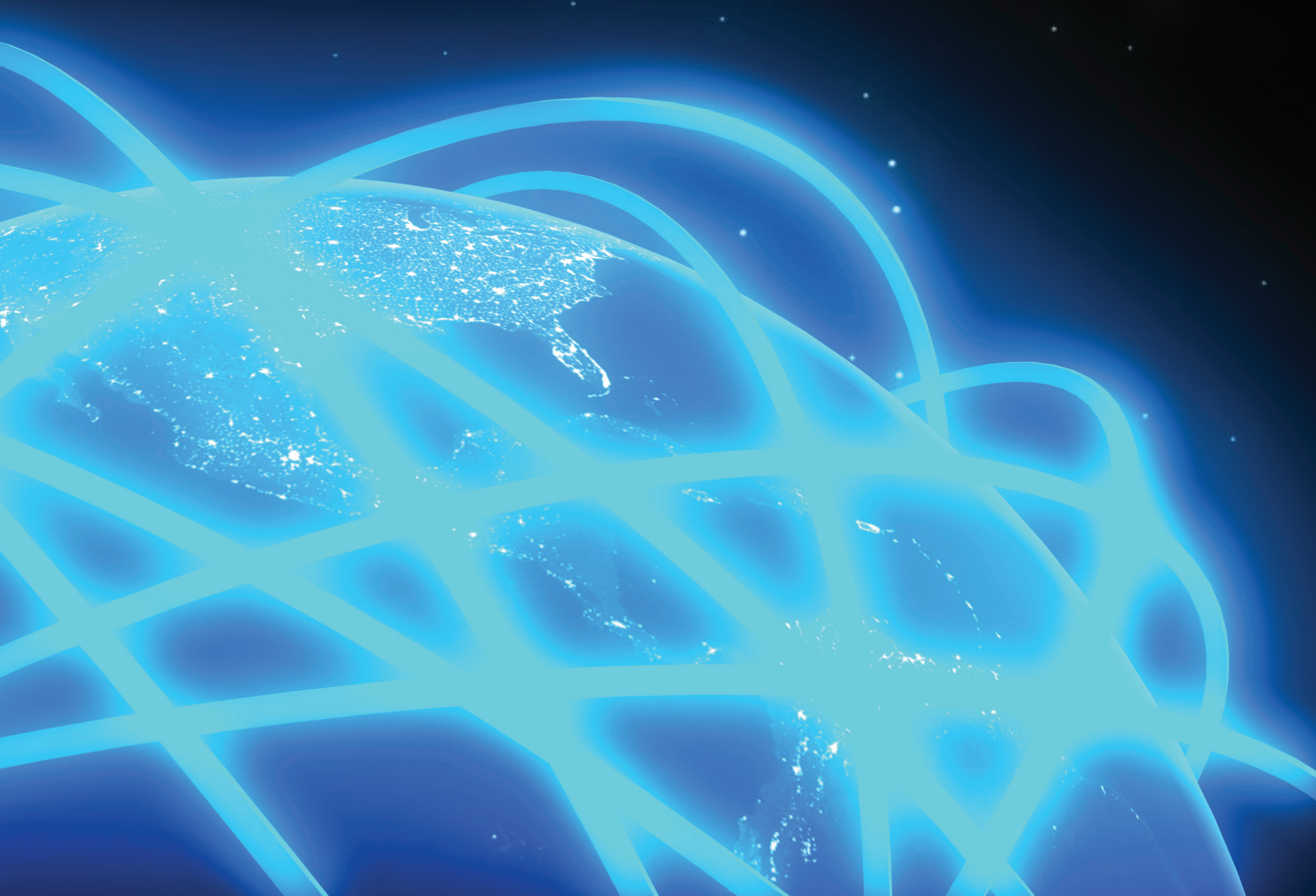
CIGI

INTERNET GOVERNANCE PAPERS

PAPER NO. 4 — OCTOBER 2013

Internet Governance: Inevitable Transitions

James A. Lewis



INTERNET GOVERNANCE PAPERS

PAPER NO. 4 — OCTOBER 2013

Internet Governance: Inevitable Transitions

James A. Lewis

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of The Centre for International Governance Innovation or its Operating Board of Directors or International Board of Governors.

Cover and page design by Steve Cross.

