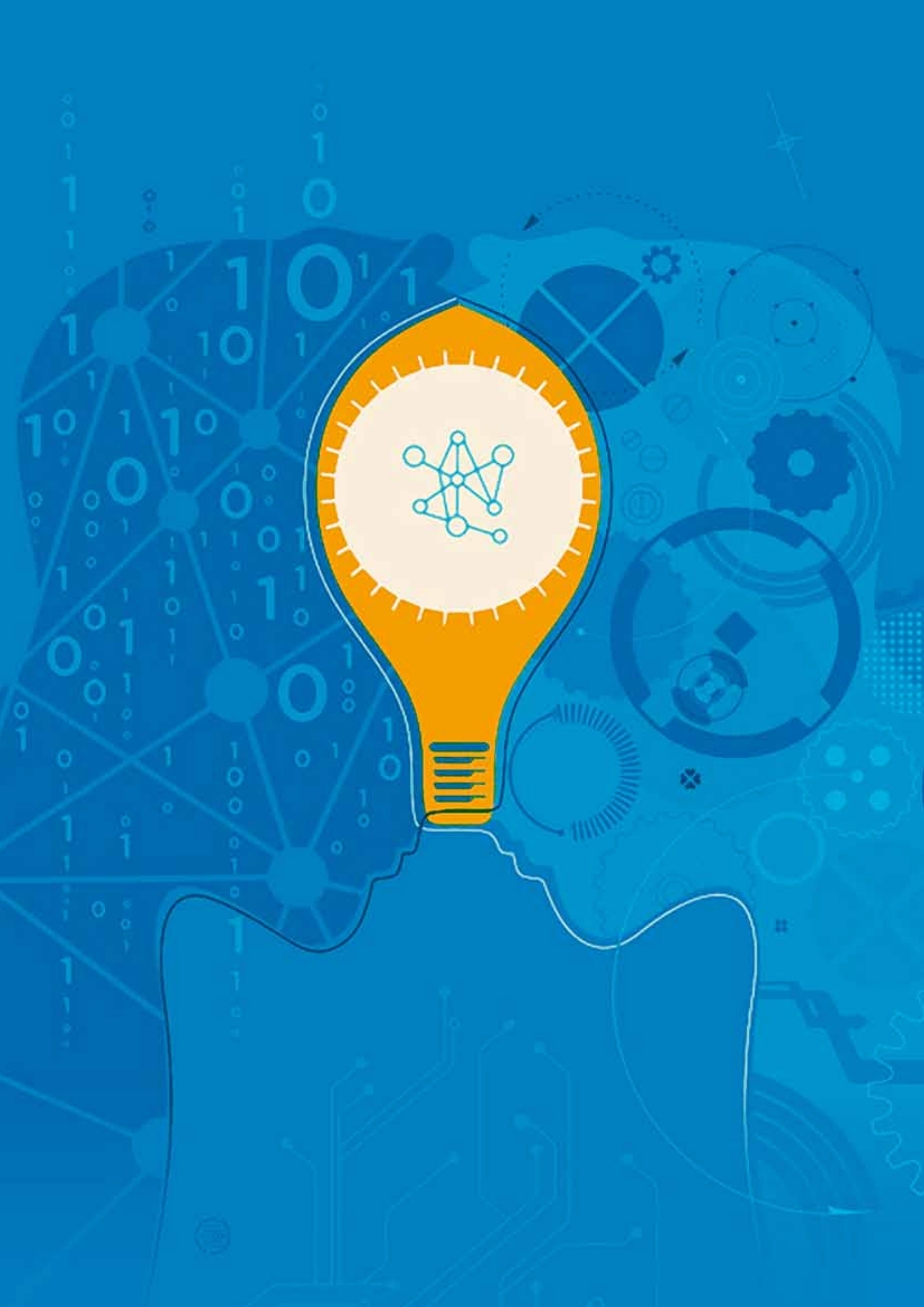
EastWest INSTITUTE

Exploring Multi-Stakeholder Internet Governance

Exploring Multi-Stakeholder Internet Governance

John E. Savage, Brown University
Bruce W. McConnell, EastWest Institute

January 2015



Exploring Multi-Stakeholder Internet Governance

Abstract

Internet governance is now an active topic of international discussion. Interest has been fueled by media attention to cyber crime, global surveillance, commercial espionage, cyber attacks and threats to critical national infrastructures. Many nations have decided that they need more control over Internet-based technologies and the policies that support them. Others, emphasizing the positive aspects of these technologies, argue that traditional systems of Internet governance, which they label "multi-stakeholder" and which they associate with the success of the Internet, must continue to prevail.

In this paper we explain multi-stakeholder Internet governance, examine its strengths and weaknesses, and propose steps to improve it. We also provide background on multi-stakeholder governance as it has been practiced in other fields for decades.

Three recommendations are made. First, echoing others, we propose simplifying Internet governance (IG) by partitioning it into issues that can be addressed by existing international agencies and those that cannot. The latter include naming, routing, security and standards. These are primarily technical issues but have a policy dimension. Second, for bodies handling technical or technically related issues, such as the Internet Corporation for Assigned Names and Numbers (ICANN), we recommend adding a multi-stakeholder oversight layer that can accept or reject opinions from these bodies but not alter them. Third, existing international agencies handling the other issues should be altered to receive Internet community input through multi-stakeholder consultative processes. With these changes IG can be made more comprehensive and manageable while protecting its most valuable characteristics.

