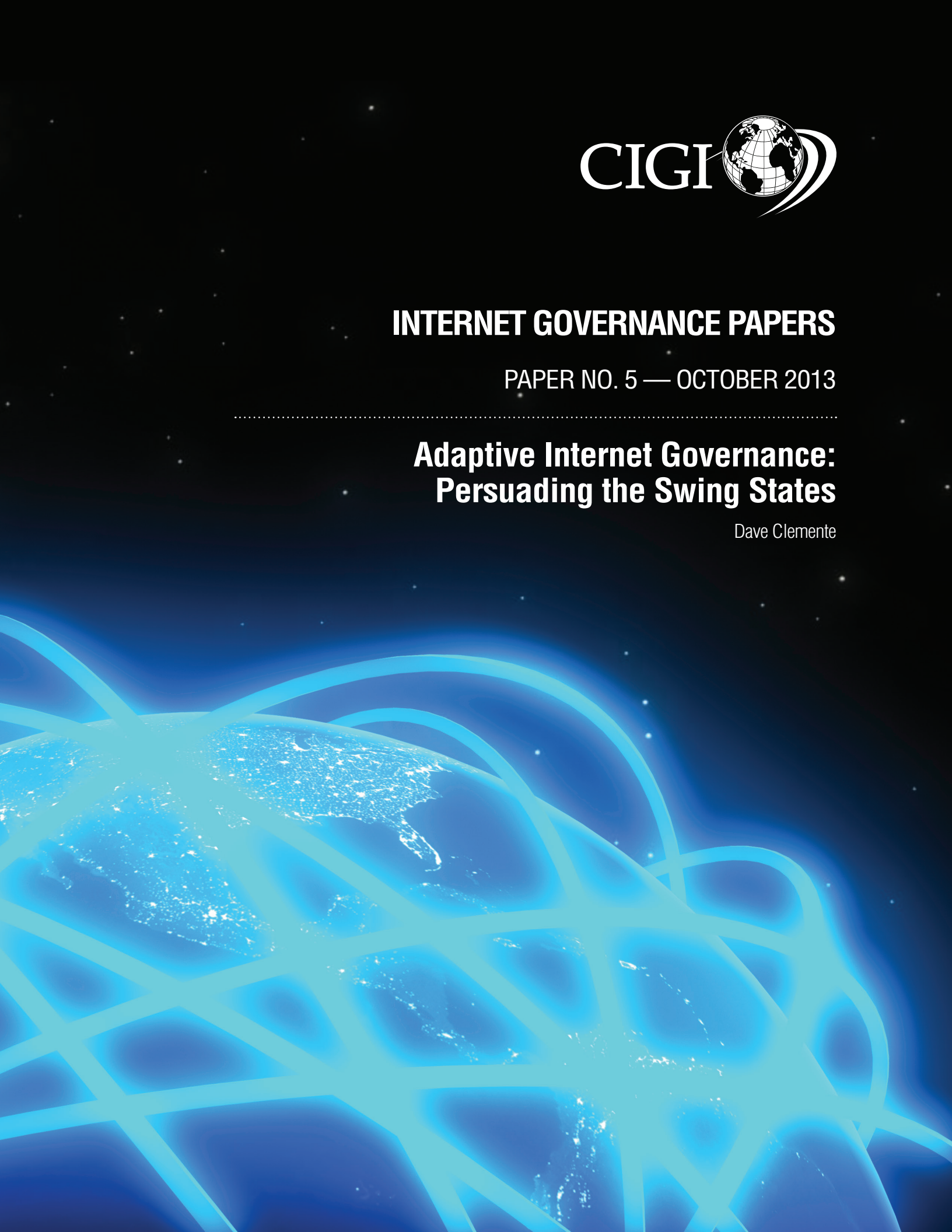

INTERNET GOVERNANCE PAPERS

PAPER NO. 5 — OCTOBER 2013

Adaptive Internet Governance: Persuading the Swing States

Dave Clemente

INTERNET GOVERNANCE PAPERS
PAPER NO. 5 — OCTOBER 2013

Adaptive Internet Governance: Persuading the Swing States

Dave Clemente

ACKNOWLEDGEMENT

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

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

CONTENTS

ABOUT ORGANIZED CHAOS: REIMAGINING THE INTERNET PROJECT

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

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

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

ABOUT THE AUTHOR

Dave Clemente is a research associate in the Chatham House International Security Department. He has worked at the International Institute for Strategic Studies and the Overseas Development Institute, and his areas of expertise include technology and cyber security policy, and US and UK security and defence policy. He is the author of *Cyber Security and Global Interdependence: What Is Critical?* (Chatham House, 2013) and co-author of *Cyber Security and the UK's Critical National Infrastructure* (Chatham House, 2011) and *On Cyber Warfare* (Chatham House, 2010).