ACKNOWLEDGEMENT

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

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

James A. Lewis is a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies (CSIS), where he writes on technology, security and the international economy. Before joining CSIS, he worked at the departments of state and commerce as a foreign service officer and as a member of the senior executive service. His government experience includes work on Asian politico-military issues, on conventional arms transfers and on technology transfer. He led the US delegation to the Wassenaar Arrangement Experts Group on advanced civil and military technologies and was the rapporteur for the United Nations 2010 Group of Government Experts on Information Security. He was assigned to US Southern Command for Operation Just Cause and to US Central Command for Operation Desert Shield.

James has authored more than 90 publications at CSIS. One series of reports explores the relationship among technology, innovation and national power. Another series examined the role of space in national security. He is an internationally recognized expert on cyber security whose work includes the bestselling *Securing Cyberspace for the 44th Presidency* (CSIS, 2008), which was praised by US President Barack Obama in his first speech on cyber security. James is the US lead for a long-running track II dialogue on cyber security with the China Institutes of Contemporary International Relations. He is frequently quoted in the press and has testified numerous times before Congress. He currently teaches at Johns Hopkins University and has been on the faculties of Georgetown and George Washington universities. His current research examines international security and governance in cyberspace, the relationship between innovation and technology, asymmetric warfare and the effect of the Internet on politics. James received his Ph.D. from the University of Chicago.

EXECUTIVE SUMMARY

The current approach to Internet governance is politically untenable because it lacks legitimacy in the eyes of many new Internet users. Legitimacy is a central issue for Internet governance.

The source of legitimacy in the existing governance model was technical expertise. This is now being displaced by political processes. While the current, informal multi-stakeholder model must be transformed, both trade and political pressures could distort any outcome. What will replace these processes remain unclear, and there is real risk that any transition could lead to an Internet that is less free, less innovative and less valuable to the nations of the world.

To be stable, a new governance system must be able to manage a global infrastructure. This will require technical expertise and perhaps new institutions, but most importantly it will require the consent of the international community. A new model must find the balance between government and private sector, between US and global, and between sovereignty and human rights. These choices are not mutually exclusive, but will be shaped by competing concepts for international security, human rights and economic systems. A clear division of labour among the multi-stakeholder community that explicitly recognizes where governments must play a leading role would be a useful and achievable first step.

INTERNET GOVERNANCE: INEVITABLE TRANSITIONS

The concept of "governance" entails a range of processes. It refers to the understandings, expectations and institutions for making rules and enforcing them, and on an international level, it refers to the provision of a framework for relations among states and their citizens to provide predictability in their interactions. Governance need not involve the participation or control of national governments, but some issues, such as security, are reserved for states.

The current approach to Internet governance is inadequate for what has become a critical global infrastructure. The existing approach to governance relies on largely informal processes among technologists and the business community. These informal processes are politically untenable because they lack legitimacy in the eyes of many new Internet users, are weakly linked to larger international processes for law enforcement and security, and can be perceived as a US construct designed to advance narrow US interests.[1]

To date, Internet governance has involved the interplay between technical and commercial interests, with the guiding principle being to preserve the interconnectedness of the Internet and the compatibility of things that connect to it. In these areas, the current multi-stakeholder model has been a tremendous success, allowing billions of devices to connect easily, quickly and reliably at a fraction of the cost of telecommunications services. Where the model has not done well, however, is in questions of security. The multi-stakeholder model also faces growing political challenges

[1] See Mark Raymond and Gordon Smith (2013), *Reimagining the Internet: The Need for a High-level Strategic Vision for Internet Governance*, CIGI Internet Governance Paper No. 1, July.

(irrespective of performance), driven largely by the shift of global influence — from the transatlantic nation (particularly European states) to emerging powers — and by the questioning of the legitimacy of existing universal standards, particularly the Universal Declaration of Human Rights. The Internet has become a source of instability in international relations — partly because of its growth, and partly because of its mélange of governance arrangements. These aspects drive governments to seek change.

Legitimacy — derived from the consent of the governed when they accept and acknowledge authority and assent to its rules — is a central issue for governance. The current model for Internet governance lacks an adequate process to obtain the consent that is necessary for legitimacy in that it has neither adequate representation nor the tools of coercion. Non-Western participants could reasonably point out that they did not consent to the existing model, and that being invited later to join is not the same thing as being involved in its drafting. The greatest challenge to the legitimacy of the existing multi-stakeholder structure is its failure to make the Internet more secure.