Introduction

Interest in Internet governance (IG) has grown steadily since the creation of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998 and is now discussed at many international forums. The World Summit on the Information Society (WSIS), held in 2003 and 2005, was a landmark event. Paragraph 24 of the WSIS outcome document, the 2005 Tunis Agenda (WSIS, 2005), contains the following working definition of IG.

> A working definition of Internet governance is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.

The Secretary General of the UN created the Internet Governance Forum (IGF) as an offshoot of WSIS and has met annually since 2006. It provides an important venue for thousands of participants to share ideas on Internet governance but has no authority to make recommendations.

In 2013 the leading Internet organizations met in Montevideo (Akplogan et al., 2013) to warn against "the undermining of the trust

and confidence of Internet users globally due to recent (Snowden) revelations of pervasive monitoring and surveillance." They also "identified the need for (an) ongoing effort to address Internet Governance challenges, and agreed to catalyze community-wide efforts towards the evolution of global multi-stakeholder Internet cooperation."

One result of the Montevideo meeting was the April 2014 NETmundial: The Global Multi-stakeholder Meeting on the Future of Internet Governance (ICANNWiki, 2014) held in Brazil. It produced a set of principles and a roadmap for the evolution of the Internet that were endorsed by most participants, but not China, India, or Russia. They prefer a "UN-led, government centric approach to Internet governance" (Corwin, 2014).

One NETmundial Internet governance process principle states "Internet governance should be built on democratic multi-stakeholder processes, ensuring the meaningful and accountable participation of all stakeholders, including governments, the private sector, civil society, the technical community, the academic community and users."

The multi-stakeholder model is now widely touted as the Internet governance model of choice. The White House endorsed it in its 2011 International Strategy for Cyberspace, as did both houses of the U.S. Congress in late 2012. ICANN describes itself as multi-stakeholder (ICANNWiki, 2014) while the International Telecommunications Union (ITU) says in a backgrounder document published for the 2013 World Telecommunications Policy Forum (WTPF), "Through its Plenipotentiary Resolutions, the ITU membership recognizes the multi-stakeholder governance model based on the WSIS principles as the framework for global Internet governance" ("Supporting Multi-stakeholderism in Internet Governance," 2013).

Given the prominence that multi-stakeholder Internet governance has assumed, it is important to understand what the concept means, explore its strengths and weaknesses, and understand how best to implement it. It is imprudent for the world community to adopt this form of governance of a global resource as important as the Internet without first having a solid understanding of these issues.

Multi-stakeholder initiatives (MSIs) are attractive because they can provide an alternative between the extremes of laissez-faire policies and government regulation by enabling cooperation between NGOs and corporations in a form of self-regulation.

Unfortunately, there is no universally accepted definition of multi-stakeholder governance. The concept came into use as a vehicle for cooperation in the solution of societal problems, such as sustainability of natural resources and protection of workers in the developing world.

We now provide a brief history of Internet governance; report on studies of multi-stakeholder initiatives outside of the Internet; and examine the current problematic state of Internet governance (IG), how approaches to it might be simplified, and the possibility of its capture by the ITU. Finally, we give a detailed breakdown of IG issues and illustrate the simplification of governance by proposing allocations of individual issues to authorities. For the technical IG issues, we recommend that if a political layer be attached to an existing body, such as ICANN, that it protects technical judgments from modification by the political layer. For non-technical IG issues, we recommend the addition of a multi-stakeholder component to international bodies that take responsibility for an IG issue.

Brief History of Internet Governance

The Internet evolved from a packet-based communications research project funded by the (Defense) Advanced Research Projects Agency (DARPA) of the U.S. Department of Defense. DARPA-funded research projects in universities and research laboratories produced a new set of communication protocols for the interconnection of networks. Once the protocols emerged, a large variety of new applications emerged, thereby stimulating the growth of a new industry.

The original DARPA research project was very popular; computer science departments and research organizations clamored to be connected to the new network. Research on packet-based networking flourished as a result. By the early 1980s, the transition began from a research network to an operational one. At that point, DARPA allowed the Internet community to develop network technologies on its own via a new non-governmental entity known today as the Internet Engineering Task Force (IETF).

The creation of Internet technologies has been done largely in a multi-stakeholder fashion. Both the IETF and the World-Wide Web Consortium (W3C), which produces web protocols and standards, are of this kind. They operate in an open and transparent manner. All interested parties are invited to participate. However, to be a credible participant requires in-depth knowledge of the technologies in question.

The IETF has created an informal but well-articulated system to guide its work (2014). Its recommendations are recorded in thousands of documents called Request for Comments (RFCs) in honor of the first report by Steve Crocker (Crocker, 1969). One of these documents, RFC 7154, explains the IETF code of conduct, namely, that participants are expected to show respect and courtesy to one another, have impersonal discussions, come prepared to contribute, and work together to devise solutions for the global Internet. Because IETF welcomes everyone, it does not maintain a membership list.

The majority of IETF's RFCs contain recommendations for Internet technologies. They become de facto standards only if widely adopted by multiple vendors of products who write software and/or design hardware that conforms to the recommendations.

The members of W3C are enterprises and research organizations. Several hundred other standards development organizations (SDOs), including the ITU and the International Standards Organization (ISO), produce standards for Internet technologies via a variety of processes, many of which are consensus-based.

The open, inclusive, transparent and permission-less philosophy that has characterized the creation of Internet technologies has encouraged the participation of engineers in their development and that of users in the creation of web content.

A narrow definition of the Internet is the set of protocols that facilitate communication between networks. A broader definition and one that is widely used today is that it constitutes the communication protocols as well as the hardware, software, applications, the local networks, the security of the components and the system, the supply chain, and the legal, policy and political dimensions of the above.

