the Internet governance ecosystem. Network operators agree to interconnect and exchange traffic and negotiate private agreements, either informal or contractual, that set out the terms to do so, either for mutual peering, paid peering or paid transit (DeNardis 2012a).

The 2012 WCIT turned into a controversial and divisive event (Raymond and Smith 2014; Mueller 2012). Negotiations faltered over numerous issues, including attempts to create a role for the ITU in Internet governance as well as procedural irregularities, but the WCIT also highlighted the disruptive potential of changes in economic models for the data transit industry. Certain telecom providers — some owned by governments — advanced proposals that would enable them to extract rents from content providers. Such proposals have complex distributional implications. They could fundamentally disrupt many Internet economy business models by, for example, privileging incumbent over-the-top service providers and content platforms at the expense of start-up firms. They would also generate windfall profits for network operators, many of which are large firms that also offer content services in addition to their roles as network operators. Thus, there are significant competition policy implications to any such decision. Further, alternate economic models for Internet interconnection may have international distributive implications, enabling states located at certain key points on the Internet's physical layer to extract revenue from the transit of Internet traffic between firms and users in other states. Over the longer term, such payment models could incentivize the construction of alternate cable routes.

TECHNICAL INFRASTRUCTURE TENSIONS

Rising contention over Internet governance includes infrastructure concerns, such as policy controversies over net neutrality and broadband competition, and technical developments, such as the depletion of the Internet Protocol version 4 (IPv4) address space and a resurgence of proprietary protocols. Net neutrality, it can be argued, is a local/national concern because it addresses Internet access policies, and, specifically, the question of whether there should be legal prohibitions on network operators prioritizing or blocking the delivery of certain types of traffic relative to other types of traffic. But, the rise in policy interest over this question — especially in the European Union and the United States — reflects rising concern over how "last mile" Internet providers can discriminate against content, either to privilege their own business models and content or in an attempt to engage in paid prioritization deals from large content companies whose business models depend on reaching the access provider's customers.

Some technical areas of contention are related to scarcity, most notably the depletion of the IPv4 address space. In February 2011, 4.3 billion addresses had been fully allocated by IANA to the five regional Internet registries. Internet governance debates relate to how to manage the remaining reserve or free up assigned but unused addresses and how this development has particular implications in the developing world and other areas without large existing stores of IPv4 addresses. The new version 6 (IPv6) standard, designed to expand the number of available Internet addresses, has not been adopted to any great extent. An ongoing concern for policy makers and the technical community, therefore, is what type of technical transition mechanisms, market interventions or government incentives are necessary to ensure sufficient Internet addresses for devices connected to the Internet and for future services, growth and innovation.

Another form of technical conflict relates to the resurgence of business models based on proprietary rather than open protocols. In contrast to the proprietary online systems of the 1990s and non-interoperable business networks, because they were based on closed protocols developed by competing companies, the Internet's core protocols were inherently designed to create interoperability among devices made by different manufacturers. Since 2010, there has been a turn back to closed models in which platform designers opted to use proprietary standards. The Web was designed to provide universal access to websites from any browser. In contrast, social media platforms, device app stores and even some voice over the Internet protocol systems are inherently designed to not be interoperable with other devices. This move away from open standards is also a form of technical contention (DeNardis 2014).

The basic technical underpinnings of Internet governance that were once largely uncontested are increasingly undermined by newly divergent interests. Contention at the technical level is often driven by business interests, which now realize the tremendous economic value of the Internet and aim to capitalize on these benefits. Yet this contention is also highly political, with regulatory decisions having large distributional effects. Scarce resources that are essential in order for people to use the Internet, such as IPv4 addresses, are finite and their limited supply could restrict the ability of new users (most of whom are in the developing world) to fully enjoy the Internet's myriad benefits. Limited supply of critical Internet resources also threatens further innovation in the Internet economy. Finally, the turn to proprietary standards (especially in combination with increasing concentration of ownership among a small number of global players in some segments of the Internet economy) risks harm to consumers, as well as the emergence of monopolies or oligopolies that may diminish innovation.

CO-OPTING INTERNET GOVERNANCE INFRASTRUCTURES

As systems of Internet governance have become increasingly visible and also recognized as sites of economic and political power, various interests are co-opting these infrastructures for purposes completely extraneous to their originally constructed operational and policy objectives (DeNardis 2012b). For example, a US court awarded victims of a Hamas suicide bombing in Jerusalem hundreds of millions of dollars in compensation from Iran because of Iranian support of Hamas. In an attempt to collect damages, plaintiffs have asked ICANN to seize and turn over Iran's country code top-level domains (ccTLDs) (Newman 2014). ICANN has resisted this ccTLD seizure for a variety of technical, political and legal reasons (ICANN 2014), but this example illustrates the turn to Internet governance infrastructures to resolve global political and economic problems. It also raises a number of questions, including who should control the fate of ccTLDs and whether this should be the purview of a private, non-profit corporation or a matter for international agreement.

The DNS, and top-level domains (TLDs) in particular, reflect tensions between territorially bound cultural/regional interests and multinational companies with cross-border economic interests. During the ICANN-initiated expansion of the number of TLDs, for example, conflicts arose between corporations proposing TLDs associated with their trademarked names (such as .amazon or .patagonia) or industries (for example, .wine or .vin), and countries that pushed back against these proposals via ICANN's Governmental Advisory Committee (GAC) because of perceptions of regional and territorial claims associated with, for example, the Amazon rainforest, the Patagonia region and France's wine region. Even the core DNS function of resolving names into numbers has been co-opted as a mechanism for blocking access (actually redirecting queries) to websites that illegally sell counterfeit trademarked luxury goods, counterfeit patented pharmaceutical products, or copyrighted music, movies or video games (Bradshaw and DeNardis 2015).

Perhaps most illustrative of the turn to infrastructure to resolve geopolitical tensions are cyber security governance developments such as Stuxnet, or politically motivated distributed denial of service attacks and government proposals that impose restrictions on where and how data is stored (data localization).

Internet governance infrastructures have become a proxy for broader geopolitical and socioeconomic contention, with disputes ranging from TLDs to manipulation of the DNS functions.

(DE)LEGITIMATION DISCOURSES AND INSTITUTIONAL DESIGN ATTEMPTS

Rising contention is illustrated by recent declarations and actions, from numerous actor types and a variety of substantive perspectives, which call into question the legitimacy and fitness-for-purpose of different components of the Internet governance regime and the broader cyber regime complex. In some cases, these efforts explicitly include calls for reform or replacement of the norms, rules and institutions that comprise the legacy Internet governance regime and the emerging cyber regime complex.

A subset of state actors is among those most insistently questioning the current system. While such efforts have gained momentum and support since 2012, they are not entirely new. The First Committee of the United Nations General Assembly (UNGA) has been the locus of such debate since Russia first introduced a resolution calling for the development of an international law dealing with the security implications of information and communication technologies in 1998 (Maurer 2011, 20). Russian efforts to pursue "information security" encompass not only arms control efforts, but also attempts to press the UN Charter protections guaranteeing members' sovereignty, territorial integrity and political independence into service as a shield against international human rights law and its commitments to freedom of speech. In its 2006 resolution on this issue, Russia was joined as a sponsor for the first time by China, Armenia, Belarus, Kazakhstan, Kyrgyzstan, Myanmar, Tajikistan and Uzbekistan (ibid., 22).

These efforts have further intensified. Russia and China concluded the negotiation of a bilateral cyber treaty that facilitates joint research and joint cyber security operations (Razumovskaya 2015). China has also increasingly asserted a positive vision of Internet governance, heavily driven by its particular security concerns, and has begun to erect an alternative discourse with an accompanying set of rules and institutions. These efforts are complicated by recent economic pressures and by the importance of the IT sector to the Chinese economy. As a result, China's Cyber Administration is engaging more with multi-stakeholder processes in ICANN and at NETmundial. The Xinhua News Agency, an official government organ, has also touted the "Internet Plus" plan, which "aims to integrate mobile Internet, cloud computing, big data and the Internet of Things with modern manufacturing, to encourage the healthy development of e-commerce, industrial networks, and Internet banking, and to help Internet companies increase international presence" (Xinhua News 2015).

This new economic policy thrust is at odds with the People's Liberation Army's attempts to use the Internet to conduct proxy operations against Western countries and the Chinese government's growing efforts to

suppress dissidents and control Internet content via the "Great Firewall" of China. On these issues, the Chinese government has justified its position by arguing that "in this virtual space where traffic is very heavy, there is still no comprehensive 'traffic rules.' As a result, 'traffic accidents' in information and cyber space constantly occur with ever increasing damage and impact. Therefore, the development of a set of universal and effective international norms and rules guiding the activities in information and cyber space has become an urgent task in maintaining information and cyberspace security" (United Nations Institute for Disarmament Research 2014). In addition to joining the long-standing Russian efforts within the UNGA's First Committee, China has also partnered with Russia to advance this agenda in the Shanghai Cooperation Organisation (SCO). The final declaration of the 2014 SCO summit in Dushanbe, Tajikistan announced the intention of SCO members to "cooperate in preventing the use of information and communications technologies which intend to undermine the political, economic, and public safety and stability of the Member States, as well as the universal moral foundations of social life, in order to stop the promotion of the ideas of terrorism, extremism, separatism, radicalism, fascism and chauvinism by the use of the Internet" (Incyder News 2014). This language fits squarely within the efforts of these governments to apply such pejorative terms to democratic opposition groups, human rights activists, journalists and others both within and outside their borders.

Beyond its emphasis on including limitations on access to particular kinds of information in global efforts to govern cyber security, China has also sought to promote a narrative of multilateral (rather than multi-stakeholder) Internet governance. The clear intent in such a discursive move is to sharply restrict or even exclude the participation of various kinds of non-state actors that currently play vital roles in Internet governance. This agenda featured prominently at the World Internet Conference, which China sponsored in late 2014. Conference organizers circulated a draft declaration to delegates that "call[ed] on the international community to work together to build an international Internet governance system of multilateralism, democracy and transparency and a cyberspace of peace, security, openness and cooperation" (Shu 2014). The appropriation of Western procedural norms and values in this language is striking, and reflects the increasing social competence of the Chinese government in operating the institutions of the international system. The draft declaration also called on parties to "respect Internet sovereignty of all countries" and "respect each country's rights to the development, use *and governance* [emphasis added] of the Internet, refrain from abusing resources and technological strengths to violate other countries' Internet sovereignty, and build an Internet order to [sic] equality and mutual benefit" (ibid.). While the draft declaration was ultimately retracted without comment or explanation for reasons that are not clear, the draft text is indicative of China's general perspective on these issues.

Many other states are uneasy with the multi-stakeholder model (Maurer and Morgus 2014). A substantial portion of the developing world views the highly privatized nature of governance in this issue area as privileging the interests of the advanced industrial democracies. It is also likely that these states view the participation of non-state actors in global negotiations as procedurally illegitimate, on the basis of international law's traditional restriction of international legal personality to states and formal international organizations. Much of this debate is framed in terms of the nature of authority relations involving ICANN. While ICANN has agreed to either accept or justify its rejection of formal advice from the GAC, the GAC is regarded by many states as an under-resourced body that, in any event, operates according to consensus decision rules. These conditions hamper its effectiveness at playing a meaningful role in the complex, decentralized processes of policy making within the ICANN community, and the GAC is not able to formally participate in the myriad of crucial Internet governance decisions that occur outside of ICANN. In an attempt to partially address concerns about the legitimacy of ICANN's unorthodox legal structure, some states have called for a transition to a new body. Most recently, Brazil and Indonesia suggested a multi-stakeholder body that would be institutionally located in the broader UN system (Wright 2015).

Increased contention among states over Internet issues has also hindered efforts to organize the decennial review for the World Summit on the Information Society. Division among states, including over the relative desirability of a stand-alone, summit-level event proposed by Russia or a more low-key event held at the United Nations in New York, led to repeated delays in finalizing the modalities for the review. Risk that the review event, currently scheduled for December 2015 in New York, becomes a focal point for contention is considerable, given that efforts to renew the IGF mandate during the 69th UNGA failed and were postponed until the 70th session (Kleinwächter 2015). This creates a linkage opportunity that may be exploited by states looking to bend the development trajectory of the broader cyber regime complex.

Contention is also evident in the aftermath of disclosures about the nature and extent of online surveillance that have undermined the legitimacy of existing Internet governance mechanisms in the eyes of a range of state and non-state actors. The Brazilian and German governments were among the leading critics of NSA activity. They pursued an array of diplomatic initiatives to register their concern over these issues, two of which are especially notable for their impact on the broader cyber regime complex. First, they partnered with ICANN and with other stakeholders to support the NETmundial conference, held in Brazil in April 2014. Second, they successfully sponsored an

UNGA resolution on privacy rights, formally adopted on December 18, 2014. Despite the adoption of the privacy resolution, the Saudi delegate insisted that each state had the right to protect its citizens from online activity including speech, and asserted that references to NETmundial in the text were improper since the meeting was not held under UN auspices (and procedural rules) and did not achieve consensus because the outcome document inadequately reflected the positions of states (United Nations 2014). This dissent reflects enduring disagreements among states about appropriate modalities for balancing order and stability with human rights, which are likely to contribute to further contention.

Efforts to push back against the legitimacy of online surveillance have also been made by the Internet community. Executives at major American technology companies have raised concerns both about brand damage and about the incompatibility of pervasive monitoring with civil liberties (ibid.). More concretely, members of the Internet Engineering Task Force (IETF) have sought to take action in order to limit the possibility of such monitoring. After the IETF's 2013 meeting in Vancouver, the Internet Architecture Board expressed its belief that "pervasive monitoring represents an attack on the Internet" and that such attacks "undermine public confidence in the Internet infrastructure, no matter the intent of those collecting the information" (Housley 2014). Accordingly, the IETF membership has begun work on a variety of responses to further encourage the widespread adoption of encryption, to revise its standards and protocols to update obsolete security provisions, and to ensure that "future protocol designs can take into account potential pervasive monitoring as a known threat model" (IETF 2013).

Some civil society groups also criticized the NETmundial outcome document, on the grounds that it inadequately reflected their concerns with regard to net neutrality and protections for human rights (Best Bits 2014). However, Internet issues include an extraordinarily diverse set of non-state actors with varying interests and values. In an attempt to exert control over the ongoing global debate, ICANN partnered with the Brazilian government and the World Economic Forum to launch the NETmundial Initiative, which was described by its organizers as "a bottom-up, action-focused movement for the global community to organically operationalize distributed Internet governance" and as "based on the Principles and roadmap developed at the 2014 NETmundial meeting" (NETmundial 2014). However, within 10 days of its official launch, the NETmundial Initiative had been clearly rejected as illegitimate by key players within the Internet community. The Internet Society (ISOC) issued a statement declaring that it "cannot agree to participate in or endorse the Coordination Council for the NETmundial Initiative" (ISOC 2014b). The statement expressed ISOC's concern "that the way in which the NETmundial Initiative is being formed does not appear to be consistent with the Internet Society's longstanding principles" (ibid.). It went on to enumerate a set of desiderata shared broadly within the Internet community, namely that governance should be decentralized, open, transparent, accountable and multi-stakeholder.

These examples demonstrate the high degree of contention in recent discussions about, and processes of, Internet governance across an array of different substantive issues. They highlight increasing consciousness among relevant actors of rising stakes, changing patterns of incentives, clashing and even incommensurate values, and tighter linkages between formerly distinct policy issues.

CONTENTION AS A FUNCTION OF SHIFTS IN PROBLEM STRUCTURE

The previous section argued that Internet issues have become more contentious in the last two years, and provided an array of illustrative examples. In this section, it is argued that this rising contention can be explained by two distinct shifts in the underlying problem structure. To do so, the chapter draws on the distinction between coordination and cooperation problems, which has been central to IR theory (Axelrod 2006; Fearon 1998; Jervis 1978; Schelling 1980; Snyder 1971; Martin and Simmons 1998). The first shift is the emergence of cooperation problems, in which actors have short-run individual incentives to engage in non-cooperative behaviour. The second is the exacerbation of existing coordination problems in ways that increase the difficulty of reaching agreement on a particular equilibrium, in particular due to an increased number of players and larger distributional consequences.

Numerous IR scholars have drawn on game theory to shed light on the nature of strategic interaction in world politics, although they have made different assumptions and drawn different conclusions in doing so. Realists have argued that cooperation problems are endemic in the international system as a result of its putatively anarchic structure (Jervis 1978; Waltz 1979). Not all cooperation problems are equally severe in their consequences. The security dilemma is one of the more severe examples of a cooperation problem, but it is known to vary in intensity (Jervis 1978). Other cases of cooperation problems are typically less severe. Nevertheless, neo-realist theories predict consistent state concern for relative gains, on the grounds that anarchy presents chronic enforcement problems or worries about non-cooperative cheating behaviour.

Institutionalist theories helpfully distinguished these cooperation problems, in which actors worry about cheating, from coordination problems, in which they worry about distribution problems pertaining to the division of gains among participants (Snidal 1985). Examples of international organizations playing coordination roles date

back to the nineteenth century: the International Telegraph Union was created in 1865 and the General Postal Union was created in 1874. Technocratic areas of global governance tend to be dominated by coordination problems with mild distributional concerns, such as coordination of rules for air traffic control or for international postal deliveries. Other coordination problems, however, are subject to more severe distributional problems; examples include the terms of global trade agreements (such as reducing barriers to agricultural goods versus manufactured goods) or the selection among different potential modalities for dealing with climate change (such as cutting coal emissions versus other types of greenhouse gases). In these cases, agreement on a particular equilibrium presents difficult negotiation problems. Such efforts are prone to actors exercising material and ideational power resources in order to secure their preferred outcomes (Krasner 1991).

The extent to which actors are concerned with the distributional consequences of specific coordinated outcomes is conditioned by their general preference for relative versus absolute gains (Powell 1991). Actors strongly concerned with their position relative to other actors will care a great deal about coordinated outcomes with large-stake distributional implications. States that only want to increase their own wealth will care less about whether a particular coordinated outcome is more favourable to others. Apart from relative gains, justice concerns are important motivators for actors attempting to resolve distributional disputes (Welch 1993; Albin 2001).

Internet governance has typically entailed solving coordination problems. Like the coordinating effects of a common language, the Internet relies upon interoperable protocols to ensure that different computers can speak to one another. Examples of such critical protocols include TCP/IP, BGP, HTTP1 and many other information and communication technology standards. The system of globally unique Internet names and numbers is another example of Internet governance mechanisms designed to resolve a coordination problem of administering a common directory translating between names and numbers and ensuring that these identifiers are globally unique. Prior to the commercialization of the Internet, few players had vested interests in particular outcomes with respect to these technological standards and protocols, which were developed by an epistemic community of engineers (Haas 1992). Thus, Internet issues presented fairly simple coordination problems typified by a small number of culturally homogenous players who were relatively indifferent between potential equilibria.

These conditions are increasingly inapplicable, but changes in the basic problem structure have not been uniform. As a result, there are examples where actors are confronted with problems relating to managing the distribution of joint gains among a large number of players with conflicting interests alongside situations in which actors are concerned primarily with creating (and ensuring compliance with) cooperation rules and norms intended to prevent defection, security dilemmas and arms races. The following section discusses two examples of the former drawn from Internet naming and addressing, and a single example of the latter. It is worth noting, however, that these two kinds of degenerative shifts in the underlying problem structure are not mutually exclusive. It is possible that a given situation involves issues of coordination and issues of cooperation (Koremenos, Lipson and Snidal 2001).

The first example of exacerbated coordination problems involves Internet names. What specific system is used to assign names to websites matters far less than whether all actors follow the same system and that individual names are globally unique. In other words, each individual actor benefits the most when they and everyone else coordinate their behaviour. The coordination nature of this Internet naming system is increasingly being complicated by the creation of new generic TLDs (gTLDs) and by conflicts involving territorially bound states and transnational companies. The expansion of gTLDs has provided a windfall profit to ICANN, and will do so for other players in the domain name provision industry. It has also created significant costs for new gTLD applicants and for existing firms and civil society actors that may need to defensively register a host of additional domain names in order to protect their brands or operational missions. Essentially, a situation has emerged where the fundamental function of gTLDs remains to coordinate behaviour, but the emerging distributional consequences of the allotment of domain names entail that more actors have significant interests in the outcome. The literature expects these conditions to significantly complicate efforts to arrive at a solution (Olson 1965, Krasner 1991; Koremenos, Lipson and Snidal 2001).

Internet numbering provides another example of the same basic set of dynamics. The IPv4 Internet numbering system is an example of a common, coordinated standard. In the abstract, the kind of system adopted has little importance aside from ensuring that numbers are globally unique; however, in practice, the initial adoption of a particular system creates powerful path dependencies. The exhaustion of the supply of IPv4 addresses as a result of the global expansion of connected devices has created a subsequent and more difficult coordination problem than that presented by the initial choice of an Internet numbering system. Because exhaustion of the stock of IPv4 addresses is not uniform across the regional Internet registries, some actors have incentives to contribute to the transition to IPv6, while others are able to extract economic rents from their existing reserves of IPv4 addresses and are not motivated to upgrade (Dell 2010; Mueller 2010). Again, the use of common IP standards helps maintain

1 TCP/IP is Transmission Control Protocol/Internet Protocol; BGP is Border Gateway Protocol; and HTTP is Hypertext Transfer Protocol.

the coordinated functionality of the Internet, but the distributional consequences that are part and parcel of different outcomes create tensions when trying to settle upon a given outcome.

Cooperation problems are most evident with respect to state security issues. Given low barriers to entry for the acquisition of significant cyber capabilities (Marquis-Boire et al. 2013), the potential for such attacks to cause significant electronic and kinetic disruption, and the technical, legal and political difficulties associated with attribution and deterrence (Raymond, Shull and Bradshaw 2015 [forthcoming]; Nye 2011), it is perhaps unsurprising that a large number of states have acquired, or are seeking to acquire, offensive cyber capabilities (Deibert 2014). Indeed, some analysts have concluded that the cyber realm is, at least at present, offense dominant (Nye 2011). This suggests that it may be unstable in the event of crisis, and prone to escalation (Jervis 1978; van Evera 1984). These conditions have prompted some authors to conclude that a "cybered Westphalian" outcome is likely (Demchak and Dombrowski 2011); however, these conditions do not necessarily mean that war is inevitable (Rid 2012). Indeed, states have proactively attempted to create rudimentary rules of the road to minimize this risk, with some degree of success (UNGA 2013; Schmitt 2013). The important point for this chapter is that states are now preparing in various ways to deal with cooperation problems that, until recently, did not exist. These kinds of problems are nascent and, at least for now, confined largely to the security realm. They reflect the development of "problematic interactions" between overlapping regimes characteristic of the emergence of a regime complex (Orsini, Morin and Young 2013). In this case, the interactions are primarily between the Internet governance regime, on the one hand, and regimes for international security, arms control and the global arms trade on the other.

UNDERLYING FACTORS IN PRODUCING SHIFTS IN PROBLEM STRUCTURE

This section presents four different theories to explain a part of the shifting problem structure giving rise to higher levels of Internet governance contention. In particular, it argues that extrinsic uncertainty, changing market conditions, hegemonic transition and social processes of regime complex formation account for much of the variation seen in the newly contentious Internet governance regime.

SUNSPOTS AND EXTRINSIC UNCERTAINTY

One explanation for the shift in Internet governance from a regime that is largely centred around simple coordination problems to one that increasingly involves complex coordination problems and instances of (sometimes failed) cooperation is that extrinsic shocks occurred that disrupted, perhaps irrevocably so, perceptions of the former system. Edward Snowden's revelations about the extent of NSA surveillance is an example. This explanation could be called the "sunspot" theory of Internet governance regime transition.

William Stanley Jevons (1887), argued that sunspots are an intrinsic factor that helps explain climatic change and agricultural productivity. However, in the more modern theory of sunspot economics (Cass and Shell 1983; Farmer and Guo 1994; Hirose 2007), uncertainty is an extrinsic variable that affects outcomes. For instance, the combination of a certain set of expectations and the fundamentals of the situation in question generate an equilibrium, with specific behavioural patterns emerging as a result. While fundamentals might be slow to change, expectations are subject to extrinsic uncertainty. In other words, people do not necessarily know that they are acting in a way that the system requires. Events can then transpire that alter people's expectations about how the system operates, rapidly generating different behavioural patterns. These events affect behaviour through both the nature of the event itself and through other actors' construction of the meaning of the event.

The Snowden disclosures represent a clear case of a significant event that originated largely outside of the Internet governance regime, but which nevertheless has significant Internet governance implications. The pathway through which the disclosures affect the governance system relies on individual expectations about how the system operates. For instance, one effect of these revelations is a decline in individual levels of trust in the Internet (CIGI-IPSOS 2014). Another is the abhorrence (perhaps merely rhetorical) that other many states expressed in response to this event. As a result of these revelations, an increasing number of states are pushing for Internet infrastructure changes, such as data localization (Chander and Le 2014), with potential implications for the universality of the Internet. Not all of these behaviours are solely caused by what Snowden revealed, but peoples' expectations of how the system operates have certainly been affected by the disclosures.

The sunspot effect of the Snowden event helps explain some of the loss of trust in the system of Internet and cyber governance. For example, a 2014 CIGI-IPSOS Global Survey on Internet Security and Trust found that of the 23,326 Internet users surveyed across 24 countries, 60 percent had heard of Edward Snowden (CIGI-IPSOS 2014). Of that 60 percent, 39 percent had taken actions to protect their online privacy and security as a result of the revelations (ibid.). Popular disclosures about the extent of government surveillance online has shaken peoples' perception of how the system operates, thereby generating behavioural changes, as the sunspot theory suggests.

The occurrence of an event that changes actors' perceptions actually has the short-run effect of reducing uncertainty. After Snowden's disclosures, people had better information about how the Internet governance regime operated, in particular the extent of US surveillance. Short-run behavioural changes result, but as time goes on, uncertainty grows larger again as people's perceptions of the fundamental operation of the system moves further away from the actual, objective operation of the system.

There is no doubt that the Internet governance regime has been subjected to the presence of extrinsic uncertainty, manifest not only from the Snowden revelations, but also from the rapid development of technology and other sources. Alone, this explanation is insufficient to explain the full extent of the emerging contention in the Internet governance regime. Many changes in the system are not due to perceptions of uncertainty about how the system is organized, but about changes to the fundamentals that underpin the Internet governance system as a whole. One such change is shifting market conditions.

CHANGING MARKET CONDITIONS

A second explanation for the shift from a coordination problem to a cooperation problem relates to changing market conditions, which point to a change in the fundamentals of the system. The Internet has dramatically altered trade and commerce in the twenty-first century. The flow of digital goods and services is reshaping society and promoting prosperity on a scale that is unprecedented. In 2014, it is estimated that digital flows added between US$250 billion and US$450 billion to global GDP growth, or 15 to 25 percent of the world's total GDP growth per year (Manyika et al. 2014).

All nations are benefiting from innovations in information and communication technologies (ICTs) and the governance transformations that facilitated their adoption. Changes in digital technologies have advanced the economic take-off of China and India, and other emerging powers, and also brought a much greater level of digital connectivity to the poor in every society. There is no doubt that the spread of the Internet has brought with it a massive increase in wealth and prosperity the world over.

The adoption of the Internet, however, has been uneven. The prosperous, democratic nations in the West that developed the Internet in the first place have also been at the forefront of ICT adoption, in particular compared to more authoritarian regimes (Milner 2006). The uneven spread of the Internet among nations entails that some countries are potentially better positioned to capitalize on the economic benefits that the Internet creates.

This inequality exacerbates some coordination problems because it means that different policies are highly likely to benefit some parties (often those best positioned to take advantage) more than others. Already, some states (particularly late adopters of Internet-based technologies) maintain that the current Internet governance architecture has been designed by Western countries without their input. From this perspective, the current Internet governance system reifies the first-mover advantages that the developed nations have both economically and politically in the Internet governance space. These ingrained economic and political advantages allow Western nations to continue to "gain relatively more," even as the Internet as a whole produces prosperity across nearly all contexts. Contention over coordinated solutions, such as the location of ICANN's incorporation or the process involved in the IANA transition, are a natural outgrowth of the fact that some nations feel that the current system, while producing absolute gains for all, overly privileges some actors over others. In such situations, actors are likely to bargain harder than in more pure coordination games, in order to preserve or acquire advantages. As in the international trade regime, they may also begin to frame the situation in justice terms and become less responsive to bargaining they believe to be illegitimate.

As market conditions continue to evolve, so does the importance of private actors in the Internet governance space. The private sector owns and operates the majority of ICT infrastructures, especially in Western countries. As a result, private companies usually hold the data that state authorities need in order to undertake their law and order and security provision functions. This distance between the private actors that hold the data and the state that needs the data to fulfil its central mandate creates points of contention. For example, in 2014, Microsoft was ordered by a US court to turn over email data produced in the United States but physically stored on a server in Ireland. Microsoft refused, arguing that the court could only compel it to turn over data that was actually stored in the United States (*The Guardian* 2014). The US government is attempting to gather evidence in a drug-trafficking case. Microsoft, for its part, is also motivated by the business consequences of government violations of online privacy. Like Google and Apple, Microsoft has cued into the idea that given both the reliance of people on ICT services and the declining trust of individuals in governments' online behaviour after the Snowden disclosures, ensuring anonymity online is good business. This means acting contentiously toward governments. As David Howard, Microsoft vice president and deputy general council put it, "Given what we know about the extent of access to personal data from the Snowden revelations, this can only undermine customers' confidence in US businesses even further. What we already know about surveillance now seems to be true for ordinary policing" (cited in ibid.). In short, due to the changing market conditions, where big money is to be had from providing online services with a strong promise to protect privacy and security, private companies and governments are increasingly at odds.

Private companies are also increasingly in contention with one another over some foundational governance principles that bring with them the potential for large economic gains or losses. One prime example of this trend involves the issue of network interconnection. Despite what the individual user experiences, the Internet is not a single network but a series of networks that are more or less independently run and operated. In 2011, the Internet effectively consisted of 5,039 interconnected Internet service providers (Woodcock and Adhikari 2011). Data traverses the expanse of the globe by being relayed across multiple networks. As recently as 2011, most peering agreements that allow traffic to flow as directly as possible across the Internet are informal agreements (99.51 percent) and based upon symmetrical terms (99.73 percent) (ibid.). Tensions between network operators, however, have flared in the past, causing small "rips in the fabric of the Internet" (Ricknäs 2008). For example, in 2008, Sprint-Nextel and Cogent stopped transferring each other's data directly, meaning that users of either network could not exchange data with one another without passing it first through a secondary network. The cause of the dispute largely comes down to issues to do with the costless or nearly costless nature of their peering arrangement (Miller 2008). When data flows between networks are roughly equal, companies can assume that costs come out in the wash. When data flows become unequal, then the company that is transiting the largest amounts of data will want to charge the company transiting less because there is economic gain to be had. As network usage patterns shift in the future due to changing market conditions, it is likely that breakdowns in current peering agreements will become more common and generate a new source of contention between private actors.

As economies have become more interdependent due to the expansion of the Internet, and as more and more economic activity shifts to web-based platforms, there is a whole host of new security vulnerabilities that emerge. These vulnerabilities produce an additional layer of potential contention in areas to do with cybercrime, since many attacks will span national borders and are hard to concretely attribute to particular actors. To quantify the effect of these attacks, a joint report written by the ICT security firm McAfee and the Centre for Strategic and International Studies (2014) estimates that the cost of cybercrime to the global economy in 2013 was around US$400 billion. Despite these huge costs, some nations still refuse to cooperate on cyber-related crimes, often for largely political reasons. Sometimes, as the recent hacks of Sony Pictures indicate, other nations might have a direct hand in the commission of cybercrimes, although the role that North Korea actually played in the attacks is unclear. The prosecution of cybercrime, therefore, becomes a source of contention.

Changing market conditions fostered by technological change create distributional contention, many of which pertain to the governance of the Internet ecosystem. Private actors are increasingly at odds with states over data and privacy issues, which have serious economic consequences for businesses. Private actors increasingly find themselves in contention with each other as the market surrounding ICT and ICT-based platforms expands and changes to fit consumer preferences. Overlaid onto all of this is the role of cybercriminals, who want to illegally capture a part of the vast wealth that the Internet creates.