Technical expertise was the source of legitimacy in the existing governance model, but this is now being challenged and displaced by interstate political processes. Greater legitimacy for Internet governance will require a closer connection to national governments and, perhaps, to the United Nations (UN). For most nations, the UN is the source of legitimate international governance. Its members are the de jure (and, in most instances, the de facto) legitimate representatives of their societies. One great failing of the current self-appointed Internet governance model is that it lacks legitimacy in the eyes of members of the international community.

What will replace the current multi-stakeholder model remains unclear; both trade and political pressures could distort any outcome. There is a real risk that any transition could lead to an Internet that is less free, less innovative and less valuable to the nations of the world. Those nations that fear the political effects of the Internet will attempt to use any transition in governance as an opportunity to promote policies that restrict human rights. As other nations promote alternative governance models, there is a risk that we will lose the idea of the market guiding technology rather than governments, and that the openness and global access to information of the current approach will be curtailed.

On the other side of the governance debate, there is an understandable reluctance to change a system that has worked so well and so quickly to create global connectivity. The resistance to any serious change by multi-stakeholder incumbents, however, increases discontent among new, non-Western Internet users and has created an opportunity to "re-architect" the Internet in ways that would diminish democratic values.

But there is also real opportunity to create a framework that accommodates both greater security and continued growth. Describing what could replace the old model is difficult. While many actors are involved, with varying degrees of influence on outcomes and with very divergent views, there is a growing international consensus that cyberspace must be governed like other global services, by a web of relations and commitments among nation-states.

Nations no longer accept the 1990s-era model that cyberspace is a borderless global commons. As they shed this perception, nations seek to extend their sovereignty into the governance of the Internet. The pioneering perception of the Internet's "terrain" foreclosed certain policy options; however, as Internet users and governments discard this perception, these options come back into play. The risk in this extension of sovereignty is that there are increasing challenges to the values of openness, free access to information and free speech. If cyberspace is not a commons[2] and must become like other global infrastructure, what rules and institutions best achieve this?

We should not think of this transition as a Manichaean struggle, but instead as a continuum of outcomes, with one extreme favouring a heavy government presence and control, while the other gives greater preference to private actors and an informal system of governance. A new model of Internet governance will fall somewhere between these extremes. The strength of ideas will determine the balance between government and private stakeholders, along with the state of international politics and the negotiating skills of participants. One way to guide this transition is to clearly identify where governments must play a greater role (most likely in trade, security or law enforcement), where the private sector should lead (in technology, development, standards and commercial arrangements) and where there are areas of ambiguity, such as the treatment of content or in control of the domain name system.

THE NEED FOR STRENGTHENED GOVERNANCE

Internet governance as it exists now draws heavily on the experience of the 1980s and 1990s. The commercialization of the Internet came after a wave of telecommunications deregulation and the breakup of state-centric monopolies that began in the 1980s. The positive effects of telecom deregulation shaped thinking about how to govern the Internet. One source of the opposition to change is a fear that the stodgy, oligopolistic world of telecom will replace the more vibrant Internet economy. We should not dismiss this fear as groundless. While some nations would like an Internet that is more amenable to government control of content, many others would like an Internet that duplicates the telecommunications arrangements for fees and payments (such as the "sender pays") that would stand Internet economics on its head and reshape international connectivity in troubling ways.

Concepts about the future of international relations from the immediate post-Cold War period also shaped Internet governance. The current model for Internet governance is an artifact of this period, when it appeared that liberal market democracy (and the values associated with it) had finally triumphed over authoritarian and statist alternatives after decades of conflict, and had become a global norm. The expectation of a benign and consensual future shaped the political foundation for Internet governance and created a set of assumptions about how governments would behave, and how politics and economies would change.

Globalization describes closer, deeper and faster economic links among nations. Researchers and policy makers expected that globalization would make national boundaries irrelevant and erode the Westphalian state. A global community of non-state actors, including transnational corporations and civil societies, would manage this borderless global commons and assume many of the functions once exercised by governments.

These millennialist expectations were wrong. There is no consensus on market-based democracy, and states remain the most powerful international actors. New digital technologies create political challenges and may bring about long-term social change that could reshape how societies govern themselves, but the Westphalian state is adjusting to the new technology and reasserting its authority. National governments want a larger say in managing what

[2] See Mark Raymond (forthcoming 2013), "Puncturing the Myth of the Internet as a Commons," *Georgetown Journal of International Affairs*.

has become an essential global infrastructure upon which their economies depend and which has become the source of new and dangerous threats. As more nations become concerned with cyberspace, and as it grows in importance for the economic health of nations, governments will seek to expand their role at the expense of the existing multi-stakeholder community.