It follows from this description that the Internet governance domain is very complex and has many players. What is remarkable is that, despite its size and complexity, it is reliably serving a population estimated at more than three billion users. In light of this, attempts to replace important parts of the current governance system must be done with great care. Another conclusion is that the Internet domain is likely too complex to be managed by one organization. It functions well because of the expertise that is distributed among the many players.

What is Multi-Stakeholder Internet Governance?

The term multi-stakeholder governance (MSG) came into use in the Internet arena around 2004. Markus Kummer, who served as executive coordinator for the IGF Secretariat, describes MSG as a vehicle "for policy dialogue where all stakeholders took part on an equal footing" via a process that is open, inclusive and transparent (Kummer, 2013). He also said that "While multistakeholder participation in the World Group on Internet Governance (WGIG[1]) and IGF meant and means that all stakeholders participate on an equal footing, it is also clear that in most organizations, whether intergovernmental or not, some structures are in place to facilitate decision-making processes" (Kummer, 2013).

Lawrence E Strickling, Administrator of the National Telecommunications & Information Administration (NTIA) in the U.S. Department of Commerce, in an April 2013 blog post he adds "consensus-based decision making" to the MSG definition (Strickling, 2013):

> "The Internet has flourished because of the approach taken from its infancy to resolve technical and policy questions. Known as the multi-stakeholder process, it **involves the full involvement of all stakeholders, consensus-based decision-making and operating in an open, transparent and accountable manner**. [Emphasis added.] The multi-stakeholder model has promoted freedom of expression, both online and off. It has ensured the Internet is a robust, open platform for innovation,

1 WGIG met between the Geneva and Tunis sessions of WSIS and provided guidance to the second session.

investment, economic growth and the creation of wealth throughout the world, including in developing countries."

These descriptions do not specify principles for the creation of multi-stakeholder organizations except to say that they should be open, transparent and inclusive. They don't specify how business is to be conducted except to say that "stakeholders participate on an equal footing" or that decisions are to be "consensus-based." These omissions call into question whether these descriptions of multi-stakeholder processes provide a sufficient basis on which to construct a global Internet governance system.

After several decades of experience with multi-stakeholder initiatives outside of the Internet, the political science community has begun to question whether self-regulation is sufficient to ensure the proper management of vital resources and protection of workers or whether a direct role for governments is warranted (Locke, 2013). This raises the question as to whether multi-stakeholder governance will suffice for Internet governance.

We now examine multi-stakeholder initiatives in areas other than Internet governance.

Studies of Generic Multi-Stakeholder Governance

Minu Hemmati (Hemmati, 2002) explains that multi-stakeholder processes (MSPs) have been used for decades to address problems in a variety of areas including biotechnology, corporate conduct, energy, gender inequality, tourism, labor, mining, paper and sustainability. She notes that MSPs inform decision makers on issues, generate support for decisions, identify solutions to problems and encourage stakeholders to take ownership of issues. It has been effective in many social, political, economic and technical contexts, especially when the problems that arise are new, fast changing and complex with important social and cultural dimensions. In these contexts, governments are typically slow to act. Through stakeholder engagement, MSG can quickly access the talent needed to address challenging new problems.

After studying 20 different multi-stakeholder processes, Hemmati (Hemmati, 2002) defines MSPs as "processes which aim to bring together all major stakeholders in a new form of communication, decision-finding (and possibly decision-making) on a particular issue. They are also based on recognition of the importance of achieving equity and accountability in communications between stakeholders and their views. They are based on democratic principles of transparency and participation and aim to develop partnerships and strengthened networks among stakeholders." She also says "MSPs cover a wide spectrum of structures and levels of engagement. They can comprise dialogues on policy or grow to include consensus-building, decision-making, and implementation of practical solutions. ... Hence, MSPs come in many shapes."

She also cautions that "MSPs are not a universal tool or panacea for all kinds of issues, problems and situations. They are akin to a new species in the system of decision-finding and governance structures and processes. They are suitable for those situations where dialogue is possible and where listening, reconciling interests and integrating views into joint solution strategies seems appropriate and within reach." Citing Kader Asmal concerning a debate over dams, she warns us, "More often, [than not] the process becomes a messy, loose-knit, exasperating, sprawling cacophony. Like pluralist democracy, it is the absolute worst form of consensus-building except for all the others."

Hemmati (Hemmati, 2002) observes that creating an MSP requires decisions concerning the secretariat, the physical support for the organization, funding, reporting and documentation, contact with the public, and whether and how there will be linkage into an official decision-making process. More specifically she notes that a wide range of decisions are needed including: a) identifying the issues to be addressed; b) deciding which stakeholders to invite; c) whether attendance is by invitation only, open to all or to a limited representation from each stakeholder group; d) setting timetables for action; e) preparing for meetings; f) communications between stakeholders, e.g. via the web or local, regional, or broader meetings; g) addressing power gaps between stakeholders as a result of expertise or access to funds; h) whether and/or how to make recommendations and/or decisions (is consensus required?); and, i) the conditions under which to terminate an MSP.

Vallejo et al. (Vallejo & Hauselmann, 2004) observe that many NGOs and business initiatives have emerged that deal with voluntary, non-state "standard setting, certification and labeling activities, collaborative arrangements for sector specific policy-making, supply chain management interventions, or ... codes of conduct. " While their analysis of multi-stakeholder initiatives is less comprehensive than Hemmati's, they observe that viability of such initiatives is strongly dependent on their legitimacy and efficiency. They cite Suchmann's 1995 definition of legitimacy as "a generalized perception or assumption that the actions of an entity are desirable, proper and appropriate within some socially constructed system of norms, values, beliefs and definitions."