EXECUTIVE SUMMARY

The complexity of negotiating global Internet governance in the coming years presents states with multiple challenges. One primary challenge for liberal democracies is to adapt their current approach (that is, the multi-stakeholder model) while enhancing its legitimacy on the international stage. A model of governance that is perceived as legitimate and capable of maintaining a stable environment is more likely to be durable, as opposed to one that lacks the ability to adapt, thereby encouraging other actors to develop competing models.

Undecided nations — or "swing states" — will need to be persuaded of the value of adopting inclusive and open governance, rather than the state-led model advocated primarily by Russia and China. Governments, businesses and civil society around the world have a great deal riding on the outcome of this process, and it is important they too have a voice.

Between now and 2020, the ideological divisions between major Internet governance actors will become clearer, forcing undecided nations to begin choosing sides or developing separate positions, and precipitating a gradual fragmentation into blocs of aligned nations. Proponents of the multi-stakeholder (or equivalently open) model need to acknowledge and understand the political and economic motivations and constraints of the swing states, and use this understanding to develop a more robust and convincing argument in support of open and inclusive Internet governance.

INTRODUCTION

The Internet is a fundamental component of economic, social and political life around the world. It currently connects 2.4 billion people, or one-third of the world's population, and it is estimated that by 2020, 50 billion "things" will be connected to the Internet (Hesseldahl, 2011). The stable and flexible functioning of the Internet is increasingly important for developed and developing countries and their citizens.

The governance of this ecosystem has long been the concern of a select group of actors, but the number of interested parties, both state and non-state, is increasing as global connectivity spreads. At the state level, many of these actors could be considered swing states. They are unsure which mix of social, technical and political governance options is right for them, and are undecided about the appropriate combination of regional or international alliances.

If current governance mechanisms wish to maintain long-term legitimacy, they must take the concerns and desires of these new actors into account. This paper's thesis is that the dominant states in cyberspace, who also tend to be the most highly connected, must anticipate and prepare now for an extended, complex and contentious debate on Internet governance. The political and technical seeds of Internet fragmentation or Balkanization (that is, segmentation into "national" networks) are currently being laid, and reflect the state-led governance approach that many nations favour. Division of the global Internet along national lines is likely to increase, due to a combination of political and commercial motivations. This will involve strenuous efforts to protect intellectual property and control content (Sutton, 2012), along with policy initiatives that, for example, make country X a "safe place to do business online." It will also include increased controls, such as large-scale Internet filtering and surveillance, which are being implemented (often with little public debate) by states on all sides of the Internet governance debate.

Fracturing, to the extent it occurs, could conceivably take place at the content level, through increasingly high levels of filtering and restrictions, as opposed

to isolated "national Internets" that do not communicate with each other. Interoperability will remain essential among global financial markets, as very few countries choose to isolate themselves, although some may be excluded by the majority of states (for example, Iran and North Korea).

For the handful of dominant actors, major challenges to the relative power they enjoy lie ahead. As digital connectivity increases around the globe, the Internet is becoming inexorably less Western-centric, and this has significant implications for the norms and values that have implicitly guided its governance thus far. Western tech giants are gradually losing their relative dominance in the commercial space; consumers in Asia, for example, have more local alternatives to choose from. At a macro level, who defines what the "true" Internet really is, when China has far more online users than any other country?

If not by sheer weight of numbers (a stance that no longer serves the West), then by what metric will governance power be judged, and by whom? Does one vote per state, as in the United Nations (UN), for example, really make sense, when there is such disparity between states in terms of connectivity and online presence or "mass"? To what extent will models of Internet governance conform to other areas of international governance, and where are new approaches needed?

These are not easy questions, but this paper offers some suggestions on understanding, framing and taking action in the current environment. It offers a potential near-term governance scenario and analyses its international political implications. Some basic terms of reference are established before looking at the role of the state, a potential scenario and two premises that the scenario is based on. It concludes by offering some recommendations for understanding and influencing the undecided states.

GOVERNANCE BASICS

Internet governance can be broadly defined as "policy and technical coordination issues related to the exchange of information over the Internet" (DeNardis, 2010: 3). However, additional nuance is helpful, given the many contested facets of the domain. For the purposes of this paper, Internet governance can be divided into six themes: architecture-based intellectual property rights enforcement; the policies enacted by information intermediaries; cyber security governance; governance of routing and interconnection; Internet standards governance; and control of critical Internet resources (DeNardis, 2013: 3).

At a fundamental level, it could be said that the purpose of Internet governance, as with any kind of governance, is to balance domain stability with flexibility. In other words, to maintain a sufficient level of security such that the domain does not collapse, but not so much security that the "permissionless innovation" (or, at a minimum, the network neutrality interpretation of the end-to-end principle) of the Internet is allowed to wither.