Nation-states will contend with a host of quasi-governmental organizations that provide organization and rules for cyberspace. These governance bodies have focussed largely on technical coordination to ensure continued connectivity, but they are of limited utility when it comes to the set of problems created by the transition of the Internet into a global infrastructure at the centre of trade and security. They lack both the authority and expertise to address the larger international issues involving trade, compliance with state commitments on universal rights, and security. Serious discussion of these issues largely takes place outside the existing Internet governance framework. These are traditional areas of government leadership, and we should not be surprised that governments are asserting themselves.

If there is a shared concern among nations, it is that the Internet has become a source of instability and risk in international relations. States will seek to act collectively to address these risks and to reduce instability, using existing mechanisms or perhaps creating new ones. The existing governance lacks both the authority and expertise to address the larger political economic and security issues between states; this is the impetus for change and it points in the direction of a greater role for governments.

THE MULTI-STAKEHOLDER MODEL

The core of the existing model of Internet governance is the multi-stakeholder model, a conceptual structure that arose from the informal, commercial and technical origins of the Internet. It is a 1990s business concept about how corporations manage their relationships with clients, suppliers and the public. The multi-stakeholder approach recognizes that the corporation's ownership and control must accommodate, to some degree, the concerns of the clientele — and a sense of ownership certainly seemed to have motivated the Internet Corporation for Assigned Names and Numbers's (ICANN's) original board.

Extending this business model to the contemporary iteration of the Internet creates areas of political ambiguity. For example, the stakeholder approach is inherently "top-down"; the majority of Internet users have no voice in governance debates — and little ability to select the voices that purport to speak for them. This undermines the multi-stakeholder model's legitimacy and authority. Unlike a corporation, which owns its assets and is responsible to both its owners and to national legal authorities for its actions, Internet ownership and responsibility are broadly distributed. As the Internet has become a global infrastructure, there are concerns among new participants over the perceived level of US control over Internet governance, and suspicion that the currently structured governance favours the commercial interest of the major Internet companies — also largely American.

By including a broader range of participants than would be the case if the Internet was purely a business activity or restricted solely to government participants, the multi-stakeholder model provides diversity and some degree of balance among competing interests. This is valuable and should be preserved, but in its current form, the multi-stakeholder model is too weak to meet the needs of global Internet governance.

Global growth in the number of Internet users means that the governance structure must accommodate an increasingly diverse community with values, cultural preferences and legal systems significantly different from those that informed the views of the first stakeholders. Initial efforts to contain and constrain these differing views led to the creation of governance institutions such as the Internet Governance Forum and the World Summit on the Information Society (both affiliated with the United Nations), but these groups have limited authority and, according to US officials, were intended primarily to provide a means to channel other nations' discontent with the multi-stakeholder model into harmless activities such as discussions in giant seminars that lacked any actual power.

The lack of a governance process integrated into the Westphalian framework of international law and practice among nation-states has serious implications for authority, stability and legitimacy. Some of the tension in the transition of Internet governance arises as governments displace the informal communities that dominated Internet governance through a gradual extension of control through various state — none of this is immediate, drastic or balkanizing, but the long-term trend is clear. The contest between governments and incumbent non-state stakeholders, who will seek to preserve their existing influence and control, will shape how Internet governance is transformed.

SOVEREIGNTY AND CYBERSPACE

Cyberspace is a physical and social construct that depends entirely upon a physical infrastructure. Such infrastructure is located within a sovereign territory or, in the very few cases where it is not (such as communications carried on undersea cables or satellites), it is still subject to sovereign control. Borders exist, which means that sovereign control can be applied to the infrastructure. The extent of sovereign control was initially obscured by the belief that cyberspace is a commons, that globalization would make borders and national governments increasingly irrelevant and that new models of governance would be required for this changed environment. The return of sovereignty means that the politics of cyberspace is in transition. There has been a fundamental revision in the political perception of cyberspace. This realization will shape international discussions of Internet governance.

The extension of Westphalian sovereignty into cyberspace has been incremental and gradual: a problem appears, the current multi-stakeholder approach fails to address it, and governments seek other solutions using their national authorities. There will be no rush to a global treaty, where the UN suddenly takes control of the Internet. Instead, nations will take steps to establish rules and penalties for behaviour on the Internet that are consistent with their national laws; over time this will aggregate into a new sovereign framework. Governments are unlikely to be involved in the day-to-day operations of the Internet, but they will put new rules in place for its operation. The process will leave proponents of the current governance structure confused and complaining as they are increasingly hemmed in by a range of national controls.