In a thoughtful and insightful 2012 study van Huijstee (Huijstee, 2012) offers a strategic guide for civil society organizations (CSOs) who intend to participate in multi-stakeholder initiatives (MSIs) designed to encourage corporations to manage natural resources in a more sustainable manner. She provides advice concerning the assessment of personalities of CSO negotiators, priorities of the organization, strategies to employ in negotiations, and the importance of understanding the priorities of companies participating in the MSI.

CSOs are also advised to determine in advance what resources they will need to attend MSI meetings, which can be very expensive, and what knowledge and expertise will be needed. CSOs must also remain in contact with their constituencies in order to maintain legitimacy. She also advises CSOs to leverage their resources by working with like-minded CSOs. To be effective van Huijstee recommends that CSOs learn as much as possible about the businesses that they are trying to influence and reflect on the influence they can exert.

Van Huijstee also says that the possible role of governments needs to be understood. She says "MSIs are, by their very nature, instruments of civil (or self-regulation from the perspective of business)." "Government agencies may play an endorsing, convening, facilitating or financing role in MSIs, but often they will not be comfortable negotiating standards with CSOs or businesses." She also notes, "In the longer term, MSIs may serve as experimental mechanisms that start as voluntary initiatives but slowly get transcribed into governmental policies and regulation along the way."

One should ask how these observations, reflecting several decades of experience, can be incorporated in the newly proposed vehicles for multi-stakeholder Internet governance.

We turn now to an analysis of Internet governance.

The Scope of Internet Governance

Most proposals for multi-stakeholder Internet governance include too many topics. This is illustrated by the 2014 IGF Istanbul meeting. Discussions were held on access to the Internet, freedom of expression, child safety, privacy, the economics of the open Internet, IPv6 deployment, accessibility to IGF by persons with disabilities, the "right to be forgotten," gender issues, climate change, the Internet of things, human rights, public access to libraries, the mobile Internet, and a safe, secure and sustainable Internet. If Internet governance is to be manageable, the problem must be simplified.

In his preface (Kapur, 2005),Vint Cerf addresses this issue by saying,

> "With few exceptions, most of the public policy issues associated with the Internet lie outside the purview of ICANN and can and should be addressed in different venues. For example, spam, and its instant messaging and Internet telephony relatives ... are pernicious practices that may only be successfully addressed through legal means, although there are some technical measures that can be undertaken by Internet Service Providers (ISPs) and end users to filter out the unwanted messages. Similarly fraudulent practices such as 'phishing' and 'pharming' may best be addressed through legal means. Intellectual property protection may, in part, be addressed through the World Intellectual Property Organization (WIPO) and business disputes through the World Trade Organization (WTO) or through alternative dispute resolution methods such as mediation and arbitration."

Recently (Castro & Atkinson, 2014) many observe that progress on Internet policy

goals is more likely if the goals are classified by whether they have a local or global impact and whether there is universal agreement on a goal or not. One can group goals into categories and identify the points of agreement, disagreement and no opinion. In the first and third cases, countries are free to act. In the remaining case, nations should engage in negotiations with other nations if a local decision has a global impact.

We explore the disaggregation of Internet governance into separate topics below. Before doing that, we examine problems that others have with the state of Internet governance.

The Current State of Internet Governance

Multi-stakeholder governance engages stakeholders who bring their expertise and enthusiasm to bear either on the generation of new technologies or web content. Not only is this process more responsive than governments, it has been a driver of innovation and economic stimulation.

Nonetheless, we need to critically examine both the way it is perceived as well as its strengths and weaknesses.

Ambassador Philip Verveer[2] said the following about MSG at a panel at the Center for Strategic and International Studies (CSIS) entitled The Geopolitics of Internet Governance on May 23, 2013 ("Supporting Multistakeholderism in Internet Governance," 2013):

> "We really don't have a definition of the multi-stakeholder process. **I tend to think of it as a kind of ethos of inclusivity, which doesn't provide much other than guidance in terms of the notion.** [Emphasis added.] To the extent that inclusivity is possible, we ought to try to achieve it. But there are a lot of specific contexts where we have to try to come to a much better understanding about how we're going to enable participation and what the limits of broad participation may be."

As discussed below, the principal weaknesses in multi-stakeholder Internet governance are the following:

1. Absence of rules for multi-stakeholder operation,
2. A perceived lack of accountability,
3. Weak legitimacy in the eyes of many states,
4. Uneven engagement of stakeholders who are not technology providers.

Formal rules for running multi-stakeholder meetings don't exist for Internet governance. Although the IETF has stated norms for good behavior, their enforcement mechanisms are limited to reducing participation in working group mailing lists or peer pressure, punishments that are rarely invoked. This has been acceptable because the work of IETF is voluntary as are its "standards." If an individual cannot get a hearing for an idea at IETF, they can move to or create other forums where their views can be heard and a "standard" possibly adopted.

Although ICANN characterizes itself as multi-stakeholder, its bylaws do not provide rules for the conduct of multi-stakeholder meetings. No provisions exist to make motions or challenge nominations that emerge from the Nominating Committee, for example. This may be due to the discovery in the late 1990s that, as a California corporation, if a person has the right to vote in an ICANN election, he/she is a statutory member of the corporation and "can bring derivative actions against the corporation, and inspect accounts and records" (Mueller, 2002). Similarly, although the Nominating Committee selects 8 of the 16 members of the ICANN board and members for other ICANN organizations, it does not publish its selection procedures. Thus, on the central question of how individuals are chosen to run ICANN, the bylaws are silent. This contributes to ICANN's perceived lack of legitimacy.