DECLINING US HEGEMONY IN INTERNET GOVERNANCE

Rising contention in the Internet governance regime might also be explained, at least in part, as a product of the declining relative power of the United States, which, through both its oversight capacity of ICANN and dominance in the information technology sector, has played a large role in the development of the current system. The growing relative capabilities and interests of other states have given rise to questions over how scarce and critical Internet resources are distributed, and over the rules and norms that govern the Internet.

Scholars studying hegemonic transitions argue that a concentration of power can facilitate cooperative outcomes because the dominance of the primary state provides other actors with a degree of certainty about the future (Wohlforth 1999). This logic is particularly powerful in the short run, where few states can effectively challenge a hegemonic power. Over the longer term, however, a concentration of power can actually generate balancing behaviour from other states. As the relative power of the hegemon declines, cooperation becomes harder to achieve and conflicts of interest tend to multiply (Gilpin 1983; Walt 2006). The relative power of the hegemonic power can diminish in relative terms for two non-exclusive reasons. First, the dominant power might experience absolute decline as a result of internal problems that sap its strength. Second, other states with considerable latent power might opt to mobilize their resources to challenge the primacy of the hegemon, particularly if the hegemonic state wields its power in a way that is seen as unjust.

The United States is a clear hegemon in the current Internet governance regime, despite the fact that the absolute number of Internet users in the developing world is vast and continues to grow rapidly, and even though non-roman scripts are increasingly used to host websites. The DOC's oversight role of ICANN places America at the root of the current Internet governance system. The global dominance of US-based telecommunication companies and content intermediaries further solidifies the hegemonic position of the United States. For example, in 2014, American companies reportedly held a 27 percent share

of the global ICT market (Statista 2014). This dominance has allowed the United States to shape outcomes in the Internet governance space.

As previously discussed, many nations are concerned about US dominance in the Internet governance regime in the wake of the NSA surveillance disclosures. As hegemonic transition theory would expect, the dominant US role in the current Internet governance regime is sparking a backlash from other nations. In 2012, Russia, China and other states put forward a proposal at the WCIT to shift the locus of Internet governance away from the United States. These countries expressed interest in placing essential functions of ICANN under the authority of the ITU. Many developing nations view ICANN as lacking legitimacy due to its close associations with the US government. Consistent with hegemonic transition theory, it is also possible that major nations such as China and Russia might think that moving core Internet governance functions into the UN system will give them more direct control over some core Internet functions, which would increase their ability to shape outcomes and obtain their interests. The United States has also recently announced its intention to relinquish its unique relationship with ICANN, provided that certain criteria are met. These examples, particularly the challenge presented at the WCIT, indicate that a part of the change in the underlying issue structure of cyber governance is at least partly driven by the relative rise of non-Western nations.

Hegemonic transition theory can partially account for some of the contentious state behaviour marring global debates concerning Internet issues. States that are currently dominant in the Internet governance regime, such as the United States, are coming into increasingly conflict with other states that hold different ideological viewpoints and that see American dominance of the system as illegitimate or even an outright security challenge. Many developing nations that have yet to fully move online are now giving voice to the fact that they are compelled to adopt a system that is governed in a way that they did not help to directly develop. Other nations, such as Russia and China, have simply transposed tensions from other areas onto the Internet governance debate, making the issue particularly fractious. Hegemonic transition theory is less able to account for the nature of the alternatives preferred by these actors, which are shaped both by domestic values and international norms (Ruggie 1982), or the processes of global rule-making by which these objectives are pursued (Brunnée and Toope 2010; Diehl and Ku 2010; Raymond 2013). Again, this highlights the interactions between distinct factors that collectively account for increased global contention over Internet issues.

SOCIAL PROCESSES OF INSTITUTIONAL CHANGE AND REGIME COMPLEX FORMATION

While acknowledging the role of exogenous shocks and a decline in US hegemony in accounting for increasing contention over Internet issues, these factors cannot provide a sufficient explanation for the kind and degree of contention observed. This is because exogenous shocks and change in the state of American global leadership occur against the backdrop of pre-existing social relationships, rules and institutions, which exert effects on the timing and form of future change, as well as on the success or failure of particular attempts to create change.

To understand the multiple pathways and logics by which institutions shape the nature and degree of contention, as well as its eventual consequences, an explicitly eclectic approach is adopted (Sil and Katzenstein 2010), comprised of rational choice and constructivist approaches. These approaches are ideal for the purposes of this chapter because there are valuable insights in this area that stem from both theories and because there is (as yet) no broadly accepted understanding of the relationship between them. In this section, relevant theoretical contributions from both camps are surveyed and the ways in which these arguments can further understanding of increased contention over Internet issues are illustrated.

One strand of rationalist scholarship emphasizes that institutional arrangements provide information to states and other parties, reduce transaction costs, facilitate the coordination of behaviour and make commitments more credible (Keohane 2005; Keohane and Martin 1995). Institutionalized regimes have these effects because they codify behavioural patterns, ensuring that people and states know how events will roughly unfold. These patterns can become very path dependent and resistant to change (North 1990). From this perspective, only large exogenous shocks, similar to the sunspot theory, can change institutional arrangements. Change, in other words, cannot occur from within the institution without first being driven by change outside of the institutional context.

Avner Greif and David D. Laitin (2004), however, propose a theory of endogenous institutional change. In their theory, institutional arrangements set up a specific way of doing things that is resistant to change in the short run, even change from outside of the system, because these arrangements condition what actors know about situations, focus their attention on specific self-reinforcing problems and coordinate behavioural responses (ibid., 637-38). At the same time, institutions generally set off processes that can have little effect on institutions in the short run, but that can be highly variable over the long run. These processes can have either positive or negative effects. Some

processes, such as the European Union's initial Common Market, might enhance trust and cooperation between states over the longer term and make the institution more resilient. Others, such as the European Union's adoption of the euro, might cause economic deprivation in some areas over the longer term and can thereby undermine the resilience of the institution. An institution, despite being designed to ensure routine, stability and predictability, can actually be its own engine of change.

Since engineers led the Internet's initial development for non-commercial and largely academic purposes, the institutional regime that developed for governing the Internet involved ideas of universality, open communication and accessibility. These initial institutional arrangements have contributed to the worldwide spread of the Internet, encouraged its adoption as a technical platform for e-commerce and generated the growth of new ways for people to interact with each other, such as social media. In some ways, the trends that the original institutional arrangements set off are now undermining the original organizational principles of the Internet governance regime. In a little over 10 years, the number of Internet users has increased from one billion to three billion, and the global number of users in developing countries now exceeds those in developed countries (ISOC 2014a).

The vast majority of future user growth will occur in the developing world. Estimates show that by 2020, China, India, Nigeria and Brazil should each house more Internet users than Great Britain, Germany or France (Kleiner, Nicholas and Sullivan 2014). This massive increase in Internet users is a direct result of the initial system of coordinated protocols and universal norms that governed the Internet in its first decades of existence. The original institutional arrangement that governed the Internet started a process that is facilitating the spread of Internet usage to every corner of the world.

While demography is not destiny, the result of this trend could have serious implications for the current Internet governance regime, especially since a clear plurality of new Internet users will be in China, which holds different normative views on things online, such as censorship, free speech and other human rights. This change could result in an increasingly fragmented Internet if China, anticipating its coming pre-eminence in the online world, tries to change the Internet governance regime in its favour. Arguably, China already attempted this to some extent during the 2012 WCIT meeting. It is possible, therefore, that the transitions seen from problems of coordination to problems of (failed) cooperation are a result of the original institutional design of the Internet governance regime.

Development of the Internet and the social institutions that govern it and make its continued operation possible have occurred in tandem. Many of these developments are explicable in part by endogenous, path-dependent processes. If the Internet had not been governed as an open and permissive system, it is unlikely to have expanded to the extent and in the way it did. Without the open architecture of early Internet standards, protocols and institutions, many of the current Internet governance challenges pitting people of different normative perspectives against one another or making the Web such a tantalizing economic prize would not have emerged.

Constructivist scholarship also sheds light on the path-dependent effects of institutions on future behaviour, but in doing so it emphasizes distinct behavioural logics of appropriateness (March and Olsen 1998; Finnemore and Sikkink 1998; Müller 2004), habit (Hopf 2010) and practice (Adler and Pouliot 2011). In doing so, it employs a more complex notion of agency and choice that acknowledges the goal-directed nature of human behaviour while broadening the conception of available goals beyond utility maximization.

As such, constructivist scholarship is well equipped to explain the extent to which Internet governance debates increasingly revolve around concerns about legitimacy, appropriateness and justice. Such concerns have been articulated in both substantive and procedural terms. Substantive concerns have to do with the nature of the rules and institutions that provide for governance of particular Internet functions, for example, provisions to encourage the adoption of IPv6, or rules about state behavior in online surveillance. Procedural concerns, for their part, have to do with the means of reaching decisions about these substantive matters, for example, whether the GAC should operate by consensus or some other voting rule, or whether it should be able to demand that the ICANN board respond to its "advice."

Increasing levels of procedural contestation are especially worthy of attention. The diversity of views on legitimate procedural rules among participants in Internet governance is striking and worrisome (Raymond and Smith 2014), and disagreement on such rules renders the resolution of substantive disagreements far more problematic (Diehl and Ku 2010; Raymond 2011; 2013). It is difficult to bridge or resolve substantive disagreements if there is no prior agreement on the legitimate procedure by which to do so (Hurd 1999; Albin 2001). International opposition to the continuation of the contractual relationship between ICANN and the NTIA for the administration of key Internet naming and numbering functions, discussed above, is one case of legitimacy concerns shaping contention over Internet governance issues. Such a claim does not require that actors advocating change to this relationship operate with pure motives. Legitimacy concerns, especially those pertaining to procedural matters, can shape outcomes even where actors may have mixed or even purely self-interested motives. This is because procedural rules affect the ways audiences respond to arguments and thus help to explain

the success or failure of particular attempts to change institutions (Raymond 2011). Further, evidence indicates actors are well aware of the benefits of framing their arguments in terms consistent with prevailing procedural rules. Debates about the future oversight mechanisms for the IANA functions are especially interesting in this regard. In these debates, states such as China and Russia have criticized the multi-stakeholder model of Internet governance for failing to meet the accepted procedural practices of the institution of multilateralism (People's Republic of China 2014). In doing so, these states seek to use practices intimately associated with the advanced industrial democracies (Ruggie 1983; Reus-Smit 1999; Ikenberry 2001) to deny legitimate standing to an array of non-state actors. In neglecting to update international procedural rules, the industrial democracies have left themselves open to this subversion of the spirit of multilateralism in the service of arresting the spread of informal contemporary practices of global governance more tolerant of the independent participation of non-state actors.

While these innovative, strategic uses of procedural rules highlight the surprising and creative ways actors exercise agency in the contemporary international system, it is worth reiterating that such examples do not negate that such rules are in many cases deployed and complied with in good faith even by powerful actors. This is true both due to genuine internalization as well as the more instrumental consideration that employing accepted procedural rules in expected ways ensures that one's actions are socially intelligible and meaningful to the relevant audience. Finally, although space constraints prevent detailed empirical analysis, this issue area contains cases of numerous theoretical mechanisms well known in the constructivist literature — including, but not limited to, strategic social construction, learning, persuasion and socialization.

Both the rational choice and constructivist literatures surveyed here are concerned with the way pre-existing institutions shape the development of institutions over time. This chapter argues that these kinds of effects are helpful in explaining why and how Internet issues have become contentious. A series of technological, economic and political developments have combined with existing institutions such that Internet issues now involve more (increasingly culturally diverse) players, higher stakes with respect to the division of joint gains and, in some cases, incentives to cheat on commitments. Internet governance now often includes actors whose primary responsibilities include Internet issues only tangentially, and actors are often tempted to accomplish objectives relating to patterns of Internet use by means of technical Internet architecture. More generally, it is clear that key aspects of social, political and economic life now occur in or through cyberspace. As a result of increased cultural diversity among the players, there is also less shared belief that existing institutions are legitimate.

In light of these developments, actors are forced to simultaneously confront a range of difficult problems, one being a high degree of attempted institutional innovation by agents pursuing diverse interests and values. Both status quo and revisionist actors are confronted with an increasing number of cases in which there is a need to reconcile rules and norms dealing with Internet governance with rules and norms regulating other issue areas that are increasingly affecting, and affected by, the Internet governance regime. Actors do not confront these problems with a tabula rasa, but rather with identities shaped in part by pre-existing regimes from a variety of issue areas and with options conditioned by those same rules and norms. Therefore, accounting for institutional endogeneity is vital to explaining ongoing processes and outcomes with respect to Internet issues.

Nye (2014) argues that Internet governance should be understood as embedded in a broader set of rules, institutions and processes that govern related issue areas including trade, development, human rights, security, law enforcement and intellectual property, among others. That is, he argues it is more productive to think in terms of a broader cyber regime complex rather than only in terms of a single Internet governance regime.[2] The authors agree, but emphasize the ongoing, incomplete nature of this process. They argue that changes in the underlying problem structure have set off a continuing process of regime complex formation as actors attempt to deal with this new reality by creating and altering institutions. This process, in turn, creates further contention, given the diversity of interests and values, the increasing number of actors involved and the heightened importance of the issues.

IMPLICATIONS OF THIS SHIFT AND PROSPECTS FOR GLOBAL COOPERATION

No other areas of IR have been marked by such a pronounced shift from relatively simply coordination problems to a challenging hybrid of cooperation problems alongside complex coordination problems characterized by large numbers of players with divergent preferences over the available equilibria. The emergence of contention in Internet governance is, therefore, a novel problem with potentially large implications for successful governance of the Internet. These include destabilization of the Internet governance ecosystem and the threat of various forms of Internet fragmentation. Typically, states have dominated

2 On regime complexes, see Raustiala and Victor (2004), Betts (2010), Keohane and Victor (2011), Orsini, Morin and Young (2013) and Drezner (2009).

in cooperation problems, raising troubling questions about whether the private sector-led multi-stakeholder approach can survive in this context.

Resolving these disputes, or at least avoiding high-consequence negative outcomes, will require a nuanced understanding of the layers of Internet governance, rather than viewing the system in monolithic terms. Global discussions and conflict over "who controls the Internet" view the system as monolithic and thus have little relevance to the complexity of the Internet governance ecosystem and how Internet governance works in practice. Strategies of decomposing issues in negotiations are therefore especially appropriate and should be encouraged. Linkage politics should be avoided where possible (Keohane and Nye 2001).

In addition to the implications of the analysis here for the study and practice of Internet governance, the findings are also of interest to IR scholars and practitioners more broadly. Scholarly work in IR examining international cooperation has typically understood problem structures as static. Little attention has been paid to the possibility for, or the dynamics of, degenerative shifts in problem structure. This chapter highlights the need for further research addressing these questions.

It is also interesting to speculate about how actors within the current Internet governance regime are going to react to growing levels of contention. Albert O. Hirschman (1970) points out that when faced with a dysfunctional system, all actors have three choices: "exit, voice, and loyalty." Determining the precise times when actors will choose each of these three strategies in response to growing contention would be a useful endeavour. More generally, the start of actions to this effect can already be seen. Russia, for example, recently announced that it plans to develop a system that would allow it to remove its Internet from the global system, an example of exit if ever there was one (Reuters 2014). Other actors are relying more on voice, as can be seen in the example of stakeholder discussions surrounding NETmundial in Brazil. Some nations and actors might also consider loyalty to the current system, as is a fairly common position among many Western states that more or less support the current Internet governance regime.

Such questions are also more than matters of academic interest. To the extent that non-state actors and emerging powers (such as the BRICS countries, that is, Brazil, Russia, India, China and South Africa) have distinct views about legitimate procedural rules that diverge from accepted international practices, it may be the case that Internet governance is simply a canary in the coal mine, and that the emergence of contention will also take place in other issue areas. Such procedural conflict could eventually compromise the basic operation of an array of global governance mechanisms and perhaps even international law more generally.

ACKNOWLEDGEMENTS

The authors would like to thank Joseph S. Nye, Jr., Robert O. Keohane, Dane Rowlands and all who have given comments on the chapter.

WORKS CITED

Adler, Emanuel and Vincent Pouliot. 2011. International Practices. *International Theory* 3 (1): 1–36.

Albin, Cecilia. 2001. *Justice and Fairness in International Negotiation*. Cambridge, MA: Cambridge University Press.

Axelrod, Robert. 2006. *The Evolution of Cooperation*. Cambridge, MA: Basic Books.

Best Bits. 2014. "Civil Society Closing Statement at NETmundial 2014." Statement, April 24. http://bestbits.net/netmundial-response/.

Betts, Alexander. 2010. "The Refugee Regime Complex." *Refugee Survey Quarterly* 29 (1): 12–37.

Bradshaw, Samantha and Laura DeNardis. 2015. "The Politicization of the Domain Name System: Implications for Internet Security, Stability, Universality and Freedom." Paper presented at the 56th Annual International Studies Association, New Orleans, LA.

Brousseau, Eric, Meryem Marzouki and Cécile Méadel, eds. 2012. *Governance, Regulation, and Powers on the Internet*. Cambridge, MA: Cambridge University Press.

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

Bygrave, Lee A. and Jon Bing, eds. 2009. *Internet Governance: Infrastructure and Institutions*. Oxford, UK: Oxford University Press.

Cass, David and Karl Shell. 1983. "Do Sunspots Matter?" *Journal of Political Economy* 91 (21): 193–228.

Chander, Anupam and Uyen P. Le. 2014. "Breaking the Web: Data Localization vs. the Global Internet." UC Davis Legal Studies Research Paper No. 378. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858.

CIGI-IPSOS. 2014. Global Survey on Internet Security and Trust. www.cigionline.org/internet-survey.

Corwin, P. S. 2013. "ICANN@15: Born in the USA — But Will It Stay?" *CircleID* (blog). www.circleid.com/posts/20131115_icann15_born_in_the_usa_but_will_it_stay_api1/.

Deibert, Ronald J. 2014. "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace." In *Organized Chaos: Reimagining the Internet*, edited by Mark Raymond and Gordon Smith. Waterloo, ON: CIGI.

Dell, Peter. 2010. "Two Economic Perspectives on the IPv6 Transition." *Info* 12 (4): 3–14.

Demchak, Chris C. and Peter Dombrowski. 2011. "Rise of a Cybered Westphalian Age." *Strategic Studies Quarterly* 5 (1): 32–61.

DeNardis, Laura. 2012a. "Governance at the Internet's Core: The Geopolitics of Interconnection and Internet Exchange Points (IXPs) in Emerging Markets." Paper presented at the Telecommunications Policy Research Conference, the 40th Research Conference on Communication, Information and Internet Policy, Arlington, VA. http://papers.ssrn.com/ sol3/papers.cfm?abstract_id=2029715.

———. 2012b. Hidden Levers of Internet Control: An Infrastructure-Based Theory of Internet Governance. *Journal of Information, Communication & Society* 15 (3): 1–19.

———. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Diehl, Paul F. and Charlotte Ku. 2010. *The Dynamics of International Law*. Cambridge, MA: Cambridge University Press.

Drezner, Daniel W. 2009. "The Power and Peril of International Regime Complexity." *Perspectives on Politics* 7 (1): 65–70.

Farmer, Roger E. A. and Jang-Ting Guo. 1994. "Real Business Cycles and the Animal Spirit Hypothesis." *Journal of Economic Theory* 63 (1): 42–72.

Fearon, James D. 1998. "Bargaining, Enforcement and International Cooperation." *International Organization* 52 (2): 269–305.

Finnemore, Martha and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52 (4): 887–917.

French Senate. 2014. "Internet: le Sénat veut démocratiser sa gouvernance en s'appuyant sur une ambition politique et industrielle européenne." www.senat.fr/presse/cp20140709b.html.

Gilpin, Robert. 1983. *War and Change in World Politics*. Cambridge, MA: Cambridge University Press.

Greif, Avner and David D. Laitin. 2004. "A Theory of Endogenous Institutional Change." *American Political Science Review* 98 (4): 633–52.

Haas, Peter M. 1992. "Epistemic Communities and International Policy Coordination." *International Organization* 46 (1): 1–35.

Hirose, Yasuo. 2007. "Sunspot Fluctuations under Zero Nominal Interest Rates." *Economics Letters* 97 (1): 39–45.

Hirschman, Albert O. 1970. *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations and States*. Cambridge, MA: Harvard University Press.

Hopf, Ted. 2010. "The Logic of Habit in International Relations." *European Journal of International Relations* 16 (4): 539–61.

Housley, Russ. 2014. "Words from the IAB Chair." *IETF Journal*. www.internetsociety.org/publications/ietf-journal-july-2014/words-from-the-iab-chair.

Hurd, Ian. 1999. "Legitimacy and Authority in International Politics." *International Organization* 53 (2): 379–408.

ICANN. 2014. Motion to Quash Writ of Attachment in the U.S. District Court for the District of Columbia, filed July 29, 2014. www.icann.org/.../ben-haim-motion-to-quash-writs-1-29jul14-en.pdf.

IETF. 2013. "Security and Pervasive Monitoring." *IETF* (blog). www.ietf.org/blog/2013/09/security-and-pervasive-monitoring/.

Ikenberry, G. John. 2001. *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order After Major Wars*. Princeton, NJ: Princeton University Press.

Incyder News. 2014. "Information Security Discussed at the Dushanbe Summit of the Shanghai Cooperation Organisation." NATO Cooperative Cyber Defence Centre of Excellence. October 27. https://ccdcoe.org/information-security-discussed-dushanbe-summit-shanghai-cooperation-organisation.html.

ISOC. 2014a. *Global Internet Report*. www.internetsociety.org/sites/default/files/Global_Internet_Report_2014_0.pdf.

———. 2014b. "Internet Society Statement on the NETmundial Initiative." www.internetsociety.org/news/internet-society-statement-netmundial-initiative.

Jervis, Robert. 1978. "Cooperation Under the Security Dilemma." *World Politics* 30 (2): 167–214.

Jevons, William Stanley. 1887. "Commercial Crises and Sunspots." *Nature* xix: 33–37.

Keohane, Robert O. 2005. *After Hegemony: Cooperation and Discord in the World Political Economy*. Princeton, NJ: Princeton University Press.

Keohane, Robert O. and Lisa Martin. 1995. "The Promise of Institutionalist Theory." *International Security* 20 (1): 39–51.

Keohane, Robert O. and Joseph S. Nye, Jr. 2001. *Power and Independence*. New York, NY: Longman.

Keohane, Robert O. and David G. Victor. 2011. "The Regime Complex for Climate Change." *Perspectives on Politics* 9 (1): 7–23.

Kleiner, Aaron, Paul Nicholas and Kevin Sullivan. 2014. "Linking Cybersecurity Policy and Performance." www.microsoft.com/en-us/download/confirmation.aspx?id=36523.

Kleinwächter, Wolfgang. 2015. "Internet Governance Outlook 2015: Two Processes, Many Venues, Four Baskets." *CircleID* (blog). www.circleid.com/posts/20150103_internet_governance_outlook_2015_2_processes_many_venues_4_baskets.

Koremenos, Barbara, Charles Lipson and Duncan Snidal. 2001. "The Rational Design of International Institutions." *International Organization* 55 (4): 761–99.

Krasner, Stephen D. 1991. "Global Communications and National Power: Life on the Pareto Frontier." *World Politics* 43 (3): 336–66.

Manyika, James, Jacques Bughin, Susan Lund, Olivia Nottebohm, David Poulter, Sebastian Jauch and Sree Ramaswamy. 2014. "Global Flows in a Digital Age: How Trade, Finance, People and Data Connect the World Economy." McKinsey & Company. August.

March, James G. and Johan P. Olsen. 1998. "The Institutional Dynamics of International Political Orders." *International Organization* 52 (4): 943–69.

Marquis-Boire, Morgan, Jakub Dalek, Sarah McKune, Matthew Carrieri, Masashi Crete-Nishihata, Ron Deibert, Saad Omar Khan, Helmi Noman, John Scott-Railton and Greg Wiseman. 2013. "Planet Blue Coat: Mapping Global Censorship and Surveillance Tools." The Citizen Lab Research Brief No. 13. https://citizenlab.org/wp-content/uploads/2013/01/Planet-Blue-Coat.pdf.

Martin, Lisa L. and Beth A. Simmons. 1998. "Theories and Empirical Studies of International Institutions." *International Organization* 52 (4): 727–57.

Mathiason, John. 2008. *Internet Governance: The New Frontier of Global Institutions*. New York, NY: Routledge.

Maurer, Tim. 2011. "Cyber Norm Emergence at the United Nations: An Analysis of the Activities at the UN Regarding Cyber-Security." Discussion Paper #2011-11. Cambridge: Belfer Center for Science and International Affairs. http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

Maurer, Tim and Robert Morgus. 2014. "Tipping the Scale: An Analysis of Swing States in the Internet Governance Debate." In *Organized Chaos: Reimagining the Internet*, edited by Mark Raymond and Gordon Smith, 151–66. Waterloo, ON: CIGI.

McAfee and Centre for Strategic and International Studies. 2014. *Net Losses: Estimating the Global Costs of Cybercrime*. Centre for Strategic and International Studies. www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2-summary.pdf.

Miller, Rich. 2008. "Peering Dispute Between Cogent, Sprint." *Data Knowledge Center* (blog), October 31. www.datacenterknowledge.com/archives/2008/10/31/peering-dispute-between-cogent-sprint/.

Milner, Helen. 2006. "The Digital Divide: The Role of Political Institutions in Technology Diffusion." *Comparative Political Studies* 39 (2): 176–99.

Mueller, Milton. 2002. *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

———. 2010. Critical Resource: "An Institutional Economics of the Internet Addressing-Routing Space." *Telecommunications Policy* 34 (8): 405–16.

———. 2012. "Threat Analysis of ITU's WCIT (Part 1): Historical Context." Internet Governance Project. www.internetgovernance.org/2012/05/24/threat-analysis-of-itus-wcit-part-1-historical-context/.

Müller, Harald. 2004. "Arguing, Bargaining and All That: Communicative Action, Rationalist Theory and the Logic of Appropriateness in International Relations." *European Journal of International Relations* 10 (3): 395–435.

NETmundial. 2014. "NETmundial Initiative Basics." www.netmundial.org/netmundial-initiative-basics.

Newman, Lily Hay. 2014. "Judge Rules That Even if Iran Owes you Money, You Can't Just Take Its Top-Level Domains." *Slate Magazine*, November 13. www.slate.com/blogs/future_tense/2014/11/13/judge_rules_that_plaintiffs_can_t_be_awarded_top_level_domains_for_iran.html.

North, Douglas. 1990. I*nstitutions, Institutional Change and Economic Performance*. Cambridge, MA: Cambridge University Press.

Nye, Joseph S., Jr. 2011. "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly* 5 (4): 18–38.

———. 2014. *The Regime Complex for Managing Global Cyber Activities*. Global Commission on Internet Governance Paper Series Paper No. 1. Waterloo, ON: CIGI. www.cigionline.org/publications/regime-complex-managing-global-cyber-activities.

Olson, Mancur. 1965. T*he Logic of Collective Action: Public Goods and the Theory of Groups*. Cambridge, MA: Harvard University Press.

Orsini, Amandine, Jean-Frédéric Morin and Oran Young. 2013. "Regime Complexes: A Buzz, a Boom, or a Boost for Global Governance?" *Global Governance* 19 (1): 27–39.

People's Republic of China. 2014. "China Calls for Multilateral Global Internet Governance." People's Republic of China: State Council. http://english.gov.cn/news/video/2014/11/20/content_281475012927255.htm.

Powell, Robert. 1991. "Absolute and Relative Gains in International Relations Theory." *The American Political Science Review* 85 (4): 1303–20.

Raustiala, Kal and David G. Victor. 2004. "The Regime Complex for Plant Genetic Resources." *International Organization* 58 (2): 277–309.

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

———. 2013. "Renovating the Procedural Architecture of International Law." *Canadian Foreign Policy Journal* 19 (3): 268–87.

Raymond, Mark, Aaron Shull and Samantha Bradshaw. 2015 (forthcoming). "Rule-making for State Conduct in the Attribution of Cyber Attacks." In *Mutual Security in the Asia-Pacific: Rules for Australia, Canada and South Korea*, edited by Kang Choi, James Manicom and Simon Palamar. Waterloo, ON: CIGI.

Raymond, Mark and Gordon Smith, eds. 2014. *Organized Chaos: Reimaging the Internet*. Waterloo, ON: CIGI.

Razumovskaya, Olga. 2015. "Russia and China Pledge Not to Hack Each Other." *Digits* (*The Wall Street Journal* blog). blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/.

Reus-Smit, Christian. 1999. *The Moral Purpose of the State: Culture, Social Identity, and Institutional Rationality in International Relations*. Princeton, NJ: Princeton University Press.

Reuters. 2014. "Russia Eyes Measures to Fend Off Western Internet Threat: Kremlin." Reuters, September 19. www.reuters.com/article/2014/09/19/us-russia-internet-idUSKBN0HE1F320140919.

Ricknäs, Mikael. 2008. "Sprint-Cogent Dispute Puts Small Rip in Fabric of the Internet." PCWorld. www.pcworld.com/article/153123/sprint_cogent_dispute.html.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5–32.

Ruggie, John Gerard. 1982. "International Regimes, Transactions, and Change: Embedded Liberalism in the Postwar Economic Order." *International Organization* 36 (2): 379–415.

Schelling, Thomas C. 1980. *The Strategy of Conflict*. Cambridge, MA: Harvard University Press.

Schmitt, Michael N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, MA: Cambridge University Press.

Security and Stability Advisory Committee. 2014. "Overview and History of the IANA Function." ICANN: Security and Stability Advisory Committee. www.icann.org/en/system/files/files/sac-067-en.pdf.

Shu, Catherine. 2014. "China Tried to Get World Internet Conference Attendees to Ratify this Ridiculous Draft Declaration." *TechCrunch*, November 20. http://techcrunch.com/2014/11/20/worldinternetconference-declaration.

Sil, Rudra and Peter J. Katzeintein. 2010. "Analytic Eclecticism in the Study of World Politics: Reconfiguring Problems and Mechanisms across Research Traditions." *Perspectives on Politics* 8 (2): 411–31.

Snidal, Duncan. 1985. "Coordination versus Prisoners' Dilemma: Implications for International Cooperation and Regimes." *American Political Science Review* 79 (4): 923–42.

Snyder, Glenn H. 1971. "'Prisoner's Dilemma' and 'Chicken' Models in International Politics." *International Studies Quarterly* 15 (1): 66–103.

Statista. 2014. "Global Market Share of the Information and Communication Technology (ICT) Market in 2014, by Country." www.statista.com/statistics/263801/global-market-share-held-by-selected-countries-in-the-ict-market/.

The Guardian. 2014. "US Court Forces Microsoft to Hand over Personal Data from Irish Server." *The Guardian*, April 29. www.theguardian.com/technology/2014/apr/29/us-court-microsoft-personal-data-emails-irish-server.

UNGA. 2013. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." www.mofa.go.jp/files/000016407.pdf.

United Nations. 2014. "Adopting 68 Texts Recommended by Third Committee, General Assembly Sends Strong Message Towards Ending Impunity, Renewing Efforts to Protect Human Rights." www.un.org/press/en/2014/ga11604.doc.htm.

United Nations Institute for Disarmament Research. 2014. "An International Code of Conduct for Information Security: China's Perspective on Building a Peaceful, Secure, Open and Cooperative Cyberspace." www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf.

Van Evera, Stephen. 1984. "The Cult of the Offensive and the Origins of the First World War." *International Security* 9 (1): 58–107.

Walt, Stephen. 2006. *Taming American Power: The Global Response to U.S. Primacy*. New York, NY: W. W. Norton & Company.

Waltz, Kenneth, N. 1979. *Theory of International Politics*. Long Grove, IL: Waveland Press.

Welch, David A. 1993. *Justice and the Genesis of War*. Cambridge, MA: Cambridge University Press.

Wohlforth, William C. 1990. "The Stability of a Unipolar World." *International Security* 24 (1): 5–41.