This extension of sovereignty is not the balkanization of the Internet — a pejorative term coined by defenders of the status quo. The definition of borders in cyberspace is no more a balkanization than the existence of borders in the physical world; only those who still believe in the one-world global commons could interpret this as such. There will still be a global network where the primary motives for design and architecture are commercial and the primary differences among nations will be over the treatment of content and expression. This extension is shaped by the larger debate over sovereign authority versus universal human rights, but it was naive to think that technology would trump politics and that nations would meekly surrender control to some US construct reflecting US values.

BALANCING NATIONAL SOVEREIGNTY AND UNIVERSAL RIGHTS IN CYBERSPACE

Another tension in the extension of sovereignty into cyberspace is an outgrowth of a larger international problem: the conflict between sovereignty and universal commitments. The sovereign rules without external interference, except in those areas where it has ceded authority — an evolution of the Westphalian model that is driven by the need for mechanisms to constrain its tendency towards interstate conflict. A range of international agreements on trade, warfare and human rights are cessations of sovereign authority in exchange for greater efficiencies or stability, but some nations are now uncomfortable with these agreements.

The most troubling aspect of this for Internet governance is the challenge that it presents to universal human rights. Many appear to have forgotten the reasons for creating the Universal Declaration of Human Rights. At the end of a devastating global war in 1945 that left millions dead, the newly established United Nations concluded that states that did not respect the rights of their citizens were also likely not to respect the rights of other nations. Diminished adherence to international commitments on human rights make the world less stable and increase the chances of war, but the issue of human rights protection is a likely fracture point for transitioning to a new model of Internet governance. The most difficult problem lies with the application of national laws to information and services that are made available on the Internet. As one Southeast Asian official explained at an Association of Southeast Asian Nations Regional Forum meeting, his country's culture and laws forbid pornography and online gambling, yet both are available over the Internet from sources in the United States, where such activities are legal. He asked why US law took precedence in cyberspace.

National laws should, in fact, apply to national networks. Countries are free to create restrictions, as long as they do not transgress their commitments to international human rights. But this approach is unsatisfactory for those governments that wish to restrict access to information. Some would prefer the extraterritorial application of content restrictions, through international agreement. The contest over how far to restrict access to information is a key tension in redesigning governance. The difficulty is in redefining and expanding the role of governments without sacrificing universal rights or creating an antagonistic or unfair cyber environment.

Held in Dubai in December 2012, the International Telecommunication Union's (ITU's) World Conference on International Telecommunications (WCIT) revealed divisions among nations that some found surprising. The WCIT made it clear that the existing open, multi-stakeholder model does not have broad support, but neither does this automatically mean the endorsement by a majority of nations of the Russian and Chinese alternatives for governance presented at the conference, which called for a central role for governments at the expense of other stakeholders. Most nations are "fence-sitters," undecided and still calculating which approach best serves their larger interest in development and economic growth. The WCIT showed the need for a new approach to governance and a positive agenda to retain support for the multi-stakeholder model.

Most countries remain undecided; they know there is a need for change, but are uncertain about what form this change should take. Nations are still calculating what approach to cyberspace best serves their larger interests in development, trade and security.

This means, in effect, there are three camps in the governance debates: Western nations, the authoritarians and the undecided — but the interests and concerns of these groups do not align. Western nations seek to preserve the multi-stakeholder model and resist efforts to reduce the role of the private sector in guiding the Internet. Authoritarian nations seek a greater degree of control over content, which may require attempting to change the Internet's architecture and protocols. The interests of the undecided are more complex. They are suspicious of the existing model and uncertain about the authoritarian alternative, but are largely united in their desire to see greater access to broadband services to drive development in their nations. It is likely that the governance model that best provides for economic development will win the broadest support.

Russia and China will continue to use the UN and the ITU as vehicles for advancing their shared vision of Internet governance based on sovereign control of what they sometimes call the"information space." Their views on the application of international law to the Internet are not necessarily consistent, however, particularly in regard to security. The International Code of Conduct for Information Security, proposed to the UN Secretary-General by China, Russia, Tajikistan and Uzbekistan, challenges the status quo by shifting the terms of debate in their favour, and providing an easy riposte to the charge that they are not serious about cyber security. The code reflects the larger international dispute over "universal" values. Russia and China want a reconsideration of international commitments that were originally developed in a time when the West had greater influence. They argue for the restructuring or reinterpretation of these commitments to increase the rights of the state vis-à-vis the rights of citizens. The code would amend the application of international law in cyberspace in this direction. In this, they are not alone — with support from some Arab states, Iran and other sympathetic regimes. Neither Russia nor China is likely to abandon the code until it becomes clearly untenable — which will only happen when there is a tangible alternative.