The governance debate is taking place in an increasingly contested online environment, where social, economic and political norms are evolving and being challenged, and where emerging and developing states understandably wish to have a vote. Some of these states gravitate towards a particular camp, while others — the swing states — remain undecided and amenable to persuasion. All are likely to form alliances with other established and emerging Internet powers. They will do this out of political or commercial self-interest, and (to the extent other states constrain these interests) in order to reduce the chances of any state or group of states dominating the governance landscape the way the United States has for two decades.

The contours of the governance debate have been taking shape for years, and have become clearer as the resources in question (that is, connectivity and the supporting ecosystem) become essential for the functioning of governments, critical infrastructure and entire societies. The debate will play out against a backdrop of shifting economic and financial balances of power. These dynamics will reduce the extent of the global digital divide (that is, disparities in connectivity between developed and developing countries), and will diminish (although not eliminate) the relative technological strengths that Western countries currently enjoy.

THE STATE AND SOCIETY

It could be said that a realist posture is evident in much of the state discourse around Internet governance. Realism, as used in this context, posits that the international system is anarchic or lacking a unifying authority; states are the primary (and rational) actors; and these states will pursue their own self-interests, in particular security (Kreisler, 2005). This is challenged (or complemented) by liberal theories, which posit that state behaviour is guided by a desire for prosperity and a commitment to liberal values, and by constructivist theories, which assert that states are guided by the beliefs of their elites and social norms and identity (Walt, 1998).

While these theories view international relations through the prism of state actors or their elites, many other actors (for example, from the technical, economic or civil society communities) exert influence on Internet governance. These other actors may adopt perspectives that diverge significantly from that of their state, and herein lies a significant source of tension. While governments, many of whom are just waking up to the importance of Internet governance, tend to approach the debate from a hierarchical and geographic perspective, their technical, economic and civil society communities recognize the value in a decentralized network that is minimally constrained by geography.

It would, however, be misleading to merely accept an "exaggerated dichotomy," as described by Milton Mueller (2010), "between the extremes of cyberlibertarianism and cyberconservativism," or between non-state and state governance models. As noted by James Lewis (2012), "there are four centres of power in cyberspace — technical, economic, government and civil society. They don't fit together very well." This is undeniably a complicating factor for any actor group that attempts to exert influence on Internet governance. It challenges the internal coherence of states that espouse a strongly liberal democratic perspective on one hand (for example, the US State Department's Internet freedom agenda), while steadily expanding global Internet surveillance on the other hand (for example, the US National Security Agency's actions).

Notwithstanding challenges by non-state actors, states like to conceive of themselves as the dominant players in cyberspace. They regulate, or attempt to regulate, the behaviour of the technical, economic and civil society actors within and beyond their borders, and they approve operating licenses on the condition that companies comply with certain standards of service, tax and legal regimes, and lawful interception (a term that is contentious and subject to a wide variety of interpretations).

Yet despite this self-perceived dominance, the vast majority of states have historically given little thought to the governance of the Internet, content instead to implicitly or explicitly encourage greater digital connectivity. This may be because the initial highly connected countries were largely Western, and they (and their technical and commercial communities) shared similar or sufficiently compatible conceptions of public-private sector interaction and regulation. In addition, the balance of power has been anything

but balanced; the majority of large technology companies have emerged from the United States, further narrowing the range of perspectives.

Connectivity has, in many cases, snuck in through the back door, joining everything to everyone and doing so under the noses of policy makers around the globe, who are now realizing the social, commercial and political implications of a highly interdependent digital environment. At a number of "technologically concealed layers, coordinated and sometimes centralized governance of the Internet's technical architecture is necessary to keep the network operational, secure, and universally accessible. This governance is enacted not necessarily through traditional nation-state authority but via the design of technical architecture, the policies enacted by private industry, and administration by new global institutions. While these coordinating functions perform highly specialized technical tasks, they also have significant economic and political implications" (DeNardis, 2013: 2).

The Internet governance debate is becoming more politicized as a result of a growing awareness of these implications, and as governments realize the potential for exerting influence in and through the digital environment. Not all states are created equal in terms of competence, particularly when it comes to considering the second- and third-order consequences of their interventions in cyberspace. Some policy makers are willing to consider tampering with Internet protocols such as the domain name system in order to protect established economic and political centres of power (Hruska, 2011). For them, civil society tends to be an afterthought, except on the rare occasions when its mobilization is sufficient to create personal political difficulty (for example, proposed US Stop Online Piracy Act/Protect IP Act legislation), or when it can be instrumentalized for political purposes (for example, online "activism" and the Arab Spring).

INCREASING STATE ADAPTATION

States are beginning to better understand how to calibrate levels of control and compulsion on the Internet. They are slowly but steadily developing internal bureaucratic processes and response mechanisms to deal with decentralized, adaptive and technologically assisted challenges to their power. In other words, they are adapting to the disruptive qualities inherent in highly networked societies.