Woodcock, Bill and Vijay Adhikari. 2014. "Survey of Characteristics of Internet Carrier Interconnection Agreement." Packet Clearing House. www.pch.net/resources/papers/peering-survey/PCH-Peering-Survey-2011.pdf.

Wright, Joseph. 2015. "IANA Transition, Accountability Highlight Top 15 Policy Points to Watch at ICANN in 2015." *Bloomberg BNA Ecommerce and Tech Blog*, January 8. www.bna.com/dns-policy-notes-b17179921944/.

Xinhua News. 2015. "China Unveils "Internet Plus" Action Plan to Fuel Growth." Xinhua News Agency, July 4. http://news.xinhuanet.com/english/2015-07/04/c_134381999.htm.

ABOUT THE AUTHORS

Samantha Bradshaw is a research associate at CIGI in the Global Security & Politics Program. She contributes to the work of the Global Commission on Internet Governance. Samantha's research focuses on Internet governance, the politics of the domain name system and cyber security cooperation. She holds an M.A. in global governance from the Balsillie School of International Affairs and a joint honours B.A. in political science and legal studies from the University of Waterloo.

Laura DeNardis, CIGI senior fellow, is a scholar of Internet architecture and governance and professor in the School of Communication at American University in Washington, DC. The author of *The Global War for Internet Governance* (Yale University Press, 2014) and several other books, her expertise has been featured in numerous publications. She serves as the director of research for the Global Commission on Internet Governance and is an affiliated fellow of the Yale Law School Information Society Project, where she previously served as executive director. Laura holds an A.B. in engineering science from Dartmouth College, a Master of Engineering from Cornell University, a Ph.D. in science and technology studies from Virginia Tech, and was awarded a post-doctoral fellowship from Yale Law School.

Fen Osler Hampson is a distinguished fellow and the director of the Global Security & Politics Program at CIGI. He is also co-director of the Global Commission on Internet Governance. He is chancellor's professor at Carleton University and a former Jennings Randolph Fellow at the United States Institute of Peace.

Eric Jardine joined CIGI as a research fellow in May 2014 in the Global Security & Politics Program. He contributes to CIGI's work on Internet governance, including the Global Commission on Internet Governance. Eric's current research focuses on cyber security, cyber terrorism, cybercrime and cyber protest. He holds a Ph.D. in international relations from the Norman Paterson School of International Affairs at Carleton University.

Mark Raymond is the Wick Cary Assistant Professor of International Security at the University of Oklahoma. His work has appeared in *International Theory,* the *Georgetown Journal of International Affairs* and the *Canadian Foreign Policy Journal*. He is also the co-editor of *Organized Chaos: Reimagining the Internet* (CIGI, 2014). He has testified before the United Nations Commission on Science and Technology for Development, and participated in the Internet Governance Forum. His current research projects examine the politics of global rule-making, as well as Internet governance. He received his Ph.D. from the University of Toronto.

CHAPTER FOUR:
LEGAL MECHANISMS FOR GOVERNING THE TRANSITION OF KEY DOMAIN NAME FUNCTIONS TO THE GLOBAL MULTI-STAKEHOLDER COMMUNITY

Aaron Shull, Paul Twomey and Christopher S. Yoo

ACRONYMS

ccTLD	country code top-level domain
DNS	Domain Name System
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICDR	International Centre for Dispute Resolution
ICG	IANA Stewardship Transition Coordination Group
IRP Panel	Independent Review Process Panel
MoU	memorandum of understanding
NIC	Network Information Center
NTIA	National Telecommunications and Information Administration
TLD	top-level domain
USC	University of Southern California

INTRODUCTION

This chapter examines the upcoming Internet Assigned Numbers Authority (IANA) transition, wherein the US government will relinquish its historic control over key technical functions making up the modern-day Internet. The chapter's most important questions are: if the Internet Corporation for Assigned Names and Numbers (ICANN), the current IANA functions operator, is no longer accountable to the US government, then who should it be accountable to? And what form should that accountability take?

The existing contractual arrangement between ICANN and the US government contains more than simple contractual terms. Rather, many of those contractual obligations actually make up the core tenets of contemporary multi-stakeholder governance, such as:

- ICANN cannot assign the IANA functions to someone else;
- ICANN must operate as a multi-stakeholder, private sector-led organization with input from the public;
- the need to ensure quality performance of the IANA functions; and
- the existence of important contractual requirements regarding the continuity of operations.

The fact is that the Internet has become too important and too global for any one state to exercise exclusive control — even historic control. Thus, the United States unilaterally giving up its historic contractual stewardship is laudable. There is a significant debate, however, about what structure should take its place — with one extreme arguing for a new international organization created by civil society, and the other extreme arguing for centralized state control under the auspices of the United Nations International Telecommunication Union.

This chapter does not engage in that debate. Rather, it seeks to advance a credible solution based on real-world facts, existing legal rules and prevailing political realities.

It advances a balanced option that could work based on existing constraints, including the rapidly approaching deadline for the transition and the more primary concern of maintaining the stability of the system during the transition period (and beyond). In advancing this option, this chapter argues that the existing core contractual requirements imposed by the US government could be migrated to the existing IANA functions customers. This would ensure that the core tenets of contemporary multi-stakeholder Internet governance are built into the DNA of the governance regime going forward. It may also go a long way to preserving (and even enhancing) the multi-stakeholder system itself. It would create one-to-one accountability between the organization delivering the IANA service and the customers of that service.

The chapter also advances modest internal accountability revisions that could be undertaken within ICANN's existing structure, in order to increase legitimacy within the broader Internet community and to enhance existing corporate governance. To that end, it argues that the independence of the Independent Review Tribunal, charged with taking an impartial, sober second assessment of certain ICANN board of directors-related decisions, could be increased by allowing the judges (arbitrators) that sit on the panel to be selected by a multi-stakeholder committee rather than being subject to approval by ICANN. Second, that the existing grounds of review could be expanded, allowing the tribunal — when warranted — to hear additional cases on a broader range of complaints. In this vein, this chapter adopts the conclusions from ICANN's own "Improving Institutional Confidence" process in 2008-2009. This process recommended that a new Independent Review Tribunal be established with powers to review the exercise of decision-making powers of the ICANN board under four general rubrics: fairness, fidelity to the power, cogency of decision making and addressing the public interest (ICANN 2009a).[1] This new tribunal could be drawn from a standing panel of internationally recognized relevant technical experts, as well as

1 The public interest rubric is an added provision by the authors, and reflects general provisions in ICANN's bylaws.

internationally recognized jurists, including persons with senior appellate judge experience (ibid.). This chapter also argues that members of ICANN's various stakeholder groups and the public be able to make comments on the proposed bench before final appointment.

BACKGROUND ON THE IANA TRANSITION

The US Department of Commerce's National Telecommunications and Information Administration (NTIA) has officially announced its intention to transition key Internet domain name functions to the global multi-stakeholder community (see NTIA 2014). In response, ICANN, the current IANA functions operator, is convening with various stakeholders to develop the transition plan. This consultative process has led to the formation of the IANA Stewardship Transition Coordination Group (ICG), which is comprised of 30 individuals representing 13 direct and indirect stakeholder communities. This group is charged with advancing a plan that would facilitate the transition of these key domain name functions. This transition would end the primary oversight role for the US government in the function and maintenance of the core technical functions implicated in the operation of the Internet.

The IANA functions are a set of different technical tasks that are foundational for the operation of the Internet, functions over which the US government currently maintains an oversight or stewardship role.[2] At their base, the IANA functions are a set of activities that offer a "coordination service for the upper-most level Internet identifiers. These functions work to ensure the secure, stable, and reliable allocation, assignment, and distribution of those identifiers, their uniqueness with respect to a well-defined identifier space, and the recording of to whom and/or for what purpose they are assigned" (ICANN 2014b, 6). One of these key stewardship functions is the oversight of changes to the authoritative root zone file (see IANA 2014).[3] The root zone file is the database that allows the Internet to function — acting as a global address book for data — containing an authoritative list of the names and Internet protocol addresses of all top-level domains.

Initially, the IANA functions were performed under a contract between an agency of the US government (the Defense Advanced Research Projects Agency) and the University of Southern California (USC), as part of a major research project. From the early 1970s, IANA assigned the Internet protocol address numbers, while the Network Information Center (NIC) at the Stanford Research Institute published them to the rest of the network. In 1990, this changed with the US Department of Defense awarding the NIC functions to Government Systems, Inc., which subcontracted it to the small private sector firm Network Solutions Inc. By 1992, with much of the Internet outside the US military, contracting authority for these publishing functions was accumulated under the US National Science Foundation, which awarded the NIC functions to Network Solutions Inc., and related directory and database services to AT&T. As this contract neared expiry in 1999, it became clear that the stable performance of the IANA and NIC functions were "vital to the stability and correct functioning of the Internet" (NTIA 2012, C.1.2). This led to the white paper process, which resulted in the formation of a multi-stakeholder organization, ICANN, to coordinate these functions. The initial contract to provide the services to perform the operation of the IANA was concluded between the US Department of Commerce and ICANN on February 8, 2000 (NTIA 2000). The publishing function was restructured under a Cooperative Research and Development Agreement between the US Department of Commerce and Verisign (which had bought Network Solutions Inc. in 2000). This contractual arrangement has continued, and it is the US government's willingness to relinquish its contractual authority over the IANA functions that provides the primary mechanism for ending its oversight role.

However, this announcement has led to the conflation of two different issues. The first is the actual technical administration of the IANA functions, which is not an issue at all. In fact, a 2013 IANA functions customer satisfaction survey indicated that there were extremely high satisfaction levels among customers for these services (Vegoda 2013). The second, and more nuanced, issue is that the US government's decision to relinquish its contractual authority over the IANA functions has exposed a broader question about ICANN's accountability. In its most basic form, the questions being asked are if ICANN is no longer accountable to the US government for the IANA functions through contract, then to which organization or community should ICANN be accountable and what form should that accountability take? This seemingly simple question has generated much confusion and political discussion.

It is worth making an important distinction here about the history of ICANN's accountability relations with the United States government since its inception. Initially, there were two established mechanisms of accountability. The first was the IANA procurement contract, which is

2 For an excellent summary on the history of the IANA functions and the role of the US government, see ICANN (2014b).

3 According to IANA (2014), "[its] functions are a set of interdependent technical functions that enable the continued efficient operation of the Internet. The IANA functions include: (1) the coordination of the assignment of technical Internet protocol parameters; (2) the processing of change requests to the authoritative root zone file of the DNS [Domain Name System] and root key signing key...management; (3) the allocation of Internet numbering resources; and (4) other services related to the management of the ARPA and INT top-level domains [TLDs]."

discussed later. The second was the memorandum of understanding (MoU) process by which the US Department of Commerce worked with the board and management of the new ICANN to ensure that it developed as was envisaged in the 1998 US white paper that had called for the establishment of a multi-stakeholder, not-for-profit entity to carry out the functions previously performed by US government agencies (ICANN 2000). In particular, the MoU process sought to ensure that ICANN "has the capability and resources to assume the important responsibilities related to the technical management of the DNS. To secure these assurances, the Parties… will jointly design, develop, and test the mechanisms, methods, and procedures that should be in place and the steps necessary to transition management responsibility for DNS functions now performed by, or on behalf of, the U.S. Government to [ICANN]. Once testing is successfully completed, it is contemplated that management of the DNS will be transitioned to the mechanisms, methods, and procedures designed and developed in the DNS Project" (ICANN 1999). In practice, the development was undertaken by the ICANN community and embedded in its bylaws, procedures, organizational structure and policy development processes. ICANN submitted 13 reports to the US Department of Commerce until 2006, when the MoU process was amended to a final three-year Joint Project Agreement. In its conclusion, the US Department of Commerce formally recognized ICANN as the body envisaged in the white paper and the two parties made a detailed statement of responsibilities to the broader Internet community. This Affirmation of Commitments agreement replaced the US Department of Commerce with an international and multi-stakeholder mechanism from within the Internet community that outlined ICANN's commitment to:

- ensure accountability, transparency and the interests of global Internet users;
- enhance the operational stability, reliability, resiliency, security and global interoperability of the DNS; and
- promote competition, consumer trust and consumer choice, especially in domain names, and commit to enforcing its existing policy relating to WHOIS, subject to applicable laws. (ICANN 2009b)

Despite the widely well-received Affirmation of Commitments,[4] at least part of the international Internet and political communities saw (and in many cases welcomed) the continuance of the IANA procurement contract as an added political patina: that the US government would continue as a critical political backstop against threats to Internet stability, and in this conception ICANN is — at least theoretically — accountable to the administration of the US government through the IANA contract.

Further confusion is created by the fact that some have failed to recognize the distinction between accountability for performing the IANA functions on the one hand, and accountability for broad policy decisions related to the DNS on the other; these are not the same thing. The Department of Commerce has made it clear that it sees the latter covered by the Affirmation of Commitments and ICANN's other similar frameworks. With respect to accountability for the former, one possible approach could be that the relevant provisions that rendered ICANN accountable to the US government for the performance of these functions and the necessary service standards, could simply be migrated from the contracts with the Department of Commerce to the contracts between ICANN and its IANA services customers. In this regard, ICANN would then be accountable to its customers through the law of contract for the functions and services performed on its behalf.

A simple two-way equal accountability to the "customers" or "partners" of the IANA functions, however, does have its limitations. In certain circumstances, the exercise of the IANA functions requires an exercise of superior power. The three clearest examples are the recognition of a new TLD, the re-delegation of an existing TLD from one administrator to another and the recognition of a new regional Internet registry. While upward community policies have been developed through the ICANN multi-stakeholder processes, building on earlier Internet community documents, such as the Internet Engineering Task Force's RFC 1591 (drafted by Jon Postel in 1994),[5] to establish the processes ICANN must follow to exercise this power,[6] circumstances require on occasions that the IANA function be exercised contrary to the narrow interests of an existing "partner." The *cause célèbre* of this is a "hostile re-delegation" of a country code TLD (ccTD). The need for IANA to be able to act to implement the re-delegation process is recognized in various ways in the existing accountability agreements between ICANN and 84 ccTLDs.[7]

Consequently, this chapter proposes that, as well as accountability of performance of the IANA processes through the contracts or exchange of letters that ICANN has with its IANA services customers, there should also be a form of administrative review through appeal to the

4 See https://archive.icann.org/en/affirmation/affirmation-reaction.htm.

5 Jon Postel originated the IANA function at USC and continued to perform the function until the task became too demanding, leading to the US government's white paper process in 1998.

6 See www.icann.org/resources/pages/background-2012-02-25-en; www.icann.org/resources/pages/global-addressing-2012-02-25-en; www.icann.org/resources/pages/new-rirs-criteria-2012-02-25-en; and www.ietf.org/rfc/rfc1591.txt.

7 See www.icann.org/resources/pages/cctlds-2012-02-25-en.

type of review panel proposed later in the chapter. This will allow parties affected by this exercise of "superior power" to have recourse to review the fidelity of the process followed by ICANN.

Accountability for policy decisions is *ab initio* more complex. Nevertheless, when engaging in discussions surrounding ICANN's accountability in the broader sense, it is important not to lose sight of three critical facts. First, ICANN already has in place a number of internal and external mechanisms related to accountability for policy decisions. Second, at present, the US government has not, nor is likely to, intervene in the decision-making process within ICANN, making this portion of the existing accountability relationship largely symbolic.[8] Third, the US government made clear at ICANN's Town Hall Meeting at the 2014 Internet Governance Forum that the discussion around enhancing ICANN's accountability mechanisms should be narrowly focused on those related to the IANA functions. In this way, it now seems unequivocal that there is no open invitation to discuss major institutional change. Rather, when determining whether it will relinquish its contractual authority, the US government is interested only in narrowly articulated issues of accountability insofar as they relate to ICANN's contractual relationship with the US government.

In addition to the constraint on the substantive elements of the accountability review, there are a number of other conditions that must be met in order for the transition plan to be accepted by the NTIA. The NTIA has indicated in no uncertain terms that to be accepted, the transition plan must:

- have broad community support;
- support and enhance the multi-stakeholder model;
- maintain the security, stability and resiliency of the Internet DNS;
- meet the needs of global customers for the IANA services;
- maintain the openness of the Internet; and
- not replace the NTIA role with a government-led or an intergovernmental organizational solution.

Currently, there is no consensus on an institutional framework that can meet these six necessary conditions. There is also no consensus on what the word "accountability" actually means in this context, or on how ICANN's broader accountability mechanisms could be strengthened in the absence of a contractual relationship with the US government.

To clear up the definitional ambiguity, this chapter employs a two-part definition of accountability. The first involves accountability for performance, meaning that the IANA functions are being performed promptly, efficiently and professionally. As a core piece of global critical infrastructure, one of the IANA accountabilities is that its processes and operations are effective 24/7/365. The second part adopts the definition put forward by Ruth W. Grant and Robert O. Keohane (2005) and assumes that accountability "functions to expose and sanction two sorts of abuses: the unauthorized or illegitimate exercise of power and decisions that are judged by accountability holders to be unwise or unjust." Thus, in order to be accountable in the absence of the traditional contractual relationship with the US government, there must be some other mechanism that can function to ensure high performance standards and that can sanction unauthorized or illegitimate actions or inactions on the part of ICANN in its performance of the IANA functions.

EXTERNAL ACCOUNTABILITY: CONTRACTUAL MIGRATION OF CORE REQUIREMENTS FOR IANA FUNCTIONS

THE IANA FUNCTIONS CONTRACT

The IANA functions contract between the US Department of Commerce and ICANN includes a number of extremely important provisions, which are principled and sensible mechanisms, and which are now deeply engrained in the structure of contemporary Internet governance. However, the absence of a contractual obligation to the US government for these provisions could undermine their legal footing.

As an example, the IANA functions contract creates important obligations regarding how ICANN relates to affected parties. Under the existing contract, ICANN is obliged to develop a close constructive working relationship with all interested and affected parties to ensure quality and satisfactory performance of the IANA functions (NTIA 2012, C.1.3). ICANN is also prohibited from subcontracting or assigning the required services to another entity (ibid., C.2.1).

With respect to the establishment and collection of fees from the IANA functions customers, there is a contractual requirement to ensure that the fee levels are fair and reasonable, and that any proposed fee structure would be based on the cost of providing the specific service in question (ibid., C.2.3). There is also a requirement to treat

8 According to Lawrence Strickling in a letter to Neelie Kroes titled "re: dot-xxx" on April 20, 2011: "While the Obama Administration does not support ICANN's decision, we respect the multistakeholder Internet governance process and do not think that it is in the long-term best interest of the United States or the global Internet community for us unilaterally to reverse the decision" (Kruger 2014).

each of the IANA functions with equal priority, and process all requests promptly and efficiently (C.2.4).

More generally, there are requirements to develop and implement performance standards (C.2.8), to process root zone file changes as expeditiously as possible (C.2.9.2.a) and to create a process for IANA functions customers to submit complaints for the timely resolution of disputes (C.2.9.2.g). The contract also creates security requirements (C.3), establishes a need for performance measures and metrics, creates a requirement to avoid conflicts of interest (C.6) and produces a robust set of requirements regarding continuity of operations (C.7).

THE AFFIRMATION OF COMMITMENTS

In the event of the US government relinquishing its IANA contract, any inferred enforcement mechanism for ICANN compliance with the Affirmation of Commitments will cease. The Affirmation is a contract that creates both rights and obligations for ICANN. The unilateral decision of the US government to remove itself from one of the central positions in Internet governance has also created an uncertain basis for the Affirmation. This is problematic because it contains some of the core tenets of contemporary Internet governance. This document includes a commitment to ensure that decisions made that are related to the global technical coordination of the DNS are made in the public interest and are accountable and transparent. The Affirmation also requires ICANN to: preserve the security, stability and resiliency of the DNS; promote competition, consumer trust and consumer choice in the DNS marketplace; and facilitate international participation in DNS technical coordination (ICANN 2009b).

These are incredibly powerful commitments, which echo some of the key tenets of Internet governance. The Affirmation also requires ICANN to "ensure that its decisions are in the public interest, and not just the interests of a particular set of stakeholders" (ibid., paragraph 4). In order to achieve this, ICANN is required to perform and publish analyses of the "positive and negative effects of its decisions on the public, including any financial impact on the public, and the positive or negative impact (if any) on the systemic security, stability and resiliency of the DNS" (ibid.). Pursuant to the Affirmation, ICANN also commits to:

- adhere to transparent and accountable budgeting processes;
- fact-based policy development and cross-community deliberations;
- responsive consultation procedures that provide detailed explanations of the basis for decisions, including how comments have influenced the development of policy considerations;
- publish each year an annual report that sets out ICANN's progress against ICANN's bylaws, responsibilities, and strategic and operating plans;
- provide a thorough and reasoned explanation of decisions taken, the rationale thereof, and the sources of data and information on which ICANN relied; and
- operate as a multi-stakeholder, private sector-led organization with input from the public, for whose benefit ICANN shall in all events act. (ibid.)

In reviewing the commitments undertaken in the Affirmation, it is clear that they are more than basic contractual functions. Rather, they are parts of the core fabric of the current model of governance, as seen with the examples of the commitment to operate as a multi-stakeholder institution with input from the public and the requirement to act in the public's interest. With the absence of a contractual obligation to the US government for these foundational principles, the transition plan should seek to incorporate external mechanisms for preserving them. One credible way of doing this is to migrate the contractual obligations now found in the IANA services contract and the Affirmation into contracts with the IANA functions customers. Another is to bolster the existing legal responsibility of the ICANN board to operate according to its mission and core values (which include many of the Affirmation of Commitments details).[9] Such bolstering could come

9 ICANN's existing legal framework establishes some administrative law requirements: first, under the California Corporations Code provisions for not-for-profit, public benefit corporations; and second, under common law. ICANN's directors are required under the California Code to implement the purposes outlined in its Articles of Incorporation: "of lessening the burdens of government and promoting the global public interest in the operational stability of the Internet by (i) coordinating the assignment of Internet technical parameters as needed to maintain universal connectivity on the Internet; (ii) performing and overseeing functions related to the coordination of the Internet Protocol ("IP") address space; (iii) performing and overseeing functions related to the coordination of the Internet domain name system ("DNS"), including the development of policies for determining the circumstances under which new top-level domains are added to the DNS root system; (iv) overseeing operation of the authoritative Internet DNS root server system; and (v) engaging in any other related lawful activity in furtherance of items (i) through (iv)….The Corporation shall operate for the benefit of the Internet community as a whole, carrying out its activities in conformity with relevant principles of international law and applicable international conventions and local law and, to the extent appropriate and consistent with these Articles and its Bylaws, through open and transparent processes that enable competition and open entry in Internet-related markets. To this effect, the Corporation shall cooperate as appropriate with relevant international organizations" (ICANN 1998).

The board members are accountable to these purposes, and the California Code empowers the Attorney General of California to intervene in the organization if they are breached. Further, a director of a non-profit public benefit corporation owes, under common law, a duty of care to the entity. It is required that the director take reasonable measures to ensure that the organization is managed and directed in a manner that is consistent with its mission. For details of how this imposes public interest duties on the directors, see www.icann.org/en/system/files/files/acct-trans-frameworks-principles-10jan08-en.pdf.

through the augmented adoption of a proposal put forward by ICANN's Improving Institutional Confidence process in 2008-2009: the establishment of a new Independent Review Tribunal with powers to review the exercise of decision-making powers of the ICANN board under four general rubrics — fairness, fidelity to the power, cogency of decision making and addressing the public interest (ICANN 2009a).

MIGRATING THE CORE CONTRACTUAL REQUIREMENTS

Given the foundational nature of the core commitments found within both the Affirmation and the IANA functions contract, any regime adopted to facilitate the transition should seek to enshrine them in the future governance structure. These requirements should be enumerated in a way that renders ICANN externally accountable for performance standards and exposed to sanction for abuses or for behaving in a manner that runs contrary to these commitments. In order to achieve this going forward, the core commitments found within both the Affirmation and the IANA functions contract could be migrated through the law of contract into individualized service agreements with IANA services customers. As a procedural matter, it would also be permissible to migrate these foundational principles into a collective services agreement between ICANN and all IANA services customers, leaving the individualized contracts to address matters unique to ICANN and the individual customer in question.

On the most important tenets, it may even be advisable to draft a clause favouring specific performance as a remedy. Specific performance is a remedy that allows a court to require a party to perform a particular act, as an alternative to monetary damages. This would create a hard external accountability check, with a meaningful remedy provision, held directly by those organizations most affected by a particular decision, action or inaction.

INTERNAL ACCOUNTABILITY: FURTHER SUPPORTING ICANN'S EXISTING STRUCTURE

ICANN is organized as a non-profit public benefit corporation under the California Nonprofit Public Benefit Corporations law. Under this framework, ICANN (1998, paragraph 4) is designed to operate "for the benefit of the Internet community as a whole" according to its Articles of Incorporation. Articles of Incorporation are considered to be the constitutional documents of any corporate structure and it is impermissible for either management of the corporation or the directors to behave in a manner that runs counter to the articles or the purposes articulated in that document. In this respect, at least some of the foundational governance principles found in the Affirmation are already part of the ICANN corporate structure. There are, however, several limited internal governance revisions, which could further increase accountability, while not adding an additional onerous administrative burden.

The existing governance structure of ICANN includes a number of mechanisms to ensure accountability within its operations.[10] However, this chapter only examines the process for reconsideration and internal review of decisions of the ICANN board of directors, and the external and independent review of board decisions.

ACCOUNTABILITY AND REVIEW

Pursuant to the bylaws, there is a mechanism under which a party aggrieved by a decision of ICANN staff or the board may request reconsideration or review of that decision. To that end, the bylaws provide that any person may submit a request for reconsideration or review, if they have been adversely affected by:

> "a. one or more staff actions or inactions that contradict established ICANN policy(ies); or
>
> b. one or more actions or inactions of the ICANN Board that have been taken or refused to be taken without consideration of material information, except where the party submitting the request could have submitted, but did not submit, the information for the Board's consideration at the time of action or refusal to act; or
>
> c. one or more actions or inactions of the ICANN Board that are taken as a result of the Board's reliance on false or inaccurate material information." (ICANN 2014a, Article IV, section 2, paragraph 2)

The Board Governance Committee reviews and considers these reconsideration requests. For all reconsideration requests involving staff, the Board Governance Committee has delegated authority to make a final determination. In practice, the Board Governance Committee makes a recommendation to the board, including a resolution, which the board typically adopts. With respect to board decisions, the bylaws provide that the "Board shall not be bound to follow the recommendations of the Board Governance Committee….The Board's decision on the recommendation is final" (ibid., paragraph 17). This is a reflection of Californian and US federal law, which stress that boards cannot delegate away their final accountability. In this way, reconsideration is permissible if information

10 There are a number of mechanisms that would fit under the broad heading of accountability that will not be considered here. These include, but are not limited to, bylaw requirements for transparency, information disclosure and financial accountability, including external audits.

was lacking at the time the impugned decision was made, or the decision runs contrary to established policy.

This provision could be strengthened by adding an additional substantive ground of reconsideration — allowing a reconsideration request to go forward if an aggrieved party alleges that a decision was undertaken in a manner that runs contrary to the public interest. Adding a public interest ground for reconsideration requests would add an additional level of assurance that decisions are being undertaken in a manner that adequately considers the implications of those decisions on the interests of the broader public. This will inevitably require weighing various interests, which may at times be conflicting. Nevertheless, if an aggrieved party can allege a prima facie breach of the public interest (recognizing that a working definition of "public interest" will need to be articulated), then a substantive ground of reconsideration on this basis would strengthen the existing governance structure.

INDEPENDENT REVIEW OF BOARD ACTIONS

There is also a separate process for independent third-party review of board actions that are alleged to be inconsistent with the Articles of Incorporation or bylaws. In these cases, an Independent Review Process Panel (IRP Panel) will be established. Pursuant to the bylaws, the IRP Panel must apply a defined standard of review, focusing on the following:

> "a. did the Board act without conflict of interest in taking its decision?;
>
> b. did the Board exercise due diligence and care in having a reasonable amount of facts in front of them?; and
>
> c. did the Board members exercise independent judgment in taking the decision, believed to be in the best interests of the company?" (ibid., section 3, paragraph 4)

As a starting point, in order to strengthen the existing governance structure, the standard of review should be broadened. The current narrowly defined standard will allow review only in the event of a decision made based on a conflict of interest, a lack of diligence or lack of independence. In order to assuage some of the community's concerns regarding accountability, just like with the reconsideration of decisions noted above, the standard could be broadened to specifically incorporate independent review on the grounds that a decision was taken in a manner that runs contrary to the public interest. This is already being done in a somewhat roundabout way. The board is obliged to undertake decisions that they believe to be in the best interest of the company, which are in turn based on a corporate fiduciary duty,[11] and those decisions must be in accordance with the Articles of Incorporation. The Articles of ICANN specifically articulate a need for operations that benefit the Internet community as a whole. Thus, there is already a mechanism through which at least a portion of the public interest would be considered, though the Internet community is a narrower subset of the public — which would include individuals who have yet to use the Internet. However, specifically incorporating a ground of review based on overall public interest would also serve to reinforce the existing review structure and buttress existing accountability mechanisms. The existing grounds of review could be further expanded along the lines articulated in the Improving Institutional Confidence to include review on the grounds of fairness, fidelity and rationality. Grounds of fairness would allow review surrounding the integrity of the decision-making process. A fidelity review would ensure that decisions were untaken in a manner that was faithful to the "scope and objects of the power being exercised."[12] A rationality review would independently confirm or deny that decisions were made in a cogent way, taking account of relevant evidence and within the scope of authority. This would also be an important step in implementing the NETmundial outcome document, which specifically recognizes that "the Internet is a global resource which *should be managed in the public interest"* (NETmundial 2014, emphasis added). Setting out a ground of review that recognizes this could garner a good amount of community support.

On the procedural side, when an independent review proceeding is brought, it is administered by an international dispute resolution provider, which is appointed by ICANN. In 2006, ICANN appointed the International Centre for Dispute Resolution (ICDR), the international division of the American Arbitration

11 Directors are subject to certain fiduciary duties in carrying out their governance responsibilities. One such obligation is often referred to as the "duty of loyalty," which places two separate legal requirements on directors. The first is that the director act in good faith when conducting the business of the corporation. The second is that the director continually act in the best interests of the corporation, placing the interests of the corporation above the interests of all others — including their own — when making decisions. See *ICM Registry, LLC, Claimant, v. Internet Corporation for Assigned Names and Numbers ("ICANN"),* Respondent, Declaration of the Independent Review Panel, February 19, 2010, Concurring and Dissenting Opinion of Judge Dickran Tevrizian, at 74 ("Directors of non-profit corporations in California owe a fiduciary duty to the corporation they serve and to its members, if any. See *Raven's Cove Townhomes, Inc. v. Knuppe Dev. Co.,* (1981) 114 CA3d 783, 799; *Burt v. Irvine Co.,* (1965) 237 CA2nd 828, 852. See also, *Harvey v. Landing Homeowners Assn.,* (2008) 162 CA4th 809, 821-822."). See also ICANN's (2014a) Article VI, Board of Directors, Section 7, Duties of Directors: "Directors shall serve as individuals who have the duty to act in what they reasonably believe are the best interests of ICANN and not as representatives of the entity that selected them, their employers, or any other organizations or constituencies."

12 See https://archive.icann.org/en/jpa/iic/iic-the-way-forward-31may09-en.pdf.

Association, as the provider. The provider coordinates the membership of the standing panel, subject to ICANN approval. The ICDR's rules give each party the right to propose an arbitrator, with the third panellist selected by the ICDR. The procedural rules for the settlement of disputes are also subject to the approval of the ICANN board. These arbitrations are also non-binding,[13] although the board has stated its intent to implement decisions of these sorts of arbitrations.