ICANN operates under an Affirmation of Commitments with the U.S. Department of Commerce. It also is under contract with this U.S. agency for administration of the Internet Assigned Numbers Authority (IANA) functions. Other governments have criticized these ties between ICANN and the U.S. government. However, since U.S. is planning to relinquish its oversight of IANA functions, some of these criticisms may disappear.

Various governments have expressed opposition to the creation of Generic Top Level

2 Verveer served from 2009-2013 as the Coordinator for International Communications and Information Policy at the U.S. Department of State.

Domains (gTLDs) in the past– most recently, the French government concerning the recent awards of the .vin and .wine domains to Donuts Inc., a new registry. This concern appears to relate primarily to second-level domain names, a matter not yet settled.

Robin Gross of the Executive Committee of ICANN's Non-Commercial Stakeholders Group also challenges ICANN's accountability (Gross, 2014)

> "ICANN is undertaking public governance duties, but lacks important responsibilities that are typically attached to governance, like protection for basic human rights such as privacy, free expression, or due process. ... **Without additional safeguards, ICANN's corporate structure is ill-suited to meet the needs of a global governance organization**." [Emphasis added.]

Jim Lewis[3] comments on the legitimacy of Internet governance in general in a recent paper (Lewis, 2013).

> "**The current approach to Internet governance is politically untenable because it lacks legitimacy in the eyes of many new Internet users.**"
>
> "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** ... What will replace these processes remain(s) unclear ... **there is real risk that any transition could lead to an Internet that is less free, ... innovative and ... valuable to the nations of the world**."

For the purpose of this paper we define legitimacy in governance institutions to have three characteristics, namely, they are effective, accountable and aligned with their constituents' values and expectations.

- By **effective**, we mean good at delivering desired results, while minimizing undesired consequences. This characteristic assumes both agility and efficiency.
- By **accountable**, we mean the institution exhibits two traits, transparency and consequence.[4] Transparency means that its constituents, members, citizens, or their representatives, can see what is being done in their name. Consequence means there are predictable and consistent sanctions against bad behavior by those who exercise power in the name of the institution.
- **Alignment** with constituent values means embodying values and expectations that are increasingly commonly held, including inclusiveness, participation, and reciprocity.

Only when governance institutions demonstrate these characteristics will people put their trust in them and legitimize them. And, in the global village, legitimacy is becoming essential to government's successful fulfillment of its purpose.

Whether democratic or autocratic, national governments want a voice in Internet governance. Some nations are concerned about information security, that is, content that threatens state stability. Others are concerned about human rights, worrying that surveillance by states has gotten out of hand and that new restrictions are needed on information aggregators and search providers. Still others insist that freedom of expression is fundamental to realizing the full benefit of the Internet. For these reasons, the debate on Internet governance is engaged.

Concerning the last weakness, Les Bloom (Bloom, 2014) argues that "Major non-traditional critical infrastructure protection sectors in all countries need to be engaged in protecting the multi-stakeholder Internet governance model, and they need to be engaged now." He believes that if sectors, such as banking and finance, transportation systems and energy, were aware of current developments on Internet, they would analyze their impact on their business plans and that this would lead them to pressure governments to take more considered positions concerning Internet governance.

3 Lewis is Senior Fellow and Director, Strategic Technologies Program at CSIS.

4 Andreas Schedler refers to these traits as "answerability" and "enforcement." [Schedler, 1999]

Is Internet Governance at Risk of Capture?

As mentioned earlier, both ICANN and ITU refer to themselves as multi-stakeholder organizations. Because there is no international agreement on what constitutes multi-stakeholder governance, this opens a door to capture of Internet governance by the ITU.

Advocates for the ITU can argue that since 193 UN nations have voting rights in the ITU and it has more than 700 sector members and associates, it can more democratically manage the Domain Name System (DNS) than ICANN. The ITU clearly signaled its intention "to play the leading if not the sole coordinating role in all aspects of cybersecurity" in its 2008 Global Cybersecurity Agenda (Sofaer, Clark, & Diffie, 2010).

While ICANN has managed the expansion of the DNS to about three billion users without a major international incident, as mentioned above, its operations have been criticized for allocating gTLDs that have the potential to violate geographical indications and for a general lack of accountability.

While ITU has been effective in handling of radio spectrum and geostationary satellite orbit allocation, traditional telephony standards, and telecommunications development, it has many shortcomings. First, its meetings are generally closed and its reports are generally private except to fee-paying sector members or associates. In this regard, they are not multi-stakeholder, although this could change. Second, it has been criticized on the grounds that "its current internal structure provides no guaranty of professional control over the content of the standards the technical committees propose," unlike other technical organizations such as the International Civil Aviation Authority (ICAO) (Sofaer et al., 2010). Finally, the ITU is a treaty organization. If nations ratify treaties, they commit to implementing them. If the ITU were to control the Internet, it could decide that ratifying nations had to apply its standards. If non-ratifying States applied other standards, considerable unpredictability in core Internet operations could result.

What Internet Issues Need Governing?

As mentioned earlier, calls have been made by Cerf (Kapur, 2005) and Castro and Atkinson (Castro & Atkinson, 2014) to simplify Internet governance by allocating responsibility for individual policy issues to relevant organizations. On this issue Laura DeNardis says, "a question such as 'who should control the Internet, the United Nations or some other organization' makes no sense whatsoever. The appropriate question involves determining what is the most effective form of governance in each specific context" (DeNardis, 2014, p226). Joe Nye observes that a large cyber regime complex exists to address many issues that constitute Internet governance (Joseph Nye, 2014).[5]

Nye lists seven cyber related issues, namely DNS/standards, crime, war/sabotage, espionage, privacy, content control and human rights. Castro and Robert Atkinson (Castro & Atkinson, 2014) identify eight issues, namely content regulation, intellectual property, data, commerce, cyber crime, network operations, network performance, and equity and access. DeNardis (DeNardis & Raymond, 2013) lists six issues, namely control of critical resources, setting Internet standards, access and interconnection coordination, cybersecurity governance, information intermediation and architecture-based IP rights enforcement.