There is a growing realization that highly distributed networks serve a purpose greater than the dissemination of cute cat pictures or adult material. In addition to connecting critical infrastructures, they also empower civil society actors to publicly expose the gaps between state rhetoric and reality. This ability for collective or individual action to embarrass or subvert governments should be acknowledged as a motivating factor for many policy makers when they plaintively ask, "can't you just make us a general-purpose computer that runs all the programs, except the ones that scare and anger us? Can't you just make us an Internet that transmits any message over any protocol between any two points, unless it upsets us?" (Doctorow, 2011). The simple answer is "no," although it won't stop some policy makers from trying to get to "yes," fragmenting the Internet in the process.

Swing states are asking these same questions, and wondering how they can simultaneously increase connectivity and maintain control over a domain that does not (yet) map neatly or consistently to sovereign borders. If stewardship of the Internet can be defined as actions that go beyond self-interest, or a "custodial, non-proprietary relationship to a resource or domain" (Hurwitz, 2012: 1), then it is clear that stewardship does not come naturally to

states. States such as China advocate a very different model of stewardship, whereby "the state agencies claim their authority to control a national cyberspace as part of caring for the society as a whole" (Hurwitz, 2012: 5).

The challenge, then, is to either scale up the multi-stakeholder model to accommodate new actors or to replace the model with something that can attain a higher degree of effectiveness and legitimacy. It is not clear what an alternative model would look like, but any replacement should seek, at a minimum, to improve on both counts. It is an understatement to note that the question of what constitutes legitimacy is complex and difficult, although it could be defined as popular acceptance of existing authority structures.

The current model of governance has scaled effectively at the technical level, although its political foundations are increasingly challenged, and it is here where the most significant challenges will arise. A model that has effectiveness without international legitimacy (the trend of the current model) or international legitimacy without effectiveness (proposed alternatives such as a UN-led model) would be short-lived.

It will require a multi-faceted and patient strategy to "persuade the rest of the world of the virtues of an alternative, civil society-based, non-sovereigntist distributed governance model" (Mueller, 2012). These efforts will meet with significant challenges, and states that may side with the United States on other areas of international governance may be willing to balance against the United States on Internet governance, at least temporarily, in order to extract political or commercial concessions. This is not a far-fetched scenario, given the high level of market penetration that Western tech giants enjoy around the world, and the desire of emerging countries to develop and protect their own tech sectors.

Current efforts to link the International Telecommunication Union (ITU) more closely to Internet governance appear to be driven more by desires to diminish US influence than by a desire to develop a model that can generate global legitimacy. These goals, however, are not mutually exclusive. Rejectionism of US influence (social, political and economic) in the digital domain could sit comfortably alongside a desire to develop a more widely accepted model of Internet governance.

Many governments that rhetorically support proposals for greater ITU influence also "lack critical mass in the Internet economy and, because most of them are authoritarian, have little popular appeal even in their own territories" (ibid., 2012). Given the current trajectory of expanding global connectivity along with increasingly clear ideological differences between major state actors, what might the current situation look like in 2020, and what are the resulting pros and cons?

SCENARIO: GRADUAL FRAGMENTATION AND ALLIANCES OF CONVENIENCE

As regionalization and fracturing of the Internet becomes a more prominent topic for *political* discussion, it is likely to be felt first in the *commercial* space. This can already be seen with regional and national geo-fencing (that is, restricted access) of digital content, and the way in which national borders are making their presence felt in cyberspace (for example, legal jurisdictions of cloud services).

States are naturally tempted to champion and protect their own tech giants, even when this goes against their long-term interests in spurring innovation. A restriction of market diversity, for example, the US government-sanctioned monopoly that was AT&T, results in greater ecosystem stability but also inertia (Wu, 2010). By reducing the number

of interdependent actors, this market consolidation also facilitates government intervention and control (for example, surveillance), and is the antithesis of the diversity and disruption that the Internet thrives on.

The political and economic implications of actions taken by a few states, but which impact many states (for example, large-scale surveillance) are likely to accelerate commercial fracturing and disruption, particularly involving the development of alternative products and services for individuals, businesses and governments who are increasingly aware of the value of data, and by extension, the value of privacy. On balance, this increased diversity is a positive outcome, except from the perspective of the states whose capacity for surveillance is eroding due to self-inflicted overreach.

At the political level, disagreements and tensions between nations are spilling more frequently into cyberspace. For better or worse, depending on one's perspective, this permits more vocal participation by non-state actors who are increasingly active online (for example, nationalists and activists), which, in turn, puts pressure on political leaders to "do something."

As the number of autonomous and semi-autonomous actors proliferate, it is becoming more difficult for any actor or group of actors to exert control in cyberspace. Policy makers have to consider how best to preserve the benefits provided by the current governance model, while adapting it to a truly global environment. The positions of the main actors are fairly settled, but many swing states remain unknown quantities. If Internet governance settles into two binary camps (that is, top-down and bottom-up models), then the current model will be put under significant strain.