The most problematic element is a lack of independence between ICANN and the individuals appointed to hear a dispute involving a decision taken by the board of that organization. Section 3, paragraph 7 of ICANN's bylaws states that all IRP Panel proceedings be administered by an international dispute resolution provider appointed by ICANN (the IRP Panel provider). The membership of the standing panel shall be coordinated by the provider, subject to approval by ICANN (ICANN 2014). The difficulty created by this potential lack of independence is that the members of the arbitral panel could be beholden to ICANN for their position on the panel. Realistically, it is unlikely that an individual arbitrator would side with ICANN in a dispute based on the fact that ICANN approved their appointment to the standing roster of arbitrators. Nevertheless, this process of confirming appointments does raise the reasonable *apprehension* of a lack of independence. In order to remedy this perceived lack of independence, a standing committee comprised of various stakeholder groups could be struck to oversee the provider's populating of the list of eligible arbitrators.

More substantially, the IRP Panel process could be replaced by the Independent Review Tribunal recommended by ICANN's Improving Institutional Confidence process. That process proposed that "the International Dispute Resolution Provider name a standing panel of internationally recognized relevant technical experts as well as internationally recognized jurists, including persons with senior appellate judge experience. The existence of a known and recognized 'bench' of 'judges' will add to the stature and authority of the Independent Review Panel. The panel's members should be appointed for either a set period of five years or until they resign, whichever is the earlier" (ICANN 2009a). This chapter proposes that the members of ICANN's various stakeholder groups and the broader public be able to make comments on the proposed bench before final appointment.

CONCLUSION

There are two major constraints on the implementation of any proposed mechanism that can meet the enumerated criteria set for any transition proposal. The first is time. The IANA functions contract expires in September 2015. The announcement that the US government was prepared to relinquish its contractual authority was made in March 2014. Based on this, the ICG has established a process timeline for the generation of the transition proposal.

Under this process timeline, the first stage involves affected communities developing their proposal text and submitting that material to the ICG. The current deadline for the submission of these materials is January 15, 2015, leaving approximately nine months before the contract expiry (or option commencement)[14] period. This would leave approximately nine months to review the various proposals put forward by the community, synthesize a draft response, receive and respond to feedback on the draft proposal, ensure that the proposed system will actually work, and then allow adequate time for the NTIA to review and respond to the proposed structure.

The second constraint is scope. In addition to the necessary conditions imposed on the transition proposal, any proposed structure must also carry domestic political support within the United States. The former Speaker of the US House of Representatives Tip O'Neill once said, "All politics is local." The case of the IANA functions transition is no different. Creating a system where the various accountability mechanisms previously held by the US government are held by the customers of the IANA services could be the type of private sector response that may carry domestic political support. Moreover, this form of modest and measured approach may also be practicable within the incredibly tight timelines associated with the transition.

Engaging in the moderate redesign set out in this chapter does not preclude the grand institutional bargain and redesign that some favour at a future point. Many states and groups within civil society are seeking a broad reimagining of the way that the Internet is governed, with some even calling existing structures illegitimate. Whether these concerns are warranted or not, the fact is that undertaking a measured approach now to the IANA transition would not necessarily prevent or impede a larger negotiation about institutional design and legitimacy. However, this could be done in a staged manner, addressing issues of immediate concern — such as the September 2015 deadline — with the larger and more contentious issues left for resolution without being imbued with a false sense of urgency.

Considering these constraints, this chapter recommends the following steps to help improve the accountability of the performance of the IANA functions by ICANN:

13 See *ICM Registry, LLC, Claimant, v. Internet Corporation for Assigned Names and Numbers ("ICANN")*, Respondent, Declaration of the Independent Review Panel, February 19, 2010.

14 Pursuant to the IANA functions contract, the base period of performance of this contract is from October 1, 2012 through September 30, 2015. However, there are two option periods, which — if exercised — would extend the period of performance to September 30, 2019.

- That the relevant provisions that rendered ICANN accountable to the US government for the performance of the IANA functions and the necessary service standards be migrated from the contracts with the Department of Commerce to the contracts between ICANN and its IANA services customers. In this regard, ICANN would be accountable to its customers through the law of contract for the functions and services performed on their behalf. It would be advisable to include a clause favouring specific performance as a remedy.
- That a new Independent Review Tribunal be established in accordance with a proposal of ICANN's Improving Institutional Confidence process.
- That the tribunal be comprised of a standing panel of relevant technical experts and jurists, including those with senior appellate judge experience, appointed for either a set period of five years or until they resign, whichever is the earlier. We propose that the members of ICANN's various stakeholder groups and the public be able to make comments on the proposed bench before final appointment.
- That if ICANN also continues with its existing independent review process, a standing committee comprised of various stakeholder groups could be struck to oversee the provider's populating of the list of eligible arbitrators. This should counter the reasonable apprehension of a lack of independence in the present model for selection of arbitrators.

The proposed solution is not a panacea. Rather, it is put forward as a principled solution that could work within the existing constraints. However, there are a number of issues that will require detailed consideration in the event that a proposal along the lines articulated is considered for implementation. One concern is the issue of the re-delegation. In the event that accountability measures vest through the law of contract in the IANA functions customers, careful consideration will need to be given to the prospect of re-delegation by those customers. It will be important to ensure clarity and transparency around the cases of re-delegation, and to allow parties who are affected by this exercise of "superior power" to have recourse to administrative review through the proposed Independent Review Tribunal.

The transition creates an important opportunity for the multi-stakeholder approach to Internet governance. A private solution ordered through contract law could create an important independent accountability check in the absence of the historical role played by the US government. At the same time, further refinements to the Independent Review Tribunal, including more robust grounds of review in line with administrative law, could refine and enhance with existing governance regime.

WORKS CITED

Grant, Ruth W. and Robert O. Keohane. 2005. "Accountability and Abuses of Power in World Politics." *American Political Science Review* 99 (1).

IANA. 2014. "IANA Functions and Related Root Zone Management Transition Questions and Answers." March 18. www.ntia.doc.gov/other-publication/2014/iana-functions-and-related-root-zone-management-transition-questions-and-answ.

ICANN. 1998. *Articles of Incorporation of Internet Corporation for Assigned Names and Numbers.* ICANN, November 21. www.icann.org/en/about/governance/articles.

———. 2009a. "Improving Institutional Confidence: The Way Forward: ICANN, May 31. http://archive.icann.org/en/jpa/iic/iic-the-way-forward-31may09-en.pdf?

———. 2009b. "Affirmation of Commitments by the United States Department of Commerce and the Internet Corporation for Assigned Names and Numbers." ICANN. www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-en.

———. 2014a. "Bylaws for Internet Corporation for Assigned Names and Numbers | A California Nonprofit Public-Benefit Corporation." ICANN, July 30. www.icann.org/resources/pages/bylaws-2012-02-25-en.

———. 2014b. *Overview and History of the IANA Functions. A Report from the ICANN Security and Stability Advisory Committee (SSAC).* August 15. www.icann.org/en/system/files/files/sac-067-en.pdf.

Kruger, Lennard G. 2014. *Internet Governance and the Domain Name System: Issues for Congress.* Congressional Research Service. June 10. http://fas.org/sgp/crs/misc/R42351.pdf.

NETmundial. 2014. "NETmundial Multistakeholder Statement." April 24. http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

NTIA. 2000. "IANA Services Contract. Awarded by the US Department of Commerce." www.ntia.doc.gov/files/ntia/publications/ianacontract.pdf.

———. 2012. "IANA Services Contract. Awarded by the US Department of Commerce." www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf.

———. 2014. "NTIA Announces Intent to Transition Key Internet Domain Name Functions." News release, March 14. NTIA: US Department of Commerce. www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

Postel, J. 1994. "Domain Name System Structure and Delegation." Network Working Group, Request for Comments: 1591. March. http://tools.ietf.org/pdf/rfc1591.pdf.

Vegoda, Leo. 2013. *IANA Functions Customer Service Survey Results.* December. www.iana.org/reports/2013/customer-survey-20131210.pdf.

ABOUT THE AUTHORS

Aaron Shull is chief operating officer and general counsel at CIGI, based in Waterloo, Ontario, Canada.

Paul Twomey is the founder of Argo Pacific, a high-level international consulting firm specializing in the Internet and digital economy sectors, and former president and CEO of the Internet Corporation for Assigned Names and Numbers.

Christopher S. Yoo is a senior fellow at CIGI and the John H. Chestnut Professor of Law, Communication, and Computer & Information Science, University of Pennsylvania.

CHAPTER FIVE:
ICANN: BRIDGING THE TRUST GAP

Emily Taylor

ACRONYMS

ATRT	Accountability and Transparency Review Team
ATRT2	Accountability and Transparency Review Team (second review)
DNS	domain name system
GAC	Governmental Advisory Committee
GNSO PDP	Generic Names Supporting Organization Policy Development Process
gTLD	generic top-level domain
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers

INTRODUCTION

A limited set of unique identifiers is the lightweight glue that holds together a single, global Internet. Management of these strategic resources was spun out by the US government to a private sector body, the Internet Corporation for Assigned Names and Numbers (ICANN), in the late 1990s. The US government's vestigial oversight of ICANN has long caused controversy in Internet governance discussions. In 2014, the United States announced intent to relinquish that oversight, provided a suitable multi-stakeholder mechanism could be found to replace it. The ICANN community has risen to the challenge with energy and commitment, and has already identified principles for transition and a proposed mechanism. Meanwhile, ICANN has been persuaded to make the Internet Assigned Numbers Authority (IANA) transition dependent on improvements to ICANN's general accountability. ICANN's leadership initially resisted that dependency, and it took unprecedented joint representations by community leaders to persuade it. At the same time, this revealed an interesting trust deficit between the ICANN community on the one hand and ICANN, the corporation, on the other.

After setting out the history of ICANN's formation and more recent developments following the US announcement, this chapter explores issues surrounding ICANN's accountability in order to assist the task of strengthening trust between the two communities.

ICANN has many strengths, including very high levels of transparency in policy-making processes. Systematic, regular review mechanisms, which contribute to creating a learning organization, even if implementation of review recommendations is uneven. In recent years, progress has been made in strengthening the effectiveness of ICANN's board of directors and beginning to internationalize participation.

Given ICANN's function and structure as a policy-making body, with diverse stakeholders representing differing (sometimes conflicting) interests, a degree of mistrust among the participants is inevitable, even healthy. But there are non-inevitable tensions, arising from ICANN's unusual structure. The lack of membership causes potential conflicts:

- between directors' fiduciary duties to the corporation on the one hand, and the public interest on the other; and
- for elected directors, between their fiduciary duties to the corporation and the expectation by the electing community that the director will represent and fight for their interests rather than for the good of the corporation or the public interest.[1]

The lack of membership also creates a cul-de-sac of authority, where the board is left to review its own decisions, and has no external mechanism to recall individual directors. With low levels of trust and high expectations of transparency, there is a risk of perverse consequences and destructive patterns of behaviour between staff and community. Meanwhile, the public interest is further undermined by not having a ready way for governments and end-users to provide timely input as an integral part of ICANN's formal policy-making processes — the Generic Names Supporting Organization Policy Development Process (GNSO PDP). Strengthening the effectiveness of financial oversight is essential as revenues increase and, with them, a pressure for scope creep.

The chapter concludes that the ICANN community is likely to reach a satisfactory outcome. However, this will not be easy or quick. Recommendations are offered in order to assist the community's deliberations, it is suggested that ICANN bridge the trust gap with the community by institutionalizing mistrust through implementing multiple checks and balances. The introduction of a membership would provide a mechanism to approve changes to ICANN's constitution, and to recall individual directors. Financial oversight should be strengthened.

BACKGROUND: IANA, THE STORY SO FAR

To understand the situation ICANN currently finds itself in, it is necessary to review its history. Over the past 17 years, ICANN has grown in size and financial strength;

1 ICANN's Bylaws, Article VI, Section 7 are clear this is not the case, but it remains a potential conflict. See www.icann.org/resources/pages/governance/bylaws-en#VI.

as a corollary, the global community has become ever more reliant on the smooth functioning of a single Internet.

When ICANN was founded in 1998, there were approximately 100 million global Internet users (Gromov 2014). By 2014, there were nearly three billion (International Telecommunication Union 2014).[2] Then, there was a handful of generic top-level domains (gTLDs); now there are more than 400, with another 500 due to launch in 2015.

THE GOVERNANCE IMPLICATIONS OF UNIQUE RESOURCES AND HIERARCHICAL ARCHITECTURE

The Internet is a distributed system, but its smooth functioning requires naming and numbering to be unique and universally resolvable. The need for uniqueness means that these resources are curated by single organizations, operating within a strict hierarchy (DeNardis 2014). Rationally, that hierarchy must have a top-most node, from which all the downstream authority flows. In the case of critical Internet resources, that top-most node is the IANA.

The strategic importance of the IANA persists, despite rampant change in the wider Internet technologies. Despite the growth of search, apps and a handful of popular Web services in the years since ICANN was founded, the domain name system (DNS) continues to play an integral role in holding together a single Internet: in Web browsing, email, certificates and/or user identifiers for online accounts. The pervasive nature of the DNS is illustrated in the struggle to create universal acceptance of internationalized domain names over the past 15 years (EURid 2014).

ICANN AND THE IANA

ICANN was founded in 1998 by the US government. It is a private, not-for-profit corporation with no members, incorporated under the laws of California. Funded by the domain name industry,[3] ICANN's role includes coordination of critical Internet resources, the DNS and Internet Protocol addressing and the protocol parameters registry. Apart from its policy-making dimension for gTLDs, ICANN is also responsible for managing and updating the domain name root zone — the so-called IANA function.

The management of the IANA is split between ICANN, which coordinates the policy and administrative aspects, and Verisign, which manages the actual database under separate contract with the US government.

ICANN has always had a contractual or quasi-contractual relationship with the US government, but the US government envisioned from the outset that it would relinquish its role as backstop authority once the ICANN model "was established and stable"(US Department of Commerce 1998, paragraph 4).

ICANN's relationship with the US government is based on two instruments:

- **The Affirmation of Commitments**, 2009, between the US Department of Commerce and ICANN (ICANN 2009). At the core of the Affirmation of Commitments is a requirement that ICANN undertake regular reviews into aspects of its operations and governance.[4] The Affirmation of Commitments is the third iteration of the relationship between the United States and ICANN, and the lightest-touch instrument so far. It can be terminated on 120 days' notice by either party.
- **The IANA contract** was most recently awarded in 2012 and expires in September 2015 (renewable for a further four-year period thereafter). The contracting parties are the US Department of Commerce and ICANN, for a consideration of $1. The contract covers the operation of the IANA database.[5]

THE US GOVERNMENT'S AUTHORITY OVER IANA: A CONTROVERSIAL HISTORY

Through the IANA contract, the US government has ultimate authority over the IANA, and hence over the Internet's entire navigation system. This has long been a focus of a power struggle within Internet governance discussions. The issue dominated discussions during the

2 See also http://news.bbc.co.uk/1/hi/technology/8552410.stm for an animated visualization of growth of Internet users from 1998 to 2008.

3 See, for example, the .com Registry Agreement between ICANN and Verisign, Inc. at www.icann.org/resources/pages/agreement-2012-12-05-en. According to Section 7.2, ICANN is entitled to $0.25 on each .com registration and renewal. New gTLDs allow for a similar percentage as well as a fixed registry fee of $25,000 per year (according to the base registry agreement; see http://newgtlds.icann.org/en/applicants/agb/agreement-approved-20nov13-en.pdf). At the same time, ICANN levies $0.18 from registrars for each domain name registration and renewal, see page 86 of the *FY15 ICANN Operating Plan and Budget* at www.icann.org/en/system/files/files/adopted-opplan-budget-fy15-01dec14-en.pdf. All currency in this chapter is in US dollars.

4 These reviews are: accountability and transparency (Section 9.1); security and stability (9.2); competition and consumer choice (9.3); and WHOIS (9.3.1). So far, two accountability and transparency reviews have taken place, and one each on WHOIS and security and stability. Competition and consumer trust review is due to take place "if and when new gTLDs...have been in operation for one year." In late 2014, an independent advisory group published suggested metrics for the Competition, Consumer Trust and Choice Metrics Review Team, but at this time it is not clear whether a review team has been formed.

5 See www.ntia.doc.gov/files/ntia/publications/sf_26_pg_1-2-final_award_and_sacs.pdf for the contract.

2003–2005 World Summit on the Information Society,[6] as reflected in the Tunis Agenda,[7] the World Conference on International Telecommunications in Mexico in 2014[8] and the NETmundial meeting in Brazil in 2014 (NETmundial 2014).

The symbolism of having a single government in control of one of the Internet's few choke points has obscured the fact that the IANA works well. There has been no credible challenge to the United States' assertion that it has never interfered in updates to the root zone.

The US government has exercised restraint in its oversight of the IANA and "has generally established a prudent policy of non-intervention in the DNS operation" (Demidov 2014). It published an overview of its role in authorizing changes to the IANA database (National Telecommunications and Information Administration 2014b), demonstrating that its primary role is administrative.

It may come as a surprise that while US government oversight of the IANA has been identified as problematic by many governments and other stakeholders for more than a decade, there have been few efforts to identify an acceptable replacement.

IANA TRANSITION

In March 2014, shortly before the NETmundial meeting in Brazil, the US government unexpectedly announced "its intent to transition key Internet domain name functions to the global multistakeholder community" as early as September 30, 2015 (National Telecommunications and Information Administration 2014a). The announcement asked ICANN to develop a transition proposal that satisfies four principles:

- support and enhance the multi-stakeholder model;
- maintain the security, stability and resiliency of the Internet DNS;
- meet the needs and expectation of the global customers and partners of the IANA services; and
- maintain the openness of the Internet.

The United States has chosen not to define a successor model. According to Lawrence E. Strickling, assistant secretary of commerce for communications and information, "I think it's a real test to the community of the multistakeholder model and can they organize themselves? Can they now focus on the important issues and get to consensus? I think upon the successful completion of this, and I do expect a successful completion, this process will be much stronger for what the community is going through right now as they try to wrestle with all of the different issues...on what is perhaps the most fundamental question ICANN has had to face since its creation back in 1998" (Strickling 2014b).

The NETmundial meeting in April 2014 showed that multi-stakeholder processes can deliver timely consensus outcomes, and this has raised confidence levels in the likelihood of a successful resolution.

ONE GOVERNMENT, ALL GOVERNMENTS OR MULTI-STAKEHOLDER GOVERNANCE?

Some critics of the US government's role in relation to the IANA have long advocated a transition to an intergovernmental model, in other words replacing a single government with all governments (India-Brazil-South Africa 2011). This has a certain logic, stemming from the inherent legitimacy of sovereign governments to oversee global resources and protect the public interest. But critics point to risks of politicization of an essentially technical function, or characterize calls for UN involvement either as a covert attempt to clamp down on Internet freedom, or a counter-revolutionary attempt by telecommunication companies to turn back the clock of the Internet and retrieve vanishing revenues and influence (Denton 2015).

What's the alternative? Over the past decade, multi-stakeholder governance has emerged as an alternative model for the Internet, associated with delivering innovation, openness and growth (although correlation doesn't necessarily prove causation). The complexity of the Internet, both in structure and issues, has led to the conclusion that "Internet governance should be built on democratic multistakeholder processes, ensuring the meaningful and accountable participation of all stakeholders" (NETmundial 2014). The Organisation for Economic Co-operation and Development and others (see US Congress 2012a; 2012b) have also advocated multi-stakeholder governance for the Internet.

In its ideal form, the multi-stakeholder system limits the power of governments and of corporates — an ever more powerful force within the ICANN environment.

6 During the World Summit on the Information Society process, the US government announced that it did not intend to transition the IANA function: "the United States...will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file….The United States will continue to provide oversight so that ICANN maintains its focus and meets its core technical mission." See www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system.

7 See www.itu.int/wsis/docs2/tunis/off/6rev1.html (paragraphs 35, 58, 63–65, 68–71 ["enhanced cooperation"]).

8 See www.itu.int/en/wcit-12/Documents/final-acts-wcit-12.pdf. While 89 states signed the updated International Telecommunications Regulations, more than 50 did not. It was the inclusion of references to spam, private network operators and network security that prompted some governments to refuse to sign. See also the remarks of US Ambassador Terry Kramer to the Washington, DC chapter of the Internet Society, December 19, 2012, www.youtube.com/watch?v=cN_PwWkv14A.

It also brings in the voice of users through civil society participation. Technical stakeholders ideally keep policy discussions anchored to operational reality. The legitimacy of multi-stakeholder governance stems from openness of process and the expertise of participants.

There are also known weaknesses in multi-stakeholder governance. Legitimacy can be weak, costs of participation are high, developed countries and industry tend to dominate, processes are slow and rambling, and overall participation is low. Having open processes does not guarantee equitable participation, and there are few effective mechanisms to prevent capture by special interest groups.

The US government announcement stated that it "will not accept a transition proposal that replaces the National Telecommunications and Information Administration role with a government-led or an intergovernmental organization solution."[9] The fact that the United States felt the need to include this caveat indicates that a multi-stakeholder solution was not deemed inevitable.

Likewise, a solution that leaves the US government in ultimate control would be unacceptable to many, as would a solution that cuts ICANN loose from any direct accountability (Carnegy 2014). The Centre for Democracy & Technology summarized the concerns: "The prospect of an unaccountable ICANN, or one subject to control by governments or special interests, has enormous implications for the open, innovative, global Internet" (Shears 2014).

SEPTEMBER 2015: DEADLINE OR TARGET?

Despite intense efforts and engagement by many in the ICANN community to define a way forward by the summer of 2015, the difficulty of untangling the issues, and of reconciling the diverse, legitimate interests, make it likely that the process will take longer. Lawrence E. Strickling (2014a) has already prepared the ground, signalling an intent to renew the IANA contract: "We have repeatedly noted that we can extend the contract for up to four years if the Internet community needs more time to develop a proposal that meets the criteria we have outlined. In the meantime, our current role will not change."

At this stage it seems likely that the process will extend beyond September 2015.

THE PROCESS: IANA STEWARDSHIP

Numerous working groups have been formed to focus on the issues. ICANN has tasked a group, called the IANA Stewardship Transition Coordination Group, to deliver a proposal to transition the stewardship of the IANA functions from the US government to the global multi-stakeholder community. The proposal will cover the three aspects of IANA's role: naming, numbering and protocol parameters.

Naming has been identified as the key issue for focus. The numbering and protocol communities have already finalized their reports on IANA transition.

RISK OF FRAGMENTATION OF IANA: DIFFERENT SOLUTIONS FOR NAMING, NUMBERING AND PROTOCOLS?

The focus of attention at ICANN is always on naming — a fact reflected in this chapter — but IANA covers other key resources: Internet Protocol addresses, Autonomous System Numbers and protocols, which are likely to increase in significance in the Internet's next iterations (such as the "Internet of Things"). There are risks to the process to be considered if the naming, numbering and protocol communities decide to pursue different courses. The communities serving numbering and protocols have always had semi-autonomous relationships with ICANN. They do not recognize ICANN as having policy-making authority over their communities, and for this reason contribute comparatively less financially than ICANN's contracted parties. These communities will get involved on an ad hoc basis when they believe their expertise is relevant, but they do not have a formal role within the GNSO PDP. When the call went out for solutions to IANA transition, the numbering and protocol communities quickly concluded their work.

Uneven progress or the prospect of different solutions may pose a risk of fragmentation. There is strength in having combined oversight linked to ICANN in some (yet-to-be-agreed) form. However, the protocols and naming community could easily function without this. Having oversight of all IANA functions under one central unit would be more efficient and would elevate the status of that oversight organization (with each arm still able to set its own policies). Separation would make it easier for individual numbering and protocol agencies to build out independent power bases, and could leave ICANN more vulnerable to external threats. Failure scenarios would also become more complex, in particular if the naming stream is out on its own in terms of oversight.

IANA: NAMING FUNCTIONS

In respect to naming, two cross-community working groups have been formed: IANA stewardship in relation to domain names (the IANA Working Group), and general accountability issues relating to ICANN (the Accountability Working Group).

9 See www.ntia.doc.gov/speechtestimony/2014/remarks-assistant-secretary-strickling-icann-high-level-governmental-meeting.

The IANA Working Group membership has already produced impressive results. ICANN proposed the formation of the IANA Working Group in June 2014, and by August a draft charter was published, which committed to follow an "open, global and transparent process" and "provide the opportunity for participation by all stakeholders and interested or affected parties" (ICANN 2014b). By November 2014, the IANA Working Group reported that agreement on key principles (ICANN 2014c) for the successor process was "nearly complete," including:

- security and stability;
- accountability and transparency of any oversight, including independence, protection against capture, appeals and redress;
- service levels — at present, the draft is exploring potentially different handling for country-code TLDs (such as .se, .de, .uk) and gTLDs (such as .com, and new endings such as .guru, .photography);
- diversity — any transition needs to reflect the diversity of arrangements between IANA and its customers;
- separability of the IANA functions from the current operator, if warranted; and
- multi-stakeholder — any mechanism must draw its membership from "a full range of stakeholders."

WHAT MECHANISMS COULD BE SUITABLE FOR THE IANA STEWARDSHIP?

While it has been straightforward to articulate high-level principles, identifying mechanisms to implement them has proved more challenging.

Mechanisms suggested by the IANA Working Group have been criticized for being overly bureaucratic (Mueller 2015), to the extent of potentially introducing risks into the system: "how will the community protect against processing delays and the potential for politicization of the system?" (Strickling 2015). While the current proposals may be over-engineered, there are clear benefits in consulting IANA customers on operational issues, and in having some form of multi-stakeholder review of the service, as the IANA Working Group is proposing. The latter could perhaps be incorporated as an additional Affirmation of Commitments review.

Of greater concern is the identity of the proposed contracting entity to replace the US government. While ICANN management and a minority of stakeholders support integrating the IANA function into ICANN, the majority favour structural separability — i.e., the ability for the IANA to be taken away from ICANN. Current proposals call for the creation of a shell company, "Contract Co.," which would have no assets and no other function. While this may fulfill the need for there to be a legal entity to enter the contract, it is hard to imagine a shell company having the self-confidence to trigger a rebid or change the IANA function provider. The jurisdiction in which Contract Co. would be formed is described as a "sleeper issue," with contributors from China, Brazil and India calling for it to be established in a "neutral country" (Mueller 2015).

Why is structural separability seen as important? As Steve DelBianco (2014) states, "The current IANA contract serves to hold ICANN accountable to an entity other than itself....Accountability means answering to someone or something that has the power to censure or correct. No such function exists for the ICANN Board today, with the imperfect exception of the IANA contract."

However mundane the reality of US government involvement, the IANA oversight provides a symbolic umbilical cord between ICANN and an external body. Once cut, there would be no external constraints on ICANN, a private, unregulated monopoly with control over global critical Internet resources.

This is the reason why the IANA transition has to take place within a wider conversation about ICANN's accountability.

LINKS TO ICANN'S GENERAL ACCOUNTABILITY

The Affirmation of Commitments requires that a review of ICANN's Accountability and Transparency be conducted every three years. To date, two such reviews have been completed by the Accountability and Transparency Review Team (ATRT). Within the framework of the ATRT reviews, ICANN's accountability issues are reasonably well understood, but by no means resolved.

Nevertheless, issues surrounding ICANN's accountability are complex and difficult to unravel. Progress on implementing the recommendations of the first and second ATRT reviews has been uneven. Key weaknesses and risks persist, such as the effectiveness of ICANN's board, the role of governments and the influence of the domain name industry in policy-making processes. There is also a systemic risk, which the IANA contract has masked to some extent: in law, directors owe fiduciary duties to the company. In a regular company, the interest of the company is interpreted as the interests of its shareholders or members (who also have the power to remove directors by ordinary resolution). ICANN has no membership, so how should we understand ICANN interest, as a company?

There are also classic corporate governance problems between the community and ICANN staff, such as

information asymmetry, information arbitrage and moral hazard. This is not always obvious, since ICANN's policy-making processes observe extremely high levels of transparency, even if the sheer number of simultaneous policy initiatives can sometimes create a fog that only insiders seem able to penetrate.

The same levels of transparency are not always observed in corporate governance issues, such as staffing and internal decision making. In other areas where improvements have been made, such as finance, effective horizontal and vertical checks and balances remain weak. ICANN's general accountability is a complex issue, and one that will take time to improve.

IANA AND ICANN'S ACCOUNTABILITY: INTERDEPENDENT OR INTERRELATED?

In its first response to the US government announcement, ICANN's leadership appeared unwilling to create a dependency between the IANA transition process and ICANN's wider accountability. It was only in the final quarter of 2014 that ICANN began to make unambiguous commitments to a parallel, and dependent, accountability stream. This reflects normative pressure from the ICANN community and the US government: "This important accountability issue will and should be addressed before any transition takes place" (Strickling 2014a).[10] In a recent consultation, 100 percent of the responses agreed with this view (Corwin 2015).

For the management of ICANN, combining IANA transition with general accountability represents a risk: "Their fear, in a nutshell, was that complex debates over the massive reorganizations required to make ICANN's policy making processes and organs fully accountable would set the bar for the transition so high that it might never happen" (Mueller 2014).

Keeping discussions focused on the narrow technical and operational detail of IANA is not only within the comfort zone of many ICANN participants, but is also capable of conclusion prior to September 2015. Throwing the issue open to include wider accountability issues risks bogging the entire process down for years. ICANN's leadership is also wary of the possibility of a UN General Assembly vote (December 2015) that could derail the process. Recent legislation (December 2014)[11] prevents the US government from spending appropriated funds on the IANA transition before September 2015, signalling that IANA transition has become a partisan issue within the US legislature. Another risk is that if discussions drag on beyond the next US presidential elections, the transition might stall. There is historical precedent for this: in 2005, the Bush administration appeared to step back from the Clinton administration's original commitment to release its hold over IANA.[12]

Conscious of these external threats and of the fact that improving accountability is "a never-ending discussion" (Chehadé 2014, 34), ICANN's executive at first resisted the IANA transition being dependent on advances in accountability: "when we talk about accountability, we talk about its interrelation with the transition, not necessarily its interdependency" (ibid.).

Meanwhile, members of ICANN's community viewed the IANA transition as perhaps a final opportunity to extract meaningful concessions on accountability — which have so far proved elusive, despite two reviews of its accountability and transparency — before the organization was cut loose from the US government.

In an unprecedented move, the leadership of all ICANN's supporting organizations and advisory committees — between which there is little love lost, and high levels of mutual suspicion — joined together to lobby the executive to change its mind (ICANN 2014a, 26 ff.; Cooper et al. 2014). Assistant Secretary Larry E. Strickling (2014a) echoed the community's view, "This important accountability issue will and should be addressed before any transition takes place." This combined normative pressure forced a change of course by ICANN's executive, but valuable time had already been lost. A separate accountability track, the Accountability Working Group, on which the IANA transition would be dependent, was formed toward the end of 2014.

ACCOUNTABILITY: IS IT ALL ABOUT TRUST?

The board's reaction to unanimous pushback from the community was to ask, "How can we strengthen the trust between all parts of the ICANN stakeholder community?" (Crocker and Chehadé 2014).

The response highlights a slightly unrealistic view of the forces at play within the broader ICANN structure.

While ICANN has quite stringent accountability mechanisms (see ICANN's Accountability and Transparency: Where Are We Now? below), these seem not to be trusted to work — at least by some vocal members of the community — and there are glaring weaknesses:

10 See also www2.itif.org/2014-key-principles-for-coordination.pdf (section 12).

11 See Omnibus Appropriations legislation, December 2014, section 540(a), www.gpo.gov/fdsys/pkg/CPRT-113HPRT91668/pdf/CPRT-113HPRT91668.pdf.

12 The US Principles on the Internet's Domain Name and Addressing System, June 30, 2005 states, "The United States...will therefore maintain its historic role in authorizing changes or modifications to the authoritative root zone file." See www.ntia.doc.gov/other-publication/2005/us-principles-internets-domain-name-and-addressing-system.

- no mechanisms for recall of individual board directors;
- the board's ability to amend the company's constitution (its bylaws); and
- the track record of board reconsideration requests (see below).

ICANN as a corporation is a largely unregulated, private sector body with control over critical Internet resources on which global economies depend. It has no natural competitors, is cash-rich (in 2014, its current assets were more than $350 million, with a further $145 million in deferred income), and directly or indirectly supports many of its participants and other Internet governance processes.

Without effective accountability and transparency mechanisms, the opportunities for distortion, even corruption, are manifold.