The response to this challenge by Western nations has been to assert that an open and free Internet, governed by a multi-stakeholder model and led by private interests, is best for prosperity and economic growth. But economic data is ambiguous when it comes to demonstrating that the Internet must be"open" to drive growth. Countries that are already tempted by the idea of sovereign control of informational resources note that a lack of Internet freedom has not stopped China from outpacing Europe and the United States when it comes to economic growth. The fundamental problem with the current defence of the multi-stakeholder arrangement is that it uses dubious commercial arguments to support a political outcome. It relies on an assumed link between the multi-stakeholder model, openness in cyberspace and economic growth. There is suspicion in non-Western countries that this is more a defence of existing business interests than a robust economic analysis.[3] Attempting to tie democratic values, commercial opportunity and security into a single package is unpersuasive and engenders increasing skepticism.

[3] See, for example,"Global Governance of the Internet Must Be Democratised!"for an exuberant account of this perception, available at: www.itforchange.net/civil_society_statement_on_democratic_internet.

MODERNIZING THE MULTI-STAKEHOLDER MODEL

Interoperability and connectivity through technical standards and protocols are the foundations of the Internet. The non-governmental processes that have worked so well to create the technical framework of the Internet face a challenge by those who wish to replace them with politicized or governmental processes. While there is general discontent with the existing governance structure and the emphasis it gives to non-governmental actors, the proposed authoritarian alternative to replace the multi-stakeholder model with the intergovernmental ITU and the Code of Conduct is entirely unacceptable, given the damage it would do to both human rights and the capacity to innovate in cyberspace. A new model for governance must give states greater weight in decision making, but it must also insulate technical processes and human rights from political interference.

Led by China and Russia, and reinforced by the ambivalence of other nations to the US-led multi-stakeholder model, alternative governance models would shift governance to the United Nations or a subsidiary body like the ITU. This approach would reduce the role of civil society and weaken the linkage between technology, governance and democratic values. Advocates of a more authoritarian cyberspace are determined to press ahead, and the lack of a coherent Western response has encouraged them. The idea that a UN body should provide governance for a global infrastructure is not in itself objectionable — this is how countries cooperate in most other transnational issues — but the push for a greater role for governments through the mechanism of the UN is also associated with a political agenda aimed at eroding universal human rights.

Describing what could replace the old model requires a complicated balancing of many interests. There are many actors with varying degrees of influence on outcomes and divergent views. There is an understandable reluctance to change a system that has worked so well and so quickly to create global connectivity. Authoritarian regimes see the governance debate as a way to control domestic political risk and at the same time undercut US power and perceived technological dominance. The Group of 77 countries see the central issue for the governance debate as development and increased access to broadband services. We cannot expect to reconcile all of these views, but there is likely a way to accommodate them without sacrificing the beneficial aspects of the multi-stakeholder governance model.

Any proposal for a new governance model that seeks to preserve key elements from the existing structure — the idea of the market guiding technology development and innovation, of openness and global access to information, a worldwide web that connects all users — must avoid the dilemmas of the Council of Europe's Convention on Cybercrime. This cannot be a transatlantic initiative, nor can it start with only a "Western" core. Important fence-sitters such as India, Brazil and other new powers in Asia, Africa, the Middle East and Latin America must be engaged from the start. While they share, to a degree, the concerns over the transatlantic foundation of "universal" values, it should be possible to build a partnership with them because of their commitment to democratic values like freedom of speech. Essentially, they are more like the West than they are like authoritarian states; initial talks with India are promising. Building partnerships with the new powers may require flexibility and concessions on issues like Internet governance, where Brazil, India and others will listen to China and Russia absent a more compelling narrative.

Modernizing the current governance model must take into account the concerns of other nations, and adjusting to the extension of sovereignty will be an important element for building a more secure cyberspace. The key issues are defining the role of the UN (some nations feel that any governance structure outside of the UN umbrella lacks legitimacy), identifying those issues where governments should lead (such as those involving international security and cooperation among states) and those best left to non-governmental actors (most, if not all technical and commercial issues). An initial step is to acknowledge that the status quo is untenable and that modernization, rather than replacement, is necessary. The recognition of sovereignty in cyberspace moves Internet governance into the realm of existing state-to-state relations and commitments, and lets nations directly address the key economic, political and security issues we confront.