Alliances of convenience, perhaps issue-based, are a more likely outcome given the diversity of nations on the international stage, and may give the existing multi-stakeholder model more time to adapt. The model has shown the ability to adapt to disruption, yet more adaptation is required, and possibly more than it is currently capable of handling. This scenario of gradual fracturing and (at least initially) loosely coupled alliances is based on two main premises.

Premise One: It's the Economy, Stupid

The political manoeuvring of states in relation to Internet governance will depend, to a significant degree, on the economic benefit they currently derive or wish to derive from greater connectivity. Open Internet architecture and protocols have made possible an immense outpouring of social and economic creativity, which citizens in developing countries will want to experience for themselves.

For many of them, the discussion revolves less around security and more around (greater) connectivity. Rather tellingly, proposals to re-engineer the Internet en masse for greater security tend to be made by military and intelligence officials, who desire greater levels of control and situational awareness. " For proponents of the multi-stakeholder model, Internet prosperity may prove a more effective rallying cry than the current emphasis on Internet freedom. Such an approach would need to be more mindful of the economic losses suffered by many states as a result of a move from circuit switching to VOIP [Voice over Internet Protocol]. Arguments that the loss of direct revenues to governments can be more than compensated for by the longer term benefits to be expected from an expansion of Web based services may be valid but are unlikely to resonate with corrupt officials" (Inkster, 2012: 3).

The prosperity narrative is not only for Western domestic consumption. It is being exported elsewhere, as the commercial focus of major technology companies, which includes hardware and software providers, as well as organizations that deliver non-digital products but are reliant on cyberspace to function, shifts eastward. As countries such as China and India gain "mass" in the Internet economy (which could be loosely defined as online products and services), this power shift will be used to extract Western commercial concessions in the Internet governance space.

In the Chinese example, an expanding middle class will drive increased domestic consumption, which in turn will produce a more valuable online population that companies around the world will seek to access ("Bottoms Up," 2013).

Premise Two: Erosion of Digital Unipolarity

Western state and non-state actors maintain near-monopolistic power in most aspects of the Internet (for example, protocols and content) — at least this is how many non-Western countries view the situation, and it contains more than a grain of truth. Whether this dominance has developed through consumer consensus (that is, non-Western consumption of Western products and services), evolutionary processes (that is, "first-mover" market advantage), power politics or a combination of these or other factors is an important question.

Methods of challenging or changing this power distribution will vary widely according to the root cause. Relative Western dominance is likely to gradually erode as connectivity spreads around the globe, providing regional or national alternatives to current products and services. Newly connected states will also have more options for collaboration in order to balance against political, economic or social monopolies of power, and nuanced strategies are needed to adapt Internet governance in response.

It should also be noted that it is not just governance of the Internet that presents significant challenges. Gaining international consensus is extremely difficult on issues such as climate change, narcotics and people trafficking, and sustainable global financial models. Over the last century, the dramatic growth in the number of sovereign states has made all areas of international governance more difficult. There are simply more actors and therefore greater difficulty gaining substantive agreement on any (even mildly contentious) issue. As noted by Randall Schweller (2010):

> The modern state system became fully defined with the completion of decolonization in the mid-1960s. It was then that the world — every territorial inch of it — was composed of states and nothing but states. The process of increasing entropy in international politics, therefore, commenced a mere forty years ago — a relatively short time period in the larger scheme of things. In international politics, the fewer the constraints on state behaviour, the greater the level of entropy. This is why much of our current state of randomness can be laid at the doorstep of unipolarity, which has shown itself to be an "anything goes" international structure.

Washington policy makers are finding that unipolarity does not yield the benefits and unfettered flexibility they had hoped, though one suspects that recent military expeditions did little to prolong the unipolarity that may have existed. External challenges such as the economic and military rise of China have

been overplayed in Western political and popular narratives, perhaps reflecting insecurity and fears of decline. The Chinese government is often framed by Western states as a unitary and cohesive actor, when the domestic reality is far more fractured and acrimonious. This narrative also tends to overlook the degree to which China's growth remains inextricably linked to economic growth in other major countries. This interdependence discourages the possibility of full-scale armed hostilities between major powers, pushing competition instead into the economic arena.

ENGAGING NEW ENTRANTS

There is, therefore, a need to make a more convincing economic argument in support of an open Internet and, at the same time, develop a robust counter-argument to those that may be swayed by China's "adaptive authoritarianism" ("China's Internet," 2013). This stance should remain flexible, and be capable of customizing the argument for the economic position of a given swing state.

These swing states may be lightweights in the "Internet economy," but this can be an inappropriate and inaccurate measure of progress, depending on the country in question. Some widely touted examples of this metric show that consumption, at least in the G20, is a significant proportion of the Internet economy, as opposed to government spending, investment or exports (Dean et al., 2012). But how much of this is just pre-existing economic activity displaced onto the Internet? How convincing is it to tell a developing country that it must increase consumption to have a vibrant Internet economy?