In such an environment, it is not sufficient simply to invoke trust.

According to P. Sztompka (1998),[13] a democratic culture of trust can be created through the institutionalization of distrust within the architecture of democracy. Accountability is highlighted as a key mechanism in achieving this. Rather than invoking trust, it may be more realistic to expect levels of mutual tension and mistrust between the executive and different parts of the community. Each has a role in holding others to account and ensuring balanced outcomes.

ICANN'S ACCOUNTABILITY AND TRANSPARENCY: WHERE ARE WE NOW?

STRENGTHS

High Levels of Transparency in Policy Process

ICANN's policy processes serve as a model for transparency and have influenced external organizations, such as the Internet Governance Forum. Every working group call and face-to-face meeting is transcribed and archived (along with mailing lists and policy documents). Even operational budgets are put out for public comment. Each stage in a policy-making process is sent out for public comment, and the quality of inputs is often extraordinarily high.

In recent years, ICANN has worked hard to internationalize its processes. Transcriptions are now provided in the six UN languages, and ICANN has a road map to improve the quality and quantity of materials available.[14]

It has also developed effective tools to assist remote participation, both in coordinating volunteers' calls and providing virtual meeting rooms, and in live streaming of meetings. While the experience of participating remotely can be frustrating (particularly for those in developing countries with poor bandwidth), ICANN has continued to improve its support for remote participants, for example by providing dial-out services to those struggling with connection.

The published archive comprises an important historical record and provides a way for new participants to read into the issues. The scale of activity can make it daunting for newcomers, and ICANN tries to address this by providing special resources and sessions at ICANN meetings for the orientation of new participants.

Systematic, Regular Review

To promote a culture of accountability and transparency, the Affirmation of Commitments provides for four types of review to take place at three-year intervals. Reviews are conducted by volunteers, who are selected by the CEO of ICANN and chair of its Governmental Advisory Committee (GAC). The fact and quality of the reviews are impressive. An area for improvement is ICANN's tracking and reporting of its implementation of review recommendations, but this is an area that continues to evolve as the cycle of regular review becomes established. For example, ICANN recently published a fairly clear digest of progress on implementation of the second ATRT review's (ATRT2's) recommendations.[15] The Affirmation of Commitments reviews have some impact as normative controls, but there are no sanctions for the board if they ignore or fail to implement their recommendations.

ICANN Board: Steady Improvement

In its evaluation of progress since the first review, the ATRT2 noted widespread improvements in board selection, performance and work practices, including declarations of interest since 2009. It also noted that community feedback indicated satisfaction with the term length for directors.

A Learning Community

ICANN as a corporation and community is committed to continuing improvement. The ATRT2 tracks progress on implementation of the ATRT review's recommendations since 2009, providing a valuable feedback loop.

13 Thanks to Jeanette Hofmann for bringing this work to the author's attention.

14 See www.icann.org/translations.

15 See www.icann.org/news/announcement-2-2015-01-30-en.

While tensions are apparent in key policy-making constituencies (such as the GNSO), other pockets of the ICANN community retain a culture of collegiality and information exchange, even as participation has internationalized and the financial stakes have increased. Examples include the security community and country-code operators. Cross community working groups are now becoming more frequently used, and this counteracts the tendency toward stakeholder silos within policy making.

Participation Is Increasing and Gradually Internationalizing

While participation in ICANN's core policy-making engine, the GNSO, continues to be dominated by North American and industry participants (ICANN 2013, A2), other communities within ICANN are internationalizing. The GAC now has 146 members and 31 observers,[16] compared with 94 members in 2009.[17] ICANN's At-Large Advisory Committee has also expanded its membership and ambitions since 2009. It now has approximately 150 At-Large Structure members, and holds regular summits.[18] The Country Code Names Supporting Organisation has also increased its membership to 152,[19] compared to about 100 in 2009.[20] These developments are helping to internationalize parts of the ICANN community.

RISK AREAS

Inevitable Tensions

All Stakeholders Are Equal, but Some Stakes Are More Equal than Others

ICANN's "community" is heterogeneous. The size and nature of stakes varies between stakeholder groups. Domain industry players are highly motivated and generally well resourced to participate in policy discussions, as the outcomes have direct operational and financial impact on their business. Conversely, for the world's three billion Internet users, while reliant on critical Internet resources, the costs of participation in ICANN processes outweigh the perceived benefits (if any), and therefore the drivers to participate are weaker. The costs of participation in ICANN's lengthy processes outweigh any perceived benefits.

End-users and governments, while recognized in the ICANN framework and increasingly active in giving policy input, do not form part of the official, bottom-up policy-making process — the GNSO PDP.

Barriers to Participation

As with any technical arena, there is a relatively high knowledge threshold for getting involved. ICANN is rich in jargon and acronyms. Policy processes are lengthy, requiring a high level of time commitment. ICANN's executive identifies "volunteer fatigue" (ICANN 2013, A19, A46) as a factor affecting participation in policy development. Some of this is inevitable in an area that intersects technology and international public policy, but it does raise questions about whether a volunteer model can scale and survive as ICANN continues to expand and internationalize.

Balancing the Conflicting Interests of Stakeholders

Any policy process needs to find ways of balancing the conflicting, legitimate interests of different stakeholder groups. In the ICANN context, while the bottom-up process unquestionably delivers multiple viewpoints to the table, it is less clear that the policy outcomes achieve the required balance. To some extent, this is a feature of any policy process. The difference is that a bottom-up process requires the board (despite having ultimate authority on behalf of the corporation) to assume a passive role in policy making. If the community delivers an outcome that threatens the public interest, the board cannot be relied upon to step in and undo the community's work. Occasionally the board has sent back policy recommendations as not being in the public interest,[21] or has intervened to set deadlines for GNSO PDP working groups. Such decisions are rare, and have generated pushback from the community against perceived overreaching by the board.

Instead, disgruntled stakeholders take their concerns to the GAC, the GNSO Council or ICANN staff (ibid., A54). This is viewed by some participants as undermining the bottom-up process; others are more sanguine, seeing it as part of the rough and tumble of policy making. For example, GAC intervention late in the gTLD program may have delayed the launch (to the detriment of potential applicants and of ICANN), but did strengthen some public interest aspects and arguably signalled a new phase of more proactive involvement in policy making by governments within the ICANN process.

16 See https://gacweb.icann.org/display/gacweb/About+The+GAC.

17 See page 7 of the House of Commons European Scrutiny Committee's *Thirteenth Report of Session 2009–10* at www.publications.parliament.uk/pa/cm200910/cmselect/cmeuleg/5-xii/5xii.pdf.

18 See https://community.icann.org/display/als2/ATLAS+II+Declaration.

19 For more details on Country Code Names Supporting Organisation membership, see http://ccnso.icann.org/about/members.htm.

20 See the Survey of Attitudes within the Country Code Names Supporting Organisation Committee regarding strategic priorities for ICANN, www.ccnso.icann.org/surveys/strategic-priorities-for-icann-oct09-en.pdf.

21 For example, ICANN Resolution 2014.0.16.16 states that the board specifically carves out the possibility of rejecting the recommendations of the Accountability Working Group if the board believes they are not in the global public interest. See www.icann.org/resources/board-material/resolutions-2014-10-16-en#2.d.

But the ad hoc workarounds highlight a problem with the bottom-up process: what happens if a policy is crazy or bad? Who looks after the public interest?

Non-inevitable Tensions

During ICANN's first decade, it was frequently referred to as "the ICANN experiment," because it is unusual to find a global public good operated through a California non-profit corporation. While ICANN generally functions well, its corporate structure can cause tensions.

Directors' Fiduciary Duties versus the Public Interest

According to ICANN's bylaws, the corporation's mission is described in technical terms: coordinating the DNS, Internet Protocol addresses, Autonomous System Numbers, and protocol port and parameter numbers; operating the DNS root server (IANA function); and coordinating "policy development reasonably and appropriately related to these technical functions."[22] The public interest is hardly mentioned (except in number six of ICANN's core values in relation to promotion of competition[23]).

Meanwhile, in law, directors owe fiduciary duties to the corporation, which normally means the members or shareholders. But ICANN has no members or shareholders. So, how can the corporation's interest be understood? In practice, it can be interpreted as avoiding decisions that may lead to the corporation being sued. An example is the handling of new gTLD applications, which many viewed as overly liberal. While the public interest may have motivated such a position, on the basis that it would introduce competition into the namespace, at least one commentator interpreted it as motivated by fear of litigation: "Specifically, in dealing with the issue of plural and singular strings, ICANN took a very liberal position that they are not confusingly similar and appear to have pushed this decision to the objection panels so as to not have to be accountable for terminating some future strings" (Gomes 2013). The "very liberal" position seems to have applied across the board to new gTLD applications, with the overwhelming majority having passed initial evaluation.[24]

Review of Board Decisions and Recall of Directors

With no membership, ICANN's directors represent the end of the line in terms of accountability. While there is a formal mechanism to review board decisions, the review is conducted by a subset of the same people. The ATRT2 noted that community perception that Reconsideration Requests "all end[ing] up in a negative decision" was borne out by analysis of the results: 100 percent were rejected (ICANN 2013, 53 ff.)! The ATRT2 recommended that the board convene a special community group to discuss options for improving the process.

One of the key powers of a company's membership is the ability to remove directors. With no membership, there is no obvious way to recall individual directors mid-term. This does not imply a "nuclear option" of removing the entire board at once, which is obviously undesirable. It means targeted intervention (removal of an individual) without creating instability.

A company's membership also serves accountability objectives by receiving financial accounts and appointing auditors. While in most companies these are treated as formalities, they can provide a focal point for shareholder activism.[25]

A company's membership is also the usual authority to change its bylaws (by super-majority or special resolution). ICANN's board has the power to change bylaws without recourse to a higher authority — and this has caused concerns in discussions over accountability.

Introducing a membership into ICANN's corporate structure would not be a straightforward task. How would balance be ensured, to prevent capture by special interests? While directly interested parties — such as registries and registrars — could be relied upon to join up in numbers, incentives to become involved are low for others, such as Internet users. The rambunctious nature of some community interactions may be viewed as risking the stability or legitimacy of ICANN as an entity if translated into direct corporate power. On this view, ICANN's board represents a more stable, predictable and responsible body than the ICANN community. Such concerns appear incompatible with support for multi-stakeholder governance; in essence, they translate to suspicion of "mob rule," and a view of ICANN's leadership as master rather than servant of the wider community.

Some entities, including some governments, may not feel able to join a California corporation as a member. Such entities have found ways to participate in the ICANN community through proxies, such as stakeholder groups or advisory committees. Consultation with relevant stakeholders will be essential to understand and remove barriers to participation.

No doubt, creating a membership would require changes to ICANN's existing bylaws, and could bring associated

22 See Section 1, www.icann.org/resources/pages/governance/bylaws-en#I.

23 Ibid.

24 See https://gtldresult.icann.org/applicationstatus/viewstatus. 1,783 out of 1,930 applications passed initial evaluation (92 percent), and a further 35 applications passed at the extended evaluation phase.

25 For example, Cedric the pig was brought to British Gas' Annual General Meeting in a shareholder protest against executive pay. See www.ft.com/cms/s/0/63ad9d3e-3b92-11df-a4c0-00144feabdc0.html#axzz3Qt9Vwq3e.

risks. Such risks are not unique to ICANN, but are shared with other non-profits and charities around the world, whose governance experiences can be learned from. One possibility may be to map the current structure of the ICANN community into a membership. A one-member, one-vote system may prevent concentrations of voting power.

But without a membership, accountability can only be achieved through normative pressures. No structure will deliver perfection; to misquote Winston Churchill, a membership is the worst form of governance except for all those other forms that have been tried.

Building Trust: The Panopticon Paradox

Literature on governance urges complete transparency as an unquestioned benefit. Jeremy Bentham's utilitarian discussion of the "panopticon" (1785) predicts that when people believe they may be watched at every moment, they will act compliantly and become, as Michel Foucault put it, "docile bodies." Transparency can help to deliver accountability in situations where there is natural information asymmetry, as between staffers and the communities they serve. Community members (and directors) do not spend all their time working in the organization and cannot know everything that goes on there. The panopticon gives the potential for anything to be made public at any moment.

But Bentham's pantopticon was a design for a prison. Prisoners think prisoners' thoughts and quickly begin to act in distorted ways (see Haney, Banks and Zimbardo 1973) — either through submissiveness, slavish adherence to rules, or even distress and anxiety. Interactions between prisoners and guards quickly become "negative, hostile, affrontive and dehumanizing," leading to a breakdown in solidarity between prisoners.

Although criticized for its ethical failings, Zimbardo's prisoner experiment has eerie similarities with anecdotal evidence from ICANN staff and former staff.[26] It is easy to feel besieged by the "community" members whose own behaviour can become distorted through a sense of power and entitlement.

Within the atmosphere of mutual distrust identified by the board, these behaviours can only intensify. Sztompka (1998) predicts that a pervasive, generalized climate of suspicion tends to mobilize defensive attitudes, hostile stereotypes, rumours and prejudices. For example, both the ATRT and the WHOIS Policy Review Team (both constituted under the Affirmation of Commitments) commented on the difficulties they encountered in getting basic operational and financial information from staff on aspects that were central to their work (ICANN 2013, Appendix E).[27]

ICANN's generous pay and reward schemes, coupled with difficulties in finding comparable employed positions elsewhere in the small domain name policy space, can become drivers against transparency. Analysis of ICANN's audited accounts and filed IRS 990 forms show that from 2011 to 2013, the average salary per person at ICANN was above $170,000. Excluding highest-paid executives (as declared on the form), average pay still exceeded $138,000,[28] and across the staff base, salaries increased by between 11 and 16 percent in fiscal years 2012 and 2013, against US inflation rates of three percent or lower. Employee benefits are exceptionally generous, including full health care, and a pension contribution of up to 15 percent of salary (and five percent paid even if the employee does not make contributions).[29] There are powerful financial and social drivers for staff to stay in position, and not to place their employment at risk by raising concerns. The ATRT2 noted that previous recommendations (in 2006 and 2007) to introduce a whistle-blowers' policy had not yet been implemented.

Another perverse consequence of expectations of hyper-transparency is a tendency to overuse legal or other confidential channels, or to overuse redaction in official communications. An example is the board's response to the WHOIS Policy Review Team's recommendations,[30] which one commentator described as "a model of non-communication, and it comes replete with Orwellian gaps in the texts, redactions which force you to ask where the words have gone and why?" (Carr 2012).

The message here is not that transparency is bad. Quite clearly, there is a requirement for transparency in ICANN's operations. But in situations where there is keen community attention focused on staff, coupled with low levels of trust, there may be perverse consequences that create accountability risks.

26 See Maria Farrell's blog (under previous ICANN leadership), http://crookedtimber.org/2011/03/19/the-hollowing-out-of-icann-must-be-stopped/. "People are afraid to speak frankly internally, and to speak unpalatable truths behind closed doors, the sorts of things that need to be discussed to allow the organization to function efficiently."

27 See also the addendum and page 44 of the *WHOIS Policy Review Team: Final Report*, www.icann.org/en/system/files/files/final-report-11may12-en.pdf.

28 See www.icann.org/resources/pages/governance/historical-en for ICANN's IRS 990 forms for the fiscal years 2011–2013. Note that with the expansion of ICANN's staff base in 2014, the average salary per person appears to have dropped to below $100,000 (fiscal year 2014 form 990 has not yet been filed).

29 See ICANN Benefits Overview for 2014 at https://icanncareers.silkroad.com/map_images/main/SiteGen/icannext/Content/Uploads/Unplaced_Documents/2014_ICANN_Benefits_Overview_Newsletter_AN_2-1.pdf a.

30 See the ICANN board response to the WHOIS Review Team recommendations, November 2012, www.icann.org/en/system/files/bm/briefing-materials-1-08nov12-en.pdf accessed 6 February 2015.

A More Inclusive Policy Process

Key stakeholder groups (users and governments) are not part of the core policy-making framework, ICANN's GNSO. The ATRT2 identified major issues affecting the GAC's ability to effectively interact with board and community, which have an "impact on the accountability, transparency, and perceived global legitimacy of ICANN" (ICANN 2013, 39, recommendations 6.1–6.9). The report also identified a lack of clarity or understanding of GAC working methods, GAC advice being poorly understood outside of government circles and GAC participation in policy development processes described as "limited to non-existent" (ibid.).

This causes problems of legitimacy and can disrupt the policy-making flow, causing ill feeling and eroding trust. N. Vallejo and P. Hauselmann (2004) observe that legitimacy suffers due to lack of stakeholder diversity, even if that diversity increases the time frames and costs of policy making. At ICANN, with the exception of the At-Large Advisory Council, there is almost no participation by advisory committees or other supporting organizations in providing comments within the formal GNSO PDP (ICANN 2013, A39, paragraph 5.1.4.3).

These key stakeholders — governments and end-users — perceive that they don't choose the policy issues or the timing, and try to respond as best they can; they have limited tools available for timely participation. However, without integration into the GNSO process, their inputs tend to be ad hoc and late. This creates tensions and inefficiencies, with stakeholders on the inside of the policy-making procedures perceiving such interventions as circumventing or undermining the bottom-up processes.

Financials: ICANN — Not Your Average Not-for-profit

The Internet governance space is replete with rather well-funded not-for-profit organizations, including ICANN. ICANN's financial strength, coupled with its unique control over global critical Internet resources and limited scrutiny of its finances, represents an accountability risk.

Even before the new gTLD program, ICANN had enviable financial reserves (current assets of $46 million in 2007 increasing to $399 million in 2013).[31] The following analysis excludes income and expenditure relating to the new gTLD program, which ICANN has accounted for separately. However, such a large influx of cash appears to have relaxed leadership attitudes toward general expenditure, as evidenced in the travel budget, for example.

ICANN's Income

Turnover (excluding exceptional items, such as the new gTLD program) increased from $51 million in 2008 to $78 million in 2013. This is generous provision for a staff base of 150–200.

ICANN's main source of income is a percentage of domain name registration and renewal fees, paid by registries[32] and registrars.[33] Because of the dynamics of the domain name market, 55 percent of ICANN's turnover is provided by two companies.[34] In any business, such financial dependence on so few customers would create risks. In a public interest company, there is even more cause for concern, particularly as ICANN also has a contractual compliance function over those companies. There are at least theoretical conflicts in the dual roles of supplier and regulator.

Expenditure Analysis

ICANN's main cost centres are staff (41 percent of turnover in 2013), travel (12 percent), meetings (5 percent) and IT (6 percent, an increase from 1 percent in 2010).[35] Lobbying represents less than one percent of turnover, but has grown from nothing prior to 2009. "Other" expenses in 2013 (excluding new gTLDs) totalled $12 million, including translation and interpretation services ($1.6 million) and consulting services of $7.4 million.

There was a sharp increase in travel and meetings expenses in 2014 (22 percent of turnover, an increase of 55 percent versus the previous year). While the total figure has reduced in the forecast for 2015, the number of public meetings has also reduced by 25 percent. The travel spending per public meeting has risen from $1.8 million in 2011 to $3.6 million in 2014.

Travel costs are partly driven by staff and board members, but ICANN also supports many members of the community. In part, this is a quid pro quo for the thousands of volunteer hours contributed to policy work by the community.

31 See www.icann.org/resources/pages/governance/historical-en for ICANN's IRS 990 forms for the fiscal years 2007–2013. Note that the majority of current liabilities comprise deferred income, which (while correctly handled in the accounts) depresses the current ratio.

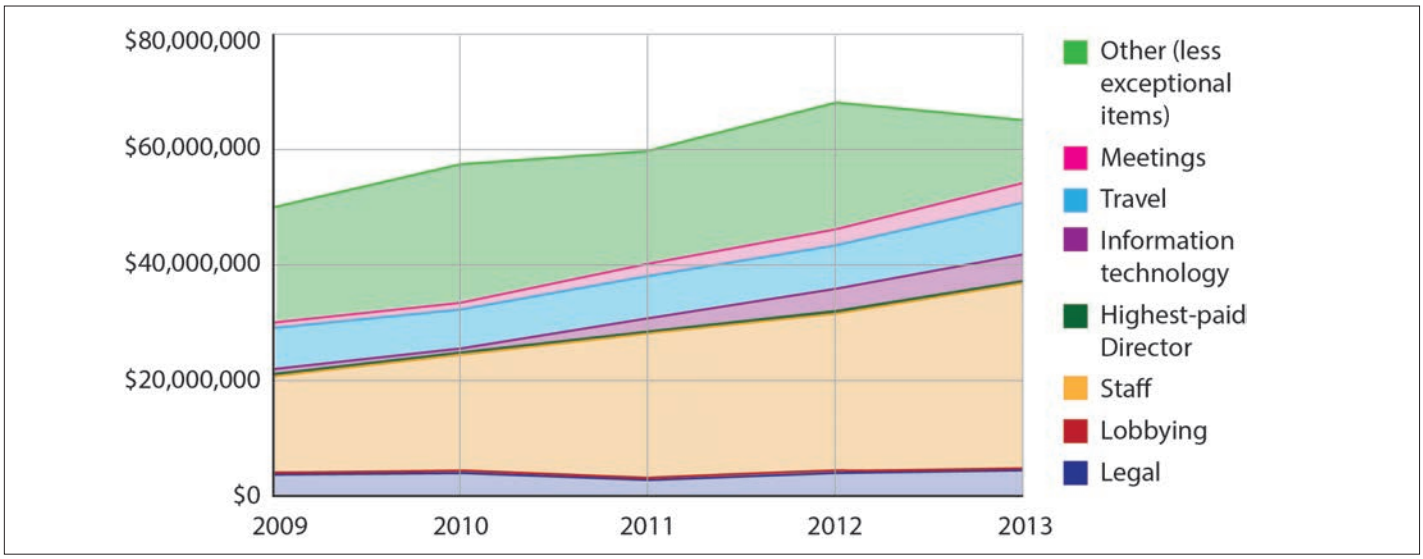
32 See footnote 3, specifically section 7.2 of the .com Registry Agreement.

33 See page 86 of the *FY15 ICANN Operating Plan and Budget* at www.icann.org/en/system/files/files/adopted-opplan-budget-fy15-01dec14-en.pdf: "Transaction based fees....This fee will be billed at $0.18 per transaction for registrars operating under the 2009 or 2013 RAA."

34 See page 22, Concentration of Credit Risk, at www.icann.org/en/system/files/files/financial-report-fye-30jun14-en.pdf.

35 Analysis excludes exceptional gTLD income and expenditure. See ICANN's IRS 990 forms for 2009–2013 at www.icann.org/resources/pages/governance/historical-en.

Figure 1: ICANN Expenses over Time



Data source: ICANN IRS 990 forms, 2009–2013. www.icann.org/resources/pages/governance/historical-en.

ICANN used to publish reports of travel support per meeting,[36] but the practice seems to have dropped off in recent years. The 2015 operating plan also details additional budget requests of $680,000, mostly comprising requests by community members for travel support, including attendance at other Internet governance meetings such as the Internet Governance Forum.[37]

This is an area where strict accountability should be observed. By way of comparison, analysis of Google's political expenditure by Public Citizen's Congress Watch concludes that through "soft power" (Nye 2004) organizations can accrue "influence in ways that are much less visible and less regulated than through conventional lobbying" (Public Citizen 2014). Not only is ICANN directly funding attendance at its own public meetings, it is also a key financial contributor to other processes such as the UN Internet Governance Forum ($330,000 in fiscal year 2015),[38] the 2014 NETmundial meeting in Brazil (figures not available at time of writing) and the new NETmundial Initiative (a reported $200,000 pledged in 2014),[39] all of which advocate the multi-stakeholder model of Internet governance.

Impact of the New gTLD Program

Opening the new gTLD application window in 2012 changed ICANN's fortunes, yielding nearly $200 million in application fees in 2012–2014. Processing the applications themselves cost ICANN more than $70 million (a net profit of more than $130 million, excluding auction fees). So far, 400 new gTLDs have been launched, totalling four million individual domain name registrations, an average of 10,000 domains per new gTLD registry.[40]

Although ICANN has observed strict separation of new gTLD income and expenditure in its accounts, the new gTLD windfall seems to have loosened ICANN's financial control. Where in earlier years, ICANN would typically have a net profit margin of approximately 14 percent (2009–2011), in 2012, this dropped to 0.8 percent, and the organization even made a small trading loss in 2014.

What Financial Accountability Measures Exist?

ICANN has professionally prepared and audited accounts, and submits required non-profit tax forms. It also consults the community on its operating budget, and staff provide a high level of detail in these consultations.

Unlike for-profit companies, where the shareholders' principal motivation is financial, members or communities of non-profits can be rather sleepy about the finances. With ICANN, the level of community input and expertise on

36 See the Summary Report on Travel Support for ICANN's 47th International Public Meeting, in Durban, South Africa, 2013, www.icann.org/en/system/files/files/funded-travel-durban-22aug13-en.pdf, which indicates total expenditure of over $800,000 on 173 community attendees, including 30 ICANN fellows, 22 GAC, 20 GNSO and 20 Nominating Committee.

37 See page 75 ff. of the *FY15 ICANN Operating Plan and Budget* at www.icann.org/en/system/files/files/proposed-opplan-budget-comments-fy15-16jun14-en.pdf.

38 See www.icann.org/resources/press-material/release-2014-12-18-en.

39 See www.theregister.co.uk/2014/12/12/im_begging_you_to_join_netmundial_initiative_gets_desperate/.

40 See ntldstats.com for data on gTLDs. In reality, registration statistics are distorted by the near giveaway policy of .xyz (780,000 domains). Otherwise, the new gTLD market is showing a typical "long tail" pattern.

financial matters is not extensive. There were only four public comments on the 2015 fiscal year operating plan,[41] although some were high quality[42] on the fiscal year 2015 operating plan. Still, the high level required for financial reporting does not allow for close scrutiny appropriate to ICANN's public trust role and large financial reserves. ICANN has not yet evolved the network of semi- or fully independent financial checks and balances (such as public accounts committees, public auditors) seen in the public sector.

CONCLUSIONS AND RECOMMENDATIONS

ICANN's community has responded positively to the challenge of transitioning oversight of the IANA functions to a suitable multi-stakeholder model, but the process will not be straightforward. The US government has signalled a willingness to renew the IANA contract in September 2015 if the deliberations are not complete. This will probably be necessary to give the ICANN community sufficient time to improve ICANN's general accountability, and to identify mechanisms that provide assurance without compromising operational and technical efficiency. Other risks specific to IANA transition include unbundling oversight of the current IANA functions, and the jurisdiction and identity of any proposed Contract Co.

Although valuable time was lost in the initial failure to recognize that IANA transition is dependent on strengthening ICANN's overall accountability, the process is now underway. As part of this, ICANN's leadership has identified the need to strengthen mutual trust between the executive and community.

ICANN observes high standards of transparency in policy making, and its practices have influenced other fora such as the Internet Governance Forum. It is a learning organization, which is gradually becoming more internationalized, and has established review mechanisms into key areas including its accountability and transparency (although implementation of recommendations is uneven).

Some accountability risks faced by ICANN are inevitable in any organization with a global policy-making function: imbalanced stakeholder engagement, barriers to participation and/or conflicting stakeholder interests. Others are particular to ICANN and need to be resolved as a priority:

- potential conflict between directors' fiduciary duties to the company and the public interest;
- lack of effective mechanisms for review of board decisions and recall of individual directors;
- perverse consequences of transparency coupled with low trust levels between staff and community;
- more effective and timely mechanisms for governments and end-users to input into policy development; and
- strengthening financial transparency and oversight.

RECOMMENDATIONS

Implementing the ATRT2 recommendations would satisfy concerns over review of board decisions and integration of key stakeholders into formal policy-making processes (the GNSO PDP).

In addition, ICANN could consider the following five recommendations:

- To avoid the risk of fragmentation, any solution for IANA oversight should apply to all current IANA functions.
- A culture of trust can be built by "institutionalizing mistrust" (Sztompka 1998), i.e., developing numerous horizontal and vertical accountability checks and balances. This can help overcome some of the paradoxes associated with high expectations of transparency and low levels of trust.
- Align ICANN the corporation's interest with the public interest by introducing a membership that reflects the diversity of ICANN's community. This will not be straightforward, and further research is needed to identify suitable models and best practices to avoid concentrations of voting power within any one stakeholder group. In future, ICANN should proactively foster two-way dialogue between corporation and membership.
- As an ultimate sanction, ICANN's membership should have the power to recall individual directors and approve changes to bylaws.
- Strengthen the effectiveness of financial transparency and oversight. Consider implementing external checks and balances found in public sector environments.

ACKNOWLEDGEMENTS

The author thanks those many people who have provided expertise, opinion and generous input to this chapter at the draft stage. Its contents and the opinions given in it are the sole responsibility of the author.

41 See www.icann.org/en/system/files/files/report-op-budget-fy15-29sep14-en.pdf.

42 See, for example, the comments of the Country Code Names Support Organisation, June 2014, http://ccnso.icann.org/workinggroups/sop-comments-op-budget-fy15-19jun14-en.pdf.

WORKS CITED

Carnegy, Hugh. 2014. "France Lashes Out at Internet Naming Body Icann." ft.com, June 22. www.ft.com/intl/cms/s/0/828ad97c-f94a-11e3-bb9d-00144feab7de.html#axzz3UkKpwa2Y.

Carr, John. 2012. "The WHOIS Saga Continues." *Desiderata* (blog), November 30. https://johnc1912.wordpress.com/2012/11/30/the-whois-saga-continues/.

Chehadé, Fadi. 2014. Board with Registries Stakeholder Group. London. https://london50.icann.org/en/schedule/tue-board-rysg/transcript-board-rysg-24jun14-en.pdf.

Cooper, Elisa, Olivier Crépin-LeBlond, Rafik Dammak, William Drake, Keith Drazek, Heather Dryden, Patrik Fälström, Byron Holland, Tony Holmes, Michele Neylon, Jonathan Robinson and Kristina Rosette. 2014. Letter to Fadi Chehadé and Stephen D. Crocker. September 3. www.icann.org/en/system/files/correspondence/cooper-et-al-to-chehade-crocker-03sep14-en.pdf.

Corwin, Philip S. 2015. "Haste Makes Waste: Comments on ICANN CWG IANA Transition Proposal Indicate Serious Process Problems." *CircleID* (blog), January 5. www.circleid.com/posts/20150105_haste_makes_waste_icann_on_cwg_iana_transition_proposal_problems/.

Crocker, Stephen D. and Fadi Chehadé. 2014. Letter to SO/AC/SG and Constituency Leadership. September 18. www.icann.org/en/system/files/correspondence/crocker-chehade-to-soac-et-al-18sep14-en.pdf.

DelBianco, Steve. 2014. "The Path Forward: Accountability through the IANA Transition." *CircleID* (blog), March 23. www.circleid.com/posts/20140323_the_path_forward_accountability_through_the_iana_transition/.

Demidov, Oleg. 2014. "IANA Accountability Transition: A Russian View from Singapore." PIR Center, May 4. http://pircenter.org/en/blog/view/id/163.

DeNardis, L. 2014. *The Global War for Internet Governance.* New Haven, CT: Yale University Press.

Denton, Timothy. 2015. "The True Faith of Internet Governance: Statism Finds Its Champion." *CircleID* (blog), February 3. www.circleid.com/posts/20150203_true_faith_of_internet_governance_statism_finds_its_champion/.

EURid. 2014. *World Report on Internationalised Domain Names.* www.eurid.eu/files/publ/IDNWorldReport2014_Interactive.pdf.

Gomes, Chuck. 2013. Letter to Fadi Chehadé. August 30. www.icann.org/en/system/files/correspondence/gomes-to-chehade-30aug13-en.pdf.

Gromov, G. 2014. "The Roads and Crossroads of Internet History." www.netvalley.com/intvalstat.html.

Haney, C., C. Banks and P. Zimbardo. 1973. "Interpersonal Dynamics in a Simulated Prison." *International Journal of Criminology and Penology* 1: 69–97.

ICANN. 2009. "Affirmation of Commitments." www.icann.org/resources/pages/affirmation-of-commitments-2009-09-30-en.

———. 2013. *Accountability and Transparency Review Team 2: Report and Recommendations.* December 31. www.icann.org/en/system/files/files/final-recommendations-31dec13-en.pdf.