Precedents for new models will come from outside the Internet community. Perhaps financial services offer useful ideas for change. Money flows easily around the world, handled by thousands of private institutions and servicing millions of customers, yet with considerable government oversight to preserve stability and public safety. There are institutions, both governmental and private, that ensure the stable operations and rules to reduce risk and criminality. There are other precedents, such as the air traffic system, where governments do not operate airlines, but work with private companies in the International Civil Aviation Organization to develop the rules for safe flight. Other global infrastructures use a mix of public-private partnerships, rules and intergovernmental institutions (usually under the UN umbrella) to increase stability and reduce risk. These sectors have been able to create such governance models without throttling innovation or creating heavy-handed governmental controls on a global scale. This is the direction that Internet governance will need to move to meet the public interest.

TOWARD A NEW MODEL OF INTERNET GOVERNANCE

The current approach to Internet governance dates back to the dawn of the commercial Internet, when it was small in size, available to only a few nations and limited in its functions. It relies on a multi-stakeholder model and a series of non-governmental associations to provide for the technical underpinnings of the Internet. In this, the model has been very successful, but the multi-stakeholder approach as it is currently configured is inadequate for both international security and for providing the basis for understandings among nations on responsible behaviour in cyberspace.

The authoritarian alternative has some appeal, as many governments are increasingly reluctant to accept the limited role assigned to them for securing an essential global infrastructure upon which their economies depend and which has become the source of dangerous new threats. The multi-stakeholder model is losing support, but this does not mean an endorsement of an alternative model that would put at risk individual rights and Internet innovation. Most nations are undecided and still calculating which approach best serves their national interests.

The largest stumbling block for transition may well be the opposition of the current incumbents to accept any change. They fear the result of granting governmental authorities a greater role. In many ways, the most likely outcome of the governance debate is that existing bodies, such as the Internet Engineering Task Force, will continue to perform the functions they perform now. Other functions that no one currently performs would become the responsibility of governments.

The hardest issue might involve ICANN. Other nations greatly overestimate both the control that ICANN exercises over the Internet, and the US government's control over ICANN. A solution might involve a US decision to abandon some of the vestigial (and unnecessary) contractual elements it has with ICANN and an agreement to an expanded and more directive role for ICANN's Governmental Advisory Committee; however, both of these ideas face opposition from the United States' reluctance to surrender the illusion of control that its contracts with ICANN provide. Further, many incumbents are unwilling to subject ICANN's non-governmental leadership to greater government control.

Developing a coordinated international approach to a governance model will be difficult. The larger political context — with the rise of Asia, the decline (perhaps temporary) of Europe and the growth of assertive new powers that challenge Western cultural and political assumptions — means that any progress on Internet governance may require a degree of progress on reaching a new political consensus for international relations or, more likely, political accommodations that allow for stronger governance without major concession on key issues by any party. Defining how governance will work when there is only weak consensus on human rights, trade rules or security issues is essential for progress.

States do not yet have enough experience with Internet sovereignty to identify anything but very broad areas of common interests. Even this will be complicated, as newly powerful nations and increasingly important regional actors gain international influence and pursue their own interests. Many of these countries have different attitudes to the relationship between government, business and society. Many governments are concerned over the informal, non-governmental and limited nature of Internet governance, and object to confiding governance to a US non-profit corporation that is seen as unresponsive and erratic, and whose ties to the US government are unclear. These nations believe that the Internet is best entrusted to formal governmental bodies anchored in the United Nations. Given the sensitivities among the various communities concerned with Internet governance and the lack of serious discussion of what an acceptable UN-based approach would look like, this is a distant prospect, at best.

Just as opponents of change coined the pejorative term "balkanization" to influence public debate over the extension of sovereignty, they have also portrayed a greater government role in Internet governance as some sort of draconian change that would lead to a return of the state monopolies that once dominated telecommunications, bringing on a range of dire consequences from crippling innovation, consumer choice and other worthy actions. This rhetorical device is intended to defend the status quo. Every year since the end of the dot-com boom, there has been a steady erosion of the concept of the Internet as a unique, *sui generis* technology where normal rules do not apply. No other global activity — finance, aviation, shipping or trade — uses a similar approach to governance as the Internet. In these, governments set and enforce rules — often with a very minimal presence and usually with the participation of non-governmental actors — and companies create and compete within the context of those rules. As the Internet matures, its governance will move in the direction of these other global activities.