Many countries that favour the multi-stakeholder model also lean towards a more liberal form of government. They already have an appreciation for the benefits that a vibrant civil society can bring to the country. Their governments also tend to have a higher threshold for tolerating internal dissent, relative to the states that favour top-down Internet governance.

Appeals to liberal democratic ideals and personal freedom will resonate with some swing states, but others will remain unpersuaded, and rent-seeking opportunism will abound. Issues of human rights are also likely to arise, particularly around online surveillance and privacy. It is here that Western states can improve transparency, in particular regarding legal processes surrounding data collection and interception, and an individual's right of redress to these activities.

There is a need for more transparency in the decision-making processes of the Internet Corporation for Assigned Names and Numbers (ICANN) and its Government Advisory Committee. It has also been suggested that ICANN could strengthen its legitimacy "via a unilateral Declaration of Independence from any government" (Inkster, 2012: 3). This is a bold proposition, yet it may be necessary to halt or forestall the emergence of rival governance models.

In addition, the United States should not squander its first-mover advantage in cyberspace. It could harness the energy in the Internet governance debate to build a coalition of like-minded or similarly motivated actors (both state and non-state) to preserve and improve upon the current model. This process would likely benefit from being rhetorically separated from the contentious debates over "cyber warfare" and espionage, to reduce the range of negotiated items to a manageable set.

Opposition to the multi-stakeholder model lacks a convincing narrative regarding alternative options. In addition, recent fears of an ITU-led UN takeover of the Internet are overblown. Indeed, one struggles to find examples of the United States going against

any of its significant political or economic interests in order to satisfy the ITU. The 2012 World Conference on International Telecommunications (WCIT) may have changed some political positions, but "the operation, governance and use of the Internet has not changed one bit. Nor will it change as a result of the WCIT, because the ITU has utterly no leverage over Internet standards, Internet operations, Internet Protocol number resources or domain names. Which demonstrates clearly just how tangential to Internet governance the whole WCIT process was to begin with" (Mueller, 2013).

Fragmentation into blocs of aligned nations may well take place outside the ITU, through regional political and economic forums and trade negotiations. The ITU could serve as a venue for identifying and gathering "like-minded" states that support a national sovereignty model, before migrating into more localized or issue-specific venues. Protocols and functions may be revealed as a secondary concern for states, used instead as tools for advancing their primary concerns — consolidation of political and economic power, as well as enhancement of social "stability" (for example, through regulation of content and behaviour).

None of this suggests that the dominant state actors in the multi-stakeholder model have a considered strategy for accommodating emerging actors, or indeed any strategy other than the perpetuation and entrenchment of the status quo. Understanding the concerns and constraints of developing countries in relation to Internet governance would be a good start. This requires engagement and a listening ear, qualities that are not always in evidence. At a 2013 speech on the future of Internet governance, Neelie Kroes, vice-president of the European Commission responsible for the Digital Agenda, pointed out that distrust of the multi-stakeholder model is growing. She suggested some potential reasons why some countries take a dissenting viewpoint:

> It is time for diplomats to realise the importance of the Internet. To prevent a major backlash, we should understand the real reasons why such countries take the positions they do. Maybe they don't have the right capacity or expertise. Maybe they feel threatened by, distanced or disenfranchised from the Internet. Maybe they see the whole issue as too complex and interrelated. We need to engage and convince those people of the merits of a distributed approach to Internet policy-making. Because the alternative could end up being an Internet that is broken up along national lines. (Kroes, 2013)

While supporting a model of open and transparent governance is laudable, this description of the "other" side is condescending. Its perspective is that states that are leaning away from Western models of Internet governance are essentially poor, scared or dumb. It lauds the virtues of the multi-stakeholder model, yet completely discounts rational actors who may understand their options very clearly and still choose another path.

The topic of Internet governance will be viewed by many states through a nation-state lens. They may have trouble believing the multi-stakeholder model is genuine, and that the United States and other Western nations do not also view Internet governance through a state-dominated lens. In many cases, they would be correct to note that highly connected countries support the multi-stakeholder model in principle, as long as it does not challenge their economic or political interests.

This disconnect has been echoed in discussions on other areas of tension, with Chinese disbelief at US government statements that it does not sanction state-sponsored economic espionage. In some ways, this betrays a mistaken belief that Washington (or any other major centre of power) can muster near-omniscient and hyper-efficient levels of coordination:

> This is the most pervasive of all Washington legends: that politicians in Washington are ceaselessly, ruthlessly, effectively scheming. That everything that happens fits into somebody's plan. It doesn't. Maybe it started out with a scheme, but soon enough everyone is, at best, reacting, and at worst, failing to react, and always, always they're doing it with less information than they need. That's been a key lesson I've learned working as a reporter and political observer in Washington: No one can carry out complicated plans. All parties and groups are fractious and bumbling. But everyone always thinks everyone else is efficiently and ruthlessly implementing long-term schemes. (Klein, 2013)

Laying suspicions of scheming to one side, Western hypocrisy regarding Internet freedom and cyber security does not help to assure wavering governments of genuine Western buy-in to the multi-stakeholder model.[1] This matters in multilateral fora such as the WCIT, where the United States could find itself in the position of being out-voted, or at least of having its authority challenged openly and with increasing regularity. Governments who are undecided on Internet governance are likely to have the perspective that the United States can afford to make noises in support of the multi-stakeholder model, because it also controls the fundamental Internet protocols. The reality of US control is largely irrelevant, as long as the perception dominates the international narrative surrounding Internet governance.