For discussion purposes, we have chosen to identify the following five policy topics:

1. Network Architecture
2. Content Control
3. Human Rights
4. Cyber Crime
5. Cyber Attacks

Network architecture refers to those issues that are central to the proper operation of the Internet; they include naming and routing, traffic management, network security, technical standards and trademarks. **Content control** includes privacy, filtering of data in transit (to prevent child pornography, spam or competing services, such as VOIP), security of data at rest and in motion, and data localization. **Human rights** include freedom of expression and belief, economic, social and cultural rights, the right to self-determination and devel-

5 A regime complex is a set of regimes each with its own set of norms.

opment, privacy, and surveillance. **Cyber crime** consists of any crime committed via the Internet including theft of intellectual property. **Cyber attacks** are actions via networks that cause serious damage to a nation, national interests, or critical national infrastructures. The latter are resources accessible via the Internet essential to the functioning of modern societies, such as gas, electricity, water, food, government and financial services, manufacturing, and medical facilities.

We now briefly examine each of the five policy topics mentioned above. Most of the international issues can be addressed in the Human Rights Council (HRC), the World Intellectual Property Organization (WIPO), the World Trade Organization (WTO), the ITU, or the UN General Assembly. In a few cases, notably that of network architecture, ICANN, suitably augmented, will suffice. Other venues include the regimes identified by Joe Nye (Joseph Nye, 2014), such as the G7, G20, and OECD, government groupings, and regional organizations, such as the Council of Europe and the Shanghai Cooperation organization.

Certainly there are Internet governance issues that are not addressed by any international body, such as security of the supply chain. For these, nations should try to either extend the mandate of existing organizations, such as the World Trade Organization, or create mutual legal assistance treaties (MLATs) for this purpose.

We recognize that many of these international organizations are not adequately prepared to deal with Internet-based issues. We also note there are organizations, such as the DiploFoundation, that help educate diplomats by offering courses in this area.

It is important to recognize that some Internet governance matters are primarily technical in nature and that carefully considered technical recommendations should either be implemented as proposed or not implemented at all. For example, Sofaer et al (Sofaer et al., 2010) examine ICAO as one of several models for Internet governance and consider it a model that should be considered for IG. ICAO regulates civil but not military aviation. Most importantly, in ICAO professionals retain control over standards, not the policy makers.

Other models for Internet governance on technical matters may be the International Labor Organization (ILO), which is being examined by the EastWest Institute, and the Red Crescent/Red Cross, which is being examined by the Bildt Commission.

Multi-stakeholder governance has been most effective in the development of the Internet. Thus, as Internet governance issues are disaggregated and allocated to new or existing organizations, a multi-stakeholder consultative function should be grafted onto them. Opportunities must be provided for the Internet community, broadly interpreted, to participate. This includes governments, civil society, business and academia.

Network Architecture

This topic concerns management of the DNS, which consists of allocation and de-allocation of gTLDs, management of the IANA functions, deciding whether some Internet traffic can be prioritized, routing operations, traffic management, network security, development of technical standards, honoring trademarks, and ICANN oversight.

Domain Name Management

While issues have arisen concerning Internet naming functions since ICANN's inception and some important ones remain, ICANN has been responsive, within its existing framework, to most of these issues. We explore ICANN oversight in the last subsection.

IANA Functions

An ICANN department manages the IANA functions. They include maintaining the list of parameters associated with protocols. This is not controversial and can be handled by ICANN, as it is done today. IANA also implements ICANN policy on the issuance of gTLDs to registries. This includes making an entry in the Root Zone with the approval of NTIA. Since NTIA intends to turn responsibility for overseeing the IANA functions to an outside multi-stakeholder organization, we offer no comments on this particular issue.

Traffic Management

Treating all traffic uniformly, hailed as "net neutrality," has an appealing ring to it. If applied zealously, it would prohibit giving priority to communications during emergencies and prevent certain techniques to protect against distributed denial of service attacks. This is a domestic issue for states to address. Similarly, while the "right to be forgotten" can be forced on companies by nations,

it is also a domestic issue.

Network Security

Security of DNS name resolution and Border Gateway Protocol (BGP) announcements are the responsibility of registries and ISPs. However, the behavior of domain name registries and ISPs should be guided by explicit norms. If norms don't adequately regulate behavior, treaties may be needed to control behavior.

Norms can help to ensure that operations conform to expectations (Hathaway & Savage, 2012). For example, when an ISP announces a path to one of its customers or to a neighboring ISP, it should either deliver packets sent via this path or explain to the sender why the packet stream cannot be delivered. Similarly, ISPs should agree to keep other ISPs informed of disruptions and/or important malware threats they discover.

Because no organization currently has responsibility for norms, either ICANN should be asked to take on this task or a new international organization created for this purpose.

Standards Development

Internet standards today are formulated in a satisfactory manner by more than 200 organizations worldwide, dominated by the IETF and W3C. Market forces determine adoption. It isn't necessary to change this system or supervise it unless it is abused, say through the deliberate corruption of standards. While many standards bodies coordinate their activities, conflicts do arise for which having some credible appeals body of senior cyber states could be useful.