———. 2014a. ICANN Public Forum, London, England, June 26, 16:00–18:00. https://london50.icann.org/en/schedule/thu-public-forum/transcript-public-forum-26jun14-en.pdf.

———. 2014b. "Cross Community Working Group (CWG) Charter." August 14. https://community.icann.org/download/attachments/48347144/CWG-DT%20Draft%20Charter%20-%2014%20August%202014%20Updated.doc?api=v2.

———. 2014c. "IANA Stewardship Transition Cross Community Working Group (CWG) on Naming Related Functions: Chairs' Statement on Frankfurt Face-to-Face Meeting." November 20. www.icann.org/news/announcement-2-2014-11-20-en.

India-Brazil-South Africa. 2011. "IBSA Multistakeholder Meeting on Global Internet Governance (September 1-2, 2011 at Rio de Janeiro, Brazil), Recommendations." www.itforchange.net/sites/default/files/ITfC/rio_recommendations.pdf.

International Telecommunication Union. 2014. "The World in 2014: ICT Facts and Figures." www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf.

Mueller, Milton. 2014. "Clarity Emerging on IANA Transition." Internet Governance Project, June 28. www.internetgovernance.org/2014/06/28/clarity-emerging-on-iana-transition/.

———. 2015. "Happy New Year, Happy New IANA." Internet Governance Project, January 1. www.internetgovernance.org/2015/01/01/happy-new-year-happy-new-iana/.

National Telecommunications and Information Administration. 2014a. "NTIA Announces Intent to Transition Key Internet Domain Name Functions." Press release, March 14. www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

———. 2014b. "NTIA's Role in Root Zone Management." December 16. www.ntia.doc.gov/files/ntia/publications/ntias_role_root_zone_management_12162014.pdf.

NETmundial. 2014. "NETmundial Multistakeholder Statement." April 24. http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Nye, Joseph S., Jr. 2004. *Soft Power: The Means to Success in World Politics.* New York, NY: PublicAffairs.

Public Citizen. 2014. *Mission Creep-y: Google Is Quietly becoming One of the Nation's Most Powerful Political Forces while Expanding Its Information-collection Empire.* Report. November. www.citizen.org/documents/Google-Political-Spending-Mission-Creepy.pdf.

Shears, Matthew. 2014. "Clear and Concrete Principles for ICANN Accountability." *Center for Democracy & Technology* (blog), August 4. https://cdt.org/blog/clear-and-concrete-principles-for-icann-accountability/.

Strickling, Lawrence E. 2014a. "Keynote Address by Lawrence E. Strickling, Assistant Secretary of Commerce for Communications and Information, 'Who Governs the Internet? A Conversation on Securing the Multistakeholder Process.'" American Enterprise Institute, Washington, DC, July 22. www.ntia.doc.gov/speechtestimony/2014/keynote-address-assistant-secretary-strickling-american-enterprise-institute.

———. 2014b. "Finished — 2014 09 05 — Dynamic Coalition on Core Internet Values — Room 10." Transcript, Ninth Annual Meeting of the Internet Governance Forum, Istanbul, Turkey, September 5. www.intgovforum.org/cms/174-igf-2014/transcripts/2021-2014-09-05-dc-on-core-internet-values-room-10.

———. 2015. "Remarks by Lawrence E. Strickling, Assistant Secretary of Commerce for Communications and Information." State of the Net Conference, Washington, DC, January 27. www.ntia.doc.gov/speechtestimony/2015/remarks-assistant-secretary-strickling-state-net-conference-1272015.

Sztompka, P. 1998. "Trust, Distrust and Two Paradoxes of Democracy." *European Journal of Social Theory* 1 (1): 19–32.

US Congress. 2012a. H. CON. RES. 127. 112th Congress, 2d session. September 10. www.govtrack.us/congress/bills/112/hconres127/text.

———. 2012b. S. CON. RES. 50. 112th Congress, 2d session. December 5. www.govtrack.us/congress/bills/112/sconres50/text.

US Department of Commerce. 1998. "Management of Internet Names and Addresses." White paper. www.icann.org/resources/unthemed-pages/white-paper-2012-02-25-en.

Vallejo, N. and P. Hauselman. 2004. "Governance and Multistakeholder Processes." International Institute for Sustainable Development. www.iisd.org/pdf/2004/sci_governance.pdf.

ABOUT THE AUTHOR

Emily Taylor is an Internet governance expert and an associate fellow of Chatham House. She is a member of the Global Commission on Internet Governance Research Advisory Network. Her research publications include the annual EURid UNESCO *World Report on Internationalised Domain Names* (lead author), reports for the UK regulator, Ofcom, on uptake of domain name security protocol, IPv6 and Carrier Grade Network Address Translation, and a review of the Internet Corporation for Assigned Names and Numbers (ICANN's) policy development process. She chaired the independent WHOIS Review Team for ICANN, and served on the Internet Governance Forum's Multi-stakeholder Advisory Group. From 2000–2009, she was at Nominet as director of Legal and Policy, and she is now a director of several IT companies.

CHAPTER SIX:
INNOVATIONS IN GLOBAL GOVERNANCE: TOWARD A DISTRIBUTED INTERNET GOVERNANCE ECOSYSTEM

Stefaan G. Verhulst, Beth S. Noveck, Jillian Raines and Antony Declercq

ACRONYMS

ARPANET	Advanced Research Projects Agency Network
CERN	European Organization for Nuclear Research
GCIG	Global Commission on Internet Governance
GIPO	Global Internet Policy Observatory
IATA	International Air Transport Association
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IP	Internet Protocol
ITU	International Telecommunication Union
JSAG	Joint Slot Advisory Group
MSC	Marine Stewardship Council
NTIA	National Telecommunications and Information Administration
WSIS	World Summit on the Information Society

INTRODUCTION AND CONTEXT

Increased Internet adoption is radically altering people's lives across the world, mostly for the better. Individuals, communities, institutions, cities, countries and regions have increasingly become "networked," with transformative implications for how we live, work, play and learn. Following the initial "Internet of links," which made computers and the information on them searchable, the growing "Internet of data" emerged — marked by big and open data — greatly expanding the variety, velocity and volume of data on the network (Dumbill 2012). The "Internet of people," enabled by social and collaborative software (often labelled Web 2.0) (Kurbalija 2014a) has similarly changed the Internet and the way it is used. We are now entering the era of the "Internet of things," where every device from watches to refrigerators to heart monitors is getting connected, generating enormous quantities of rich and revealing data that promise further innovations and challenges in coming years (Weber and Weber 2010; Chui, Löffler and Roberts 2010; Leung 2014; Cooper 2014; Schulze 2014).

The precise shape of these changes — and how they affect society — is likely to depend to a significant extent on how the Internet is governed domestically and internationally. Historically, Internet governance has been seen as an arcane and even marginal topic, of interest primarily to a few "geeks" and government officials. But in recent years, the topic has been receiving greater attention, particularly following the disclosure of classified US National Security Agency documents by Edward Snowden. That episode highlighted how connected and vulnerable to surveillance we all are; it shed a spotlight on some of the key issues (for example, privacy and security) central to discussions about Internet governance. In addition, Internet governance has begun to assume greater significance in a number of sectors not traditionally seen as Internet-enabled — for instance, health care, education, manufacturing or even government. Overall, there is a new level of awareness that the way in which the Internet is governed at global and domestic levels will have a significant effect on our society, economy and polity.

Despite this awareness, however, global collective action and coordination on Internet-related issues have to date been considered by many as ineffective, too slow and often illegitimate for a global public good such as the Internet, whose value stems from interoperability. Concerns about governance fragmentation undermining the global nature of the medium arise as a result of often divergent and hard to reconcile national approaches to privacy, security, freedom of expression and access. Existing decision-making mechanisms designed for addressing these problems within national borders have not kept pace with advances in society. It is increasingly clear that in order to accelerate and broaden the potential of the Internet, new paradigms of governance are needed that embrace the global, distributed and open nature of the Internet. Such paradigms must integrate and embrace new tools and methods that help to realize twenty-first-century principles such as openness, collaboration (Young et al.) and inclusiveness, along with a respect for human rights and freedom of expression (Lewis 2014). Crucially, all these principles must be applied without damaging or limiting the technical layer of the Internet, which has been so central to the rapid growth and success of the network (Meinel and Sack 2014). In short, a system of governance that is as innovative as the network itself is needed.

Several recent developments suggest that the contours of such new paradigms are emerging — encompassing a shift in Internet governance from an interest-driven, disordered and entitled exercise to one that is more expertise based and coordinated at and across local, national and global communities; this emerging paradigm suggests a distributed, yet collaborative approach, one supporting ad hoc groups of engaged actors and experts working together through open information exchanges across the ecosystem. The recent developments catalyzing

this shift include: the US government's announcement in March 2014 of its intention to transition stewardship of Internet addressing functions to a global multi-stakeholder community (National Telecommunications and Information Administration [NTIA] 2014); the Global Multi-stakeholder Meeting on the Future of Internet Governance held in Brazil; and the principles outlined in the outcome document of that meeting, the NETmundial Multi-stakeholder Statement (NETmundial 2014). In addition, the Panel on Global Internet Cooperation and Governance Mechanisms, chaired by Estonian President Toomas Ilves, produced a report earlier this year on the evolution of Internet governance that focused on new distributed governance approaches, titled "Towards a Collaborative, Decentralized Internet Governance Ecosystem" (Panel on Global Internet Cooperation and Governance Mechanisms 2014), and the Internet Corporation for Assigned Names and Numbers (ICANN) Panel on Multi-Stakeholder Innovation offered a range of detailed proposals for innovating upon current problem-solving practices to make them legitimate, effective and evolving. At the time of writing, a NETmundial Initiative was launched, convening leaders of government, academia, civil society and business, with the intention of developing a pathway to execute on the spirit of NETmundial through "dialogue and concrete cooperation" (World Economic Forum 2014). All of these developments present significant opportunities for the global Internet community to begin to meaningfully address current challenges, in particular the need for coordinated action across the ecosystem in order to produce effective and legitimate approaches to a breadth of interconnected issues caused by the rapid growth of the Internet.

This chapter reflects on these developments and their underlying rationales in order to articulate a needed and emerging framework of Internet governance that is distributed, open and collaborative. It describes this new model and shows how it builds on the existing theory and practice of open governance. Several key functions of the proposed distributed model are outlined, in the process explaining how such a model is based on the underlying technology of the Internet, and how the model is related — similar but distinct — to the existing multi-stakeholder model of Internet governance. Real-world case studies of networks and institutions that embody key characteristics of this distributed governance framework are provided. Finally — because coordinating the formulation of more legitimate, effective and flexible responses to increasingly complex and connected Internet governance issues requires going beyond the merely conceptual — this chapter describes a set of tools that can be used to support such a distributed governance ecosystem. It concludes by presenting and expanding on a few open questions that will inform the adoption of the proposed distributed governance framework.

THE NEED FOR DISTRIBUTED INTERNET GOVERNANCE

The World Wide Web — the Internet as a mass, consumer-based platform with a global audience — is now over two decades old. In that time, the network has evolved significantly. In some ways, including Internet Protocol (IP) adoption rates, active domain names, search functionality and social media usage, it is unrecognizable from the network of the early 1990s, or even the early years of this millennium. For the most part, Internet governance has not kept pace with these changes. Existing governance mechanisms are largely outdated and insufficient to the needs of the current network.

The framework for distributed Internet governance proposed in this chapter (and described in detail below) encompasses the following key functions that could enable adopting diverse, multi-institutional approaches to the governance of different, technical and non-technical, Internet-related issues:

- enhanced coordination and cooperation across institutions and actors;
- increased interoperability in terms of identifying and describing issues and approaches for resolution throughout the ecosystem (i.e., creating a common Internet governance ontology);
- open information sharing and evidence-based decision-making; and
- expertise- or issue-based organization to allow for both localization and scale in problem solving.

Through these functions, a distributed framework seeks to address some shortcomings present in existing governance models — from the completely centralized approach[1] to the more prevalent multi-stakeholder[2] and devolved

1 For critiques of a purely centralized governance approach, see Johnson, Crawford and Palfrey (2004) and Ivanova and Roy (2007) who discuss, in part, the ineffectiveness of centralization in global environmental policy as a result of the fact that environmental problems stem from a variety of causes, rather than from a single, central cause.

2 Multi-stakeholderism has surfaced as the most workable and prevalent approach for governing the Internet, especially in terms of its technical aspects, as it anticipates the need for global participation to ensure sound functioning of one, unified network. In support of the multi-stakeholder model, see Costerton (2014), Cooper (2012), Higgins (2012), and Hintz and Milan (2009). How multi-stakeholderism works in practice, however, often centres around interests rather than expertise and, as a result, has been critiqued at times for being slow, "messy," ineffective or illegitimate as a result of under- or insufficient representation of relevant global actors. See DeNardis and Raymond (2013), Dickinson (2014), and Hintz and Milan (2014).

national governance[3] approaches used in Internet governance today. This framework also goes beyond a model of pure decentralization, which key work in the field has made clear does not always work (Cheema and Rondinelli 2007). It promotes the development of decision-making mechanisms that are more flexible, decentralized, accommodating and innovative, and further supports the creation of new collaborative arrangements for actors and institutions to coordinate collective action. Broadly, a distributed framework embodying these functions would address two key shortcomings in the existing approaches: the need for great innovation, and the need for more cooperation and coordination.

THE NEED FOR GREAT INNOVATION IN HOW WE GOVERN THE NET

Internet governance, like the Internet itself, has humble beginnings. When the Advanced Research Projects Agency Network (ARPANET) emerged in 1969, consisting of a few connected computers located in the basements of university and military buildings, there appeared to be little need for governance or any process of decision making (Think Team 2001). The subsequent creation of TCP (Transmission Control Protocol)/IP protocols by US academics and the development of World Wide Web protocols at CERN (the European Organization for Nuclear Research) in Geneva, laid the foundations for a global expansion of the Internet during the mid-1990s (Kurbalija 2014a). Internet governance also evolved during this period of rapid network expansion; in general, it did so in a bottom-up, participatory manner, shepherded by the private sector and civil society, and in cooperation with national governments. Essential Internet governance mechanisms grew from this approach, such as the Internet Engineering Task Force (IETF), formed in 1986 to coordinate the setting of standards for the Net; the Internet Society, created in 1992 to promote the open development, evolution and use of the Internet; and ICANN, incorporated in 1998 to coordinate the development of policies related to the Internet's addressing systems, particularly the Domain Name System (ibid.).

In addition to these civil society-driven, participatory approaches to governing some of the Internet's technical functions, national governments "layered on" domestic regulations that impact how businesses and people can use the Net (that is, to address more non-technical, "informational" or "behavioural" issues). For example, Iranian authorities restricted access to online content in advance of the parliamentary elections in March 2012, when the Iranian Office of the General Prosecutor threatened to block any website that would "boycott, protest, or question the validity of" the election (Freedom House 2012). In the United States, the Supreme Court's recent Aereo copyright law ruling restricted how businesses can stream live broadcast content to consumers (Brandom 2014). In China, the Standing Committee of the National People's Congress issued rules in 2012 requiring individuals who use pseudonyms online to provide their real names to Internet service providers. This would make it easier to identify and hold users accountable for content they produce online, with potentially chilling effects to online expression (Bradsher 2012).

By the late 1990s, however, it had become clear that Internet governance needed a more coordinated and more global approach. In 2003, the World Summit on the Information Society (WSIS) took place in Geneva, followed by another round two years later in Tunis. WSIS, inspired by the model pioneered by the G8 Digital Opportunity Taskforce or DOT Force, laid the foundations for multi-stakeholdership as the preferred way forward in global Internet governance (International Telecommunication Union [ITU] 2005). WSIS also helped identify several important challenges facing Internet governance, and made it clear that existing mechanisms had not kept pace with the underlying technology. It brought into sharp relief the necessity of a system that was better equipped to respond to the needs of a global, distributed network.

All these applications and technological advances have shaped the Internet into something like a global commons, or a "global public resource" (ICANN Strategy Panel on Multistakeholder Innovation 2014; Kroes 2014) that benefits and potentially empowers the entire planet.[4] For instance, in the education sector, students throughout the world have greater access than ever before to learning resources to expand their knowledge (CyberEthics 2011). Increasingly, and to an extent never seen before, the Internet has enabled people to "seek, receive and impart information and ideas...regardless of frontiers," as envisaged by the Universal Declaration of Human Rights.

Even as the Internet's unprecedented growth and globalization (ITU 2014) have increased the complexity and dynamic nature of the associated governance-related

3 The devolved governance model is typically applied to informational or behavioural Internet issues, as it allows for countries to govern speech and information exchange according to its own values systems. See Trebilcock and Howse (1998), arguing that regulatory diversity can "minimize the threat points that each country brings to these negotiations so as to reduce the risk of coerced forms of harmonization reflecting asymmetric bargaining power, or worse, coerced forms of discriminatory managed trade arrangements." Governance diversity as a model, however, does pose challenges when its application results in "legal competition[, which] could have unintended consequences, ranging from increased collisions of laws and inter-state tensions to cyberspace fragmentation" (Internet & Jurisdiction Project 2014c).

4 Notably, this process of globalization is only likely to intensify over the coming years and decades, with a growing majority of the next billion connected users coming from the developing world. See Evan (2014).

issues,[5] our methods for addressing those issues remain largely confined to national borders. As a result, issues relating to the flow of information across the network, such as messaging abuse (spam), though global in nature, are governed in a fragmented manner, where isolated national approaches do little to remedy the spam mail received by an Internet user connected to a global communications platform.

To be fair, the participating patchwork of institutional players in Internet governance has experimented with a variety of different forms of decision making. For example, the IETF adopted a "rough consensus" model to make decisions around setting standards, a model that was supposed to be more flexible and adaptable (Van Beijnum 2011; Hoffman 2012). The European Union has applied a layered approach in attempts to resolve informational or behavioural issues in Internet governance, working to balance input from public and private, individual and institutional, and national and international entities (Walker and Akdeniz 1998); ICANN has experimented with "direct governance" by "netizens" to make decisions regarding the Internet's unique identifier systems (GovLab 2013); and in the early 2000s, as mentioned previously, DOT Force paved the way both for multi-sector and multi-stakeholder governance models with experiments in cross-sector engagement (United Nations ICT Task Force 2004) that were adopted by WSIS and the Internet Governance Forum (IGF).

However well-intentioned they may have been, these initial experiments have not mitigated the serious and complex governance challenges of today, especially around issues such as privacy, access and spam. The more general crisis of legitimacy with regard to governance around the world only exacerbates this (Pew Research 2013; Sannon 2013). Add to this a growing fear of fragmentation on the Internet — a result of the divergent approaches among various nation-states to find ways for dealing with issues such as surveillance, censorship, data security and privacy — and the current crisis of governance becomes apparent (Internet & Jurisdiction Project 2014a; 2014b; Kaspersky 2013).

THE NEED FOR COOPERATION AND COORDINATION

In addition to being challenged by new technologies and patterns of innovation, Internet governance must also address the increasingly cross-border and cross-sector nature of the network — factors that make securing legitimacy in decision making (something traditionally derived from citizenship within a given territory) a more problematic endeavour. Across fields and sectors, globalization is leading to new tensions and frictions within the existing patchwork of often irreconcilable social and legal norms (Castro and Atkinson 2014).

There is consensus that issues that affect the technical operation of the Internet require global coordination to ensure the Internet functions as one coherent system (*the* Internet). Emerging and complex issues like spam, privacy or security, however, are increasingly analyzed and addressed in a fragmented way (discussed above), posing a risk to the sustained operation of the Internet if not better coordinated. When it comes to issues touching on informational or behavioural aspects, although not a consensus view, there has been an operating presumption that each nation regulates speech and information exchange (for example, copyright, pornography and so on) according to its own laws or the laws of the multinational associations, such as the European Union, of which it is a part. This has worked well to incentivize production of locally relevant content and the development of local digital economies (Wooding 2014), as well as in those instances where certain types of content are allowed, promoted or outlawed based on national or cultural circumstances and values. But this governance diversity also presents challenges when not well coordinated: take, for example, the laws passed by the United States in 2006 to block foreign Internet gambling websites, which significantly affected the economies of countries hosting online gambling websites such as Antigua and Barbuda, setting in motion a dispute resolution process at the World Trade Organization (USC 5361-5366 2006). This chapter does not aim to espouse one set of rules of the road in terms of approaches to Internet governance. Rather, governance diversity should be respected for its ability to allow each country to make decisions according to the value systems of its citizens. Yet, in instances where governance diversity threatens to undermine national sovereignty or contributes to the possibility of Internet fragmentation, a need for greater coordination across the ecosystem exists.

Furthermore, ecosystem practices like forum shopping, in which institutional actors choose to engage solely with governance bodies seen as sympathetic to their agenda, demonstrate how enhanced cooperation in the ecosystem could prove meaningful. Relatedly, jurisdictional competition, in which companies or other entities seek to shelter themselves under the policies or laws of a particular nation, also poses problems. Both of these issues further contribute to crises of legitimacy or inclusiveness (Hadge 2010), where individual institutions are seen as inappropriately addressing (or "hijacking") issues that do not fall within their competencies or jurisdictions, or where bilateral arrangements between nations exclude other nations or actors. Such crises are perhaps most apparent in the sense of exclusion felt by users and stakeholders from developing countries (Esterhuysen 2014). Take, for instance, the Internet Ungovernance Forum, first organized

5 The Internet increasingly affects all areas of society, from education to health care to politics to development to the environment. See Internet Live Statistics (2014).

by Turkish activists in September 2014, which was held in parallel to the 2014 IGF. The Internet Ungovernance Forum brought stakeholders away from the "main IGF" to protest unfair representation and to raise awareness of groups left out of Internet governance proceedings (Arora 2014).

For all these reasons, more coordination, cooperation, collaboration and harmonization in the Internet governance ecosystem prove necessary. Such coordination is important at the technical layer and beyond in order to enable an increasingly diverse group of institutions and actors to determine together, from a diversity of approaches, which is appropriate to adopt for handling Internet issues spanning borders and cultures. This requires (and in turn can build) greater trust and transparency among actors. It also requires a greater effort at inclusiveness, and more rigorous use of evidence, data and case studies to help stakeholders and governments from all countries determine where to turn to address issues within the intricate — and largely fragmented — matrix of Internet governance.

DISTRIBUTED INTERNET GOVERNANCE: A FRAMEWORK PROPOSAL

This section discusses how to operationalize greater innovation, collaboration and coordination via a distributed framework, which is described in terms of its key functions. It considers how the proposed distributed model builds on the theory and practice of open governance and then lays out the framework's key functions and shows how they are inspired by the Internet's architecture. It also identifies how the model builds on, but is distinct from, multi-stakeholderism. Finally, this section provides case studies of real-world networks embodying key distributed features from which we can learn.

WHAT IS OPEN GOVERNANCE AND HOW DOES IT INFORM DISTRIBUTED INTERNET GOVERNANCE?

The emerging distributed Internet governance framework draws inspiration from the theory and practice of the open governance movement. Although the meaning of open governance is debated and constantly evolving (Longo 2013), the World Bank Institute explains the movement as one that "ensures citizens have access to government (information, data, processes) in order to engage governments more effectively and that governments have the willingness and ability to respond to citizens and to work collaboratively to solve difficult governance issues" (World Bank 2012). An open governance framework supports more transparent, participatory and collaborative decision making (Obama 2009) with the intention of enabling legitimate, effective and dynamic governance structures and processes. Three main features characterize open governance in general, and form the foundations of the distributed Internet governance framework proposed in this chapter.

Transparency and Innovative Problem-solving

The open governance movement has promoted the creation and sharing of data, often held by government agencies, through downloadable, machine-readable and reusable formats. Open data allows for diverse participation in governance — it provides a vital resource that any interested party can use for the development of new applications and research (Longo 2013). In fields as varied as medicine and citizen engagement, open data has shown great potential for problem solving using collaborative intelligence and increased transparency. For example, the Multiple Myeloma Research Foundation has made available open genomic data on a digital platform called the MMRF Research Gateway to engage scientists and scientist networks throughout the world to accelerate research (Multiple Myeloma Research Foundation 2013). Through the tool, scientists can share information and work collaboratively, using the most robust data available to develop therapies and cures (ibid.). Platforms for crowdsourced data collection have also generated new insights. The India-based citizen-reporting platform I Paid a Bribe, for instance, allows individuals to publicly log instances when they were shaken down for bribes in an effort to find new approaches to combatting government corruption. The platform enables the filing of official reports to the media and top government officials, raising awareness and providing data as an initial step toward changing the system.[6]

In Internet governance, ensuring that the public has access to open and available data about decision-making processes and governance practices, issues and responses is necessary to enable inclusive participation in a distributed framework. The framework should promote the development of such data in open and reuseable formats, as well as ensure a way to inject new and open data into decision-making processes, thus providing "two-way" transparency (Matt 2011). Increased availability of open data could allow Internet governance stakeholders to track and contribute to the progress of issues and responses over time, and would provide the data needed for actors to learn from others' successes and failures and to hold each other responsible for actions taken. Transparency and accountability through open data could,

6 See www.ipaidabribe.com/#gsc.tab=0. Other examples in crowdsourcing and open data include: for education, Unigo, a crowdsourced review of colleges that provides data regarding the true cost of colleges from current students (see www.unigo.com/colleges/); for energy, Earth Networks uses data from networks throughout the world to monitor weather, lightning and greenhouse gases — it then publishes this data for use by enterprises and governments for fast weather alerts (see www.earthnetworks.com).

therefore, help to decentralize accountability and increase information sharing and collaboration in a distributed Internet governance ecosystem.

Participation

One of the key features — and benefits — of open governance is that it promotes citizen engagement in all aspects of governance. This has helped to devolve and diversify the types of expertise and knowledge involved in decision making. In a variety of fields, new and collaborative engagement tools have enabled greater and more accessible participation opportunities to citizen "experts" who were previously unknown or whose knowledge was previously untapped (Noveck 2008). Large-scale knowledge-sharing projects such as Wikipedia and volunteer initiatives such as Apache Webserver demonstrate that ordinary citizens possess information and expertise that can enhance decision making. The application of participatory decision-making processes have in some cases also proved to lead to better services, ultimately improving lives. Brazil, for instance, has become an international leader in participatory budgeting, directly incorporating citizen input into budget allocation decisions, which researchers have found are correlated to positive policy outcomes in areas such as infant mortality: by 2008, over 120 of Brazil's 250 cities had adopted participatory budgeting. In these same municipalities, infant mortality rates decreased by almost 20 percent — an improvement that researchers found statistically significant even after accounting for political and economic factors (Wampler and Touchton 2014). Adoption of such participatory techniques and tools, in Brazil and elsewhere, has helped to inform, diversify and legitimize decision making. Such tools have also helped realize a shift in power from institutions to networks, and from centralized decision-making authorities to knowledge at the edge.[7]

Enabling distributed groups within the Internet governance ecosystem with these participation techniques and tools would help operationalize this shift in power. Leveraging and expanding on emerging tools and techniques (for example, expert networking, crowdsourcing and open data) could also help to break down barriers between experts in different disciplines, and foster collaboration between networks and locations of expertise (Raines 2014b; 2014d). Such a shift could help to empower Internet users with meaningful opportunities to participate and collaborate directly in decision making, rather than merely provide feedback from the outside. It would, in effect, move users of the Internet to the centre of Internet governance.

Experimentation

Finally, open governance embraces agile, iterative decision making in order to ensure that institutions and citizens can respond to a rapidly evolving governance landscape and leverage and learn from past successes as well as failures. The movement places an emphasis on experimentation, enabled through the generation and sharing of quantitative as well as qualitative data. This data is used to determine best practices and ensure that results and decisions can be meaningfully analyzed, replicated or iterated-upon for various needs and in different contexts. The distributed Internet governance framework proposed here would embrace the development and use of open data to, in particular, shift decision making from a "faith-based" to an "evidence-based" approach (Noveck 2014).

WHAT ARE THE KEY FUNCTIONS OF DISTRIBUTED INTERNET GOVERNANCE?

Distributed governance for the Internet builds on these general elements of open governance to add several features that are specific to the Internet. The following is a brief overview of the main characteristics of distributed governance on the Internet.

First, distributed governance facilitates cooperation between existing and emerging actors and organizations, in the process eliminating the need for new institutions or bureaucracy and enabling more flexibility, fluidity and creativity in the actions of existing actors. Cooperation is very much at the heart of a distributed system. By focusing on cooperation, distributed governance moves away from a top-down system in which a single authority sets agendas and decides on responses. Instead, it facilitates a decentralized dialogue about issues, implementation and accountability. In a distributed system, a diversity of actors and institutions are provided with the tools to help share and digest information, experiences and knowledge. In doing so, they are able to link up with other actors on issues and responses and form issue-based networks.

Distributed governance also employs a "routing" function to enable interoperability (Gasser and Palfrey 2012) and collaboration within the Internet governance ecosystem through the adoption and use of common "languages" or "standards" — a common ontology — among players and across actors. Issue-based networks are by their nature more flexible, fluid and creative. They have none of the formality or bureaucracy of traditional government structures; they can form and dissolve over time, with cooperation and coordination as their driving purpose.

7 Citizen engagement tools, whether created within or outside government, exist to engage citizens to contribute in more networked ways to governance on a variety of issues, for example, from vetting potential patent applications (Peer-to-Patent) to helping in disaster response and relief (see www.ushahidi.com) to lawmaking and voting. See examples included in Raines (2014a; 2014e) and Declercq (2014). Citizen engagement tools have also emerged at a variety of levels of government down to municipalities (see, for example, Skillville, a micro-volunteering platform for city projects in San Francisco) (Knight Foundation 2013).

In addition, because distributed governance networks source ideas from multiple and dispersed actors, they also encourage more creative responses to problems. In particular, a distributed governance approach recognizes that knowledge and viable responses often exist "at the edges" (Lagace 2006), away from official bodies and mechanisms of governance. Distributed governance shifts power to experts or individuals who may not otherwise have the ability to participate in power systems. It facilitates collective action and information sharing between these new actors at the edge and existing decision makers.

Distributed governance on the Internet relies very much on information sharing and evidence-based decision making. This is in part an outcome of the dispersed nature of distributed governance structures: because they prioritize coordination and knowledge sharing, they are able to collect, analyze and act upon a wide variety of evidence and data.

In an evidence-based approach to governance, different actors replicate experiments in rigorous ways that allow for comparisons, which can be shared between actors in different contexts. As such, an evidence-based approach can deepen opportunities to accurately answer questions about the impacts and effectiveness of specific governance initiatives over time. It can help us better understand whether programs work differently in different geographic spheres, what factors contributed to successes and how we can learn from failures (Barnett, Dembo and Verhulst 2013). For example, through the use of comparable metrics and indicators, an evidence-based approach could tell us about different challenges to IPv6 interoperability in different parts of the world, thus helping to develop governance techniques and policies that ensure maximum global interoperability.[8]

Distributed governance allows for both granularity (localization) and scale (globalization) by adopting expert- or issue-based organizing principles that help coordinate decision making on issues across and between the local, national, regional and global levels. Distributed networks enable greater localization. In addition to better incorporating actors at the edges of the network (many of whom would by definition be closer to the local origins of an issue), distributed networks permit local actors with shared interests to discover each other and coalesce into expert- or interest-based bodies. Distributed networks in effect permit a "re-localization" of issues that may otherwise have unproductively escalated to the national or regional level. In this sense, a distributed, collaborative network can be a powerful tool in helping overcome the sense of marginalization that some stakeholders in Internet governance (particularly in developing countries) have felt over the years.

HOW DOES DISTRIBUTED INTERNET GOVERNANCE BUILD ON THE INTERNET'S ARCHITECTURE?

The collaborative and cooperative nature of the distributed governance approach is inspired by the nature of the Internet's technological architecture, an idea promoted by Lawrence Lessig and others, who view the Internet and "Internet governance" — that is, how the Internet is *used* and how the Internet technically *works* — as mutually constructive and inextricable processes.[9] Any proposed framework must, therefore, draw from an understanding of the Internet's architecture.