This does not mean that the United States or its liberal democratic allies should be held to unreasonable standards of unflagging consistency. But it does mean that Western policy makers must realize that their global cyber power is diminishing relative to emerging powers. This is true in soft power terms such as cultural influence, but also hard power such as the ability to regulate technology giants (which have largely sprung out of Western countries). It is certainly true for the United States, whose Internet governance agenda has suffered thanks to revelations

---

1 According to Hurwitz (2012): "the United States has financially, rhetorically, technologically, and selectively supported 'cyber stewardship' as part of its foreign policy. In its policy-makers' views, this aid helps the US gain influence, increase its cultural attraction, bolster Internet freedom for its own sake, and in some cases, promote regime change at a low cost. Such aid may have unwittingly contributed to Mubarak's downfall, but the US has not reproached its allies Saudi Arabia and Bahrain for their very restrictive Internet policies. The policy can also clash with other American efforts to shape the cyber commons. While the US State Department criticized China's blocking access to sites, the US Congress considered legislation that would require American service providers to do the same to foreign sites alleged to serve pirated movies and music. The targets of this sponsored stewardship can thus easily accuse the US of hypocrisy in promoting cyber rights."

of large-scale surveillance of global Internet traffic by the US National Security Agency.

These sort of glaring inconsistencies will have consequences, and may influence states that are sitting on the fence between a national sovereignty model of governance and the more diffuse multi-stakeholder model. It also sets a very poor example for states that are looking to enhance control over their domestic networks. Many of them will look to the United States as a model, and emulate increasingly close public-private sector collaboration, in what is now a "security industrial complex reaping the economic windfall of the cyber security market in an era of otherwise economic austerity" (Deibert, 2013).

CONCLUSION AND RECOMMENDATIONS

The legitimacy of the multi-stakeholder model will be called into question with increasing frequency in the coming years, and is likely to precipitate a gradual fracturing of the current model. Wholesale replacement is unlikely, given the political and economic costs that would be required. Those participating in the governance debate would be advised to be realistic regarding the adaptability of the current model, given the challenges it will face in the coming years.

Despite putative US leadership, many parts of the Internet lack, and indeed resist, a unifying authority. This loosely coupled model with minimal centralization is, on balance, a good thing. The challenge remains then, to convince swing states to lean towards the current model or a close variant. These states may naturally lean towards a state-centric model of governance, but value the benefits of being seen to embrace civil society and non-state actors.

There are many ways of attracting these states, but the most durable arrangement will likely take the longest to implement. It will come through patient diplomacy, demonstrating the complementarity between liberal democracy and social and economic prosperity, and a nuanced understanding of the swing states' political and economic constraints. Many developing countries and regions have yet to extend online connectivity beyond their elites, and expansion of the Internet will challenge entrenched notions of control, propriety and "stability."[2]

Several research questions emerge from this analysis. First, there is a need for more robust examination of the supposed causality between digital connectivity and economic prosperity, and this should look beyond the G20 towards developing economies. Second, it would be worth looking at how technological disruption (beyond Wu's US-centric examples) has influenced and forced the evolution of governance regimes in other parts of the world, and at the international level. Third, an analysis of the trade-offs between information and communications technology-enabled prosperity and political stability could usefully situate states along the spectrum of completely closed or completely open models of connectivity (polar opposites that no major state currently occupies). This would provide a more nuanced explanation of the potential options facing policy makers.

Just because parts of the Internet governance problem have digital roots does not mean the whole problem is new or novel. If "Internet governance" was replaced with "climate change," many stumbling blocks would appear wearily and worryingly familiar. However, this is no reason for despair. Advocates of an open Internet with minimal

2 Barnett and Duvall (2005) suggest that "analysis of power in international relations, then, must include a consideration of how social structures and processes generate differential social capacities for actors to define and pursue their interests and ideals."

centralized governance would be advised to adopt strategic patience and adhere to principles. In the words of Winston Churchill, "this is not the end. It is not even the beginning of the end. But it is, perhaps, the end of the beginning" (Churchill, 1942).

WORKS CITED

Barnett, Michael and Raymond Duvall (2005). "Power in International Politics." *International Organization* 59, no. 1: 42.

"Bottoms Up: Consumption in China May Be Much Higher than Official Statistics Suggest" (2013). *The Economist*, March 30. Available at: www.economist.com/news/china/21574503-consumption-china-may-be-much-higher-official-statistics-suggest-bottoms-up.