The political landscape points to outcomes where the multi-stakeholder model is modernized, made more globally inclusive and allows for the roles of the stakeholders to be rebalanced, so that governments gain a greater role in those areas of traditional governmental concern (security, trade and law enforcement). This is the direction that Internet governance will take, but there is no agreement on the institutional auspices these expanded governmental roles will be exercised to make cyberspace more secure and more stable.

A new model must find the balance between government and private sector, between US and global, and between sovereignty and human rights. These choices are not mutually exclusive, but will be determined by a test of influence in the international community among the competing concepts for international security, human rights and economic systems. A clear division of labour among the multi-stakeholder community that explicitly recognizes those issues where governments must play a leading role would be a useful and achievable first step. To be stable, the new system must be adequate to collectively manage a global infrastructure; this will require technical expertise and perhaps new institutions, but most importantly it will require global recognition that the new structure is legitimate, holding the consent of the international community to govern the Internet.

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

Managing Editor, Publications
Carol Bonnett

Publications Editor
Jennifer Goyder

Publications Editor
Sonya Zikic

Assistant Publications Editor
Vivian Moser

Media Designer
Steve Cross

EXECUTIVE

President
Rohinton Medhora

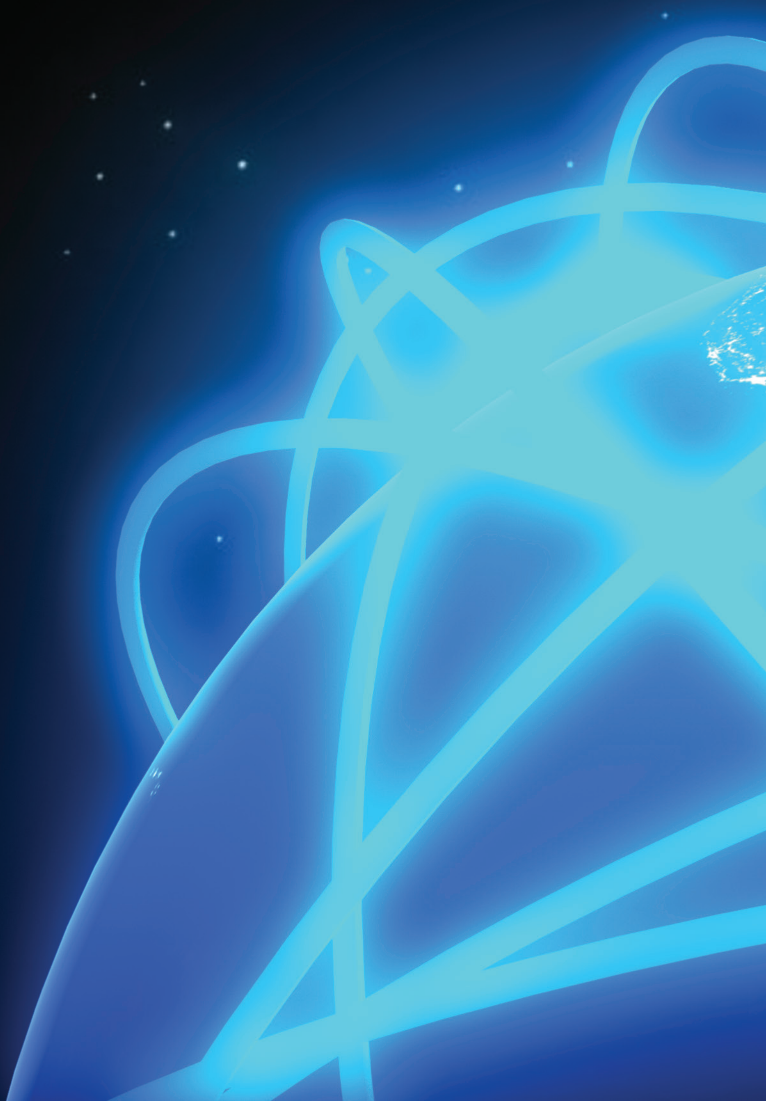
Vice President of Programs
David Dewitt

Vice President of Public Affairs
Fred Kuntz

Vice President of Finance
Mark Menard

COMMUNICATIONS

Communications Specialist
Kevin Dias
kdias@cigionline.org
1 519 885 2444 x 7238



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