That architecture is based on principles of interoperability and neutrality — network engineering principles that value simplicity across distributed technology: "Every computer connected to the Internet is capable of doing a few, very simple tasks very quickly. By linking millions of comparatively simple systems together, complex functionality is achieved" (Zuckerman and McLaughlin 2003).

These same principles of neutrality and interoperability can be applied to how the Internet is governed. Responses to complex issues that we face today are more likely to be reached when dispersed institutions and actors have simple and accessible means for finding each other and coordinating around a particular issue or a given stage of decision making, in particular through the use of shared data. Collaboration on a distributed network can provide access to information about a variety of issues, including what governance efforts have succeeded (or failed) elsewhere, and the landscape of actors and institutions involved in working on a given issue over time.

In computer networking, interoperability describes the ability of devices to interact with other devices regardless of their specific hardware or software specifications (Slater 2012). The Internet is a "network of networks" — an "inter-network" — in which different networks can exchange information in a useful and meaningful manner. For this to work, however, it is critical that networked machines use a common set of protocols that allow for a standardized interpretation of sent and received information. The information itself must also be encoded using a common set of standards. This challenge is usually described as one of "universal adoption," which requires that network operators and software developers voluntarily adopt common protocols and standards. Interoperability is

8 A concept promoted by the NETmundial Initiative, and currently being tested by CGI in Brazil, which is working to share data and best practices around the creation of regional and national multi-stakeholder Internet governance structures.

9 See Lessig (1999) arguing that "code is law" and can have profound social effects as a result, and the work of anthropologist Clifford Geertz, who argued that "legal thought is constructive of social realities rather than merely reflective of them" (Geertz 1985, 232).

important because it allows for increased interconnectivity and exchange of information and services online.

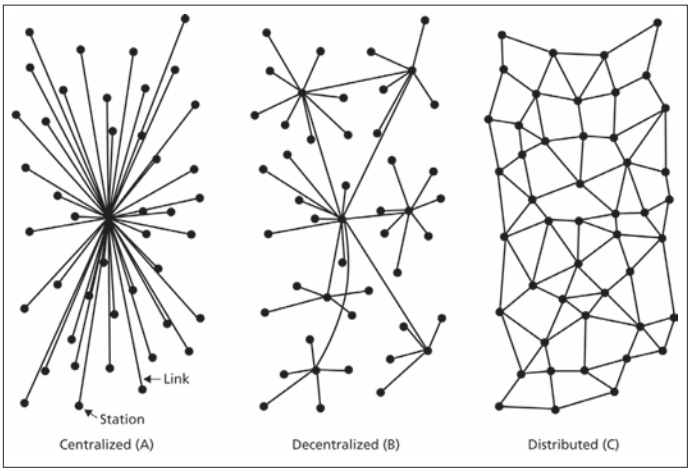
Similarly, to facilitate a robust governance environment, it is critical that actors can cooperate by being able to speak a "common language." In the technology context, this can mean a common set of standards. In the governance context, it means a mutually understood ontology of Internet-related issues and responses (Kurbalija 2014b). The global Internet governance ecosystem thus requires "cross-domain" interoperability — that is, the ability for diverse social, political, organizational, legal and technical systems to meaningfully work together and collaborate around setting this common ontology.

HOW IS DISTRIBUTED GOVERNANCE DIFFERENT FROM MULTI-STAKEHOLDER GOVERNANCE?

Multi-stakeholderism[10] in the Internet context reflects the view that there are different groups with diverse interests in governing the Internet, and that each of these interest groups should have an equal opportunity to participate. Interest groups include those who operate Internet-based businesses such as Amazon or Google. They also include those that make their living selling Internet access services such as Internet service providers or domain name registries. Multi-stakeholderism also accommodates the individual views of national governments that have a responsibility to safeguard the values of their societies and citizens. Those having a "stake" also include individuals and groups with an interest in safeguarding certain values such as economic flourishing, creative expression or educational achievement. By emphasizing interests and stakes, however, the multi-stakeholder model tends toward the concept of entitlement over expertise.

The notion of "respective roles" in the multi-stakeholder model represents its most contested aspect. Different organizations in today's ecosystem (for example, ICANN, the IETF or the ITU) engage in different "flavours" of multi-stakeholderism in that their schemes of prioritization of particular interests or roles vary. For instance, the ITU supports a multilateral approach, which tends to question whether participating non-governmental stakeholders are truly representative of certain segments of society. Alternatively, those advocating for ICANN's multi-stakeholder model, for instance, often question the multilateral approach and the legitimacy of governments to regulate the Internet without greater involvement from non-governmental stakeholders. These varied approaches to multi-stakeholderism can perhaps be taken as proof, as some have put it, that the Internet is "resistant to traditional forms of regulation" (Verhulst 2004), and that many debates over Internet governance end up being a "battlefield" (Stone 2012) of political ideologies, at the expense of solving real issues.

Figure 1: Centralized, Decentralized and Distributed Networks



Option (c) in the above graphic helps to visualize how a distributed network enables easier linkages and connections across nodes (i.e., actors and issues) compared to a centralized or entirely decentralized approach.

Source: Paul Baran. 1964. "On Distributed Communications: I. Introduction to Distributed Communications Networks." Memorandum RM-3420-PR. August. The RAND Corporation. www.rand.org/pubs/research_memoranda/RM3420.html. Reprinted with permission.

Distributed governance in fact mediates between the "purely multi-stakeholder" and "purely multilateral" approaches. Its goal is not to replace or devalue the existing model, but rather to enhance it by adding a way to operationalize notions of collaborative, transparent and bottom-up responses to pressing and complex issues. The mediating function is apparent in the fact that the fundamental unit of governance in a distributed model is the *issue at hand* and not the *stakeholder*. Thus, positioning and agreeing to respective stakes as to a specific issue (or range of issues) is no longer the (often impossible) prerequisite for participation; rather, legitimacy is derived from one's capacity and willingness to contribute information and approaches for problem solving around specific issues. This point was made at the April 2014 NETmundial meeting and is reflected in the NETmundial Multi-stakeholder Statement:

> Internet governance should be built on democratic, multi-stakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including

10 The 2005 WSIS working group described multi-stakeholderism as: "Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet." See Working Group on Internet Governance (2005).

> governments, the private sector, civil society, the technical community, the academic community and users. The respective roles and responsibilities of stakeholders should be interpreted in a flexible manner with reference to the *issue* under discussion. (NETmundial 2014, emphasis added)

The focus of a distributed governance model is thus less on the internal mandates of specific stakeholders, and more on the specific features of issues at hand. In such a governance context, the use of evidence in decision making and evaluations is critical. Furthermore, it is essential that evidence is shared across the distributed governance ecosystem, so that a common "information architecture" exists for all Internet governance actors, regardless of sector or role to identify issues, and identify and test responses — in the process building common understanding as to what has worked (and what has not) over time.

DO REAL WORLD CASES EXHIBIT ANY OF THE DESIRED FEATURES OF DISTRIBUTED GOVERNANCE?

Distributed governance is a fledgling concept in the context of Internet governance, but a variety of examples, many drawn from non-technical fields, do exist. Considering such examples can help us better understand the principles of distributed governance and how they could be applied to Internet governance.

The following discussion focuses on the key functionalities and properties that are brought to the fore by distributed governance and, for each, points to some existing examples.

Function 1: Facilitating and Enhancing Cooperation between Actors and Organizations

OpenStand is a movement driven by groups from industry, civil society, government, the technical community and academia to promote a unified set of standards for the Internet and the Web (OpenStand 2014a). The OpenStand community experiments with new designs and technologies, and provides ongoing feedback based on these experiences to shape the next generation of standards. In this way, existing organizations coordinate to build a global standards environment that is straightforward and easy to navigate. This process eliminates the burden of country-by-country standard requirements that slow technological innovation (OpenStand 2014b).

To support the establishment of a modern paradigm for global, open Internet standards, OpenStand has a guiding set of principles that include:

- cooperation among standards organizations;
- adherence to due process, broad consensus, transparency, balance and openness in standards development;
- commitment to technical merit, interoperability, competition, innovation and benefit to humanity;
- availability of standards to all; and
- voluntary adoption (Kolkman 2014).

Function 2: Serving as a "Routing" Function Using a Common Ontology to Ensure Interoperability throughout the Ecosystem

The Marine Stewardship Council (MSC), which was initiated in 1997, serves as a good example of an organization that provided a routing function aimed at empowering actors around specific issues and actions. The MSC emerged as a response to growing pessimism about the status of fish stocks, the impacts of fishing on the marine environment and the future of the fishing industry and communities (Vallejo and Hauselmann 2004). In an effort to increase the overall sustainability of the world's seafood supply, groups and individuals with a stake in or concern for the fishing industry and fish population joined to develop and maintain a common MSC standard, which serves as the basis for their eco-label certification. This certification was developed as a result of consensus from all affected and concerned players as to the criteria for indicating via MSC eco-label that seafood comes from a sustainable fishery. This standard evolves over time, to reflect input from the MSC Stakeholder Council and, as part of the certification process, requires input from local stakeholders, ensuring that local interests are consistently incorporated in this global effort.

The effort began when diverse stakeholders and concerned parties organized around a specific issue, using evidence-based policies to inform the development of their certification. Over the years, the certification has served as a common standard for the industry's networks and has gained significant legitimacy in the global markets, with major corporations vying for the official MSC eco label (Skoll and Osberg 2013).

Another frequently cited example of a distributed governance network involves the International Air Transport Association's (IATA) Joint Slot Advisory Group (JSAG). This airline industry working group consists of an equal number of IATA member airlines and airline coordinators. Since 1947, JSAG has met twice a year to agree on slot allocations, defined as the scheduled time of an airplane's arrival or departure on a specific date. In the 1960s, increased congestion at several major airports prompted the IATA to broaden slot allocation discussions

to include acceptable levels of anticipated delays. Today, the need to hold biannual meetings where members jointly consider proposals for changes to IATA continues the Worldwide Slot Guidelines. Through bilateral discussions, the process established by the JSAG working group ensures that all airline operators follow a common set of coordinated standards that are consistent for all airports throughout the world (IATA 2014).

Function 3: Promoting Open Information Sharing, Capacity Building and Evidence Gathering to Enable Open Participation and Support Coordinated Action

A growing international concern involves maritime governance of oceans (Schiffman 2014), in particular the Arctic Ocean. This body of water is experiencing dramatically reduced ice coverage each year, creating the potential for major changes in worldwide shipping and access to new energy resources. Since there is a severe lack of information and no single entity with sovereignty over the Arctic Ocean, the US Coast Guard, along with traditional maritime governance organizations from around the world, are pursuing a new strategy to broaden international partnerships to enhance critical information-collecting efforts. The US Coast Guard describes this as a "collective effort that includes international collaborative forums, drawing upon their cumulative authorities, capabilities and experience" (Lagan 2013).

An information-sharing arrangement has emerged from this initiative, called the North American Ice Service (a collaborative partnership featuring a diverse set of actors including the International Ice Patrol, the National Ice Center and the Canadian Ice Service), which provides ice information and services to marine interests throughout North America. The group shares data on weather and environmental modelling, international treaty obligations and ecological analyses for safe and efficient maritime operations, and publishes this information online via a regular bulletin and chart visualizations (US Coast Guard Navigation Center 2012).

Function 4: Allow for Granularity (Localization) and Scale (Globalization) by Adopting Expert- or Issue-based Organizing Principles to Help Coordinate Decision Making across Spheres

VIVO is an open-source semantic web application originally developed and implemented at Cornell University in 2003, further developed by a National Institute of Health-funded consortium, and is now being established as an open-source project with community participation from around the world (VIVO 2014). At the "local" level, when installed at an institution and populated with a researcher's interests, activities and accomplishments, the application enables the discovery of research and scholarship across disciplines at the institution and provides data to facilitate connections and information sharing around specific research topics or agendas. The VIVO web also scales beyond individual universities and enables the discovery of research and scholarship from experts on particular issues across institutions by creating a semantic cloud of information that can be searched and browsed. Current efforts aim to also extend VIVO to enable searching and links "to cover research resources, ranging from datasets to spacecraft and their scientific instruments, to agriculture, cell lines, and research impact" (ibid.). VIVO had over 20 countries and 50 organizations provide information in VIVO format on more than one million researchers and research staff, including publications, research resources, events, funding, courses taught and other scholarly activity at the close of 2012.

Another example of this function is exemplified in Nextdoor, a social networking site built for neighbours grouped within a community to communicate on topics such as safety, services and crime.[11] On a granular level, the website enables neighbourhood-specific networks and allows for individual connections and hyperlocal information sharing around particular topics (for example, an individual can share information regarding the sale of furniture within a single building).

Additionally, the platform allows for larger-scale communications and more dynamic coordination. The site has the capacity to deliver real-time city alerts, crowdsourced reports and crisis maps that connect users to resources (Brown 2014). Expanding its scale, Nextdoor partnered with AlertSF, a text-based notification system in order to alert an entire community about a massive fire in the Mission Bay area in San Francisco (Shueh 2014).

ENABLING AN EFFECTIVE, EVOLVING AND LEGITIMATE DISTRIBUTED INTERNET GOVERNANCE ECOSYSTEM

To realize a framework for distributed Internet governance — one that is effective, evolving and legitimate — the Ilves panel report suggests that the decision-making process should be deconstructed into four "elements" that could help simplify what is and often appears as a complex set of abstract governance processes. These elements include issue identification, mapping, response formulation and response implementation. Other observers have likewise suggested the value of a deconstructed approach in simplifying and clarifying opaque governance ecosystems. For example, Bertrand de la Chapelle — echoing the policy sciences literature on the stages of decision making in every policy-making process (Anderson 2000; Bardach 2000; Birkland 2001; Dye 2001; Gramberger 2001; Munger

11 See https://nextdoor.com/.

2000; Stone 2002) — has described a five-stage "workflow model" of governance (agenda setting, drafting, adoption, implementation, monitoring and enforcement) that allows for "participation by various stakeholders" in the "creation of a flexible global architecture" (de la Chapelle 2003).

Separating out the various elements of Internet governance would help actors identify their roles in developing responses to issues. It would also help coordinate the different responsibilities of actors within the ecosystem (ICANN Strategy Panel on Multistakeholder Innovation 2014). A staged decision-making approach provides a road map for operationalization and helps to address the current fragmentation of governance on the Internet. For instance, by clearly demarcating decision-making processes and institutional responsibilities, a staged approach can mitigate previously discussed challenges such as forum shopping, jurisdictional overlap and competition, and the prevalence of "orphan issues" (Kleinwächter 2014) such as spam, privacy rights and intellectual property rights. A staged approach also promotes greater inclusivity while simplifying and making clearer the pathways for collaboration and participation in governance.

This chapter (building on The GovLab's work in support of the ICANN Panel on Multistakeholder Innovation) proposes a breakdown of the distributed Internet governance process into six "stages":

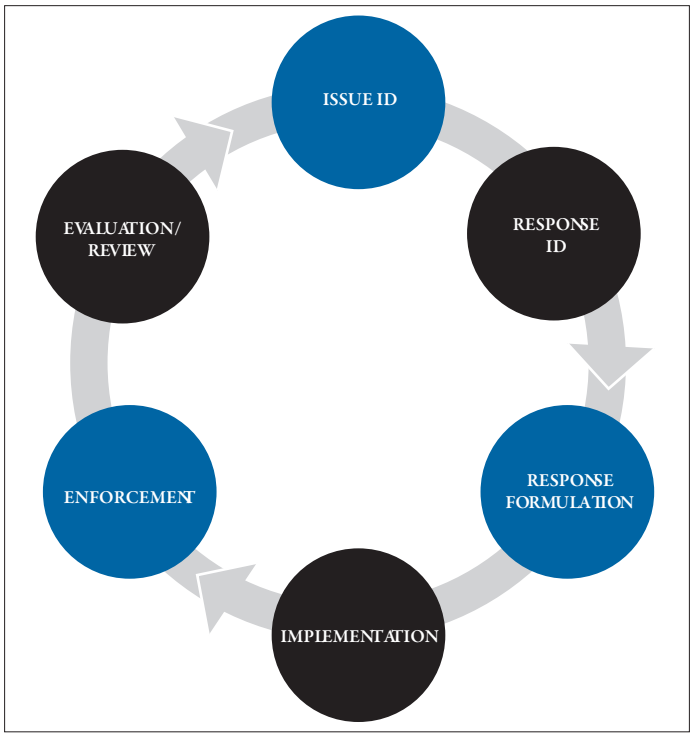
- issue identification;
- response identification;
- response formulation;
- implementation;
- enforcement; and
- evaluation or review.

The following discusses each of these stages at greater length, suggesting enabling mechanisms for participation and collaboration within the global Internet community that emphasize open data, information sharing and experimentation.

ISSUE IDENTIFICATION

Issue identification refers to the process by which the distributed Internet governance ecosystem would identify a problem or challenge that needs addressing. The process of issue identification also involves identifying the appropriate geographic sphere or level at which an issue should be addressed — i.e. at the local, national, regional or global levels. During the issue identification stage, cooperation is required to understand the various facets of a challenge or issue, so that existing responses can be understood and, if necessary, new approaches can be crafted (for example, policy model responses or technical standards responses). Cooperation is needed here also so that the most responsible or capable actors can be engaged to generate action on an issue. It is therefore necessary to develop a standardized ontology for identifying and describing issues.

Figure 2: Six Stages of the Distributed Internet Governance Process



Source: The GovLab.

Currently, the Internet governance ecosystem lacks a systematic approach to understanding existing and emerging issues, as well as each actor's roles and responsibilities with regard to any given issue. One resulting problem is the previously mentioned issue of "forum shopping" (IGF 2013). Information sharing and better dissemination of information is essential to addressing such problems. For the issue identification stage to be most productive, those within the distributed governance networks must be able to access existing data and share and understand it so that issues can be quickly identified, situated and described.

Issue identification in a distributed governance environment may at times employ crowdsourcing techniques. Crowdsourcing (outsourcing a task or function to a large group of actors) is a technique for broadening participation; it can be done in person or online, and engages networked groups to expand the tool kit for problem solving. Sourcing ideas, opinions and data from the global Internet community can play a valuable role in identifying trends in Internet-related issues (Halpin

2014). Using semantic tagging can reveal similarities between crowdsourced submissions and highlight various common or dividing aspects between issues (Rao 2010). Similarly, ranking and voting systems can highlight which issues are most widely relevant and, when combined with semantic analysis[12] can show which issues are important to which stakeholders. Ultimately, issue identification in a distributed governance environment can be supported through technical means while allowing for greater transparency and sharing of open data and information.

RESPONSE IDENTIFICATION

Once an issue is identified and better understood, a response must be identified. The response identification stage of our distributed governance framework involves the network working toward the formulation of a particular response or set of potential responses to an identified issue. To identify the "solution space," it is important to create and communicate a shared understanding regarding the several types of responses and outcomes that are already in existence (for example, laws, policy guidelines and models, technical requirements, contractual models, incentives and funding, procurement provisions, certification criteria or more informal procedures). In addition, response identification should consider mapping and supporting coordination of the organization(s) responsible for further formulation and implementation, as well as possible timetables.

Today, actors within the Internet governance ecosystem are either inundated with complex requests for participation or left out of the loop on decisions that most directly affect them. This creates an environment where players are responsive largely only to formal mandates and where actions taken on issues are identified in a fragmented way, with little information sharing across the ecosystem. This system is inimical to innovative and flexible problem solving. Institutional players in particular tend to rely on their internal structures to navigate complexity, and are not able to perform comprehensive scans to identify new or viable responses or collaborators (Jenks and Jones 2013). New mechanisms for coordination and collaboration are needed so that different actors can come together to identify possible responses. New means of navigating "solution spaces" are required to overcome redundancies and gaps that lead to "orphan issues" (Carter 2014).

Information shortcomings are at the heart of such challenges, but they can be overcome in a distributed governance environment. For example, information technologies that identify and collect responses or outcomes can help various actors identify and learn about possible responses. They can also help map new and innovative "solution spaces." To the greatest extent possible, such information-sharing mechanisms should be based on open data. Much as the US government has done with federal data through Data.gov (White house n.d.), vast amounts of Internet governance-related information can also be made available to the global Internet community. Data must be presented in the most accessible form possible, and tagged and cross-linked — "layered" or "linked" data (Shadbolt et al. 2012) — so that it is easy to form connections between different types of data in the search for responses. Overall, a robust response identification stage would benefit greatly from the existence of a "living data platform" of information that is updated as the Internet governance ecosystem evolves.

FORMULATION OF RESPONSE

The "response formulation" stage refers to the period during which the most responsible, capable or interested actors can be identified and engaged to collaborate in order to develop actionable responses to problems. These responses can then be compared and evaluated using objective criteria and data in a transparent process. Selecting the relevant criteria for evaluation is itself part of the process. Responses should be evaluated on the basis of technical feasibility, economic feasibility, political viability, administrative viability, legality and so on.

Central to the response formulation process is the use of agreed-upon benchmarks, metrics and indicators — that is, the use of evidence derived for the particular context and geographic sphere relevant to the issue at hand. Objective evaluation criteria are critical to build and maintain trust in a distributed governance environment, where responsibilities for implementing responses are to be allocated to different actors based on capacity.

Response formulation can be achieved in a distributed manner through the use of shared platforms that make information about Internet issues available in open formats. Techniques that allow for the standardized description of expertise, skills and experience ("expert networking" technologies) may be particularly useful in this regard (Raines 2014b). Expert networks and expert networking technologies — such as those developed by VIVO, the interdisciplinary network of research scientists discussed above, or Kaggle, an expert network and competition platform for data scientists — can be constructed using information that describes each actors' relevant expertise or knowledge (Börner et al. 2012). This can allow for the breakdown of issues into component parts that can then be matched to specific experts or areas of expertise. Expert networking can also introduce a diversity of viewpoints in the formulation of responses and, when combined with incentives for participation, can provide access to a diverse set of ideas from a wide variety of sources.

12 For example, along a Likert scale, as employed by the survey/polling software Agreeble. See www.agreeble.com.

IMPLEMENTATION

At the implementation stage, actors within a distributed governance network can work collaboratively to ensure that recommended responses or binding decisions are implemented and monitored. Such monitoring must include both those identified in the response formulation stage as being most equipped for execution, and those who will be most affected by the response. Issue-based distributed networks can help facilitate this and assist in overseeing the process of implementation so that needed changes can be responsively identified and addressed, and so that those tasked with bringing about a desired response have access to the required knowledge and expertise both from those within and without the network (Panel on Global Internet Cooperation and Governance Mechanisms 2014).

This type of networked, collaborative and distributed approach to response implementation differs quite significantly from what exists today. At present, proposed responses too often lack adequate direction for execution and adoption. One could argue this is the result of response formulation processes that tend to prioritize notions of "multi-stakeholdership" over all else. As a result, response development and response implementation often get conflated into one decision-making phase focused almost entirely on achieving consensus around broad objectives rather than on first collaborating around the discovery, design and testing of more nuanced and tailored responses derived from shared knowledge.

Response implementation proves difficult in today's ecosystem when the actors affected by many actions and responses are not consulted; when the processes impacted by a given response are not analyzed, evaluated or experimented with during the response-formulations stage; and in cases where proposed responses address meta-governance issues, for example improving the process of making policy on generic top-level domain names (GNSO 2014).

ENFORCEMENT

As noted, Internet governance is characterized today by significant jurisdictional confusion and overlap; this complicates the "enforcement" stage of decision making. A good example can be found at events surrounding the 2012 World Conference on International Telecommunications that reviewed the International Telecommunication Regulations global treaty, which was ultimately signed by fewer than half the members of the ITU (Reporters Without Borders 2012).

The effectiveness of enforcement requires a strong focus on measurement, using metrics and indicators to understand the impact of responses. The enforcement stage can thus provide for monitoring adherence in implementation to agreed-upon governance principles and values, such as those articulated in the NETmundial Multistakeholder Statement (NETmundial 2014). Enforcing adherence also requires identification of the responsible, capable or willing actors within the distributed governance networks during the response identification and response formulation stages. This could be achieved, for example, through the use of "dashboard" visualizations that trace the relationship of certain indicators to specific objectives over time to show impact.

Any meaningful enforcement mechanism is likely to reveal shortcomings or problems in response implementation; in a distributed governance environment, such problems need to be collaboratively resolved. This highlights the importance of information sharing and collaborative processing of data, as various actors responsible for enforcement may be distributed across regions and sectors, and require a way to access and communicate findings. For example, in many online community forums, certain users may be active enough or have gained enough "reputation points" to become forum moderators who can flag content as spam or inappropriate. In much the same way, a distributed Internet governance ecosystem could enable or suggest specific actors to enforce specific responses based on evidence of their competencies or abilities, or based on community agreement that those actors are the best suited to conduct enforcement.

EVALUATION OR REVIEW

The distributed governance network will also be responsible for re-evaluating and adjusting responses throughout or after implementation. This evaluation or review stage envisions the creation of further evidence to inform subsequent identification of issues and response formulation stages. Without comprehensive, evidence-based evaluation of implemented responses, there would exist a lack of ecosystem-wide understanding about the appropriateness or effectiveness of any given response. Similarly, there would exist a lack of collective understanding regarding the competencies or abilities of specific actors tasked with responding.

Currently, evaluation processes for Internet governance responses focus largely on internal organizational mandates: organizations rely on adherence to internal processes to the detriment of critically assessing whether issues that are relevant to the entire ecosystem are appropriately addressed (Jenks and Jones 2013). A far better solution would be for evaluation to be collaborative, and achieved in a way that allows the global Internet community to assess the impact and quality of specific responses and actions. Once again, information sharing is key. For example, Stimulus Watch technologies — a platform created following passage of the Recovery Act and the creation of Recovery.gov to help track US federal government spending of stimulus funds technologies — employs a distributed crowd in monitoring

stimulus spending by the federal government by asking citizens to share their knowledge on local stimulus projects and discuss and rate those projects (Sanchez 2009).

The evaluation stage could also generate open "scorecards" developed in a transparent and inclusive manner by the global Internet community.[13] These scorecards would help identify priorities across the Internet governance ecosystem and inform the further identification of issues and responses. Moreover, evidence gained from the evaluation and review of responses can inform the selection of relevant criteria for response formulation and thus contributes to the development of a set of metrics and benchmarks that can help actors better understand the issues at hand. Given that the selection of indicators and metrics for assessment involves a determination of what is deemed important, actors in a distributed governance ecosystem must collaborate on and coordinate measurement criteria, so that information is useful for everyone. Because this scorecard approach has already been used in a number of sectors and industries,[14] best practices already exist to guide a pilot or trial implementation in the Internet governance ecosystem.

TOOLS TO REALIZE DISTRIBUTED INTERNET GOVERNANCE — A MAP OF INTERNET GOVERNANCE APPROACHES AND KNOWLEDGE NETWORKS

It is not enough simply to formulate a theoretical or conceptual framework for distributed Internet governance. A practical road map is also required. Such a road map would guide actors within the Internet governance ecosystem so that, confronted with an issue requiring a governance response, they could identify at least the following elements:

- the nature of the issue;
- the severity of the issue;
- the geographic sphere within which the issue may be most appropriately addressed;
- the appropriate actors to respond to the issue; and
- any existing frameworks and/or organizations that may already be equipped to address the issue, or indeed that may already be addressing it.

The purpose of this section is to introduce a number of tools and techniques that constitute at least an initial road map toward practical implementation of the proposed framework. From the Open Governance movement, we know that a number of innovative tools and techniques for connecting people and enabling collaborative decision making already exist. For instance, open data helps facilitate information sharing; expert networks and systems can help locate and leverage the skills, credentials, experiences and passions within the global Internet governance community to help solve issues. In addition, Web SMS and in-person crowdsourcing techniques can be applied to source new, diverse and expert input for identifying and framing issues, crafting responses or participating in the enforcement and review stages mentioned above (Raines 2014c).

While these techniques and tools may all be leveraged, it is possible that the existing tool kit will prove insufficient, and that a set of new tools will be needed to test and realize our proposal for a distributed Internet governance framework. This section discusses two key components of this supplementary tool kit: a map of Internet governance approaches and Internet governance knowledge networks.

A MAP OF INTERNET GOVERNANCE APPROACHES

Both the Ilves report and the NETmundial Multistakeholder Statement strongly recommended the development of mechanisms to map Internet governance issues to responses and actors (Panel on Global Internet Cooperation and Governance Mechanisms 2014). Several initiatives are exploring various purposes and functionalities of such a mapping mechanism.[15]

An Internet governance mapping mechanism that supports the distributed Internet governance framework in practice should begin with the development of a "living database" of data on Internet-related issues, actors and approaches. An issue-to-response-to-network mapping tool could serve as an "information architecture" for Internet governance. Such an "open data" platform could include a variety of interactive infographic tools that Internet policy makers, journalists, activists and Internet users could use to map top-level issues to existing initiatives and responses, and to find corresponding institutions and experts for a given geographic sphere (using data on the role, capacities and previous actions taken by such institutions). Such a

13 See, for example, the Sunlight Foundation's "Open States Transparency Report Card," which uses a set of criteria to evaluate the "openness" of state legislative data in the United States (Turk 2013).

14 See, for example, the US Department of Education's College Affordability and Transparency Center College Scorecard (www.whitehouse.gov/issues/education/higher-education/college-score-card).

15 For example, The GovLab at New York University is crowdsourcing and mapping an open data set of Internet issues, responses and actors for the NETmundial Initiative, while the European Commission's Global Internet Policy Observatory (GIPO) is intended to provide resources for the global Internet community, with an emphasis on "automation" (European Commission 2013); William Drake and Lea Kaspar suggest a "coordinated clearinghouse function" to "access, assess and compare…a plethora of governance activities underway in technical and policy bodies at the national, regional and global levels" (Drake and Price 2014).

mapping tool could define an information model for the issues, responses and geographic spheres that comprise the field of Internet governance. Following from the staged problem-solving model laid out in the section "The Need for Distributed Internet Governance," the mapping tool could specifically support the development of a common understanding of existing Internet governance arrangements by sphere, issue type or response type.

Such a tool would assist the Internet governance community in rethinking how decision making can and should occur in a distributed fashion by helping to enable two key functions: cooperation among actors and institutions, and open information sharing. The mapping tool could also provide a means for understanding the existing field of governance and the types of tried-and-tested responses already undertaken (whether successful or not).

Additionally, the mapping tool could embrace an information ontology that describes the various entities of the distributed model as well as relationships within that model. For example, geographic spheres could include local, national, regional and global. Issues could be categorized according to five themes: access, content, code/standards, trust and trade. Responses may take the form of policies and laws, initiatives and events, research and advocacy, tools and resources, or standards. The information model will also define the flow and life cycle of the content to be produced, and will seek and be subject to advice from the wider governance community to ensure openness and inclusivity in the design and development of the mapping tool.

Development of this tool would embrace a coordinated and distributed effort to map issues to their appropriate governance networks within a given geographic sphere. It would additionally document "solution spaces" by providing information on responses or actions taken around a given issue, in the process helping to identify gaps in action. For instance, child pornography would map to various initiatives around the world and point to institutions working on the topic, as well as relevant laws and local experts who can be engaged in problem solving. The tool would point to all relevant data about the issue, as well as to active actors and responses already underway. In order to scale development and optimize for the Internet community, the mapping tool should be designed to enable user contribution, for example, through crowdsourced authoring of content in combination with the knowledge networks described below.

INTERNET GOVERNANCE KNOWLEDGE NETWORKS

Similarly built on a "living platform" describing the expertise and skills of experts, the knowledge networks (or knowledge net) could take the form of an expert network for Internet governance. Using expert discovery and networking technologies, the tool could model itself after existing systems, including reputation-based systems such as LinkedIn recommendations, credential-based systems such as ResearchGate and experience-based systems such as StackOverflow. Ultimately, this tool could present a searchable index that would allow for the tracking of skills and experiences of experts who could be tapped locally in countries or other jurisdictions to help in the various stages of governance described above.

The knowledge net could address the need for expertise at all stages of the Internet governance process. Sources and types of expertise would be diversified by allowing people to participate directly in the knowledge net, thus opening them to the chance of being called upon by Internet governance actors to contribute to issues that match their skills profile. Participants in the network could be asked to fill out a profile describing their relevant skills, experiences and interests, including, for example, courses taken or taught related to Internet issues (such as through ICANN Learn), Internet governance forums or conferences attended, online campaigns or projects they were part of, technology skills or applications built, and so on.