Trademarks

Trademark issues that arise in domain name allocation can continue to be addressed in the current ad hoc manner or can be referred to the World Intellectual Property Organization (WIPO) if a generic issue is identified.

Oversight of ICANN

Calls for strengthening the legitimacy of ICANN can be addressed in several ways. First, a replacement could be created for the ICANN Independent Review Panel (IRP) process. This replacement should exhibit the qualities of transparency in its operating methods and independence in its membership. The range of issues over which the panel would have oversight could be circumscribed, but could include for example, the allocation and de-allocation of gTLDs and DNS and BGP standards proposed for deployment. A similar approach could be devised for managing the keys used in securing DNS and BGP, bolstering confidence in Internet security and encouraging ISPs to speed the deployment of DNS and BGP security.

Content Control

Ensuring privacy of communications is primarily a domestic issue. It becomes international when a nation asserts the right to command one of its domestic ISPs to make available private information held on computers within the territory of a foreign state. Such matters could be handled either in the UN General Assembly (UNGA) or via the World Trade Organization (WTO).

Nations are the first line of defense concerning the control of undesirable content, such as spam or child pornography. Cooperation in control of content is difficult when national values are in conflict, such as freedom of speech versus state security. When disagreements arise, the Human Rights Council is a good first place to air them.

ISPs can play a useful role in reducing spam. Often they can detect and help customers eliminate malware. If the volume of spam is high, it is in the ISP's interest to reduce it. Sharing of ISP best practices on such issues can be done via various organizations including, possibly, the Internet Society or FIRST, the incident response organization.

Securing data at rest, that is, in databases and clouds, is largely a private matter. Nations have a role to play when the data in question concerns a large fraction of its citizenry. Some insist on data localization. Securing data in motion is both a domestic and an international issue. It is domestic when the data transits only domestic networks. It can become an international issue when it crosses territorial boundaries, for example, when data is encrypted. In this case, the WTO may be the best venue.

Nations have an interest in protecting international communication resources on which they rely, such as the undersea cable systems, which carry more than 95% of the international Internet traffic. The ITU is an appropriate venue for this issue.

Human Rights

The Universal Declaration of Human Rights identifies the right of personal freedom of expression while noting that a person's freedoms may be subject to limitations to protect national security, public order or the rights and freedoms of others. This tension between expression and security arises in the Internet governance context particularly concerning content control.

Human rights issues can generally be decided either domestically or via the Human Rights Council (HRC). Some issues, such as surveillance, are both domestic and international. At the international level, UNGA may be the venue to address the latter.

Cyber Crime

Cyber crime consists of any crime committed via the Internet. It includes hate crimes, cyber bullying, child pornography, fraud, theft of cash and intellectual property, identity theft, unauthorized trespass, damage to hardware and software, data corruption, damage to physical systems controlled via the Internet, disruption of network traffic, and other similar activities.

Given the global reach of the Internet, each of these issues is both domestic and international. Although the Council of Europe Convention on Cybercrime is in effect in more than 40 countries, important countries, such as China or Russia, have not adopted it. Nonetheless, these countries do share some cyber crime information. Regional and international organizations, NGOs, SCO and UNGA committees are venues to further expand cooperation in this area.

Cyber Attacks

Cyber attacks are actions via networks that cause serious damage to a nation, national interests, or critical national infrastructures. The latter are resources accessible via the Internet that are essential to the functioning of modern societies, such as gas, electricity, water, food, and military, medical and emergency facilities. Given that a national economy can be severely damaged by a cyber attack, nations must take steps to reduce the risk of this occurring (Bloom & Savage, 2011).
To illustrate the importance of a cyber attack, we note that more than $10 trillion in financial transactions occur daily via undersea telecommunications cables and close to $5 trillion in the U.S. federal banking system daily. Compare this to the gross domestic product of the U.S., which was about $17 trillion in 2013. If either system were to be disrupted for a day, very serious damage would be done to the U.S. and world economies.

The UNGA First Committee is an appropriate venue to address these threats. Others include some of the regimes identified by (Joseph Nye, 2014), such as government groupings and regional organizations.

Conclusions and Recommendations

Internet governance is a topic in need of simplification and refinement. Following the lead of others, we recommend that it be simplified by disaggregating it into topics that can be handled by existing international bodies, such as the HRC, WIPO, WTO, ITU, CoE, as well as government groupings and regional bodies. If these organizations lack expert knowledge of the Internet, this can be remedied. Technical issues can largely be handled by technical organizations.

When existing organizations are handling Internet governance matters, we recommend that they invoke multi-stakeholder consultative units to seek the opinions of Internet stakeholders. However, since many technical and technically related issues have a policy dimension, we recommend the addition of a small carefully crafted oversight layer with limited authority to validate the technical or technically related decisions.

As suggested earlier, this additional layer would exhibit the qualities of transparency in its operating methods and independence in its membership. It would have the power to approve or disapprove, but not to modify, the technical or technically-related decisions of the technical organization.

The creation of this independent review layer could be undertaken by a small, multi-stakeholder body with representation from key state cyber powers supplemented by corporate, nonprofit and technical representatives. A key question will be whether states constitute a majority or a plurality.[6]

6 The Brazilian Internet Steering Committee (www.CGI.br) provides one model of this kind of body.

Bibliography

Akplogan, A., Curran, J., Wilson, P., Housley, R., Chehade, F., Arkko, J., . . . Jaffe, J. (2013). The Montevideo Statement on the Future of Internet Cooperation.

Retrieved from ICANN website: https://www.icann.org/news/announcement-2013-10-07-en

Bloom, L. (2014). What is at stake at Busan?, NetNod News (2), 13-15.