"China's Internet: A Giant Cage" (2013). *The Economist*, April 6. Available at: www.economist.com/news/special-report/21574628-internet-was-expected-help-democratise-china-instead-it-has-enabled.

Churchill, Winston (1942). "The End of the Beginning." Speech at the Lord Mayor's Day Luncheon at the Mansion House, London, November 9.

Dean, David et al. (2012). *The Connected World: The $4.2 Trillion Opportunity: The Internet Economy in the G-20*. The Boston Consulting Group, March. Available at: https://publicaffairs.linx.net/news/wp-content/uploads/2012/03/bcg_4trillion_opportunity.pdf.

Deibert, Ronald J. (2013). "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace." Working paper presented at April workshop at CIGI. June 28 revision.

DeNardis, Laura (2010). "The Emerging Field of Internet Governance. "Yale Information Society Project Working Paper Series. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1678343.

DeNardis, Laura (2013). *Internet Points of Control as Global Governance*. Internet Governance Papers No. 2. August. Waterloo: CIGI.

Doctorow, Cory (2011). "Lockdown: The Coming War on General-purpose Computing." Boing Boing. December. Available at: http://boingboing.net/2012/01/10/lockdown.html.

Hesseldahl, Arik (2011). "Cisco Reminds Us Once Again How Big the Internet Is, and How Big It's Getting," All Things D, July 14, https://allthingsd.com/20110714/cisco-reminds-us-once-again-how-big-the-Internet-is-and-how-big-its-getting/.

Hruska, Joel (2011). "How SOPA could actually break the Internet." ExtremeTech, December 19. Available at: www.extremetech.com/computing/109533-how-sopa-could-actually-break-the-Internet.

Hurwitz, Roger (2012). "Taking Care: Four Takes in the Cyber Steward." Cyber Dialogue 2012: What Is Stewardship in Cyberspace? University of Toronto, March. Available at: http://ecir.mit.edu/images/stories/Cyber-steward.pdf.

Inkster, Nigel (2012). "Panel 2: Alternative Modes and Challenges Posed by States to Western Governance." Cyber Norms Workshop 2.0. September. Available at: http://citizenlab.org/cybernorms2012/panel2summary.pdf.

Klein, Ezra (2013). "What China's Hackers Get Wrong about Washington," *The Washington Post*, February 25. Available at: www.washingtonpost.com/blogs/wonkblog/wp/2013/02/25/what-chinas-hackers-get-wrong-about-washington/.

Kreisler, Harry (2005). "Balancing American Power in the Post-9/11 World — Conversation with Stephen M. Walt." Institute of International Studies, UC Berkeley. November 15. Available at: http://globetrotter.berkeley.edu/people5/Walt/walt-con3.html.

Kroes, Neelie (2013). "Stopping a Digital Cold War." Speech given at a round table event on the Future of Internet Governance, European Parliament, Brussels, February 28. Available at: http://europa.eu/rapid/press-release_SPEECH-13-167_en.htm.

Lewis, James (2012). "Highlights from Cyber Dialogue 2012: What is Stewardship in Cyberspace?" University of Toronto, September 19. Available at: www.cyberdialogue.ca/2012/09/highlights-from-cyber-dialogue-2012-what-is-stewardship-in-cyberspace/.

Mueller, Milton (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge: The MIT Press.

——— (2012). "ITU Phobia: Why WCIT Was Derailed." Internet Governance Project December 18. Available at: www.Internetgovernance.org/2012/12/18/itu-phobia-why-wcit-was-derailed/.

——— (2013). "Let's Keep This Dead Horse Alive, So We Can Beat It Some More." Internet Governance Project, January 28. Available at: www.Internetgovernance.org/2013/01/28/lets-keep-this-dead-horse-alive-so-we-can-beat-it-some-more/.

Schweller, Randall L. (2010). "Ennui Becomes Us," *The National Interest*, January. Available at: www.readperiodicals.com//201001/1930036301.html.

Sutton, Maira (2012). "Special 301 Report 2012: The USTR's Bogus List of Countries That 'Don't Enforce' Copyrights." Electronic Frontier Foundation, May 2. Available at: www.eff.org/deeplinks/2012/05/special-301-report-2012-ustrs-absurd-list-international-disappointments.

Walt, Stephen (1998). "International Relations: One World, Many Theories." *Foreign Policy*, no. 110. Available at: http://links.jstor.org/sici?sici=0015-7228%28199821%290%3A110%3C29%3AIROWMT%3E2.0.CO%3B2-3.

Wu, Tim (2010). *The Master Switch: The Rise and Fall of Information Empires*. New York: Knopf.

ABOUT CIGI

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

CIGI's current research programs focus on four themes: the global economy; global security; the environment and energy; and global development.

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

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

CIGI MASTHEAD

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