Embedded within the knowledge network there could be functionalities allowing individuals to self-select and form open groups around issues that they know or care about, perhaps in their specific region. Being able to self-identify around skills and expertise rather than institutional membership could remove barriers to entry for newcomers to the governance space. And, once part of the network, an expert would be able to take advantage of open discussion forums, brainstorming or Q&A tools, or challenge platforms where participants could form groups or launch challenges related to a particular Internet governance issue (for example, to design a draft evaluation scorecard for broadband deployment in a small city, or to help promote IPv6 adoption around the world).

Having a comprehensive network for Internet governance and related fields would also make it easier to identify and target experts with specific questions related to Internet governance. For example, if an institution or other actor is trying to gain insight into Internet access and affordability issues in a specific region, a policy maker will want to reach those who have actual technical, regulatory, business and specific regional experience. The database could be extremely useful in helping to identify experts who have collected, analyzed or published relevant data. Finally, a database of willing contributors with rich expertise and access to data could itself help formulate governance policies; the network could function, in essence, as a repository of knowledge that could underpin efforts to develop and operationalize the proposed new, distributed Internet governance framework.

KEY OPPORTUNITIES FOR OPERATIONALIZING THE FRAMEWORK

If a convincing case for innovating within and enabling new forms of coordination in Internet governance has been made (the "what"), then the prospect of constructing new platforms, mechanisms and tool kits to support such distributed governance arrangements can be taken up by a variety of global initiatives (the "how"). This chapter proposes two specific supporting tools — a map of Internet governance approaches and Internet governance knowledge networks — both of which are actively under development. The value in both of these information tools relies on accurate and up-to-date Internet governance-related content and data. Like other open data projects, these tools will grow in both usefulness and value when experts and enthusiasts alike build an "ecosystem" of specific applications using the shared data.

The distributed governance framework presented within this chapter is achievable through an action-based, participatory, experimental and analytically rigorous approach. Opportunities for action on this approach are ripe, for example in connection with the NETmundial Initiative and the Global Commission on Internet Governance (GCIG), launched by the Centre for International Governance Innovation and Chatham House.

NETMUNDIAL INITIATIVE

The NETmundial Initiative can provide an additional forum for transparent and inclusive consultations to solicit input from the global Internet community to further develop the mapping tool, including its desired functionalities, content structure, moderation processes and legal framework. Such consultations can be supported by related actions including the development of global, regional and national multi-stakeholder dialogues to deepen understanding of Internet policy issues (World Economic Forum 2014) (inspired, for example, by Brazil's Marco Civil legislation and the NETmundial Meeting).

GCIG

The GCIG, launched in January 2014, seeks to present "a comprehensive stand on the future of multi-stakeholder Internet governance." Over a two-year period, the GCIG intends to address four key themes: enhancing governance legitimacy, preserving innovation, ensuring rights online and avoiding systemic risk. The GCIG and its associated research advisory network will provide another important platform for conducting consultations with the global Internet community, convening meetings with regard to the four themes, and bridging disciplines in the construction of new models of governance for the Internet. The GCIG's research will help identify the best techniques for promoting cooperation and incentives for actors to function cooperatively in a distributed and complex governance environment.

The Internet is doubtless one of the most significant human accomplishments in history, and it should follow that Internet governance has similar significance. Clearly, the Internet has both technical and non-technical components, as must its governance. The endeavour of developing an effective and legitimate system of governance has been and will continue to be a global one, requiring not only the participation from all, but also a diversity of expertise that crosses borders, languages and disciplines. This framework proposal suggests a "construction plan" for a governance ecosystem that is distributed, flexible, collaborative and global. But this framework is not exhaustive, and critical questions must be answered to inform operationalization:

- Issue identification: How and when to decide and who decides whether an issue requires global coordination or devolution? What data is needed to help facilitate that process?
- Network identification: How do we move from actor identification to the facilitation of distributed networks capable of addressing a global issue?
- Response development: How do responses get developed in a distributed fashion, across disciplines? Acknowledging that we all have a stake in the future of the Internet, what techniques work best for promoting cooperation, not competition, in problem solving?
- Oversight: Who will, and how to, monitor adherence to principles of Internet governance in order to ensure accountability?
- Coordination: In addition to the development of the tools articulated in this chapter, how do we coordinate across issue areas, sectors, cultures and regions? How do we systematically add, translate and share knowledge accumulated openly, responsively and responsibly within the ecosystem?
- Incentives: What incentives exist to use tools that support a distributed Internet governance ecosystem, and what incentives might make such tools more useful? What incentives exist to overcome issues of self-selection bias? How can we increase participation on global issues from those presently "unwilling" or "unable" (politically, technologically or otherwise) so as to avoid reinforcing existing ecosystem divisions?

- Case studies: What examples of distributed governance exist that embody the necessary functions of the distributed framework? What groups and mechanisms serve as "building blocks" for the conceptual model described here? What can we learn from these examples and how should we connect with those involved?

- Limitations: What are the limits of such an information-based approach? What are the problems it cannot solve?

It is necessary to further study whether and how a distributed framework for Internet governance could present a truly viable alternative to existing models of Internet governance. Surely many more initiatives will be launched with mandates to coordinate Internet governance approaches and to develop more effective and legitimate forms of problem solving. It is clear that the capacity to deliver a framework such as the one outlined in this chapter exists, and the authors look forward to further innovations in the field.

WORKS CITED

Anderson, J. E. 2000. *Public Policymaking: An Introduction*. Boston, MA: Houghton Mifflin.

Arora, K. 2014. "Internet Governance and "Ungovernance" Meet ups in Instanbul." *The Times of India*, September 3. http://timesofindia.indiatimes.com/business/india-business/Internet-governance-and-ungovernance-meet-ups-in-Istanbul/articleshow/41565623.cms.

Bardach, E. 2000. *A Practical Guide for Policy Analysis: The Eightfold Path to More Effective Problem Solving* (2nd ed.). New York, NY: Chatham House Publishers, Seven Bridges Press.

Barnett, A., D. Dembo and S. G. Verhulst. 2013. "Toward Metrics for Re(imagining) Governance: The Promise and Challenge of Evaluating Innovations in How We Govern." GovLab, April 18. http://thegovlab.org/wp-content/uploads/2013/04/GovLabMetrics.pdf.

Birkland, T. A. 2001. *Introduction to the Policy Process*. Armonk, NY: M.E. Sharpe.

Börner, K., M. Conlon, J. Corson-Rikert and Y. Ding. 2012. "VIVO: A Semantic Approach to Scholarly Networking and Discovery." Morgan Clay Pool. www.morganclaypool.com/doi/abs/10.2200/S00428ED1V01Y201207WBE002.

Bradsher, K. 2012. "China Toughens Its Restrictions on Use of the Internet." *The New York Times*, December 28. www.nytimes.com/2012/12/29/world/asia/china-toughens-restrictions-on-internet-use.html?_r=0.

Brandom, R. 2014. "Aereo to Suspend Service at 11:30 EST Today." The Verge, January 28. www.theverge.com/2014/6/28/5852116/aereo-to-suspend-service-at-11-30-est-today.

Brown, J. 2014. "How the Sharing Economy Is Changing Disaster Response and Recovery." Emergency Management, September 3. www.emergencymgmt.com/disaster/How-the-Sharing-Econoomy-Is-Changing-Disaster-Recovery.html.

Carter, J. 2014. "Internet Governance Series: Tech Community Launches Debate @the 8th IGF." London School of Economics and Political Science, Media Policy Project Blog. http://blogs.lse.ac.uk/mediapolicyproject/2013/10/24/internet-governance-series-tech-community-launches-debate-the-8th-igf/.

Castro, D. and R. Atkinson. 2014. "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy." The Information Technology & Innovation Foundation, September. www2.itif.org/2014-crossborder-internet-policy.pdf.

Cheema, G. S. and D. A. Rondinelli. 2007. "From Government Decentralization to Decentralized Governance." In *Decentralizing Governance*, edited by G. S. Cheema and D. A. Rondinelli. Washington, DC: Brookings Institution Press. www.brookings.edu/~/media/press/books/2007/decentralizinggovernance/decentralizinggovernance_chapter.pdf.

Chui, M., M. Löffler and R. Roberts. 2010. "The Internet of Things." *McKinsey Quarterly*, March. www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things.

Cooper, D. 2014. "Future Contraceptives Will Let Women Remote-control Their Fertility." engadget, July 7. www.engadget.com/2014/07/07/wireless-implant-microchips-gates-foundation/.

Cooper, M. 2012. "Why Growing Up Is Hard to Do: Institutional Challenges for Internet Governance in the 'Quarter-life Crisis' of the Digital Revolution." September. http://bestbits.net/wp-uploads/2012/10/Quarterlife-Crisis-of-the-Digitall-Revolution-9-3.pdf.

Costerton, S. 2014. "The Multi-Stakeholder Model of Internet Governance: Developing a New Governance Model for the 21st Century." Event at Chatham House, London, UK, September 22. www.chathamhouse.org/event/multi-stakeholder-model-internet-governance-developing-new-governance-model-21st-century.

CyberEthics. 2011. "Benefits of Internet Use." CyberEthics. www.cyberethics.info/cyethics1/index.php?option=com_content&view=article&id=186&Itemid=83&lang=en.

Declercq, A. 2014. "Proposal 6 for ICANN: Enhance Decision-Making Legitimacy by Experimenting with Innovative Voting Techniques." GovLab, February 11. http://thegovlab.org/proposal-6-for-icann-enhance-decision-making-legitimacy-by-experimenting-with-innovative-voting-techniques/.

De la Chapelle, B. 2003. "Beyond Absolute Sovereignty: New Foundations for a Global Polity." Yale Center for Environmental Law and Policy, October 23. www.yale.edu/gegdialogue/docs/dialogue/oct03/papers/07De%20La%20Chapelle%20final.pdf.

DeNardis, L. and M. Raymond. 2013. "Thinking Clearly About Multistakeholder Internet Governance." SSRN, November 14. http://dx.doi.org/10.2139/ssrn.2354377.

Dickinson, S. 2014. "Multistakeholder Processes Are Messy." Lingua Synaptica, February 19. http://linguasynaptica.com/multistakeholder-processes-are-messy/.

Drake, W. and M. Price, eds. 2014. *Beyond NETmundial: The Roadmap for Institutional Improvements to the Global Internet Governance*. Internet Policy Observatory, August. http://globalnetpolicy.org/wp-content/uploads/2014/08/BeyondNETmundial_FINAL.pdf.

Dumbill, E. 2012. "Volume, Velocity, Variety: What You Need to Know about Big Data." *Forbes*, January 19. www.forbes.com/sites/oreillymedia/2012/01/19/volume-velocity-variety-what-you-need-to-know-about-big-data/.

Dye, T. R. 2001. *Top Down Policymaking*. London, UK: Chatham House.

Esterhuysen, A. 2014. "Remarks from APC on the NETmundial Intiative (NMI) Initial Scoping Meeting Held in Geneva on 28 August 2014." Association for Progressive Communication. www.apc.org/en/news/remarks-apc-NETmundial-initiative-nmi-initial-scop.

European Commission. 2013. *The Global Internet Policy Observatory (GIPO)*. European Commission. http://ec.europa.eu/digital-agenda/en/global-internet-policy-observatory-gipo.

Evan, C. 2014. "What Will the Next Billion Internet Users Look Like?" The Digital Beyond, September 11. www.thedigitalbeyond.com/2013/09/what-will-the-next-billion-internet-users-look-like/.

Freedom House. 2012. "Iran." *Freedom on the Net 2012*. www.freedomhouse.org/sites/default/files/Iran%202012.pdf.

Gasser, U. and J. Palfrey. 2012. *Interop: The Promise and Perils of Highly Interconnected Systems*. New York, NY: Basic Books.

Geertz, C. 1985. *Local Knowledge: Further Essays in Interpretive Anthropology*. New York, NY: Basic Books.

GNSO. 2014. "Summary." June 9. https://gnso.icann.org/en/group-activities/active/policy-implementation.

GovLab. 2013. "ICANN Primer: Primer on the Internet Corporation for Assigned Names and Numbers." GovLab, October 13. http://images.thegovlab.org/wordpress/wp-content/uploads/2013/11/icann-primer-the-govlab.pdf.

Gramberger, M. R. 2001. *Citizens as Partners: OECD Handbook on Information, Consultation and Public Participation in Policy-making*. Paris: OECD.

Hadge, K. 2010. "Legitimacy and Accountability in Internet Governance: Civil Society Participation in the World Summit on the Information Society." *gnovis*, August 25. http://gnovisjournal.org/2010/08/25/legitimacy-and-accountability-internet-governance-civil-society-participation-world-summit-i/.

Halpin, H. 2014. "Crowdsourcing a Magna Carta for the Web at the Internet Governance Forum." World Wide Web Consortium, September 3. www.w3.org/blog/2014/09/crowdsourcing-a-magna-carta-for-the-web-at-the-internet-governance-forum/.

Higgins, P. 2012. "Congressional Witnesses Agree: Multi-stakeholder Processes Are Right for Internet Regulation." Electronic Frontier Foundation, June 1. www.eff.org/deeplinks/2012/05/congressional-witnesses-agree-multistakeholderism-right-way-regulate-internet.

Hintz, A. and S. Milan. 2009. "At the Margins of Internet Governance: Grassroots Tech Groups and Communication Policy. *International Journal of Media and Cultural Politics* 5 (1&2): 23–28.

———. 2014. "In Multistakeholderism We Trust: On The Limits of the Multistakeholder Debate." Center for Global Communications Studies Media Wire, Annenberg School for Communication, University of Pennsylvania. www.global.asc.upenn.edu/in-multistakeholderism-we-trust-on-the-limits-of-the-multistakeholder-debate/.

Hoffman, P. 2012. "The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force." www.ietf.org/tao.html.

IATA. 2014. "Slot Conference Questions." www.iata.org/policy/slots/Pages/faq.aspx.

ICANN Strategy Panel on Multistakeholder Innovation. 2014. "The Quest for a 21st Century ICANN: A Blueprint." May. http://thegovlab.org/wordpress/wp-content/themes/hustle/icann/images/icann-strategy-panel-report.pdf.

IGF. 2013. "WS232 Internet Infrastructure and Terminology Explained." IGF, October 23. www.intgovforum.org/cms/component/content/article?id=1385:ws232-internet-infrastructure-and-terminology-explained.

Internet & Jurisdiction Project. 2014a. "The IGF 2014 Fragmentation Track." www.internetjurisdiction.net/igf-2014-fragmentation-track/.

———. 2014b. "IGF 2014 I&J Workshop: Will Cyberspace Fragment along National Jurisdiction." September 4. www.internetjurisdiction.net/igf-2014-workshop/.

———. 2014c. "Towards a Multi-Stakeholder Framework for Transnational Due Process." August. www.internetjurisdiction.net/wp-content/uploads/2014/08/Internet-Jurisdiction-Project-White-Paper-3.pdf.

Internet Live Statistics. 2014. "Internet Users." July 1. www.internetlivestats.com/internet-users/.

ITU. 2005. "Tunis Agenda for the Information Society." WSIS, November 18. www.itu.int/wsis/docs2/tunis/off/6rev1.html.

———. 2014. "Mobile-broadband Penetration Approaching 32 per cent: Three Billion Internet Users by End of this Year." ITU Press Release, May 5. www.itu.int/net/pressoffice/press_releases/2014/23.aspx#.VCRri9nNm7x.

Ivanova, M. and J. Roy. 2007. "The Architecture of Global Environmental Governance: Pros and Cons of Multiplicity." www.umb.edu/editor_uploads/images/centers_institutes/center_governance_sustain/IvanovaandRoy-Architecture-2007.pdf.

Jenks, B. and B. Jones 2013. *United Nations Development at a Crossroads.* New York University Center on International Cooperation. August. www.dropbox.com/s/5zs83s5dzjcnjvx/jenks_jones_un_development_crossroads.pdf.

Johnson, D. R., S. P. Crawford and J. G. Palfrey. 2004. "The Accountable Net: Peer Production of Internet Governance." *Virginia Journal of Law and Technology* 9 (9): 11–13.

Kaspersky, E. 2013. "What Will Happen if Countries Carve Up the Internet?" *The Guardian,* December 17. www.theguardian.com/media-network/media-network-blog/2013/dec/17/internet-fragmentation-eugene-kaspersky.

Kleinwächter, W. 2014. "Internet Governance Outlook 2014: Good News, Bad News, No News?" CircleID, December 31.

Knight Foundation. 2013. "How Might We Improve the Way Citizens and Governments Interact?" Knight News Challenge, March 14. http://opengov.newschallenge.org/open/open-government/submission/skillville/.

Kolkman, O. 2014. "Keeping the Internet Open: Happy Anniversary, OpenStand." August 29. www.internetsociety.org/blog/tech-matters/2014/08/keeping-internet-open-happy-anniversary-openstand.

Kroes, N. 2014. "Global Governance for a Global, Common, Public Resource." European Commission, April 23. http://ec.europa.eu/commission_2010-2014/kroes/en/content/global-governance-global-common-public-resource.

Kurbalija, J. 2014a. "An Introduction to Internet Governance." DiploFoundation. www.diplomacy.edu/sites/default/files/An%20Introduction%20to%20IG_6th%20edition.pdf.

———. 2014b. "Welcome to the IG Restaurant." DiploFoundation. www.diplomacy.edu/blog/welcome-ig-restaurant.

Lagace, M. 2006. "Open Source Science: A New Model for Innovation." Working Knowledge, November 20. http://hbswk.hbs.edu/item/5544.html.

Lagan, C. 2013. "Strengthening Maritime Governance Partnerships in Norway." Coast Guard Compass, June 3. http://coastguard.dodlive.mil/2013/06/strengthening-maritime-governance-partnerships-in-norway/.

Lessig, L. 1999. *Code and Other Laws of Cyberspace.* New York, NY: Basic Books.

Leung, S. 2014. "5 Ways the Internet of Things Will Make Marketing Smarter." *Forbes*, August 20. www.forbes.com/sites/salesforce/2014/08/30/5-ways-iot-marketing-smarter/.

Lewis, J. 2014. "Internet Governance: Inevitable Transitions." In *Organized Chaos: Reimagining the Internet*, edited by Mark Raymond and Gordon Smith. Waterloo, ON: CIGI.

Longo, J. 2013. "Open Government — What's in a Name?" GovLab, August 5. http://thegovlab.org/open-government-whats-in-a-name/.

Matt, R. 2011. "Transparency Is a Two-Way Street." Sunlight Foundation, April 20. http://sunlightfoundation.com/blog/2011/04/20/transparency-is-a-two-way-street/.

Meinel, C., and H. Sack. 2014. "Internet and Transport Layer." Internetworking. April 4, www.internetworking-book.com/internet-and-transport-layer/.

Multiple Myeloma Research Foundation. 2013. "The Multiple Myeloma Research Foundation (MMRF) Launches Revolution in Precision Medicine to Accelerate Cures at New York Event." September 24. www.themmrf.org/multiple-myeloma-research-foundation-mmrf-launches-revolution-precision-medicine-accelerate-cures-new-york-event/.

Munger, M. C. 2000. *Analyzing Policy: Choices, Conflicts, and Practices.* New York, NY: W. W. Norton and Company.

NETmundial. 2014. "NETmudial Multistakeholder Statement." April 24. http://NETmundial.br/wp-content/uploads/2014/04/NETmundial-Multi-stakeholder-Document.pdf.

Noveck, B. S. 2008. "Wiki-Government." Democracy (winter). www.democracyjournal.org/7/6570.php?page=all.

———. 2014. "From Faith-Based to Evidence-Based: The Open Data 500 and Understanding How Open Data Helps the American Economy." *Forbes*, August 1. www.forbes.com/sites/bethsimonenoveck/2014/01/08/from-faith-based-to-evidence-based-the-open-data-500-and-understanding-how-open-data-helps-the-american-economy/.

NTIA. 2014. "NTIA Announces Intent to Transition Key Internet Domain Name Functions." NTIA. March 14. www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions.

Obama, B. 2009. "Memorandum for the Heads of Executive Departments amd Agencies." December 8. www.whitehouse.gov/open/documents/open-government-directive.

OpenStand. 2014a. "About." http://open-stand.org/about-us/.

———. 2014b. "OpenStand FAQs." http://open-stand.org/about-us/faqs/.

Panel on Global Internet Cooperation and Governance Mechanisms. 2014. *Towards a Collaborative, Decentralized Internet Governance Ecosystem.* May. http://internetgovernancepanel.org/sites/default/files/ipdf/XPL_ICAN1403_InternetGovernanceiPDF_06.pdf.

Pew Research. 2013. "Public Trust in Government: 1958–2013." October 18. Rew Research Center for People & the Press. www.people-press.org/2013/10/18/trust-in-government-interactive/.

Raines, J. 2014a. "Expanding Insights — #Crowdlaw Session 2 Highlights Need for Experimentation & Collaboration." GovLab, June 24. http://thegovlab.org/expanding-insights-crowdlaw-session-2-highlights-need-for-experimentation-collaboration/.

———. 2014b. "Proposal 1 for ICANN: Get Smart With Expert Networks." GovLab, January 31. http://thegovlab.org/proposal-1-for-icann-get-smart-with-expert-networks/.

———. 2014c. "Proposal 2 for ICANN: Get Broad-Based Input by Crowdsourcing Each Stage of Decisionmaking." GovLab, January 31. http://thegovlab.org/proposal-2-for-icann-get-broad-based-input-by-crowdsourcing-each-stage-of-decisionmaking/.

———. 2014d. "Proposal 7 for ICANN: Increase Transparency by Using Open Data Open Contracting." GovLab. February 13. http://thegovlab.org/proposal-7-for-icann-increase-transparency-by-using-open-data-open-contracting/.

———. 2014e. "Toward More Inclusive Lawmaking: What We Know & Still Most Need to Know About Crowdlaw." *GovLab* (blog), June 4. http://thegovlab.org/toward-more-inclusive-lawmaking-what-we-know-still-most-need-to-know-about-crowdlaw/.

Rao, L. 2010. "IdeaScale Powers 23 Crowdsourcing Sites for the U.S. Government." TechCrunch, February 7. http://techcrunch.com/2010/02/07/ideascale-powers-24-crowdsourcing-sites-for-the-u-s-government/.

Reporters Without Borders. 2012. "New Treaty Signed But Not By All." December 21. http://en.rsf.org/internet-s-future-at-stake-at-itu-10-12-2012,43776.html.

Sanchez, J. 2009. "Stimulus Stimulates Crowdsourced Oversight, Activism." Ars Technica, February 2.

Sannon, S. H. 2013. "The GovLab Index: Trust in Institutions (Updated and Expanded)." GovLab, November 6. http://thegovlab.org/govlab-index-trust-in-institutions-updated/.

Schiffman, R. 2014. "Are the Oceans Failed State?" *Foreign Policy*, July 8. www.foreignpolicy.com/articles/2014/07/08/are_the_oceans_failed_states_overfishing_climate_change?utm_content=buffer635e9&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer.

Schulze, J. 2014. "Cloudwash — Our Prototype Connected Washing Machine." Berg, February 25. http://blog.bergcloud.com/2014/02/25/cloudwash/.

Shadbolt, N., K. O'Hara, T. Berners-Lee, N. Gibbins, H. Glaser, W. Hall and M. C. Schraefel. 2012. "Linked Open Government Data: Lessons from Data.gov.uk." *IEEE Intelligent Systems* 27 (3): 16–24.

Shueh, J. 2014. "San Francisco Partners with Nextdoor for Emergency Alerts." Govtech, April 29. www.govtech.com/public-safety/San-Francisco-Partners-with-Nextdoor-for-Emergency-Alerts.html.

Skoll, J., and S. Osberg. 2013. "McDonald's Signals Good News for Sustainable Fishing." *San Jose Mercury News*, March 14. www.mercurynews.com/opinion/ci_22775756/jeff-skoll-and-sally-osberg-mcdonalds-signals-good.

Slater, T. 2012. "What Is Interoperability?" Network Centric Operations Industry Consortium. www.ncoic.org/what-is-interoperability.

Stone, D. A. 2002. *Policy Paradox: The Art of Political Decision Making*. New York, NY: W. W. Norton and Company.

Stone, M., ed. 2012. *Pluralism and Internet Governance*. Dushanbe, Tajikistan: The Representative on Freedom of the Media.

Think Team. 2001. "A Technical History of the ARPANET." April 11. www.cs.utexas.edu/users/chris/nph/ARPANET/ScottR/arpanet/timeline.htm.

Trebilcok, M. and R. Howse. 1998. "Trade Liberalization and Regulatory Diversity: Reconciling Competitive Markets with Competitive Politics." *European Journal of Law and Economics* 6 (1): 5–37.

Turk, J. 2013. "Open States: Transparency Report Card." Sunlight Foundation, March 11. http://sunlightfoundation.com/blog/2013/03/11/openstates-report-card/.

United Nations ICT Task Force. 2004. *Internet Governance: A Grand Collaboration*. New York, NY: United Nations Publications.

USC 5361-5366. 2006. "Unlawful Internet Gambling Enforcement Act of 2006: Overview." US Federal Deposit Insurance Corporation. www.fdic.gov/news/news/financial/2010/fil10035a.pdf.

US Coast Guard Navigation Center. 2012. "About North American Ice Service." www.navcen.uscg.gov/?pageName=NAIceService.

Vallejo, N. and P. Hauselmann. 2004. "Governance and Multi-stakeholder Processes." May. www.iisd.org/pdf/2004/sci_governance.pdf.

Van Beijnum, I. 2011. "25 Years of IETF: Setting Standards without Kings or Votes." Ars Technica, January 17. http://arstechnica.com/tech-policy/2011/01/25-years-of-ietf-setting-standards-without-kings-or-votes/.

Verhulst, Z. B. 2004. "A New Model for Global Internet Governance." www.markle.org/sites/default/files/ahs_global_internet_gov.pdf.

VIVO. 2014. "About: What Is Vivo?" www.vivoweb.org/about.

Walker, C. and Y. Akdeniz. 1998. "The Governance of the Internet in Europe with Special Reference to Illegal and Harmful Content." *Criminal Law Review, December Special Edition: Crime, Criminal Justice and the Internet*, 5–19.

Wampler, B. and M. Touchton. 2014. "Brazil Let its Citizens Make Decisions about City Budgets. Here's What Happened." *The Washington Post*, January 22. www.washingtonpost.com/blogs/monkey-cage/wp/2014/01/22/brazil-let-its-citizens-make-decisions-about-city-budgets-heres-what-happened.

Weber, R. H., and R. Weber. 2010. *Internet of Things: Legal Perspectives.* New York, NY: Springer Science & Business Media.

White House. n.d. *The Obama Administration's Commitment to Open Government: A Status Report.* http://fas.org/sgp/obama/status.pdf.

White House Open Government Initiative. 2014. "Peer-to-Patent." White House Open Government Initiative. www.whitehouse.gov/open/innovations/Peer-to-Patent.

Wooding, B. 2014. "The Role of IXPs in Growing the Local Digital Economy." IGF 2014 Session Proposal. www.intgovforum.org/cms/wks2014/index.php/proposal/view_public/65.

Working Group on Internet Governance. 2005. *Report of the Working Group on Internet Governance.* June. www.wgig.org/docs/WGIGREPORT.pdf.

World Bank. 2012. "Supporting Open Governance." Washington, DC: The World Bank Institute. http://wbi.worldbank.org/wbi/content/supporting-open-governance.

World Economic Forum. 2014. "NETmundial Initiative-Debrief with Founding Partners." www.weforum.org/issues/global-internet-governance.

Young, J., L. Shaxson, H. Jones, S. Hearn, A. Datta and C. Cassidy. n.d. *ROMA: A Guide to Policy Engagement and Influence.* Overseas Development Institute. www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/9011.pdf.

Zuckerman, E. and A. McLaughlin. 2003. "Introduction to Internet Architecture and Institutions." August. http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

ABOUT THE AUTHORS

Stefaan G. Verhulst is co-founder and chief research and development officer of The Governance Lab (GovLab), where he is responsible for building a research foundation on how to transform governance using advances in science and technology. Stefaan spent more than a decade as chief of research for the Markle Foundation, where he continues to serve as senior advisor. He is also an adjunct professor in the Department of Culture and Communications at New York University (NYU). Previously at Oxford University he co-founded and was the head of the program in comparative media law and policy at the Centre for Socio Legal Studies, and also served as senior research fellow of Wolfson College. He is still an emeritus fellow at Oxford. Stefaan has served as a consultant to numerous international and national organizations and has authored and co-authored several books.

Beth S. Noveck directs The GovLab and its MacArthur Research Network on Opening Governance. The Jerry Hultin Global Network Visiting Professor at NYU's Polytechnic School of Engineering, she is also a professor of law at New York Law School. She served in the White House as the first United States Deputy Chief Technology Officer and director of the White House Open Government Initiative (2009–2011). A graduate of Harvard University and Yale Law School, she serves on the Global Commission on Internet Governance and chaired the Internet Corporation for Assigned Names and Number (ICANN) Strategy Panel on Multi-Stakeholder Innovation. She tweets @bethnoveck.

Jillian Raines previously served as a Legal & Policy Fellow at The GovLab where she worked as research support team leader and panel coordinator to the ICANN Strategy Panel on Multistakeholder Innovation. In addition to her work in Internet governance, Jillian's research focuses on tackling legal and policy impediments to open government. Jillian earned her B.A. in English, journalism and international studies from Pennsylvania State University (2009), and her J.D., magna cum laude, from New York Law School (2012). You can follow her on Twitter @Jillian_Raines.

Antony Declercq is a research fellow at The GovLab. Antony previously served as a research fellow under the Policy Development Support Department of ICANN. His research focuses on collaborative decision making in global governance systems, public sector innovation and Internet governance. Antony earned his bachelor's degrees in anthropology and in political science from New York University. At NYU, he completed an independent study in anthropology detailing emerging open governance initiatives in China, focusing on how Internet activism in China affects public policy making. You can follow him on Twitter @antdeclercq.

ABOUT CIGI

We are the Centre for International Governance Innovation: an independent, non-partisan think tank with an objective and uniquely global perspective. Our research, opinions and public voice make a difference in today's world by bringing clarity and innovative thinking to global policy making. By working across disciplines and in partnership with the best peers and experts, we are the benchmark for influential research and trusted analysis.

Our research programs focus on governance of the global economy, global security and politics, and international law in collaboration with a range of strategic partners and support from the Government of Canada, the Government of Ontario, as well as founder Jim Balsillie.

Au Centre pour l'innovation dans la gouvernance internationale (CIGI), nous formons un groupe de réflexion indépendant et non partisan qui formule des points de vue objectifs dont la portée est notamment mondiale. Nos recherches, nos avis et l'opinion publique ont des effets réels sur le monde d'aujourd'hui en apportant autant de la clarté qu'une réflexion novatrice dans l'élaboration des politiques à l'échelle internationale. En raison des travaux accomplis en collaboration et en partenariat avec des pairs et des spécialistes interdisciplinaires des plus compétents, nous sommes devenus une référence grâce à l'influence de nos recherches et à la fiabilité de nos analyses.

Nos programmes de recherche ont trait à la gouvernance dans les domaines suivants : l'économie mondiale, la sécurité et les politiques mondiales, et le droit international, et nous les exécutons avec la collaboration de nombreux partenaires stratégiques et le soutien des gouvernements du Canada et de l'Ontario ainsi que du fondateur du CIGI, Jim Balsillie.

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

Executive

President	Rohinton P. Medhora
Director of Finance	Shelley Boettger
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Chief Operating Officer and General Counsel	Aaron Shull
Director of Communications and Digital Media	Spencer Tripp

Publications

Publisher	Carol Bonnett
Senior Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Sharon McCartney
Publications Editor	Lynn Schellenberg
Graphic Designer	Melodie Wakefield

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

Communications

For media enquiries, please contact communications@cigionline.org.

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

RECYCLED
Paper made from recycled material
FSC® C023070