Bloom, L., & Savage, J. E. (2011). On Cyber Peace, Atlantic Council. Retrieved from their website: http://www.atlanticcouncil.org/publications/issue-briefs/on-cyber-peace.

Castro, D., & Atkinson, R. (2014). Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy, The Information Technology & Innovation Foundation. Retrieved from their website: http://www2.itif.org/2014-crossborder-internet-policy.pdf

Corwin, P. (2014). NETmundial Multistakeholder Statement Concludes Act One of 2014 Internet Governance Trifecta, Circle ID. (May 3, 2014). Retrieved from their website: http://www.circleid.com/posts/20140504_netmundial_multistakeholder_statement_concludes_act_one_of_2014/

Crocker, S. (1969). Request for Comment: 1, Host Software, IETF. Retrieved from their website: http://tools.ietf.org/html/rfc1

DeNardis, L. (2014). The Global War for Internet Governance. New Haven: Yale University Press.

DeNardis, L., & Raymond, M. (2013). Thinking Clearly about Multistakeholder Internet Governance. Retrieved from the Social Science Research Network, SSRN 2354377: http://ssrn.com/abstract=2354377

Gross, R. (2014). Comments on Enhancing ICANN Accountability, ICANN. Retrieved from the ICANN website: http://forum.icann.org/lists/comments-enhancing-accountability-06may14/msg00036.html

Hathaway, M., & Savage, J. E. (2012). Stewardship of Cyberspace: Duties for Internet Service Providers. CYBERDIALOGUE 2012, the Munk School of Global Affairs at the University of Toronton. Retrieved from their website: http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_hathaway-savage.pdf

Hemmati, M. (2002). Multi-stakeholder Processes for Governance and Sustainability: Earthscan Publishing.

Huijstee, M. v. (2012). Multi-Stakeholder Initiatives: A Strategic Guide for Civil Society Organizations, The Social Science Research Network, SSRN 2117933 Retrieved from their website: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2117933

ICANNWiki. (2014). Multistakeholder Model. Retrieved from the ICANN website: http://icannwiki.com/index.php/Multistakeholder_Model

IETF. (2014). The IETF Process: an Informal Guide, IETF. Retrieved from their website: http://www.ietf.org/about/process-docs.html

Joseph Nye, J. (2014). The Regime Complex for Managing Cyber Activities, The Global Commission on Internet Governance Retrieved from their website: https://www.ourinternet.org/

Kapur, A. (2005). Internet Governance: A Primer: Reed Elsevier, India.

Kummer, M. (2013). Multistakeholder Cooperation: Reflections on the emergence of a new phraseology in international cooperation, Internet Society. Retrieved from their website: http://www.internetsociety.org/blog/2013/05/multistakeholder-cooperation-reflections-emergence-new-phraseology-international

Lewis, J. A. (2013). Internet Governance: Inevitable Transitions (Vol. 4), The Centre for International Governance Innovation. Retrieved from their website: https://www.cigionline.org/publications/2013/10/internet-governance-inevitable-transitions

Locke, R. M. (2013). The Promise and Limits of Private Power: Promoting Labor Standards in a Global Economy, Cambridge University Press.

Mueller, M. L. (2002). Ruling the Root: Internet Governance and the Taming of Cyberspace: MIT Press.

Schedler, A. "Conceptualizing Accountability" The Self-Restraining State: Power and Accountability in New Democracies. Ed. Andreas Schedler, Larry Diamond, and Marc F. Plattner. Boulder and London: Lynne Rienner Publishers, 1999. 13-28.

Sofaer, A. D., Clark, D., & Diffie, W. (2010). Cyber Security and International Agreements, Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 179 - 206, National Academies Press. Retrieved from their website: http://www.nap.edu/openbook.php?record_id=12997&page=179

Strickling, L. (2013). Moving Together Beyond Dubai, blogpost, The National Telecommunications and Information Adminstriation. Retrieved from their website: http://www.ntia.doc.gov/blog/2013/moving-together-beyond-dubai

Supporting Multi-stakeholderism in Internet Governance. (2013). WTPF Backgrounder Series. Retrieved from the ITU website: http://www.itu.int/en/wtpf-13/Documents/backgrounder-wtpf-13-internet-governance-en.pdf

Vallejo, N., & Hauselmann, P. (2004). Governance and Multi-Stakeholder Processes, The International Institute for Sustainable Development. Retrieved from their website: http://www.iisd.org/pdf/2004/sci_governance.pdf

WSIS. (2005). Tunis Agenda for the Information Society, International Telecommunications Union. Retrieved from their website: http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

Acknowledgements

The first author is pleased to acknowledge many helpful conversations with Les Bloom on Internet governance.

—

The EastWest Institute seeks to make the world a safer place by addressing the seemingly intractable problems that threaten regional and global stability. Founded in 1980, EWI is an international, non-partisan organization with offices in New York, Brussels, Moscow and Washington. EWI's track record has made it a global go-to place for building trust, influencing policies and delivering solutions.

—

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.
+1-212-824-4100

—

communications@ewi.info
www.ewi.info

Building Trust
Delivering Solutions

The EastWest Institute seeks to make the world a safer place by addressing the seemingly intractable problems that threaten regional and global stability. Founded in 1980, EWI is an international, non-partisan organization with offices in New York, Brussels, Moscow and Washington. EWI's track record has made it a **global go-to place for building trust, influencing policies and delivering solutions.**

–

Learn more at **www.ewi.info**

EastWest INSTITUTE

EWInstitute
EastWestInstitute