CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 17 — JULY 2015

The Emergence of Contention in Global Internet Governance

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

THE EMERGENCE OF CONTENTION IN GLOBAL INTERNET GOVERNANCE

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

CHATHAM HOUSE
The Royal Institute of International Affairs

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

CIGI

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

CHATHAM HOUSE
The Royal Institute of International Affairs

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

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

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

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

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

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

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

www.ourinternet.org

ABOUT THE AUTHORS

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 postdoctoral 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.

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

EXECUTIVE SUMMARY

Internet governance has rapidly shifted from a technocratic area of governance to one characterized by considerable contention. This shift is unprecedented among the large and increasing number of technocratic regimes essential to contemporary global governance and is, therefore, of broader interest and significance beyond Internet governance scholars and practitioners. This paper draws on international relations (IR) theory to argue that the emergence of contention in Internet governance entails a twofold shift in the nature of the problems posed by Internet governance. First, cooperation problems have emerged where few previously existed. Second, existing coordination problems have become increasingly difficult to manage as a result of a rapidly increasing number of players and heightened distributional consequences. The paper further provides four complementary explanations for the shift in the underlying problem structure: extrinsic uncertainty, changing market conditions, declining US dominance in the Internet governance system and social processes of institutional change and regime complex formation.

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 paper is organized around three questions. First, what does the emerging contention in Internet governance look like? The paper 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 paper draws on 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 paper 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 paper 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 paper 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 paper 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

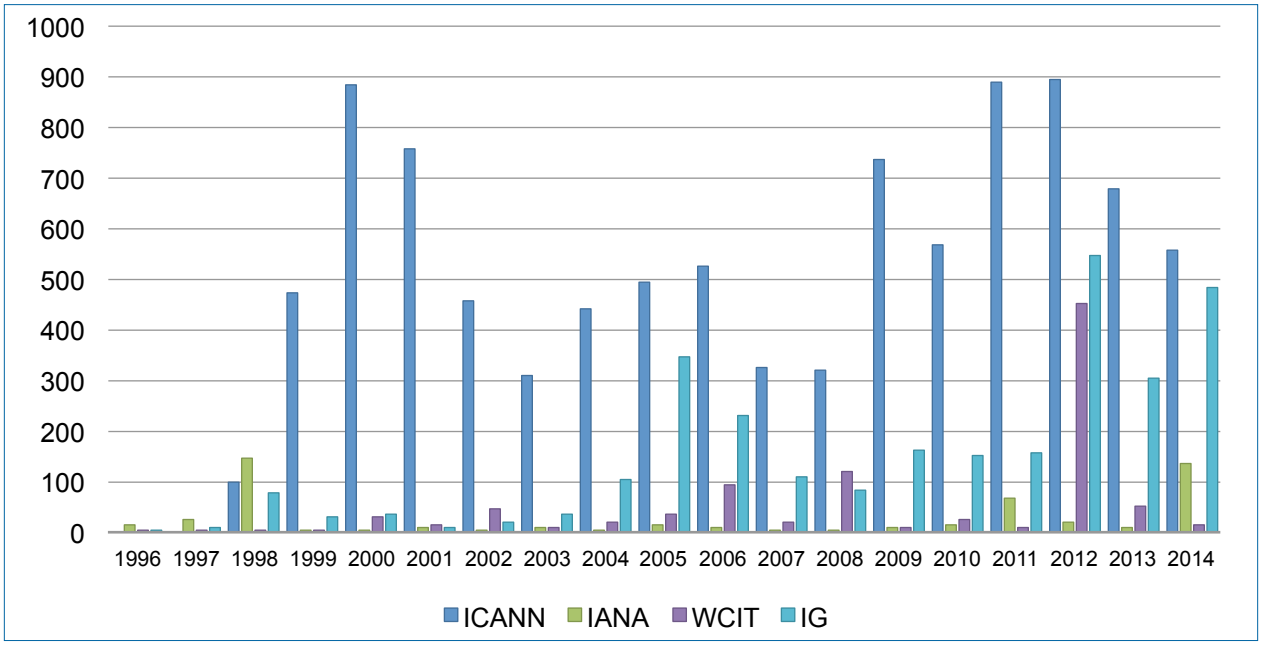
Contention over Internet governance predates Edward Snowden's disclosures about the expansive surveillance practices of the NSA (see Figure 1). Current disputes reflect the high-profile controversies mentioned above, as well as an inherent asymmetry between the rapid growth of Internet adoption in emerging 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

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



Source: Authors.

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.

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 paper 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).

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

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 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 paper 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 benefitting 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 paper 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 paper 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.

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

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 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 paper 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 paper.

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/.

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

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*, Vol. 15 (3): 1–19.

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

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

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.

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.

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

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.

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. 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 Centre*. 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.

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.

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/.

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, Jr., Joseph S. 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. T*allinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, MA: Cambridge University Press.

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.

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

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

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.

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.

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/.

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

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 CIGI

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

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

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

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

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

ABOUT CHATHAM HOUSE

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

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
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
Vice President of Public Affairs	Fred Kuntz
Director of the Global Economy Program	Domenico Lombardi
Vice President of Finance	Mark Menard
Chief of Staff and General Counsel	Aaron Shull

Publications

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

Communications

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

CIGI
67 Erb Street West
Waterloo, Ontario N2L 6C2
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